Initial IEEE 802.1 Working Group ballot on Draft 2.0 of the

IEC/IEEE 60802 Time-Sensitive Networking Profile for Industrial Automation

Working Group ballot start date: 2023-03-20

Working Group ballot closing date: 2023-04-20

This is an unapproved draft prepared by the IEC/IEEE 60802 Joint Project.

NOTE – This page is not subject to ballot comments.

CONTENTS

FOREWORD 7
INTRODUCTION 9
1 Scope 10
2 Normative References 10
3 Terms, definitions, symbols, abbreviated terms and conventions 13
3.1 General 13
3.2 List of terms, abbreviated terms and definitions given in various standards 13
3.3 Terms defined in this document 15
3.4 Abbreviated terms and acronyms 17
3.5 Conventions 20
3.5.1 Principles for (sub) clause selections of referenced documents 20
3.5.2 Convention for capitalizations 20
3.5.3 Unit conventions 20
3.5.4 Conventions for YANG contents 20
4 Overview of TSN in industrial automation 21
4.1 Industrial application operation 21
4.2 Industrial applications 22
4.2.1 General 22
4.2.2 Control loop tasks 24
4.2.3 Start of control loop tasks 25
4.3 IA-stations 25
4.4 Ethernet interface 25
4.5 Mechanisms that can be used to meet control loop latency requirements 26
4.6 Translation between middleware and network provisioning 27
4.6.1 Interfaces of type l2vlan 27
4.6.2 PTP Instances 28
4.7 Industrial traffic types 30
4.7.1 General 30
4.7.2 Traffic type characteristics 30
4.7.3 Traffic type categories 30
4.7.4 Traffic types 31
4.8 Security for TSN-IA 33
4.8.1 General 33
4.8.2 Security configuration model 33
4.8.3 NETCONF/YANG processing 34
4.8.4 NETCONF/YANG access control 35
4.8.5 Identity checking 36
4.8.6 Secure device identity 37
5 Conformance 39
5.1 General 39
5.2 Requirements terminology 39
5.3 Profile conformance statement (PCS) 40
5.4 Conformance classes 40
5.5 IA-station requirements 40
5.5.1 IA-station PHY and MAC requirements for external ports 40

5.5.2 IA-station topology discovery requirements ... 41
5.5.3 IA-station requirements for time synchronization ... 41
5.5.4 IA-station requirements for security ... 42
5.5.5 IA-station requirements for management ... 42
5.5.6 IA-station requirements for digital data sheet ... 43
5.6 IA-station options ... 43
5.6.1 IA-station PHY and MAC options for external ports ... 43
5.6.2 IA-station options for time synchronization ... 44
5.6.3 IA-station options for security ... 44
5.6.4 IA-station options for management ... 44
5.7 Bridge component requirements ... 45
5.7.1 Common Bridge component requirements ... 45
5.7.2 ccA Bridge component requirements ... 45
5.7.3 ccB Bridge component requirements ... 46
5.8 Bridge component options ... 46
5.8.1 Common Bridge component options ... 46
5.8.2 ccA Bridge component options ... 46
5.8.3 ccB Bridge component options ... 47
5.9 End station component requirements ... 47
5.9.1 Common End Station Component Requirements ... 47
5.9.2 ccA end station component requirements ... 48
5.9.3 ccB end station component requirements ... 48
5.10 End station component options ... 48
5.10.1 Common end station component options ... 48
5.10.2 ccA end station component options ... 49
5.10.3 ccB end station component options ... 49
5.11 CNC requirements ... 49
5.12 CNC options ... 50
5.13 CUC requirements ... 50
6 Required functions for an industrial network ... 50
6.1 General ... 50
6.2 Synchronization ... 50
6.2.1 General ... 50
6.2.2 PTP Instance requirements ... 50
6.2.3 PTP protocol requirements ... 51
6.2.4 Clock states ... 54
6.2.5 Grandmaster PTP Instance requirements ... 55
6.2.6 Application framework ... 55
6.2.7 Working Clock domain framework ... 56
6.2.8 Global Time domain framework ... 57
6.2.9 IA-station model for clocks ... 57
6.2.10 Clock usage for the Ethernet interface ... 59
6.2.11 Error model ... 60
6.2.12 gPTP domains and PTP Instances ... 61
6.2.13 Split and combine cases for a PTP domain ... 61
6.3 Security model ... 63
6.3.1 General ... 63
6.3.2 Security functionality ... 64
6.3.3 IDevID Profile ... 66

6.3.4 Security setup based on IDevID 70
6.3.5 Secure configuration based on LDevID-NETCONF 74
6.4 Bridge delay Requirements 74
6.5 Bridge FDB requirements 74
6.6 Bridge reporting requirements 75
6.7 Management 75
6.7.1 General 75
6.7.2 IA-station management model 75
6.7.3 Discovery of IA-station internal structure 80
6.7.4 Network engineering model 80
6.7.5 Operation 84
6.7.6 Engineered time-synchronization spanning tree 90
6.7.7 Diagnostics 92
6.7.8 Data sheet 94
6.7.9 YANG representation of managed objects 96
6.8 Topology discovery and verification 109
6.8.1 Topology discovery and verification requirements 109
6.8.2 Topology discovery overview 110
6.8.3 Topology verification overview 112
6.9 CNC 112
6.9.1 General 112
6.9.2 Stream destination MAC address range 112
Annex A (normative) PCS proforma – Time-sensitive networking profile for industrial automation 114
A.1 General 114
A.2 Abbreviations and special symbols 114
A.2.1 Status symbols 114
A.2.2 General abbreviations 114
A.3 Instructions for completing the PCS proforma 115
A.3.1 General structure of the PCS proforma 115
A.3.2 Additional information 115
A.3.3 Exception information 115
A.3.4 Conditional status 116
A.3.5 Electronic datasheet 116
A.4 Common requirements 117
A.4.1 Implementation identification 117
A.4.2 Profile summary, IEC/IEEE 60802 117
A.4.3 Implementation type 117
Annex B (informative) Representative Configuration Domain 118
Annex C (informative) Error model 119
C.1 General 119
C.2 Time error components due to relaying of time 119
C.3 Time error components due to providing time to the Grandmaster or to an end application 120
Annex D (informative) Description of Clock Control System 121
D.1 Introduction 121
D.2 Transfer function for control system 122
D.3 Frequency response for control system 123
D.4 Example 128

Annex Z (informative) Gaps ... 130
Z.1 Gaps for Release 1: ... 130
Z.2 Topics for Edition 2: ... 131
Bibliography ... 132

Figure 1 – Data flow in a control loop ... 21
Figure 2 – IA-station interaction with CNC – Transmit path ... 23
Figure 3 – IA-station interaction with CNC – Receive path ... 24
Figure 4 – IA-station example ... 25
Figure 5 – Model for cycles ... 26
Figure 6 – Traffic type translation example ... 27
Figure 7 – IETF Interfaces used for Traffic Type Translation ... 28
Figure 8 – PTP Instance Translation Example ... 29
Figure 9 – IETF Interfaces used for PTP Instance Translation ... 29
Figure 10 – NETCONF/YANG security processing steps ... 35
Figure 11 – IA-station conformance model ... 40
Figure 12 – Externally controlled ClockSource of a Grandmaster ... 55
Figure 13 – Clock states ... 56
Figure 14 – Example clock usage principles for PTP End Instances ... 58
Figure 15 – Example clock usage principles for Grandmaster PTP Instances ... 59
Figure 16 – Error budget scheme ... 60
Figure 17 – Split and combine using BMCA ... 62
Figure 18 – Split and combine using hot standby ... 63
Figure 19 – Generic IEEE 802.1Q YANG Bridge management model ... 76
Figure 20 – Internal LAN connection management model ... 76
Figure 21 – IA-station example with IETF interfaces ... 77
Figure 22 – VID/FID/MSTID example ... 78
Figure 23 – Structure and interfaces of a CNC ... 82
Figure 24 – IA-station structure example ... 83
Figure 25 – CNC interaction ... 83
Figure 26 – Operational management model ... 84
Figure 27 – UNI service model ... 85
Figure 28 – CNC southbound ... 85
Figure 29 – NETCONF usage in a configuration domain ... 86
Figure 30 – Boundary port model ... 87
Figure 31 – Observer model ... 93
Figure 32 – Creation of the digital data sheet of an IA-station ... 96
Figure 33 – Usage example of LLDP ... 110
Figure 34 – Stream Destination MAC Address ... 113
Figure D.1 – Reference model for clock control system ... 121
Figure D.2 – Frequency response for the control system of Figure D.1, for damping ratio equal to 0,3, 0,5, 0,707, 1,0, 2,0, 3,0, 4,0, and 5,0 ... 124
Figure D.3 – Detail of frequency response for the control system of Figure D.1 for dimensionless frequency in the range 0,1 to 10 ... 125

Figure D.4 – Gain peaking, expressed as a pure fraction, as a function of damping ratio 127
Figure D.5 – Gain peaking in dB as a function of damping ratio 128
Figure D.6 – Example Frequency response 129

Table 1 – List of terms 13
Table 2 – Traffic type characteristics 30
Table 3 – IA time-aware stream characteristics 31
Table 4 – IA stream characteristics 31
Table 5 – IA traffic engineered non-stream characteristics 31
Table 6 – IA non-stream characteristics 31
Table 7 – Industrial automation traffic types summary 31
Table 8 – Example traffic class to traffic type mapping 33
Table 9 – Required values 51
Table 10 – Protocol settings 51
Table 11 – Error generation limits for Grandmaster PTP Instance 52
Table 12 – Error generation limits for PTP Relay Instance 52
Table 13 – Error generation limits for PTP End Instance 54
Table 14 – Error budget 61
Table 15 – gPTP domains 61
Table A.1 – Implementation identification template 117
Table A.2 – Profile summary template 117
Table A.3 – Implementation type template 117

Time-sensitive networking profile for industrial automation

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC document(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation.

   IEEE Standards documents are developed within IEEE Societies and Standards Coordinating Committees of the IEEE Standards Association (IEEE SA) Standards Board. IEEE develops its standards through a consensus development process, approved by the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of IEEE and serve without compensation. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, IEEE does not independently evaluate, test, or verify the accuracy of any of the information contained in its standards. Use of IEEE Standards documents is wholly voluntary. *IEEE documents are made available for use subject to important notices and legal disclaimers (see* https://standards.ieee.org/ipr/disclaimers.html *for more information).*

   IEC collaborates closely with IEEE in accordance with conditions determined by agreement between the two organizations. This Dual Logo International Standard was jointly developed by the IEC and IEEE under the terms of that agreement.

2) The formal decisions of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees. The formal decisions of IEEE on technical matters, once consensus within IEEE Societies and Standards Coordinating Committees has been reached, is determined by a balanced ballot of materially interested parties who indicate interest in reviewing the proposed standard. Final approval of the IEEE standards document is given by the IEEE Standards Association (IEEE SA) Standards Board.

3) IEC/IEEE Publications have the form of recommendations for international use and are accepted by IEC National Committees/IEEE Societies in that sense. While all reasonable efforts are made to ensure that the technical content of IEC/IEEE Publications is accurate, IEC or IEEE cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.

4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications (including IEC/IEEE Publications) transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC/IEEE Publication and the corresponding national or regional publication shall be clearly indicated in the latter.

5) IEC and IEEE do not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC and IEEE are not responsible for any services carried out by independent certification bodies.

6) All users should ensure that they have the latest edition of this publication.

7) No liability shall attach to IEC or IEEE or their directors, employees, servants or agents including individual experts and members of technical committees and IEC National Committees, or volunteers of IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE SA) Standards Board, for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC/IEEE Publication or any other IEC or IEEE Publications.

8) Attention is drawn to the normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.

9) Attention is drawn to the possibility that implementation of this IEC/IEEE Publication may require use of material covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. IEC or IEEE shall not be held responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patent Claims or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility.

IEC/IEEE 60802 was prepared by subcommittee 65C: Industrial networks, of IEC technical committee 65: Industrial-process measurement, control and automation, in cooperation with IEEE 802.1: Higher Layer LAN Protocols Working Group of IEEE 802: LAN/MAN Standards Committee of the IEEE computer society, under the IEC/IEEE Dual Logo Agreement between IEC and IEEE. It is an International Standard.

This document is published as an IEC/IEEE Dual Logo standard.

The text of this International Standard is based on the following IEC documents:

Draft	Report on voting
XX/XX/FDIS	XX/XX/RVD

Full information on the voting for its approval can be found in the report on voting indicated in the above table.

The language used for the development of this International Standard is English.

This document was drafted in accordance with the rules given in the ISO/IEC Directives, Part 2, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/publications/.

The IEC Technical Committee and IEEE Technical Committee have decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under webstore.iec.ch in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

Editor's note: This profile has been drafted per the IEC style guide. The use of introductory boilerplate text, editorial conventions and clause numbering may differ from those outlined in the IEEE style guide.

For the convenience of the reviewer, references to the IEC/IEEE cooperation process and to the IEC organization and style guidelines are listed below:

IEC-IEEE 60802 Joint Project Cooperation Process:

http://www.ieee802.org/1/files/public/docs2018/admin-IEC-IEEE-JWG-cooperation-process-0118.pdf

IEC organization:

http://www.iec.ch/

Home of the IEC organization of the Joint Project IEC/IEEE 60802 is: IEC 65C/WG18:

https://www.iec.ch/dyn/www/f?p=103:14:506767825234046::::FSP_ORG_ID,FSP_LANG_ID:26299,25Assistance to experts drafting IEC documents:

http://www.iec.ch/standardsdev/resources/draftingpublications/

Reference material:

http://www.iec.ch/members_experts/refdocs/

ISO/IEC Directives, Part 2:2021

edition 9.0 (2021-05)

Principles and rules for the structure and drafting of ISO and IEC documents:

https://www.iec.ch/members_experts/refdocs/iec/isoiecdir2%7Bed9.0%7Den.pdf

ISO/IEC Directives, Part 1:2021 + IEC Supplement:2021 edition 17.0 (2021-05) consolidated with IEC Supplement, edition 15.0 (2021-05) contains the redline version

Procedures for the technical work - Procedures specific to IEC:

https://www.iec.ch/members_experts/refdocs/iec/isoiecdir1-consolidatedIECsup%7Bed17.0%7Den.pdf

This document defines a Time-Sensitive Networking profile for industrial automation. The profile selects features, options, configurations, defaults, protocols, and procedures of bridges, end stations, and LANs to build industrial automation networks.

The profile meets the industrial automation market objective of converging Operations Technology (OT) and Information Technology (IT) networks by defining a common, standardized network infrastructure. This objective is accomplished by taking advantage of the improvements that Time-Sensitive Networking provides to IEEE 802.1 and IEEE 802.3 standard Ethernet networks by providing guaranteed data transport with bounded low latency, low latency variation, zero congestion loss for critical traffic, and high availability.

The profile helps the convergence of industrial communication networks by referring only to international standards to build the lower layers of the communication stack and their management.

Ethernet extended with Time-Sensitive Networking technology provides the features required in the area of industrial communication networks, such as:

- Meeting low latency and latency variation requirements concerning data transmission.
- Efficient exchange of data records on a frequent time period.
- Reliable communications with calculable downtime.
- High availability meeting application requirements.
- Efficient mechanisms for bandwidth utilization of exchanges of data records, with zero congestion loss.
- Improved clock synchronization mechanisms, including support of multiple gPTP domains.

Time-sensitive networking profile for industrial automation

1 Scope

This document defines a time-sensitive networking profile for industrial automation. The profile selects features, options, configurations, defaults, protocols, and procedures of bridges, end stations, and LANs to build industrial automation networks.

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/IEC 9594-1:2020 (ITU-T Recommendation X.500), *Information technology: Open systems interconnection – Part 1: The Directory: Overview of concepts, models and services*

ISO/IEC 9594-2:2020 (ITU-T Recommendation X.501), *Information technology: Open systems interconnection Part 2: The Directory: Models*

ITU-T Recommendation G.781.1, *Synchronization layer functions for packet-based synchronization*

ITU-T Recommendation G.810, *Definitions and terminology for synchronization networks*

ITU-T Recommendation G.8260, *Definitions and terminology for synchronization in packet networks*

IEEE Draft Std P1588e[1] (Draft 0.2, March 2022), *Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems Amendment: MIB and YANG Data Model*s

IEEE Std 802c-2017[2], *IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture Amendment 2: Local Medium Access Control (MAC) Address Usage*

IEEE Std 802.1AB-2016, *IEEE Standard for Local and Metropolitan Area Networks: Station and Media Access Control Connectivity Discovery*

IEEE Std 802.1ABcu-2021, *IEEE Standard for Local and Metropolitan Area Networks: Station and Media Access Control Connectivity Discovery Amendment 1: YANG Data Model*

IEEE Std 802.1AC-2016, *IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Service Definition*

IEEE Std 802.1AR-2018, *IEEE Standard for Local and Metropolitan Area Networks: Secure Device Identity*

IEEE Std 802.1AS-2020, *IEEE Standard for Local and Metropolitan Area Networks: Timing and Synchronization for Time-Sensitive Applications*

IEEE Draft Std P802.1ASdm (Draft 0.5, January 2022), *IEEE Standard for Local and Metropolitan Area Networks: Timing and Synchronization for Time-Sensitive Applications Amendment: Hot Standby*

———————

[1] Numbers preceded by P are IEEE authorized standards projects that were not approved by the IEEE SA Standards Board at the time this publication went to Sponsor ballot/press. For information about obtaining drafts, contact the IEEE

[2] The IEEE standards or products referred to in Clause 2 are trademarks of The Institute of Electrical and Electronics Engineers, Incorporated.

IEEE Std 802.1CB-2017, *IEEE Standard for Local and Metropolitan Area Networks: Frame Replication and Elimination for Reliability*

IEEE Std 802.1CS-2020, *IEEE Standard for Local and Metropolitan Area Networks: Link-local Registration Protocol*

IEEE Std 802.1CBcv-2021, IEEE *Standard for Local and Metropolitan Area Networks: Frame Replication and Elimination for Reliability — Amendment 1: Information Model, YANG Data Model and Management Information Base Module*

IEEE Std 802.1Q-2018, *IEEE Standard for Local and Metropolitan Area Network: Bridges and Bridged Networks*

IEEE Std 802.1Qcc-2018, *IEEE Standard for Local and Metropolitan Area Networks: Bridges and Bridged Networks Amendment 31: Stream Reservation Protocol (SRP) Enhancements and Performance Improvements*

IEEE Std 802.1Qcp-2018, *IEEE Standard for Local and Metropolitan Area Networks: Bridges and Bridged Networks Amendment 30: YANG Data Model*

IEEE Draft Std P802.1Qcw (Draft 1.3, February 2021), *Draft Standard for Local and Metropolitan Area Networks: Bridges and Bridged Networks, Amendment: YANG Data Models for Scheduled Traffic, Frame Preemption, and Per-Stream Filtering and Policing*

IEEE Draft Std P802.1Qdj (Draft 0.3, June 2022), *Draft Standard for Local and Metropolitan Area Networks: Bridges and Bridged Networks, Amendment: Configuration Enhancements for Time-Sensitive Networking*

IEEE Std 802.3-2022, *IEEE Standard for Ethernet*

IEEE Draft Std P802.3de (Draft 3.0, March 2022), *Draft Standard for Ethernet Amendment 6: Enhancements to MAC Merge and Time Synchronization Service Interface for Point-to-Point 10 Mb/s Single-Pair Ethernet*

IETF RFC 2986, Nystrom, M. and Kaliski, B., *PKCS #10: Certification Request Syntax Specification Version 1.7,* November 2000, available at https://www.rfc-editor.org/info/rfc2986

IETF RFC 5246, Dierks, T. and Rescorla, E., *The Transport Layer Security (TLS) Protocol,* August 2008, available at https://www.rfc-editor.org/info/rfc5246

IETF RFC 5280, Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and Polk, W., *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, May 2008, available at https://www.rfc-editor.org/info/rfc5280

IETF RFC 5652, Housley, R., *Cryptographic Message Syntax (CMS),* September 2009, available at https://www.rfc-editor.org/info/rfc5652

IETF RFC 6020, Bjorklund, M., YANG: *A Data Modeling Language for the Network Configuration Protocol (NETCONF)*, October 2010, available at https://www.rfc-editor.org/info/rfc6020

IETF RFC 6022, Scott, M. and Bjorklund, M., *Transport Layer Security (TLS) Extensions: Extension Definitions*, January 2011, available at https://www.rfc-editor.org/info/rfc6022

IETF RFC 6066, Eastlake, D, *YANG Module for NETCONF Monitoring*, October 2010, available at https://www.rfc-editor.org/info/rfc6066

IETF RFC 6125, Saint-Andre, P. and Hodges, J., *Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS),* March 2011, available at https://www.rfc-editor.org/info/rfc6125

IETF RFC 6241, Enns, R., Bjorklund, M., Schoenwaelder, J. and Bierman, A., *Network Configuration Protocol (NETCONF),* June 2011, available at https://www.rfc-editor.org/info/rfc6241

IETF RFC 6470, Bierman, A., *Network Configuration Protocol (NETCONF) Base Notifications*, February 2012, available at https://www.rfc-editor.org/info/rfc6470

IETF RFC 6961, Pettersen, Y., *The Transport Layer Security (TLS) Multiple Certificate Status Request Extension*, June 2013, available at https://www.rfc-editor.org/info/rfc6961

IETF RFC 7317, Bierman, A. and Bjorklund, M., *A YANG Data Model for System Management*, August 2014, available at https://www.rfc-editor.org/info/rfc7317

IETF RFC 7407, Bjorklund, M., and Schoenwaelder, j., *A YANG Data Model for SNMP Configuration*, December 2014, available at https://www.rfc-editor.org/info/rfc7407

IETF RFC 7589, Badra, M., Luchuk, A. and Schoenwaelder, J., *Using the NETCONF Protocol over Transport Layer Security (TLS) with Mutual X.509 Authentication*, June 2015, available at https://www.rfc-editor.org/info/rfc7589

IETF RFC 7748, Langley, A., Hamburg, M., and Turner, S., *Elliptic Curves for Security*, January 2016, available at https://www.rfc-editor.org/info/rfc7748

IETF RFC 7950, Bjorklund, M., *The YANG 1.1 Data Modeling Language*, August 2016, available at https://www.rfc-editor.org/info/rfc7950

IETF RFC 8341, Bierman, A. and Bjorklund, M., *Network Configuration Access Control Model*, March 2018, available at https://www.rfc-editor.org/info/rfc8341

IETF RFC 8342, Bjorklund, M., Schoenwaelder, J., Shafer, P., Watsen, K. and Wilton, R., *Network Management Datastore Architecture (NMDA)*, March 2018, available at https://www.rfc-editor.org/info/rfc8342

IETF RFC 8343, Bjorklund, M., *YANG Data Model for Interface Management*, March 2018, available at https://www.rfc-editor.org/info/rfc8343

IETF RFC 8525, Bierman, A., Bjorklund, M., Schoenwaelder, J., Watsen, K. and Wilton, R., *YANG Library*, March 2019, available at https://www.rfc-editor.org/info/rfc8525

IETF RFC 8640, Voit, E., Clemm, A., Gonzalez Prieto, A., Nilsen-Nygaard, E. and Tripathy, A., *Dynamic Subscription to YANG Events and Datastores over NETCONF*, September 2019, available at https://www.rfc-editor.org/info/rfc8640

IETF RFC 8641, Clemm, A. and Voit, E., *Subscription to YANG Notifications for Datastore Updates*, September 2019, available at https://www.rfc-editor.org/info/rfc8641

IETF RFC 9196, Lengyel, B., Clemm, A. and Claise, B., *YANG Modules Describing Capabilities for Systems and Datastore Update Notifications*, February 2022, available at https://www.rfc-editor.org/rfc/rfc9196.html

Editor's note: The "„Internet-Draft (I-D)“" will be substituted before IEEE SA ballot and IEC CDV with the IETF RFC numbers, which are not yet known. The reference to the draft will also disappear.

IETF RFC „Internet-Draft (I-D)“, *A YANG Data Model for a Truststore* (draft-ietf-netconf-trust-anchors-19), Internet Draft, Work in Progress by NETCONF WG, available at https://datatracker.ietf.org/doc/draft-ietf-netconf-trust-anchors/19/

IETF RFC „Internet-Draft (I-D)“, *A YANG Data Model for a Keystore* (draft-ietf-netconf-keystore-26), Internet Draft, Work in Progress by NETCONF WG, available at https://datatracker.ietf.org/doc/draft-ietf-netconf-keystore/26/

IETF RFC „Internet-Draft (I-D)“, *YANG Data Types and Groupings for Cryptography* (draft-ietf-netconf-crypto-types-25), Internet Draft, Work in Progress by NETCONF WG, available at https://datatracker.ietf.org/doc/draft-ietf-netconf-crypto-types/25/

NIST FIPS 186-4, *Digital Signature Standard (DSS),* July 2013, available at https://csrc.nist.gov/publications/detail/fips/186/4/final

Editor's note: Any draft standards will be removed prior to CDV and SA Ballot.

3 Terms, definitions, symbols, abbreviated terms and conventions

3.1 General

For the purposes of this document, the terms and definitions given in ITU-T G.781.1, ITU-T G.810, ITU-T G.8260, IEEE Std 802-2014, IEEE Std 802.3-2022, IEEE Std 802.1Q-2018, IEEE Std 802.1AS-2020, and the following apply:

- IEC Electropedia: available at https://www.electropedia.org/
- ISO Online browsing platform: available at https://www.iso.org/obp
- IEEE Standard: available at https://standards.ieee.org/standard/index.html
- ITU-T recommendation: available at https://www.itu.int/ITU-T/recommendations/index.aspx

NOTE Definitions in IEC 60050 can be found in the Electropedia link above.

3.2 List of terms, abbreviated terms and definitions given in various standards

For the purposes of this document, the terms and definitions given in Table 1 apply.

Editor's note: Any standard referenced in the section title but not referenced in the table will be removed prior to CDV and sponsor ballot.

For ease of understanding, the most important terms used within this profile document are listed in Table 1 but the definitions are not repeated.

Table 1 – List of terms

Term	Source
acquiring mode	ITU-T G.781.1
BMCA	IEEE Std 802.1AS-2020
Bridge	IEEE Std 802.1Q-2018
Bridge Port	IEEE Std 802.1Q-2018
CFM	IEEE Std 802.1Q-2018
Clock	IEEE Std 802.1AS-2020
ClockMaster	IEEE Std 802.1AS-2020
ClockSlave	IEEE Std 802.1AS-2020
ClockSource	IEEE Std 802.1AS-2020
ClockTarget	IEEE Std 802.1AS-2020
CNC	IEEE Std 802.1Qcc-2018
constant time error (cTE)	ITU-T G.8260
CQF	IEEE Std 802.1Q-2018
Customer Virtual Local Area Network (C-VLAN) component	IEEE Std 802.1Q-2018
CUC	IEEE Std 802.1Qcc-2018
DLL	IEEE Std 802-2014
DTE	IEEE Std 802.3-2022
dynamic time error (dTE)	ITU-T G.8260
EEE	IEEE Std 802.3-2022
end station	IEEE Std 802-2014
Ethernet	IEEE Std 802.3-2022

Term	Source
FDB	IEEE Std 802.1Q-2018
FID	IEEE Std 802.1Q-2018
fingerprint	IETF RFC 7589
FQTSS	IEEE Std 802.1Q-2018
fractional frequency offset	IEEE Std 802.1AS-2020
frame	IEEE Std 802.1Q-2018
frame preemption	IEEE Std 802.1Q-2018
free-run mode	ITU-T G.781.1
FRER	IEEE Std 802.1CB-2017
gating cycle	IEEE Std 802.1Q-2018
gPTP communication path	IEEE Std 802.1AS-2020
gPTP domain	IEEE Std 802.1AS-2020
Grandmaster Clock	IEEE Std 802.1AS-2020
Grandmaster PTP Instance	IEEE Std 802.1AS-2020
Independent Virtual Local Area Network [VLAN] Learning (IVL)	IEEE Std 802.1Q-2018
ISS	IEEE Std 802.1AC-2016
IST	IEEE Std 802.1Q-2018
jitter	ITU-T G.810
LAN	IEEE Std 802-2014
latency	IEEE Std 802.1Q-2018
Listener	IEEE Std 802.1Q-2018
LLDP	IEEE Std 802.1AB-2016
LLDPDU	IEEE Std 802.1AB-2016
LocalClock	IEEE Std 802.1AS-2020
locked mode	ITU-T G.781.1
logical link	IEEE Std 802-2014
LPI	IEEE Std 802.3-2022
LRP	IEEE P802.1CS
MAC	IEEE Std 802.1Q-2018
maximum absolute relative time error (max|TE_R|)	ITU-T G.8260
maximum absolute time error (max|TE|)	ITU-T G.8260
MMRP	IEEE Std 802.1Q-2018
MST	IEEE Std 802.1Q-2018
MVRP	IEEE Std 802.1Q-2018
NETCONF	IETF RFC 6241
PCP	IEEE Std 802.1Q-2018
PDU	IEEE Std 802.1Q-2018
PHY	IEEE Std 802.3-2022
PLS	IEEE Std 802.3-2022
Port	IEEE Std 802.1Q-2018
primary domain	IEEE Draft Std P802.1ASdm
PSFP	IEEE Std 802.1Q-2018

Term	Source
PTP End Instance	IEEE Std 802.1AS-2020
PTP Instance	IEEE Std 802.1AS-2020
PTP Link	IEEE Std 802.1AS-2020
PTP Port	IEEE Std 802.1AS-2020
PTP Relay Instance	IEEE Std 802.1AS-2020
PVID	IEEE Std 802.1Q-2018
redundancy	IEC 60050-192
relative time error (TE_R)	ITU-T G.8260
residence time	IEEE Std 802.1AS-2020
secondary domain	IEEE Draft Std P802.1ASdm
station	IEEE Std 802-2014
stream	IEEE Std 802.1Q-2018
synchronized time	IEEE Std 802.1AS-2020
Talker	IEEE Std 802.1Q-2018
time error	ITU-T G.8260
time-sensitive stream	IEEE Std 802.1Q-2018
traffic class	IEEE Std 802.1Q-2018
TLV	IEEE Std 802.3-2022
Configuration Domain	IEEE P802.1Qdj
UNI	IEEE Std 802.1Qcc-2018
VID	IEEE Std 802.1Q-2018
VLAN	IEEE Std 802.1Q-2018
YANG	IETF RFC 6020

3.3 Terms defined in this document

3.3.1
application clock
clock used by the application to time events

Note 1 to entry: Events can be periodic or aperiodic.

3.3.2
Bridge component
Customer Virtual Local Area Network (C-VLAN) component as defined in IEEE Std 802.1Q-2018

3.3.3
control latency
time delay between the input to a sensor application and the output from an actuator application

Note 1 to entry: For the purposes of this document, control latency does not include latencies in the sensor, actuator, or the physical system above the process interface in Figure 1.

3.3.4
deadline
application defined fixed time reference point that represents a time when data is required by the application

3.3.5
End station component
end station entity as defined in IEEE Std 802-2014

3.3.6
Global Time
synchronized time, derived from a gPTP domain, that is traceable to the PTP timescale

3.3.7
IA-controller
industrial automation function, consisting of a comparing element and a controlling element, that performs a specified control function

Note 1 to entry: An IA-controller exchanges data with several IA-devices or other IA-controllers for the purpose of control of a system.

Note 2 to entry: The primary categories of IA-Controllers are distributed control system (DCS), programmable logic controller (PLC), and programmable automation controller (PAC).

3.3.8
IA-device
industrial automation function, consisting of sensor and/or actuator elements to read and/or write process data

Note 1 to entry: An IA-device exchanges data with an IA-controller or other IA-devices for the purpose of control of a system.

3.3.9
IA-station
material element or assembly of one or more end station components, and zero, one or more bridge components

Note 1 to entry: IA-controllers and IA-devices are industrial automation functions of IA-stations.

Note 2 to entry: An IA-station is often colloquially called an "IA-controller" or "IA-device" based on its primary function, for example, "IA-controller" for an IA-station that includes an IA-controller function and an IA-device function.

3.3.10
imprinting
<security> equipping IA-stations with an LDevID-NETCONF credential as defined in IEEE Std 802.1AR, corresponding trust anchor as defined in IETF RFC 6024, and certificate-to-name mapping instructions as defined in IETF RFC 7589, Clause 7

3.3.11
management entity
IA-station function responsible for configuration of Bridge components, end station components and ports

Note 1 to entry: The management entity interacts with remote management.

3.3.12
network diameter
longest of all the calculated shortest paths between each pair of nodes in the network

Note 1 to entry: The shortest path between 2 nodes is the path between the two nodes that contains the fewest number of logical links.

3.3.13
network provisioning
process of defining a consistent network configuration, which is applied to all stations

3.3.14
nominal frequency
ideal frequency with zero uncertainty

Note 1 to entry: The nominal frequency of the PTP timescale is further explained in IEEE Std 1588-1029, 7.2.1, 7.2.2, and Annex B.

3.3.15
pDelay interval
Tpdelay2pdelay
interval between transmission of two consecutive pDelay request messages

3.3.16
pDelay turnaround time
TpdelayTurnaround
interval between reception of a pDelay request message and transmission of the consequent pDelay response message

3.3.17
ppm
µHz/Hz

Note 1 to entry: Ppm refers to a pure multiplicator of 0,000 001 and is used in the context of this document as an SI unit term to allow readable terms conformant to various rules related to expressions.

3.3.18
Sync residence time
Tresidence
interval between reception of a Sync message and transmission of the consequent Sync message

3.3.19
Sync drift interval
Tsync2driftTLV
interval between tranmission of a Sync message and transmission of the consequent Drift measurement TLV

3.3.20
Sync Interval
Tsync2sync
interval between transmission of two consecutive Sync messages

3.3.21
Working Clock
synchronized time derived from a gPTP domain that is traceable to the PTP timescale, or to an ARB timescale that is continuous

Note 1 to entry: In general, the Working Clock time is traceable to an ARB timescale; however, the Working Clock time can be correlated to a recognized timing standard.

3.4 Abbreviated terms and acronyms

Editor's note: This section will be checked and completed prior to CDV and SA ballot.

AEAD	Authenticated Encryption with Associated Data
AES	Advanced Encryption Standard
ARB	Arbitrary
ASCII	American Standard Code for Information Interchange
ASN	Abstract Syntax Notation
BMCA	Best Master Clock Algorithm
CA	Certification Authority
CBC	Cipher Block Chaining
ccA	Conformance Class A
ccB	Conformance Class B
CFM	Connectivity Fault Management
CMS	Cryptographic Message Syntax
CN	Common Name
CNC	Centralized Network Configuration
CQF	Cyclic Queuing and Forwarding

CRL	Certificate Revocation List
CRUDX	Create Read Update Delete eXecute
CSR	Certificate Signing Request
CUC	Centralized User Configuration
C-VLAN	Customer VLAN
DAC	Discretionary Access Control
DER	Distinguished Encoding Rules
DH	Diffie-Hellman
DHE	Diffie-Hellman Ephemeral
DLL	Data Link Layer
DMAC	Destination MAC Address
DNS	Domain Name Service
DSA	Digital Signature Algorithm
DTE	Data Terminal Equipment
EC	Elliptic Curve
ECC	Elliptic Curve Cryptography
EE	End Entity
EEE	Energy Efficient Ethernet
FDB	Filtering Database
FID	Filtering Identifier
FQDN	Fully Qualified Domain Name
FQTSS	Forwarding and Queuing Enhancements for time-sensitive streams
FRER	Frame Replication and Elimination for Redundancy
GCM	Galois Counter Mode
gPTP	generalized Precision Time Protocol
HMAC	Keyed-Hashing for Message Authentication Code
HW	HardWare
IA	Industrial automation
IDevID	Initial Device IDentifier
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
ISS	Internal Sublayer Service
IST	Internal Spanning Tree
ITU	International Telecommunication Union
IVL	Independent Virtual Local Area Network Learning
LDevID	Locally significant Device IDentifier
LLDP	Link Layer Discovery Protocol
LLDPDU	Link Layer Discovery Protocol Data Unit
LPI	Low Power Idle
LRP	Link-local Registration Protocol
MAC	Media Access Control
MD	Media-Dependent

MDI	Media Dependent Interface
MMRP	Multiple MAC Registration Protocol
MST	Multiple Spanning Tree
MVRP	Multiple VLAN Registration Protocol
N/A	Not applicable
NACM	Network configuration Access Control Model
NETCONF	Network Configuration Protocol
NMDA	Network Management Datastore Architecture
NPE	Network Provisioning Entity
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PCP	Priority Code Point
PCS	Profile Conformance Statement
PDU	Protocol Data Unit
PE	Path Entity
PEM	Privacy Enhanced Mail
PFS	Perfect Forward Secrecy
PHY	Physical Layer devices
PII	Personally Identifiable Information
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
PLS	Physical Signaling Sublayer
ppm	Parts per million
PSFP	Per-Stream Filtering and Policing
PTP	Precision Time Protocol
PVID	Port VLAN Identifier
RBAC	Role-Based Access Control
RFC	Request for Comments
RPC	Remote Procedure Call
RSA	Rivest-Shamir-Adleman
RAE	Resource Allocation Entity
SAN	Subject Alternative Name
SHA	Secure Hash Algorithm
STE	Sync Tree Entity
TDE	Topology Discovery Entity
TLS	Transport Layer Security
TLV	Type, Length, Value
TOFU	Trust On First Use
TSN	Time-Sensitive Networking
TSN-IA	Time-Sensitive Networking for Industrial Automation
TTP	Trusted Third Party
UNI	User/Network Interface

URL	Uniform Resource Locator
VID	VLAN Identifier
VLAN	Virtual Local Area Network
YANG	Yet Another Next Generation data modeling language

3.5 Conventions

3.5.1 Principles for (sub) clause selections of referenced documents

Normative statements in Clause 5 are established based upon the following principles:

- This document shall explicitly identify which parts (clauses, subclauses, figures, lists, tables, etc.) of the cited standards apply to this profile.
- The features of any cited standard that are mandatory (identified by shall), optional (identified by may), prohibited (identified by shall not), or not applicable shall be explicitly identified.
- Additional constraints for features of any cited standard shall be identified.

Editor’s note: This subclause (3.5.1) is provided for reference only and will be removed prior to CDV and SA ballot.

3.5.2 Convention for capitalizations

Capitalized terms are either based on the rules given in the ISO/IEC Directives Part 2 or emphasize that these terms have a specific meaning throughout this document.

Throughout this document "bridge" can be used instead of "Bridge", except when

- it occurs at the beginning of a sentence or
- it is being used as (or part of) a specific term such as "VLAN Bridge" rather than being used to identify bridges (potentially of any type) in general. If "VLAN Bridge" is meant where only "Bridge" is written, a change to "VLAN Bridge" would be appropriate.

3.5.3 Unit conventions

This document uses

- Gb/s for gigabits per second and
- Mb/s for megabits per second.

3.5.4 Conventions for YANG contents

YANG modules and XML instance data for YANG shown in this document uses the following style:

Text style `higher-layer-if` text style

Contents of a YANG module use the following style:

```
<ieee802-dot1q-bridge xmlns="urn:ietf:params:xml:ns:yang:ieee802-dot1q-bridge">
    <bridges>
        <bridge> <!-- list -->
            <name>functional-unit-x</name>
            ...
```

4 Overview of TSN in industrial automation

4.1 Industrial application operation

Industrial network applications are based on three main types of building blocks, which may be combined in one IA-controller or provided as a combination of an IA-controller and IA-devices interconnected through a suitable communication network.

These basic building blocks are:

- IA-device Sensor subsystems, which provide input signals indicating the value of the parameter or state being monitored, such as temperature, pressure, or discrete input information.
- IA-controller subsystems, which operate on combinations of measurements and external demand settings to develop output requests, such as position corrections in a motion application.
- IA-device Actuator subsystems, which implement output requests that result in physical changes to the process or machine under control, such as a level in a storage tank, the speed of a printing press, or movement of a robot.

NOTE 1 In general, all subsystems have an internal state, based upon initial settings, and derived from execution; therefore, the application inputs are combined with the internal state to develop an updated internal state and associated outputs.

A control loop is formed when the process or machine responds to the actuator output and produces a new measured value at the sensor. The complete loop is shown in Figure 1 where the IA-controllers and IA-devices are connected as end stations in the network.

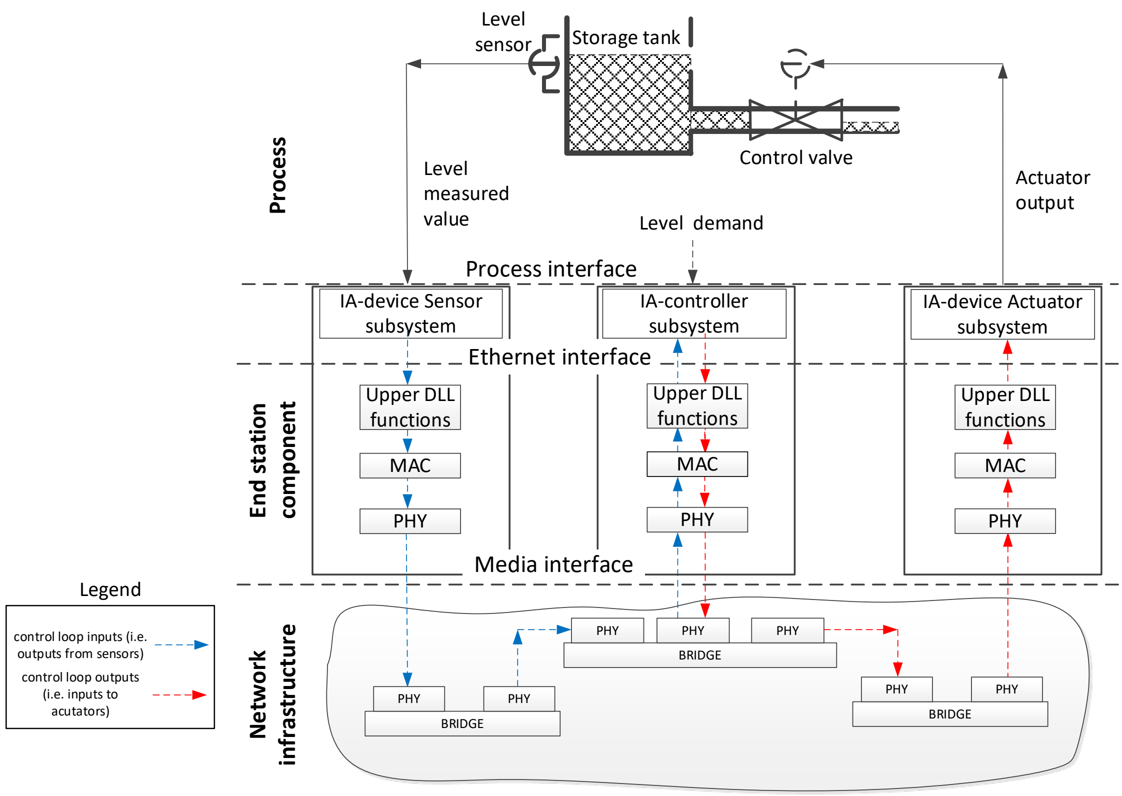


Figure 1 – Data flow in a control loop

In operation, the IA-device Sensor subsystem samples the measured value and the sampled values are transferred through the network as data packets for the IA-controller subsystem to compare with the demand value. After the required computational time, the required output is transferred from the IA-controller subsystem to the IA-device Actuator subsystem for implementation as a change in the external process.

This sequence repeats continuously as a regular operation using a Working Clock. The Working Clock can be traceable to an ARB or PTP timescale, but this traceability is not required by all applications. For stability, the time constant of the process response needs to be on the order of five to ten times (or more) the sequence repetition time (i.e., sampling time).

NOTE 2 In common Industrial Network deployments, it has been observed that a ratio of 5 to 10 (or more) provides effective control of the automated process. The actual ratio of the process response time constant to sampling time required for stability depends on the implementation.

Control latency is a critical factor in all types of control and needs to be bounded.

Components of the control latency time are shown in Figure 1.

- Application time for sampling, computation, and processing within each IA-controller and IA-device. These are specific to the IA-device and IA-controller and known to the IA-device or IA-controller makers.
- The time for data transfer through the upper DL functions, MAC and PHY layers within each IA-controller and IA-device. This time depends on the implementation of these components, their situation-dependent load and performance, and configuration elements related to QoS and TSN that some of these components may support.
- End Station and Bridge scheduling and transfer time through the network. These are influenced by the configuration process, which allocates available bandwidth and priorities to various types of application messages.

Offline engineering of the network is possible, including the calculation of the control latency time. During system operation, management services are provided for diagnostics and checking the performance indicators of an installed network.

4.2 Industrial applications

4.2.1 General

Industrial applications can contain multiple tasks. These tasks are executed based upon time or other events. Thus, an industrial application can have multiple tasks executing on different cycles as shown in Figure 2 and Figure 3.

Examples of these tasks are listed below.

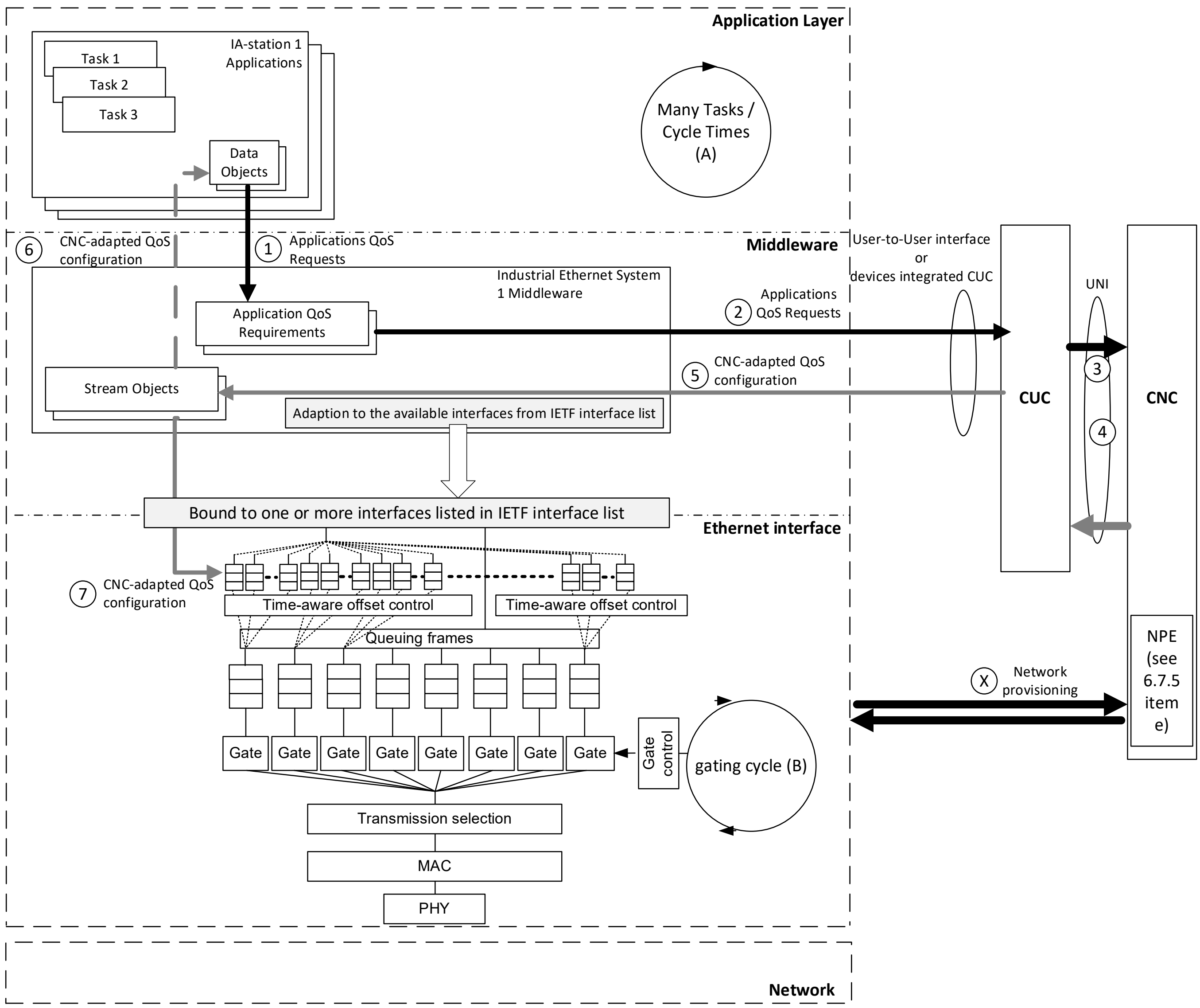
- Background tasks, which are executed when no other task is running. There can be zero, one, or more such tasks in an industrial application.
- Main task which executes periodically. The start and execution of this task is often based upon the ARB timescale. There can be zero or one such task, in an industrial application.
- Global Time tasks. The start and execution of these tasks is often based upon Global Time (for example, at noon every day, at noon every Friday, etc). There can be zero, one or more such tasks in an industrial application.
- Process driven tasks which are started by an event (for example, a sensor value reaches a defined point, a process fault occurs, etc.). There can be zero, one or more such tasks in an industrial application.
- Control loop tasks which are bound to Working Clock and started periodically. There can be zero, one or more such tasks in an industrial application.

A user defines the required automation tasks along with the data objects required as output and input for these tasks and the end station which hosts these tasks. Thus, these tasks are bound to data objects, which need to be exchanged between end stations per the user's definition. Many of these tasks have timing requirements, which are added as attributes to the assigned data objects. Examples of these attributes include:

- [DataObject_Update_Interval] an update interval (time between two consecutive updates at the transmitting end station);
- [DataObject_Deadline] a deadline (latest receive time at the end station, relative to the start of the DataObject Update Interval);

- [DataObject_Data_Size] the size of the DataObject;
- Other attributes as needed to form a stream-list request according to IEEE Draft P802.1Qdj, 46.1.5.

NOTE These attributes are provided for illustration purposes. The list is not representative of all industrial applications. These are not network attributes.



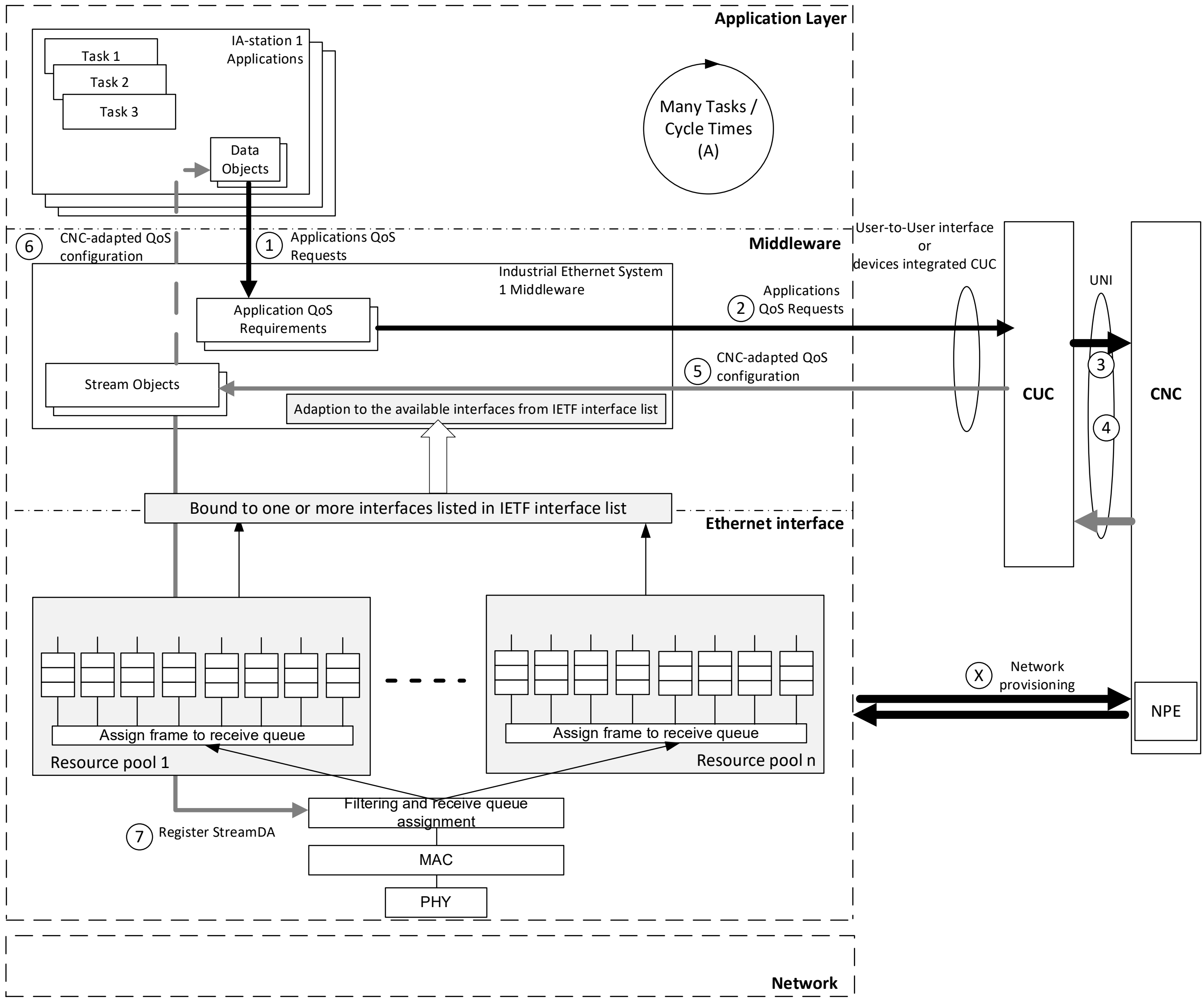
Legend:

X IA-stations are configured by the CNC before any CUC to CNC action happens. Configuring includes for example the gating cycle and transmission selection. Later accesses may happen concurrently to a CUC to CNC sequence.

1 … 7 Sequence of actions taken

Time-aware offset control Queues are shared between multiple middlewares.

Figure 2 – IA-station interaction with CNC – Transmit path



Legend:

X IA-stations are configured by the CNC before any CUC to CNC action happens. Configuring includes for example the gating cycle and transmission selection. Later accesses may happen concurrently to a CUC to CNC sequence.

1 … 7 Sequence of actions taken

Resource pool x Different resource pools to support decoupling of middlewares.

Figure 3 – IA-station interaction with CNC – Receive path

4.2.2 Control loop tasks

Control loops rely on the behavior of synchronized tasks by each of the IA-devices and IA-controllers involved in that control loop. For example, this behavior can be implemented by using a common Working Clock, a common starting point relative to the Working Clock and a common duration for this control loop task at the involved IA-devices and IA-controllers. The data objects associated with the control loop share common values for some attributes (for example, the same values for DataObject_Update_Interval and DataObject_Deadline). Multiple control loop tasks can be implemented and running in parallel at the involved automation devices.

4.2.3 Start of control loop tasks

The calculation of the starting point for a control loop task is independent from the time when the device is powered up or connected to the Configuration Domain. The start of a control loop task, which is based on the Working Clock, can be calculated in the following manner:

> Divide the Working Clock value, expressed as an integer, by the duration of the control loop task, expressed as an integer, whenever the Working Clock value increases by one. A remainder of zero provides the basis for the start of the control loop task.

NOTE The units of the Working Clock value and the duration of the control loop task are the same.

Stations in the network associated with the control loop synchronize to a Working Clock using IEEE Std 802.1AS-2020.

4.3 IA-stations

An IA-station can be a simple end station acting as source or destination for control data traffic. In addition, an IA-station can be a combined functional unit that includes an end station component together with a Bridge component in one chassis. IA-stations, incorporating multiple functional units with several end station components and Bridge components within one chassis, can also be found in industrial automation. Within this kind of combined IA-station various components can be connected by internal ports and internal LANs. All components utilize a common management entity as shown in Figure 4.

Figure 4 shows an example IA-station incorporating three functional units in one chassis. Functional unit 1 and functional unit 2 each consist of a Bridge component and an end station component. The end station components are connected by internal ports via internal LANs to the Bridge components. The Bridge components include two external ports each. Functional unit 3 includes only a single end station component with one external port.

IA-controllers and IA-devices as well as the management entity are IA-station functions acting as source of and/or destination for link layer data traffic. Thus, each IA-station incorporates at least one end station component where these functions can be located. Figure 4 shows that IA-station functions can either reside in a single end station component (IA-device 1, IA-controller 1, IA-device 2) or in multiple end station components (IA-controller 2, management entity).

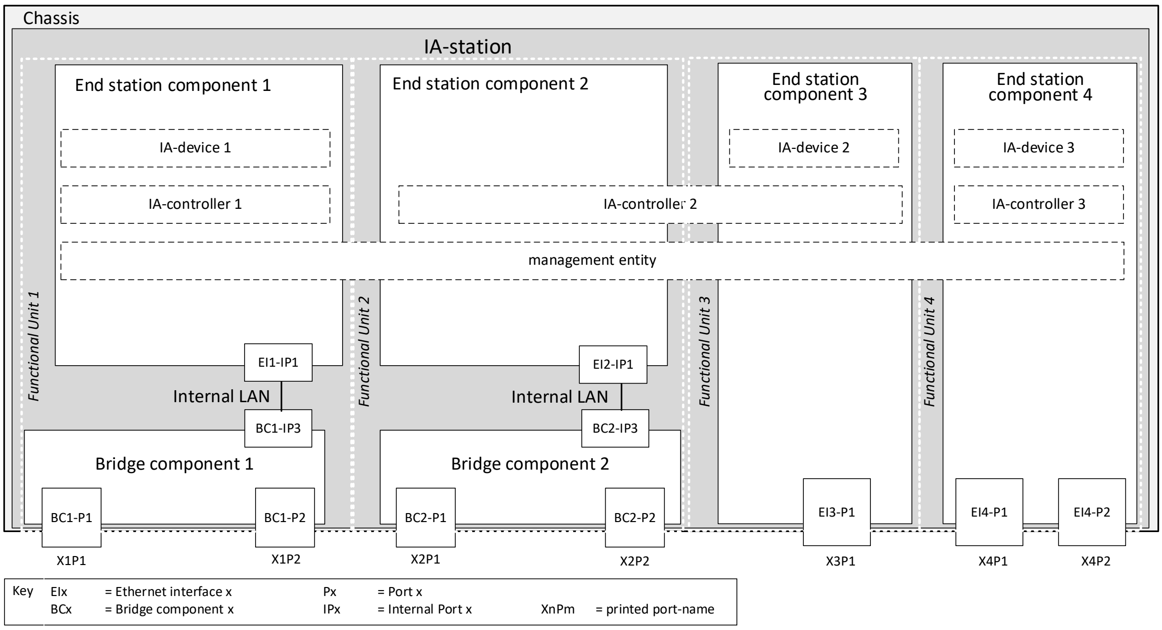


Figure 4 – IA-station example

4.4 Ethernet interface

One or more middleware components act as a layer between applications and the Ethernet interface. Figure 2 and Figure 3 show the relation between applications, middleware, Ethernet interface and the network. Various applications can run in parallel on an automation device.

Data objects represent the information exchanged between applications running in different end stations. The application requirements contained in these data objects are translated by the middleware into stream requirements for use by the CUC. This translation can be accomplished in one of the following ways:

a) The user defines the data objects and translates them into stream requirements and end-station communication-configurations. A user-specific mechanism is used to configure the network components and establish paths.

b) The user defines the data objects and associates them with QoS requirements for each stream (application QoS requirements). These can be forwarded as stream requirement requests by a CUC to a CNC. The CNC would respond by providing a stream configuration response. The request and response are specified in IEEE P802.1Qdj. The CUC can be integrated into the end station or can be accessed via a user-to-user protocol. The middleware uses this information for configuring Talkers and Listeners. This information is also used to add additional timing information to the data objects for application usage.

c) Time-aware offset control utilizes per-stream queues (see IEEE Std 802.1Q-2018, figure 34-1) and the traffic specification of the streams, including transmission offsets, provided by the CNC to ensure the order of stream transmission.

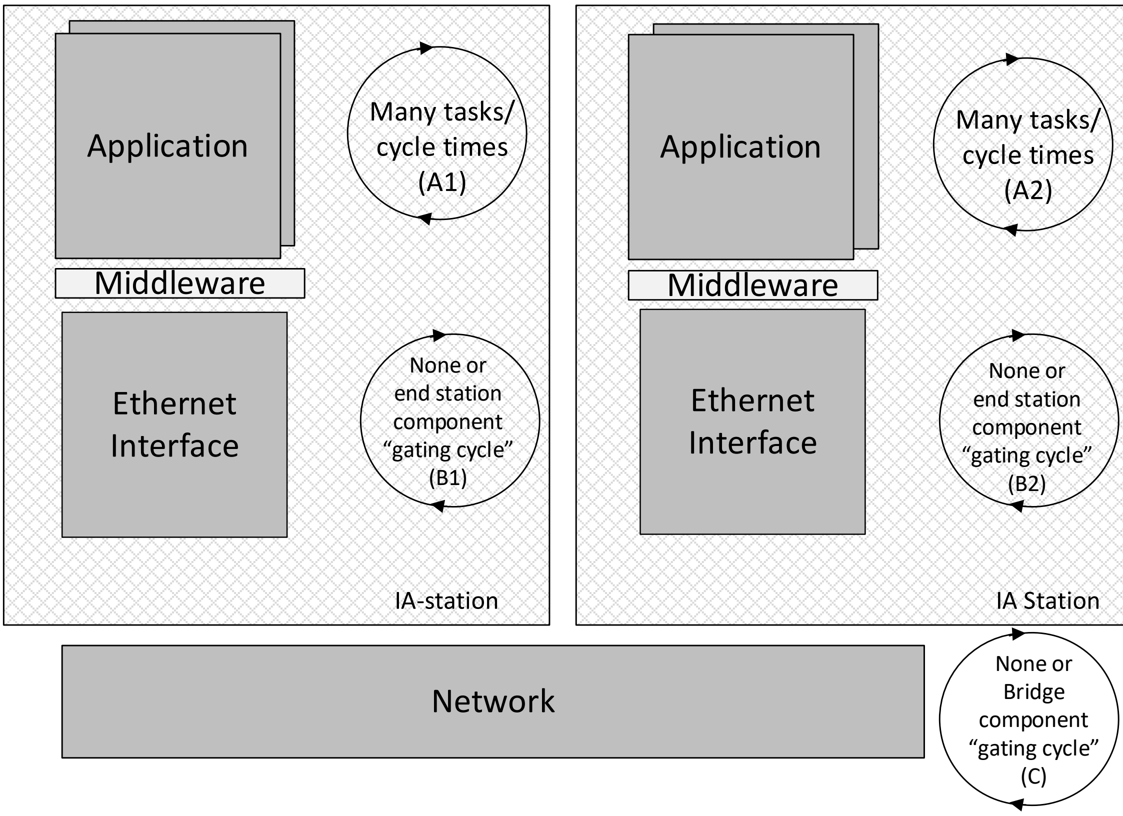


Figure 5 – Model for cycles

These automation systems, which are built from various end stations and connected via bridges, can share a common gating cycle or each station can have its own gating cycle. Alternatively, a bridge or end station can have no gating cycle (expressed as "none" in Figure 5).

4.5 Mechanisms that can be used to meet control loop latency requirements

Meeting latency requirements on a network can be accomplished using one or more combinations of the mechanisms enumerated below. The choice of a mechanism or a subset of the mechanisms listed below depends on the nature of the application(s) and the corresponding latency requirements:

a) Defining, testing, and simulating all possible application combinations and associated traffic patterns
b) Overprovisioning the network
c) Providing scheduled time slots for each application to transmit on the network
d) Preempting lower priority traffic
e) Providing scheduled time slots for certain traffic classes
f) Time-aware offset control
g) Enforcing deterministic queuing delays in bridges

NOTE This list is not comprehensive and not all mechanisms mentioned here are part of this specification. For specific mechanisms covered by this document please refer to Clause 5.

Frame preemption is specified in IEEE Std 802.1Q-2018 and IEEE Std 802.3-2022.

Reserving time on the network for certain traffic types can be done through enhancements for scheduled traffic according to IEEE Std 802.1Q-2018, 8.6.8.4. An aligned gating cycle needs to be defined for this method to work. Once these aligned gating cycle times are defined, portions of that cycle time can either be allocated to streams or classes of streams.

Multiple Talker/Listener(s) pairs can be used for streams between end stations. Engineered time triggered transmit can be used to coordinate transmission of all the traffic that shares a network to keep application requirements.

Creating a traffic load model in advance will allow analysis of resulting traffic. It can be used to select and implement appropriate mechanisms to achieve latency requirements.

4.6 Translation between middleware and network provisioning

4.6.1 Interfaces of type l2vlan

Application engineering can be done without knowledge of the network provisioning. Thus, application engineering is not able to align the use of, for example, PCP or VID with network provisioning. This problem is solved by providing a translation table (by a YANG module definition for example) to the middleware. The IA-station's local YANG database will store this information.

Figure 6 and Figure 7 show examples of the translation models.

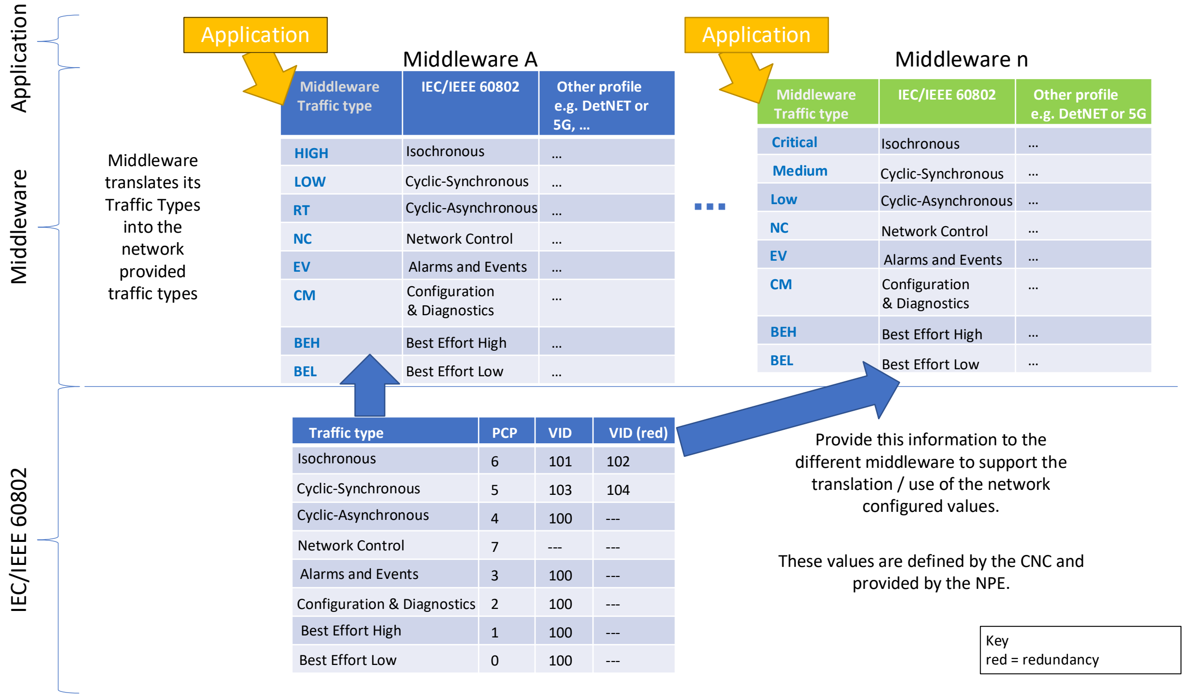


Figure 6 – Traffic type translation example

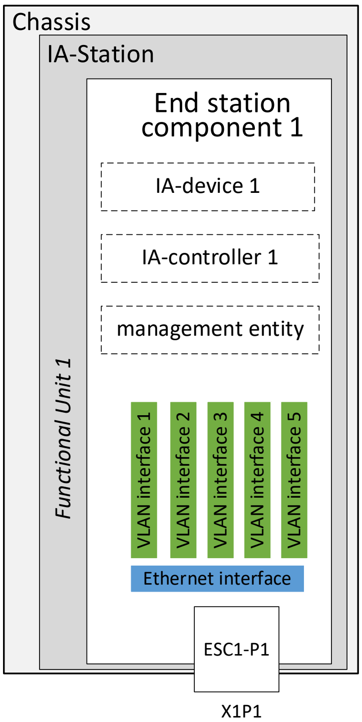


Figure 7 – IETF Interfaces used for Traffic Type Translation

Interfaces of type l2vlan can be used to provide the required mapping information to all installed middleware and applications.

The name string of the l2vlan interfaces can provide the vlan-id, the assigned traffic types with their PCP values and redundancy information (see 6.7.2.3).

4.6.2 PTP Instances

Another item of information which is configured during network provisioning is the PTP domain number. The middleware needs to know which PTP domain is assigned to which target clock. This is done by providing well-defined descriptionDS.userDescription names according to IEEE Std 1588-2019, 8.2.5.5 in order to create a translation table.

Editor’s note: descriptionDS.userDescription is not currently part of the IEEE Std 802.1AS-2020. It is expected that it will be incorporated as part of IEEE P802.1ASdm. It may be necessary to update the reference at that time.

descriptionDS.userDescription names allow the support of multiple middlewares at one IA-station using the same PTP Instances (see 6.2.12). Station's local database would store this information.

Figure 8 and Figure 9 show examples of the translation models.

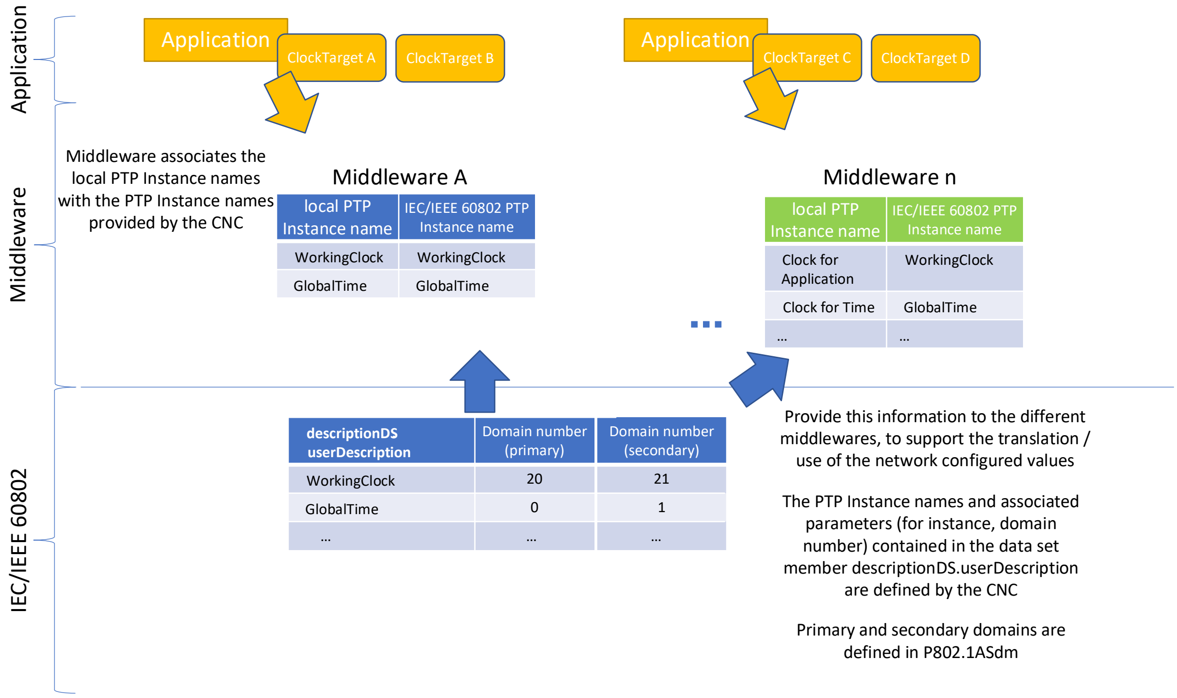


Figure 8 – PTP Instance Translation Example

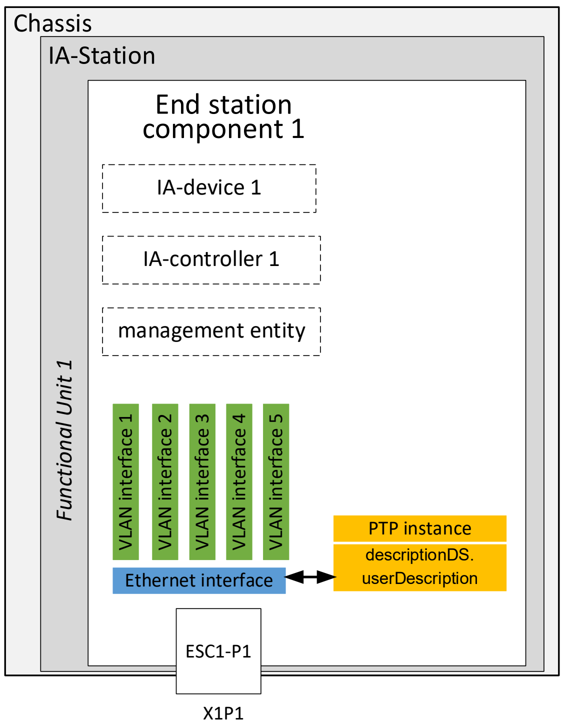


Figure 9 – IETF Interfaces used for PTP Instance Translation

The userDescription contains the clock type (i.e., WorkingClock, GlobalTime, or both) and the attached Ethernet interfaces.

This information is used by the middleware to align to the intended ClockTarget or ClockSource.

4.7 Industrial traffic types

4.7.1 General

Industrial automation applications make use of different traffic schemes/types for different functionalities (for example, parameterization, control, alarming). The various traffic patterns have different characteristics and thus, impose different requirements on a network. To specify these traffic types, a two-step approach is used:

a) First define characteristics of generic traffic types (traffic-type-categories) and

b) Second define instances of the generic types, i.e. the traffic types.

4.7.2 Traffic type characteristics

The traffic type characteristics in Table 2 enable the identification of several distinct traffic types that are shared among sets of industrial applications.

Table 2 – Traffic type characteristics

Characteristic	Description
Cyclic	Traffic types consist of frames that can either be transmitted on a reoccurring time period (cyclic) or at no set period (acyclic). Available selections are: • Required: cyclic • Optional: Implementation of cyclic traffic is at the discretion of the user.
Data delivery requirements	Denotes the delivery constraints for the traffic. Four options are specified: • Frame Latency: data delivery of a frame for a given Talker-Listener pair occurs within a bounded timespan. • Flow Latency: data delivery up to a certain number of frames or data size (including bursts of frames) occurring over a defined period. • Deadline: data delivery of a frame to a given Listener occurs at or before a specific point in time. • No: Denotes the case of traffic types with no special data delivery requirements
Time-triggered transmission	Talker data transmission occurs at a specific point in time based upon the Working Clock. Available selections are: • Required • Optional: Implementation of time-triggered transmission is at the discretion of the user. Enhancements of scheduled traffic is only one means of achieving time-triggered transmission. Other, application-based, methods are possible

4.7.3 Traffic type categories

4.7.3.1 General

This two-step approach allows a clear differentiation between characteristics as seen from the “network” point of view and “application” point of view. Traffic-type-categories allow different IEEE 802 feature selections to achieve the specified goals. Four traffic-type-categories are identified in Industrial Automation (IA) systems:

a) IA time-aware stream

b) IA stream

c) IA traffic engineered non-stream

d) IA non-stream

4.7.3.2 IA time-aware stream

The characteristics of this traffic are shown in Table 3.

Table 3 – IA time-aware stream characteristics

Characteristics	
Cyclic	Required
Data delivery requirement	Deadline or Frame Latency
Time-triggered transmission	Required

4.7.3.3 IA stream

The characteristics of this traffic are shown in Table 4.

Table 4 – IA stream characteristics

Characteristics	
Cyclic	Required
Data delivery requirement	Frame Latency
Time-triggered transmission	Optional

4.7.3.4 IA traffic engineered non-stream

The characteristics of this traffic are shown in Table 5.

Table 5 – IA traffic engineered non-stream characteristics

Characteristics	
Cyclic	Optional
Data delivery requirement	Flow Latency
Time-triggered transmission	Optional

4.7.3.5 IA non-stream

The characteristics of this traffic are shown in Table 6.

Table 6 – IA non-stream characteristics

Characteristics	
Cyclic	Optional
Data delivery requirement	No
Time-triggered transmission	Optional

4.7.4 Traffic types

4.7.4.1 General

Table 7 summarizes relevant industrial automation traffic types and their associated characteristics. In an industrial automation system, other applications, such as audio or video, would utilize one of these traffic types. Traffic Type codes are needed for the VLAN naming scheme defined in this document. See 6.7.2.4 for more information.

Table 7 – Industrial automation traffic types summary

Traffic type name	Traffic type code	Cyclic	Data delivery requirements	Time-triggered transmission	Traffic-type-category
Isochronous	H	Required	Deadline	Required	IA time-aware-stream
Cyclic-synchronous	G	Required	Frame Latency	Required	IA time-aware-stream

Traffic type name	Traffic type code	Cyclic	Data delivery requirements	Time-triggered transmission	Traffic-type-category
Cyclic-asynchronous	F	Required	Frame Latency	Optional	IA stream
Alarms & Events	E	Optional	Flow Latency	Optional	IA traffic engineered non-stream
Configuration & Diagnostics	D	Optional	Flow Latency	Optional	IA traffic engineered non-stream
Network Control	C	Optional	Flow Latency	Optional	IA traffic engineered non-stream
Best Effort High	B	Optional	No	Optional	IA non-stream
Best Effort Low	A	Optional	No	Optional	IA non-stream

4.7.4.2 Isochronous

A type of IA time-aware stream traffic. This type of traffic is transmitted cyclically using time-triggered transmission. Listeners have individual deadline requirements. Cycle times are typically in the range of microseconds to tens of milliseconds. Frame size is typically below 500 octets. Talker-Listener pairs are synchronized to the Working Clock. The network is configured by the CNC to provide zero congestion loss for this traffic type. This type of traffic is normally used in control loop tasks.

4.7.4.3 Cyclic-synchronous

A type of IA time-aware stream traffic. This type of traffic is transmitted cyclically using time-triggered transmission. Talker-Listener pairs have individual latency requirements. Cycle times are typically in the range of hundreds of microseconds to hundreds of milliseconds. Frame size is unconstrained except as indicated in 5.5.1. Talker-Listener pairs are synchronized to the Working Clock. The network is configured by the CNC to provide zero congestion loss for this traffic type. This type of traffic is normally used in control loop tasks.

4.7.4.4 Cyclic-asynchronous

A type of IA stream traffic. This type of traffic is transmitted cyclically with latency requirements bounded by the interval as defined in IEEE Std 802.1Qcc-2018, 46.2.3.5.1. Talker-Listeners pair have individual latency requirements. Cycle times are typically in the range of milliseconds to seconds. Frame size is unconstrained except as indicated in 5.5.1. Data exchanges between Talker-Listener pairs are typically not dependent on the Working Clock. This traffic type typically tolerates limited congestion loss. The network is configured by the CNC to handle this traffic type without loss, up to a certain number of frames or data size.

4.7.4.5 Alarms and events

A type of IA traffic engineered non-stream. This type of traffic is transmitted cyclically or acyclically. This traffic expects bounded latency including time for retransmission in the range of milliseconds to hundreds of milliseconds. The source of the alarm or event typically limits the bandwidth allocated to this traffic. Frame size is unconstrained except as indicated in 5.5.1. Congestion loss can occur. Retransmission to mitigate frame loss is expected. The network is configured by the CNC to handle these frames, including bursts of frames, up to a certain number of frames or data size over a defined period.

4.7.4.6 Configuration and diagnostics

A type of IA traffic engineered non-stream. This type of traffic is transmitted cyclically or acyclically. This traffic expects bounded latency, up to seconds, including time for retransmission. The source of configuration or diagnostics frames typically limits the bandwidth allocated to this traffic. Frame size is unconstrained except as indicated in 5.5.1. Congestion loss can occur. Retransmission to mitigate frame loss is expected. The network is configured by the CNC to handle these frames, including bursts of frames, up to a certain number of frames or data size over a defined period.

4.7.4.7 Network control

A type of IA traffic engineered non-stream. This type of traffic can be transmitted cyclically or acyclically. This traffic expects bounded latency including time for retransmission. Frame size is unconstrained except as indicated in 5.5.1. The network is configured by the CNC to handle these frames, including bursts of frames, up to a certain number of frames or data size over a defined period. If these limits are exceeded congestion loss may occur. Network control is comprised of services required to maintain network operation. Examples include time synchronization, loop prevention, and topology detection.

4.7.4.8 Best effort

A type of IA non-stream. The network is configured by the CNC to ensure that these frames do not interfere with other traffic types. These frames are forwarded when resources are available. Congestion loss can occur; therefore, frames may be dropped. It is sometimes desirable to have more than one traffic class for best effort traffic (see Table 8)

4.7.4.9 Traffic class to traffic type mapping

Table 8 provides an example for the usage of traffic classes based on the traffic type:

Table 8 – Example traffic class to traffic type mapping

Traffic class	PCP	Traffic Type
7	6	Isochronous
6	5	Cyclic-Synchronous
5	4	Cyclic-Asynchronous
4	7	Network Control
3	3	Alarms and Events
2	2	Configuration & Diagnostics
1	1	Best Effort High
0	0	Best Effort Low

NOTE 1 The example in Table 8 assumes an implementation supporting eight queues.

NOTE 2 An example mapping of PCP and traffic type to an application is provided in Figure 6.

The traffic-type-categories definition allows different IEEE 802 feature selections to achieve specified goals. Moreover it helps in identification of the traffic protection mechanisms. Adherence to this example of a common mapping helps minimize potential conflicts between traffic types.

4.8 Security for TSN-IA

4.8.1 General

Subclause 4.8 describes selected aspects of TSN-IA security in an informative way. Protecting the management of industrial communication is the main objective of TSN-IA security. The protection of communications that use industrial traffic types is left to an individual middleware and/or application that uses TSN-IA.

4.8.2 Security configuration model

Security configuration is a part of system engineering and configuration. The security configuration in this document does not encompass the supply of configuration objects for middleware and application security. Security configuration settles the prerequisites for protecting the establishment and management of communications that use industrial traffic types (see 4.7). It ensures that the security features of IA-stations (including CNCs) can be used for protecting message exchanges and authorizing the resource accesses during stream establishment and management. This security configuration supplies deployment-specific configuration objects to IA-stations. They encompass:

- Instructions about cryptographic algorithms
- Credentials and trust anchors
- Instructions to interpret the outcome of peer entity authentication in course of enforcing resource access controls
- Access control rules and permissions

This security configuration uses NETCONF/YANG request/response exchanges:

- The to-be-configured IA-stations act in NETCONF server role with respect to their security configuration.
- A NETCONF client is responsible for setting-up IA-stations for security. This NETCONF client possesses information about the security relationship to be established during security configuration or about the expectations on the IA-stations in a domain. It can be implemented as part of an interactive component (for example, engineering tool) or an automated component (for example, CNC). As an implication, the security configuration includes options for interactive and automated setup, i.e., security configuration is done by human and/or non-human actors.

NOTE NETCONF notifications can also be used to recognize events such as a near-term end-of-life of certificate objects, especially EE certificate objects.

- The security configuration exchanges supply deployment-specific objects (trust anchors, credentials etc.) to IA-stations and manage them. This is security critical. IA-stations that are in factory default state can only possess manufacturer-specific security objects (trust anchors, credentials etc.) when booting initially. The protected NETCONF/YANG exchanges with IA-stations that are in factory default state are outlined in 4.8.3 to 4.8.6.

4.8.3 NETCONF/YANG processing

Securing NETCONF/YANG resources on NETCONF servers is mandated by IETF RFC 6241 (NETCONF). This demands message exchange protection between NETCONF clients and servers as well as resource access authorization by NETCONF servers:

- IETF RFC 7589 (NETCONF-over-TLS) specifies a solution to protect NETCONF message exchanges by TLS.
- IETF RFC 8341 (NACM) specifies three access control points, covering the request/response and notification model in NETCONF according to IETF RFC 8341, 2.1.

NETCONF servers enforce the mandated security as shown in Figure 10. The processing steps are executed upon the current configuration of the NETCONF server’s YANG modules.

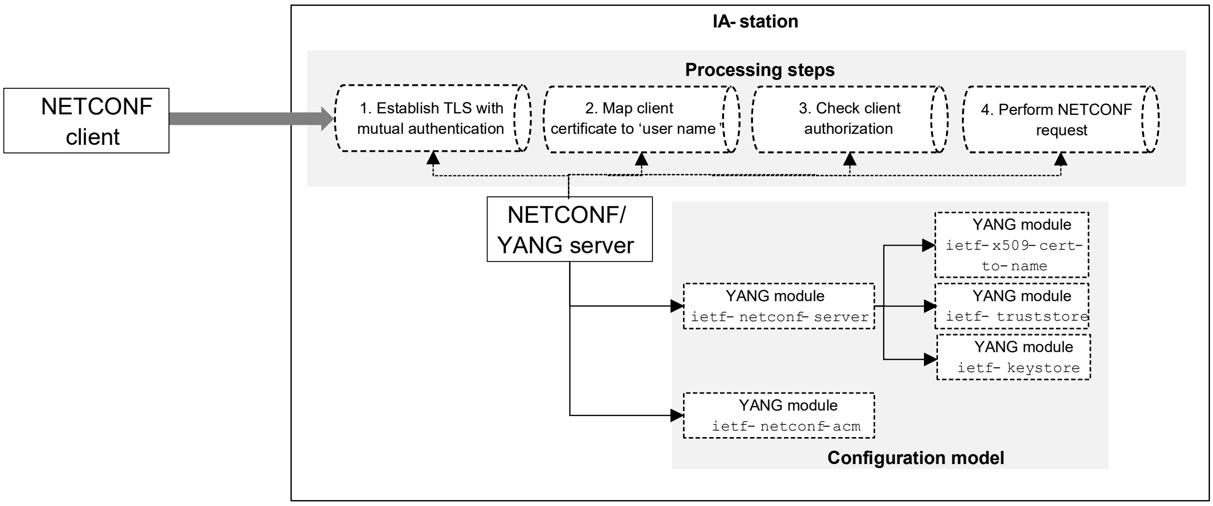


Figure 10 – NETCONF/YANG security processing steps

The processing steps on the side of NETCONF servers are:

1) Establish a TLS connection with mutual authentication: The NETCONF server acts as TLS server and awaits connection requests of NETCONF clients (TLS clients). During the TLS handshake the NETCONF server authenticates itself towards the NETCONF client by a credential from its ietf-keystore YANG module. In addition, the NETCONF server challenges the NETCONF client for authentication and verifies its authentication by trust anchors in its ietf-truststore YANG module according to 6.3.4. A successful mutual authentication is a prerequiste for proceeding to the next step.

2) Map the client certificate to a username: The NETCONF server maps the authenticated TLS client certificate to a “NETCONF username”[3] by applying an ordered list of mapping instructions. These instructions are provided in its ietf-x509-cert-to-name YANG module. The applicable list item is identified by matching its configured fingerprint (according to IETF RFC 7589, Clause 7) against the certification path that was used for TLS client authentication (an end entity certificate or a CA certificate). According to the map type of the identified list item, the NETCONF server determines the “NETCONF username”. This can be done by extracting information from the end entity certificate of the NETCONF client. A successful certificate-to-”NETCONF username” mapping is a prerequiste for proceeding to the next step.

3) Check client authorization: The NETCONF server checks if the NETCONF client has the permission to access the requested NETCONF/YANG resource based on its “NETCONF username” and the access control rules available in its ietf-netconf-acm YANG module. See 4.8.4 for more information about NETCONF/YANG access control. A successful authorization is a prerequiste for proceeding to the next step.

4) Perform NETCONF request: If all preceding steps succeeded, the NETCONF server performs the NETCONF request.

4.8.4 NETCONF/YANG access control

NACM defines a YANG information model for describing permitted/denied access operations. NETCONF servers are responsible to enforce access control to their resources according to the information in their ietf-netconf-acm YANG modules. In the conceptual dimension of resources, NACM allows the description of access controlled resources in terms of NETCONF protocol operations, nodes in YANG datastores and/or types of notification events. In the conceptual dimension of subjects, NACM uses character strings to represent the subject actors i.e., NETCONF clients. These character strings are known as “NETCONF username”. The NACM access control information of a NETCONF server needs to be created, updated, and deleted per IA-station. The management of this information needs to happen along the IA-

[3] In this document, NETCONF username’ values do not present references to human users – in almost all cases.

station lifecycle for example, manufacturing, bootstrapping, operation, maintaining, re-owning, destructing. Moreover, the management of the NACM access control information itself is subject to NACM access control.

This document employs multiple YANG information models for fulfilling its purposes. This extends beyond the above identified YANG modules (see 4.8.3). The NETCONF server on an IA-station needs to enforce access control for NETCONF/YANG resources. To meet this objective the NETCONF server on an IA-station needs to be supplied with access control information for the used NETCONF/YANG resources. NACM is employed for this purpose and profiles default access control information for the NETCONF/YANG resources (see 6.3.2.2). This relieves other organizations or individuals for example, manufacturers, integrators, operators, owners from being responsible to create NACM access control information for the respective NETCONF/YANG resources.

With respect to the conceptual dimension of subjects, a dedicated profiling strategy is needed to meet the constraints that are given by NACM:

- NACM relies on character strings (known as “NETCONF username”) to refer to clients.
- The actual names of individual entities in organizations are not known while writing this document.

NACM access control information as specified in this document, populates the “NETCONF username” character strings in NACM with role names specified in 6.3.2.1.4, c). This allows to create default NACM information without knowing actual names of individual entities. A role name can refer to 0, 1 or more individual entities. It is the responsibility of users to assign role names to individual entities. This happens by binding the assigned role names to the credentials of individual entities. The current form to express this binding is a role extension in the identity certificates of end entities defined in this document. These are NETCONF clients, i.e., these role extensions appear in the end entity certificates of LDevID credentials for NETCONF clients.

4.8.5 Identity checking

IETF RFC 7589 (NETCONF-over-TLS) requires NETCONF clients to check the identity of NETCONF servers as well as NETCONF servers to check the identity of NETCONF clients.

The NETCONF server identity check happens inside NETCONF clients. It matches an actual against an expectation:

- The actual server identity is established by the end entity certificate of the NETCONF server (authenticated by means of TLS).
- The expectations on server identity are established by the information that is used to connect to the NETCONF server.

IETF RFC 7589 refers to IETF RFC 6125 for the details of retrieving the actual and comparing it against expected.

The NETCONF client identity check happens inside NETCONF servers. It also matches an actual against an expectation:

- The actual client identity is established by the end entity certificate of the NETCONF client (authenticated by means of TLS).
- The expectations on client identity are established by the contents of the YANG modules ietf-netconf-acm and ietf-x509-cert-to-name.

The details of this check are subject to the requested NETCONF operation. IETF RFC 7589, Clause 7, specifies the mapping of an authenticated client certificate to a “NETCONF username” whose permissions are then enforced by IETF RFC 8341 (NACM). More information is provided in 4.8.3, steps 2 and 3.

4.8.6 Secure device identity

4.8.6.1 Device Identity

The term ‘device’ originates from IEEE Std 802.1AR. It matches the term IA-station in this document.

The device identity refers to a set of information items about a device respectively an IA-station that:

- describes a device as a physical or virtual entity in a distributed system (identifier and/or attribute information)
- is used by a device to describe itself as such entity (identifier and/or attribute information)
- allows to interact with this device (addressing information i.e., a specific identifier class).

The targeted use case, for example application data exchanges, configuration exchanges, inventory, or ordering, determines the required amount of identity information about a device respectively an IA-station.

The device identity of any single IA-station encompasses:

- MAC addresses, IP addresses, TCP ports, DNS names
- ietf-hardware YANG module contents (IETF RFC 8348)

4.8.6.2 Verifiable Device Identity

Certain aspects of device identity demand verification before relying on them during online interactions. These are examples.

- DNS names or IP addresses are used to call the management entity of an IA-station i.e., its NETCONF/YANG server. Their value represents the caller's expectation on the identity of their responder in network communications. Its verification allows to defeat DNS spoofing, component impersonation and man-in-the-middle attacks. This is mandated by IETF RFC 7589 and described in IETF RFC 6125. Passing this check is a prerequisite before NETCONF application exchanges can happen.
- mfg-name values in instances of the ietf-hardware YANG module. These values make claims about the IA-station manufacturer. Their verification is a means to protect against counterfeiting.

The verification of IA-station identity happens according to a model that is fully specified by this document and whose checking can be done in a manufacturer-agnostic manner. This verification is important before supplying locally significant credentials especially LDevID-NETCONF to IA-stations that are in factory-default state.

4.8.6.3 Verification Support Mechanisms

4.8.6.3.1 General

Subclause 4.8.6.3 considers mechanisms that support device identity verification during online interactions with IA-stations.

4.8.6.3.2 Secure Transports

Sending information in plain form over a protected channel, e.g., ietf-hardware YANG module contents via NETCONF-over-TLS protects the transferred information during its transit through the network but does not vouch for the correctness of the received information e.g., the mfg-name value.

4.8.6.3.3 Secure Information

Protecting information objects by means of cryptographic checksums allows to verify the authenticity and integrity of the provided information. Cryptographic checksums may use symmetric or asymmetric schemes. In case of asymmetric schemes, raw and self-signed public keys need to be distinguished from CA-signed public keys.

Asymmetric schemes with CA-signed public keys are preferable for the verifiable device identity use case: claimants and verifiers share a public key; the claimant possesses the corresponding private key. The establishment and storage of the shared public keys uses public key certificates. For this approach self-signed CA certificates are to be established in an authentic manner. Their amount is independent from the number of verifiers (CNCs) as well as claimants (IA-stations).

4.8.6.3.4 IDevID and LDevID Credentials

IDevID and LDevID credentials are specified by IEEE Std 802.1AR. These objects are comprised of a certification path and a private key. The certification path encompasses an end entity certificate which contains verifiable device identity in a CA-signed form. The device identity verification happens after validating the certification path (IETF RFC 5280) and checking the proof-of-possession for the private key (IETF RFC 5246 in case of TLS 1.2). The certification path validation demands trust anchors as input arguments (IETF RFC 5280, 6.1.1 input argument (d)).

Two types of credentials are distinguished by IEEE Std 802.1AR:

- IDevIDs are issued by device manufacturers. They represent an initial identity as it is known at device production-time. The initial device identity is not locally significant: it cannot contain deployment-specific information such as DNS names or IP addresses.
- LDevIDs are issued by other actors e.g., a device user. They represent a locally significant device identity: they can contain deployment-specific information e.g., DNS names or IP addresses.

IEEE Std 802.1AR uses signature suites to describe the subject public key and the signature fields in IDevID and LDevID certification paths. This notion is different from TLS cipher suites.

NOTE IDevID and LDevID credentials also serve purposes beyond secure device identity, for instance the realization of secure transports. This facilitates the use case of NETCONF/YANG security setup from factory default state.

4.8.6.3.5 IDevID Items beyond IEEE Std 802.1AR

IEEE Std 802.1AR represents the initial device identity as serialNumber (OID 2.5.4.5) attribute in the subject field of the EE certificate. Its value provides the serial number of the device. This value is required to be unique within the domain of significance of the EE certificate issuer. The serialNumber attribute is an optional capability. This allows to verify following identity items:

- certificate issuer (not necessarily: manufacturer) by issuer field (data type: ASN.1 Name)
- if present: device instance by serialNumber value (data type: ASN.1 PrintableString).

NOTE This verification can happen after certification path validation (see IETF RFC 5280) and the proof-of-possession checking for the private key (see IETF RFC 5246 in case TLS 1.2).

The following bullet points describe options for verifying the device identity of IA-stations in factory default state. It also identifies informational items needed for the corresponding checks:

- IA-station manufacturer check: using names that identify IA-station manufacturers e.g., mfg-name in ietf-hardware YANG module
- IA-station type check: using attributes that identify IA-station types e.g., model-name, hw-revision, description in ietf-hardware YANG module
- IA-station instance check: using values that identify IA-station instances e.g., serial-num in ietf-hardware YANG module.

The following model described in the bullet points applies to the verification of the initial device identity of IA-stations:

- the set of to-be-conducted checks is determined by IA-station and CNC users

- an IA-station uses IDevID credentials to prove its device identity. The checking happens by means of online interactions in the operational network. It happens automatically and is done by CNCs. This does not depend on configuration-domain external repositories
- other stakeholders e.g., middleware/application consortia or individual manufactures are allowed to additionally express information items in IDevID credentials to reflect their device identity model. CNCs do not assess such additional information.

4.8.6.3.6 Device Identity Representation in IDevID and LDevID Credentials

The best practices for representing verifiable device identity information in IDevID and LDevID credentials are.

- Corresponding information (actual values or references to them) appears in EE certificates:
  - IDevID EE certificates bind initial device identity items that are known by the device manufacturer at production time e.g., mfg-name.
  - LDevID EE certificates bind locally significant device identity items that are known by other actors such as device users e.g., DNS names or IP addresses. They may also bind initial device identity information.
- Items that encode device naming information appear in the subjectAltName extension.

NOTE This is required by IETF RFC 5280, 4.2.1.6. It is also backed by IETF RFC 6125, 2.3.

- A binding can take one of following forms. Multiple forms can appear in one EE certificate:
  - By-value: the verifiable device identity information is represented by its value inside the IDevID resp. LDevID EE certificate. Examples are:
    - the product serialNumber in IDevID credentials (IEEE Std 802.1AR)
    - the hostname of the NETCONF/YANG server in LDevID-NETCONF credentials (IETF RFC 7589 and IETF RFC 6125)
  - By-ref: the verifiable device identity information is represented by a reference inside the IDevID resp. LDevID EE certificate, not by its value:
    - The actual value may be provided by the device itself or by a device-external source.
  - If it is provided in form of an unprotected information object, then the reference object that is embedded to EE certificates should include a digest value.

5 Conformance

5.1 General

A claim of conformance to this document is a claim that the behavior of an implementation of an IA-station (see 5.5, 5.6) with its bridge components (see 5.7, 5.8) and end station components (see 5.9, 5.10) meets the mandatory requirements of this document and may support options identified in this document.

5.2 Requirements terminology

a) Requirements terminology is provided in the ISO/IEC Directives Part 2:2021, Clause 7. This document can be found at www.iec.ch/members_experts/refdocs.

b) The Profile Conformance Statement (PCS) proformas (see Annex A) reflect the occurrences of the words “shall,” “may,” and “should” within this document.

c) The document avoids needless repetition and apparent duplication of its formal requirements by using is, is not, are, and are not for definitions and the logical consequences of conformant behavior. Behavior that is permitted but is neither always required nor directly controlled by an implementer or administrator, or whose conformance requirement is detailed elsewhere, is described by can. Behavior that never occurs in a conformant implementation or system of conformant implementations is described by cannot. The word allow is used as a replacement for the phrase “Support the ability for,” and the word capability means “can be configured to.”

5.3 Profile conformance statement (PCS)

The supplier of an implementation that is claimed to conform to this document shall provide the information necessary to identify both the supplier and the implementation and shall complete a copy of the PCS proforma provided in Annex A.

5.4 Conformance classes

This profile includes conformance requirements and options, which are related to an entire IA-station, as well as conformance requirements and options, which are related to single Bridge or end station components within an IA-station. Figure 11 illustrates this conformance model.

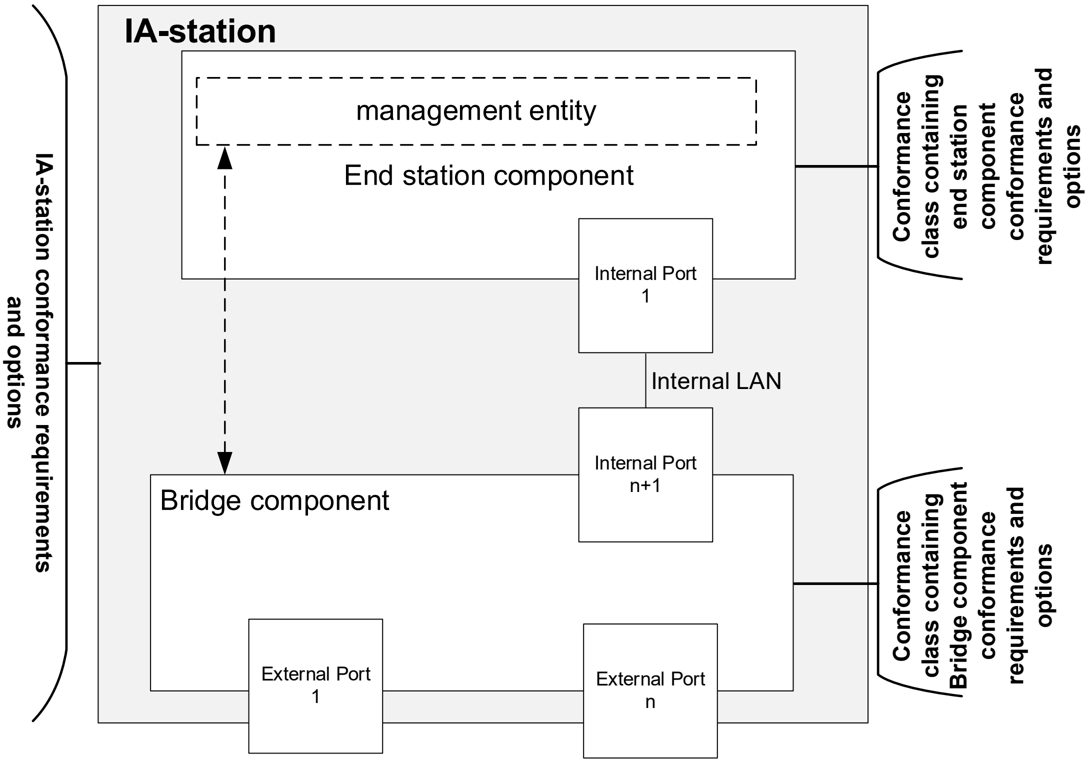


Figure 11 – IA-station conformance model

This profile supports a variety of industrial use cases. In some of these use cases, support of certain TSN features might be mandatory, while in others, supporting these features could lead to non-optimal implementations. Therefore, this document defines two conformance classes that are applicable both to Bridge components and end station components. Conformance Class A (ccA) is feature rich, i.e., tailored to use cases requiring support of many TSN-IA Profile features. Conformance Class B (ccB) targets implementations that are more resource constrained. The details for the conformance classes are specified in 5.7 and 5.8 for Bridge components, and in 5.9 and 5.10 for end station components.

NOTE 1 It is the responsibility of the IA-station manufacturer to carefully consider the implications of mixing ccA and ccB Bridge components and end station components in a single IA-station.

NOTE 2 It is the responsibility of the user to carefully consider the implications of mixing ccA and ccB Bridge components and end station components in a single Configuration Domain.

NOTE 3 Any Bridge compliant to this document is an IA-station. Any IA-station contains a management entity (i.e., an end station component).

5.5 IA-station requirements

5.5.1 IA-station PHY and MAC requirements for external ports

IA-stations for which a claim of conformance to this document is made shall support the following requirements for external ports:

a) Media Access Control (MAC) service specification according to IEEE Std 802.3-2022, Clause 2.

b) Media Access Control (MAC) frame and packet specifications according to IEEE Std 802.3-2022, Clause 3, especially the MAC Client Data field size according to IEEE Std 802.3-2022, 3.2.7, item c).

c) Layer Management according to IEEE Std 802.3-2022, 3.2.7 c).

d) Implement at least one IEEE Std 802.3-2022 MAC that shall operate in full-duplex mode, and associated IEEE Std 802.3-2022 PHY with a data rate of at least one of speed: 10 Mb/s, 100 Mb/s, 1 000 Mb/s, 2,5 Gb/s or 5 Gb/s together with the corresponding managed objects on each port.

   1) 10BASE-T1L MAU type according to IEEE Std 802.3-2022, Clauses 22 and 146.

   2) 100BASE-TX and 100BASE-FX MAU types according to IEEE Std 802.3-2022, Clauses 21, 22, 24, 25, 26, 30, 31 and IEEE Std 802.3-2022, Annexes 23A, 28A, 28B, 28C, 28D, 31A, 31B, 31C, and 31D.

   3) 1000BASE-T and 1000BASE-SX MAU types according to IEEE Std 802.3-2022, Clauses 28, 34, 35, 36, 37, 38, and 40.

   4) 2.5GBASE-T and 5GBASE-T MAU types according to IEEE Std 802.3-2022, Clauses 28, 125, and 126.

   5) 2.5GBASE-T1 and 5GBASE-T1 MAU types according to IEEE Std 802.3-2022, Clause 149.

   6) 10GBASE-T and 10GBASE-SR MAU types according to IEEE Std 802.3-2022, Clauses 44, 46, 47, 49, 51, 52, 55, and IEEE Std 802.3-2022, Annexes 48A and 55A.

   7) 10GBASE-T1 MAU type according to IEEE Std 802.3-2022, Clause 149.

   8) 100BASE-T1 MAU type according to IEEE Std 802.3-2022, Clause 96.

   9) 1000BASE-T1 MAU type according to IEEE Std 802.3-2022, Clause 97.

e) Support the YANG features and leaves of the ieee802-ethernet-interface module according to 6.7.9.2.2.

NOTE Clauses and subclauses not mentioned can be implemented but are not part of a conformity assessment.

5.5.2 IA-station topology discovery requirements

IA-stations for which a claim of conformance to this document is made shall:

a) Support the required capabilities according to IEEE Std 802.1AB-2016, 5.3 and IEEE Std 802.1ABcu-2021, 5.3.

b) Support IA-station internal structure discovery according to 6.7.3.

c) Support the YANG features and leaves of the ieee-dot1ab-lldp module according to 6.7.9.2.3.

5.5.3 IA-station requirements for time synchronization

These requirements are related to the entire IA-station with all its PTP Instances and PTP Ports. IA-stations for which a claim of conformance to this document is made shall:

Editor's note - Cross-references to Clause 5 of 802.1AS-2020 will be updated prior to SA ballot to reflect edits, additions, and deletions to Clause 5 made by IEEE 802.1ASdm and IEEE 802.1AS-2020/Cor1.

a) Support the implementation of a time-aware system according to IEEE Std 802.1AS-2020, 5.3.

b) Support the PTP Instance requirements according to IEEE Std 802.1AS-2020, 5.4.1 items a) through i).

NOTE A domain in a PTP End Instance can be used for Global Time, Working Clock, or both.

c) Support timing and synchronization management according to IEEE Std 802.1AS-2020, 5.4.2 items j) and k).

d) Support the PTP Instance requirements according to 6.2.2 and the PTP Protocol requirements according to 6.2.3.

e) Support the transmission of the Drift tracking TLV according to IEEE P802.1ASdm

f) Support external port configuration capability according to IEEE Std 802.1AS-2020, 5.4.2 item g).

g) Support MAC-specific timing and synchronization methods for IEEE Std 802.3 full-duplex links according to IEEE Std 802.1AS-2020, 5.5 items a) through d) and item h).

h) Support the YANG features and leaves of the:

    i) ieee-1588ptp module according to 6.7.9.2.4.1.

    ii) ieee-dot1as-ptp module according to 6.7.9.2.4.2.

i) Support the message timestamp point according to IEEE802.1AS-2020, 11.3.9

Editor's note: The allowable variation of inter-message interval for each message type needs to be further defined for the industrial use case.

Editor’s note: The establishment of a drift-tracking TLV is the subject of a proposed PAR modification to P802.1ASdm.

5.5.4 IA-station requirements for security

These requirements are related to the secured management of an entire IA-station independent of the internal component structure. IA-stations for which a claim of conformance to this document is made shall support the following requirements as defined in 6.3 and 6.7.9.2.5:

a) NETCONF-over-TLS (IETF RFC 7589) with the cipher suite TLS_ECDHE_ECDSA_WITH_ AES_128_GCM_SHA256, based on the elliptic curves, according to 6.3.2.1 and 6.3.4:

    1) Curve25519 (IETF RFC 7748)

    2) P-256 (NIST FIPS 186-4)

b) Secure Device Identity according to 6.3.3 and IEEE Std 802.1AR-2018, 5.3.

c) PKIX (IETF RFC 5280) according to 6.3.2.1.4.

d) NACM (IETF RFC 8341) according to 6.3.2.2.

e) Support the YANG features and leaves of the:

    1) [draft-]ietf-keystore module according to 6.7.9.2.5.1,

    2) ietf-netconf-acm module according to 6.7.9.2.5.2,

    3) [draft-]ietf-truststore according to 6.7.9.2.5.3,

5.5.5 IA-station requirements for management

5.5.5.1 General

These requirements are related to the remote management capabilities of an IA-station independent of the internal component structure.

5.5.5.2 Network Configuration Protocol (NETCONF)

IA-stations for which a claim of conformance to this document is made shall support the Network Configuration Protocol (NETCONF) with the following capabilities:

a) NETCONF Server functionality according to IETF RFC 6241.

b) NETCONF over TLS with Mutual X.509 Authentication as described in IETF RFC 7589, including support of DHCP (IETF RFC 2131), IPv4 (IETF RFC 791) and TCP (IETF RFC 793).

NOTE The SSH transport protocol, which is mandatory in IETF RFC 6241, 2.3, is out of scope for IEC/IEEE 60802 conformant IA-stations.

c) Candidate configuration capability as described in IETF RFC 6241, 8.3.
d) Rollback-on-Error capability as described in IETF RFC 6241, 8.5.
e) Validate capability as described in IETF RFC 6241, 8.6.
f) NETCONF Event Notifications as described in IETF RFC 5277.
g) Dynamic Subscription to YANG Events and Datastores over NETCONF as described in IETF RFC 8640.
h) NETCONF Extensions to Support the Network Management Datastore Architecture (NMDA) as described in IETF RFC 8526.
i) Network Configuration Access Control Model (NACM) as described in IETF RFC 8341.

5.5.5.3 IA-station management YANG modules

IA-stations for which a claim of conformance to this document is made shall support the YANG features and leaves for IA-station management of the:

a) ietf-system-capabilities module according to 6.7.9.2.6.1,
b) ietf-yang-library module as according to 6.7.9.2.6.2,
c) ietf-netconf-nmda module according to 6.7.9.2.6.3,
d) ietf-yang-push module according to 6.7.9.2.6.4,
e) ietf-notification-capabilities module according to 6.7.9.2.6.5,
f) ietf-subscribed-notifications module according to 6.7.9.2.6.6,
g) ietf-netconf-monitoring module according to 6.7.9.2.6.7.
h) ietf-system module according to 6.7.9.2.6.8,
i) ietf-hardware module according to 6.7.9.2.6.9,
j) ietf-interfaces module according to 6.7.9.2.6.10,
k) ieee802-dot1q-bridge module according to 6.7.9.2.6.11,
l) ieee-iec-60802-iastation-datasheet module according to 6.7.9.2.6.12.

5.5.6 IA-station requirements for digital data sheet

For IA-stations for which a claim of conformance to this document is made a shall:

– Provide a 60802 YANG module as according to 6.7.8 in the form of an XML file containing the instance data set according to IETF RFC 9195. A manufacturer may reduce the instance data set by removing private YANG modules and/or statistical config-false YANG nodes.

NOTE This includes all YANG modules required by this document, as well as all additional modules that have been added by the manufacturer.

5.6 IA-station options

5.6.1 IA-station PHY and MAC options for external ports

IA-stations for which a claim of conformance to this document is made may support the following requirements:

a) Power over Ethernet over 2 Pairs according to IEEE Std 802.3-2022, Clause 33.
b) Power Interfaces according to IEEE Std 802.3-2022, Clause 104.
c) Power over Ethernet (PoE) according to IEEE Std 802.3-2022 Clause 145.

5.6.2 IA-station options for time synchronization

IA-stations for which a claim of conformance to this document is made may :

Editor's note - Cross-references to Clause 5 of 802.1AS-2020 will be updated prior to SA ballot to reflect edits, additions, and deletions to Clause 5 made by IEEE 802.1ASdm and IEEE 802.1AS-2020/Cor1.

a) Support PTP Instance options according to IEEE Std 802.1AS-2020, 5.4.2 items b) through f) and items h), and i).

b) If more than one PTP port is supported, support PTP Relay Instance requirements according to IEEE Std 802.1AS-2020, 5.4.3 and the PTP Instance options according to IEEE Std 802.1AS-2020, 5.4.2 items b) and d).

c) Support hot standby redundancy requirements according to P802.1ASdm.

Editor's note: Specific defaults and options from IEEE Draft Std P802.1ASdm may be required for an implementation of hot standby for an industrial system.

Editor's note: The Time-aware system options in IEEE Std 802.1AS-2020, 5.4.2 should be examined carefully to determine if any of those options should be mandatory for the purposes of this profile. A contribution is welcome.

5.6.3 IA-station options for security

IA-stations for which a claim of conformance to this document is made may support the following requirements as defined in 6.3:

a) NETCONF-over-TLS, according to IETF RFC 7589, with one or more of the following cipher suites
   1) TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
   2) TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256

b) TLS according to 6.3.2.1.2 based on one or more of the following elliptic curves:
   1) Curve448 (IETF RFC 7748)
   2) P-521 (NIST FIPS 186-4)

c) Support the YANG features and leaves of the:

   ietf-keystore (IETF RFC „Internet-Draft (I-D)“) A YANG Data Model for a Keystore - draft-ietf-netconf-keystore) with component-internal or component-external generation of asymmetric key pairs according to 6.3.4.3.2.

NOTE The use of component-internal key generation is recommended for IA-stations.

d) External key generation according to 6.3.4.3.3.

IA-stations for which a claim of conformance to this document is made should support the following requirements as defined in 6.3:

– Internal key generation according to 6.3.4.3.2.

5.6.4 IA-station options for management

a) Writable-Running capability as described in IETF RFC 6241, 8.2.
b) Confirmed Commit capability as described in IETF RFC 6241, 8.4.
c) Distinct Startup capability as described in IETF RFC 6241, 8.7.
d) URL capability as described in IETF RFC 6241, 8.8.
e) XPath capability as described in IETF RFC 6241, 8.9.

5.7 Bridge component requirements

5.7.1 Common Bridge component requirements

A bridge component implementation of any conformance class for which a claim of conformance to this document is made shall:

a) Support C-VLAN component requirements according to IEEE Std 802.1Q-2018, 5.5 and 5.4 except item o) in IEEE Std 802.1Q-2018, 5.4.

b) Support the use of Customer VLAN Identifiers (C-VID).

c) Allow the FDB to contain Static and Dynamic VLAN Registration Entries for a minimum of 8 VIDs, up to a maximum of 4 094 VIDs, according to IEEE Std 802.1Q-2018, 8.8.

NOTE 1 An example use case for 8 VIDs would be: 2 VIDs for IA time-aware stream or IA stream traffic, 2 VIDs for IA time-aware stream or IA stream redundancy, and 4 VIDs for IA traffic engineered non-stream or IA non-stream traffic.

d) Allow translation of VIDs through support of the VID Translation Table or through support of both the VID Translation Table and Egress VID translation table on one or more Bridge Ports according to IEEE Std 802.1Q-2018, 6.9.

e) Support the strict priority algorithm for transmission selection on each port for each traffic class according to IEEE Std 802.1Q-2018, 8.6.8.1.

f) Support the capability to disable Priority-based flow control if it is implemented according to IEEE Std 802.1Q-2018, Clause 36.

g) Support the Priority Regeneration requirements according to IEEE Std 802.1Q-2018, 5.4.1, item o).

h) Support MST according to IEEE Std 802.1Q-2018, 5.4.1.1.

i) Support TE-MSTID according to IEEE Std 802.1Q-2018, 8.6. and 8.8 and IEEE Std 802.1Qcc-2018, 5.5.2.

j) Support spanning tree, VLAN, and TE-MSTID configuration according to 6.7.2.4.

k) Support forwarding database (FDB) requirements according to 6.5.

l) Support Flow meters including support of at least 3 flow meters per port, according to IEEE Std 802.1Q-2018, 8.6.5, 8.6.5.1.3 items a) through c) and item f) and 8.6.5.1.1 item e 2). A flow meter should set following IEEE Std 802.1Q-2018, 8.6.5.1.3 parameters to values:

- Item d) Excess Information Rate (EIR) = 0
- Item e) Excess burst size (EBS) = 0
- Item g) Color mode (CM) = color_blind

NOTE 2 When CM = color_blind, DropOnYellow (IEEE Std 802.1Q-2018, 8.6.5.1.3, item h), MarkAllFramesRed (IEEE Std 802.1Q-2018, 8.6.5.1.3, item j), and MarkAllFramesRedEnable (IEEE Std 802.1Q-2018, 8.6.5.1.3, item i) are not used.

NOTE 3 For example, an implementation could contain one flow meter for broadcast traffic, one flow meter for multicast traffic and one flow meter for unicast traffic.

5.7.2 ccA Bridge component requirements

A Bridge component implementation for which a claim of conformance to ccA of this document is made, shall:

a) Support common bridge component requirements according to 5.7.1.

b) Support at least 2 PTP Instances according to 802.1AS-2020, 5.4.1 items a) through i).

c) Support eight queues according to IEEE Std 802.1Q-2018, 8.6.6.

d) Support the enhancements for scheduled traffic for data rates of 100 Mb/s and 1 Gb/s according to IEEE Std 802.1Q-2018, 5.4.1 items ab) and ac) including:

   1) a tick granularity of less than or equal to 10 ns according to IEEE Std 802.1Q-2018, 8.6.8.4.

2) The allowable error budget between the transmission selection timing point and the on-the-wire timing point, less any error budget for the PHY (see figure 12.6 in IEEE Std 802.1Q-2018), shall be less than or equal to 10 ns.

NOTE Transmission selection timing points have a granularity of 1 ns; however, operation is determined by the precision of the "tick" event.

3) Support the YANG features and leaves of the ieee-dot1q-sched module according to 6.7.9.3.2.

e) Support frame preemption according to IEEE Std 802.1Q-2018, 5.4.1 item ad), for data rates of 100 Mb/s and 1 Gb/s, including:

1) Support of Interspersing Express Traffic with preemptable traffic according to IEEE Std 802.3-2022, Clause 99, including support of the Additional Ethernet Capabilities for TLV in an LLDPDU to indicate supported functions of preemption according to IEEE Std 802.3-2022, 79.3.7.

2) Support of the YANG features and leaves of the ieee-dot1q-preemption module according to 6.7.9.3.3.

5.7.3 ccB Bridge component requirements

A Bridge component implementation for which a claim of conformance to ccB of this document is made, shall:

a) Support common bridge component requirements according to 5.7.1.

b) Support at least 1 PTP Instance according to IEEE Std 802.1AS-2020, 5.4.1 items a) through i).

c) Support at least four queues according to IEEE Std 802.1Q-2018, 8.6.6.

Editor's note: It is expected that P802.1ASdm will make support of domain 0 optional.

5.8 Bridge component options

5.8.1 Common Bridge component options

A bridge component implementation of any conformance class for which a claim of conformance to this document is made may support the following requirements:

a) Support the operation of the credit-based shaper algorithm according to 802.1Q, 8.6.8.2 on all Ports as the transmission selection algorithm for at least 4 traffic classes.

b) Support the YANG features and leaves of the <ieee-cbs> module according to 6.7.9.3.4.

c) Support PSFP according to IEEE Std 802.1Q-2018, 5.4.1.8.

d) Support FRER according to IEEE Std 802.1CB-2017, 5.15.

NOTE While redundancy and high availability are frequently addressed by upper layer protocols, it is intended that an optional implementation of FRER would follow the recommended mechanisms of this specification to ensure network convergence.

5.8.2 ccA Bridge component options

A Bridge component implementation for which a claim of conformance to ccA of this document is made, may:

a) Support any or none of the common bridge component options according to 5.8.1.

b) Support more than 2 PTP Instances according to IEEE Std 802.1AS-2020, 5.4.1 items a) through i).

c) Support the enhancements for scheduled traffic for data rates of 10 Mb/s, 2,5 Gb/s, 5 Gb/s, and 10 Gb/s according to IEEE Std 802.1Q-2018, 5.4.1 items ab) and ac) including:

1) a tick granularity of less than or equal to 10 ns according to IEEE Std 802.1Q-2018, 8.6.8.4.

2) The allowable error budget between the transmission selection timing point and the on-the-wire timing point, less any error budget for the PHY (see figure 12.6 in IEEE Std 802.1Q-2018), shall be less than or equal to 10 ns.

3) Support the YANG features and leaves of the ieee-dot1q-sched module according to 6.7.9.3.2.

d) Support frame preemption according to IEEE Std 802.1Q-2018, 5.4.1 item ad), for data rates of 10 Mb/s, 100 Mb/s and 1 Gb/s, including:

NOTE IEEE Std 802.3de-2022, 99.1, comprises 10 Mb/s.

1) Support of Interspersing Express Traffic with preemptable traffic according to IEEE Std 802.3-2022, Clause 99, including support of the Additional Ethernet Capabilities for TLV in an LLDPDU to indicate supported functions of preemption according to IEEE Std 802.3-2022, 79.3.7.

2) Support of the YANG features and leaves of the ieee-dot1q-preemption module according to 6.7.9.3.3.

5.8.3 ccB Bridge component options

A Bridge component implementation for which a claim of conformance to ccB of this document is made, may:

a) Support any or none of the common bridge component options according to 5.8.1.

b) Support up to eight queues according to IEEE Std 802.1Q-2018, 8.6.6.

c) Support more than 1 PTP Instance according to IEEE Std 802.1AS-2020, 5.4.1 items a) through i).

d) Support the enhancements for scheduled traffic according to IEEE Std 802.1Q-2018, 5.4.1 items ab) and ac) including:

1) a tick granularity of less than or equal to 10 ns according to IEEE Std 802.1Q-2018, 8.6.8.4.

2) The allowable error budget between the transmission selection timing point and the on-the-wire timing point, less any error budget for the PHY (see figure 12.6 in IEEE Std 802.1Q-2018), shall be less than or equal to 10 ns.

3) Support the YANG features and leaves of the ieee-dot1q-sched module according to 6.7.9.3.2.

e) Support frame preemption according to IEEE Std 802.1Q-2018, 5.4.1 item ad), including:

1) Support of Interspersing Express Traffic with preemptable traffic according to IEEE Std 802.3-2022, Clause 99 including support of the Additional Ethernet Capabilities for TLV in an LLDPDU to indicate supported functions of preemption according to IEEE Std 802.3-2022, 79.3.7.

2) Support of the YANG features and leaves of the ieee-dot1q-preemption module according to 6.7.9.3.3.

5.9 End station component requirements

5.9.1 Common End Station Component Requirements

An end station component implementation of any conformance class for which a claim of conformance to this document is made, shall:

a) Support the use of at least one customer VLAN Identifier for IA traffic engineered non-stream or IA non-stream traffic.

b) Support the use of an additional customer VLAN Identifier for IA time-aware stream traffic if that traffic type category is supported.

c) Support the use of an additional customer VLAN Identifier for IA stream traffic if that traffic type category is supported.

d) Support the use of an additional customer VLAN Identifier for IA time-aware stream traffic if redundancy for that traffic type category is supported.

e) Support the use of an additional customer VLAN Identifier for IA stream traffic if redundancy for that traffic type category is supported.

f) Participate in only a single configuration domain.

5.9.2 ccA end station component requirements

An end station component implementation for which a claim of conformance to ccA of this document is made, shall:

a) Support common end station component requirements according to 5.9.1.

b) Support end station requirements for enhancements for scheduled traffic according to IEEE Std 802.1Q-2018, 5.25, for data rates of 100 Mb/s and 1 Gb/s including:

   1) a tick granularity of less than or equal to 10 ns according to IEEE Std 802.1Q-2018, 8.6.8.4.

   2) The allowable error budget between the transmission selection timing point and the on-the-wire timing point, less any error budget for the PHY (see figure 12.6 in IEEE Std 802.1Q-2018), shall be less than or equal to 10 ns.

   3) Support the YANG features and leaves of the ieee-dot1q-sched module according to 6.7.9.3.2.

c) Support end station requirements for frame preemption according to IEEE Std 802.1Q-2018, 5.26, for data rates of 100 Mb/s, and 1 Gb/s, if the IA time-aware stream traffic or the IA stream traffic type categories are supported, including:

   1) Support of Interspersing Express Traffic according to IEEE Std 802.3-2022, Clause 99, including support of the Additional Ethernet Capabilities TLV in an LLDPDU to indicate supported functions of preemption according to IEEE Std 802.3-2022, 79.3.7 and table 79-8.

   2) Support of the YANG features and leaves of the ieee-dot1q-preemption module according to 6.7.9.3.3.

5.9.3 ccB end station component requirements

An end station component implementation for which a claim of conformance to ccB of this document is made, shall:

Support common end station component requirements according to 5.9.1.

5.10 End station component options

5.10.1 Common end station component options

An end station component implementation of any conformance class for which a claim of conformance to this document is made, may:

a) Support more than 1 PTP Instance according to IEEE Std 802.1AS-2020, 5.4.1 items a) through i).

b) Support the operation of the credit-based shaper algorithm according to 802.1Q, 8.6.8.2 on all Ports as the transmission selection algorithm for at least 4 traffic classes.

c) Support the YANG features and leaves of the <ieee-cbs> module according to 6.7.9.3.4.

d) Support Talker end system behaviors according to IEEE Std 802.1CB-2017, 5.6, 5.7, and 5.8.

e) Support Listener end system behaviors according to IEEE Std 802.1CB-2017, 5.9, 5.10, and 5.11.

5.10.2 ccA end station component options

An end station component implementation for which a claim of conformance to ccA of this document is made, may:

a) Support common end station options according to 5.10.1
b) Support end station requirements for enhancements for scheduled traffic according to IEEE Std 802.1Q-2018, 5.25, for data rates of 10 Mb/s, 2,5 Gb/s, 5 Gb/s, and 10 Gb/s including:
   1) a tick granularity of less than or equal to 10 ns according to IEEE Std 802.1Q-2018, 8.6.8.4.
   2) The allowable error budget between the transmission selection timing point and the on-the-wire timing point, less any error budget for the PHY (see figure 12.6 in IEEE Std 802.1Q-2018), shall be less than or equal to 10 ns.
   3) Support the YANG features and leaves of the ieee-dot1q-sched module according to 6.7.9.3.2.
c) Support end station requirements for frame preemption according to IEEE Std 802.1Q-2018, 5.26, for data rates of 10 Mb/s, 2,5 Gb/s, 5 Gb/s, and 10 Gb/s.

NOTE IEEE Std 802.3de-2022, 99.1, comprises 10 Mb/s.

   1) Support of Interspersing Express Traffic according to IEEE Std 802.3-2022, Clause 99, and IEEE P802.3de, 99.1, including support of the Additional Ethernet Capabilities TLV in an LLDPDU to indicate supported functions of preemption according to IEEE Std 802.3-2022, 79.3.7 and table 79-8.
   2) Support of the YANG features and leaves of the ieee-dot1q-preemption module according to 6.7.9.3.3.

5.10.3 ccB end station component options

An end station component implementation for which a claim of conformance to ccB of this document is made, may:

a) Support common end station component options according to 5.10.1
b) Support end station requirements for enhancements for scheduled traffic according to IEEE Std 802.1Q-2018, 5.25 including:
   1) a tick granularity of less than or equal to 10 ns according to IEEE Std 802.1Q-2018, 8.6.8.4.
   2) The allowable error budget between the transmission selection timing point and the on-the-wire timing point, less any error budget for the PHY (see figure 12.6 in IEEE Std 802.1Q-2018), shall be less than or equal to 10 ns.
   3) Support the YANG features and leaves of the ieee-dot1q-sched module according to 6.7.9.3.2.
c) Support end station requirements for frame preemption according to IEEE Std 802.1Q-2018, 5.26.
   1) Support of Interspersing Express Traffic according to IEEE Std 802.3-2022, Clause 99, and IEEE P802.3de, 99.1, including support of the Additional Ethernet Capabilities TLV in an LLDPDU to indicate supported functions of preemption according to IEEE Std 802.3-2022, 79.3.7 and table 79-8.
   2) Support of the YANG features and leaves of the ieee-dot1q-preemption module according to 6.7.9.3.3.

5.11 CNC requirements

CNCs for which a claim of conformance to this document is made shall:

a) Support TSN CNC station requirements according to IEEE Std 802.1Qcc-2018, 5.29.

b) Be integrated in an IA-Station that supports NETCONF with the following capabilities:
   1) NETCONF Client functionality according to IETF RFC 6241.
   2) NETCONF Server functionality according to IETF RFC 6241.
   3) NETCONF capabilities according to 6.3.2.1.

Editor's note: IEEE 802.1Q-2022 5.29 TSN CNC station requirements has to be analyzed.

c) Support the common YANG modules, features, and leaves according to 6.7.9.2.
d) Support the optional YANG modules, features, and leaves according to 6.7.9.3.
e) Support the TSN UNI YANG module, features, and leaves according to 6.7.9.2.7.

5.12 CNC options

There are no optional CNC features.

5.13 CUC requirements

CUCs for which a claim of conformance to this document is made shall:

a) Support the Network Configuration Protocol (NETCONF) with the following capabilities:
   1) NETCONF Client functionality according to IETF RFC 6241.
   2) NETCONF capabilities according to 6.3.2.1.
b) Support the TSN UNI YANG module, features, and leaves according to 6.7.9.2.7.

6 Required functions for an industrial network

6.1 General

Clause 6 provides requirements specific to this document and the industrial use case.

6.2 Synchronization

6.2.1 General

An IA-station can contain more than one Grandmaster PTP Instance and PTP End Instance to support:

a) hot-standby use cases, or
b) Working Clock or Global Time.

6.2.2 PTP Instance requirements

A Grandmaster PTP Instance, a PTP Relay Instance and a PTP End Instance, and the Working Clock or Global Time clocks connected to them, shall meet the following requirements under their allowed working conditions and for their lifetime:

a) The fractional frequency offset of the LocalClock relative to the PTP timescale frequency shall be according to Table 9.
b) The range of the rate of change of fractional frequency offset of the LocalClock shall be according to Table 9.
c) During operation, the Working Clock and Global Time at Grandmaster PTP Instances and PTP End Instances shall increase monotonically, where monotonic means that for a time *y* that occurs after time *x*, the ClockTarget's timestamp of *y* is greater than or equal to the ClockTarget's timestamp of *x*.
d) Working Clock and Global Time at a PTP End Instance can be controlled by applying a frequency change over a period of time. This will also result in a phase change of the Working Clock or Global Time, as the phase change of a clock due to an applied frequency

change is the product of the applied frequency change and the duration of time of the frequency change. The frequency applied can have a fine resolution to speed up or slow down the clock smoothly, and it has a total range of frequency adjustment.

e) For the Global Time at a PTP End Instance, the maximum value of frequency adjustment shall be according to Table 9.

f) For the Working Clock at a PTP End Instance, the maximum value of frequency adjustment shall be according to Table 9.

For Working Clock or Global Time, decoupled from a ClockTarget, a higher maximum rate of frequency adjustments and maximum rate of change of fractional frequency offset are allowed. As soon as its coupled (or coupled again) a) to f) apply.

Table 9 – Required values

Topic	Value
Local Clock, range of fractional frequency offset relative to the nominal frequency	-50 ppm to +50 ppm
Local Clock, range of rate of change of fractional frequency offset	-1,35 ppm/s to +2,12 ppm/s
Working Clock at Grandmaster PTP Instance (acting as ClockSource), range of fractional frequency offset relative to the nominal frequency	-50 ppm to +50 ppm
Working Clock at Grandmaster PTP Instance, range of rate of change of fractional frequency offset	-1,35 ppm/s to +2,12 ppm/s
Working Clock at PTP End Instance, maximum value of frequency adjustment	±250 ppm over any observation interval of 1 ms
Global Time at Grandmaster PTP Instance (acting as ClockSource), range of fractional frequency offset relative to the nominal frequency	-200 ppm to +200 ppm
Global Time at Grandmaster PTP Instance, range of rate of change of fractional frequency offset	-10 ppm/s to +10 ppm/s
Global Time at PTP End Instance, maximum value of frequency adjustment	±1000 ppm over any observation interval of 1 ms

NOTE The Maximum value of frequency adjustment represents an upper bound that limits how much a PTP End Instance can change the frequency of its Working Clock or Global Time during a given period. However, these adjustments would be incremental rather than instantaneous over the defined interval.

Editor's note: The assumptions and values listed in 6.2.2 and 6.2.3 are preliminary. Simulations and analyses are ongoing to determine the final values.

6.2.3 PTP protocol requirements

Table 10 shows the required protocol times.

Table 10 – Protocol settings

Topic	Working Clock	Global Time
Nominal time between successive Announce messages (announce interval)	1 s	N/A
Nominal time between successive Pdelay_Req messages (Pdelay_Req message transmission interval)	125 ms	N/A
Range of allowed time between successive Pdelay_Req messages	119 ms to 131 ms	N/A

Topic	Working Clock	Global Time
Nominal time between successive Sync messages at the Grandmaster (Sync message transmission interval)	125 ms	N/A
Range of allowed time between successive Sync messages at the Grandmaster	119 ms to 131 ms	N/A
Time between reception of a Sync message and transmission of the subsequent Sync message (i.e. residence time) at a PtP Relay instance	Maximum 15 ms Mean ≤ 5 ms Standard deviation ≤ 1,8 ms	N/A
Maximum time between transmission of a Sync message and transmission of the related Follow_Up message	2,5 ms	N/A
ClockSlave (servo controller)	Maximum Bandwidth (Hz): 2,6 Hz Maximum Gain Peaking (dB): 1,3 dB Minimum absolute value of Roll-off: 20 dB/decade	???

NOTE 1 Some of the requirements in tables 9 and 10 apply only to GM-Capable PTP instances.

NOTE 2 A consequence of having a single allowed value of mean sync interval is that syncLocked mode is achieved, which is required for the desired performance. If the master port sync interval is the same as that of the slave port, syncLocked mode is achieved.

Table 11 shows the required limits on error generation at a PTP Relay instance when its Maximum absolute value of rate of change of fractional frequency offset for LocalClock is ≤0,1 ppm/s.

Table 11 – Error generation limits for Grandmaster PTP Instance

Topic	Value
Working Clock when Sync message is transmitted minus (preciseOriginTimestamp + correctionField) in Sync message	-6 to +14 ns or ? Mean +4 ns +/- 2 ns Standard Deviation ≤ 2 ns
Rate Ratio between Working Clock and Local Clock when Sync message is transmitted minus rateRatio field in Sync message	Mean 0 ppm +/- 0,1 ppm Standard deviation ≤ 0,1 ppm

Table 12 shows the required limits on error generation at a PTP Relay instance when its Maximum absolute value of rate of change of fractional frequency offset for LocalClock is ≤0,1 ppm/s.

Table 12 – Error generation limits for PTP Relay Instance

Topic	Value
Output Correction Field error* when • Maximum absolute value of rate of change of fractional frequency offset for LocalClock at the Grandmaster is ≤0,1 ppm/s (Origin Timestamp) • Input Rate Ratio field is zero. • Correction field is zero. • Maximum absolute value of rate of change of fractional frequency offset for LocalClock at upstream node is ≤0,1 ppm/s (determining pDelayResp, from which NRR is calculated, but not affecting Input Rate Ratio field)	Mean 0 ns +/- 2 ns Standard deviation ≤ 2 ns

Topic	Value
Output Rate Ratio error** when • Maximum absolute value of rate of change of fractional frequency offset for LocalClock at the Grandmaster is ≤0,1 ppm/s (Origin Timestamp) • Input Rate Ratio field is zero. • Correction field is zero. • Maximum absolute value of rate of change of fractional frequency offset for LocalClock at upstream node is ≤0,1 ppm/s (determining pDelayResp, from which NRR is calculated, but not affecting Input Rate Ratio field)	Mean 0 ppm +/- 0,1 ppm Standard deviation ≤ 0,05 ppm
Output Rate Ratio error** when • Maximum absolute value of rate of change of fractional frequency offset for LocalClock at the Grandmaster is ≤0,1 ppm/s (determining Input Origin Timestamp) • Input Rate Ratio field increasing at 2 ppm/s with each input field including a noise component with uniform distribution between -1 ppm/s and + 1 ppm/s. • Correction field is zero. • Maximum absolute value of rate of change of fractional frequency offset for LocalClock at upstream node is ≤0,1 ppm/s (determining pDelayResp, from which NRR is calculated, but not affecting Input Rate Ratio field)	Mean 0 ppm +/- 0,1 ppm Standard deviation ≤ 0,2 ppm
Output Rate Ratio inverse error*** when • Maximum absolute value of rate of change of fractional frequency offset for LocalClock at the Grandmaster is ≤0,1 ppm/s (determining Input Origin Timestamp) • Input Rate Ratio field is zero. • Correction field is zero. • Maximum absolute value of rate of change of fractional frequency offset for LocalClock at upstream node is increasing at 2 ppm/s with each input field including a noise component with uniform distribution between -1 ppm/s and + 1 ppm/s. (determining pDelayResp, from which NRR is calculated, but not affecting Input Rate Ratio field)	Mean 0 ppm +/- 0,1 ppm Standard deviation ≤ 0,1 ppm

* Output Correction Field error is:

Output correctionField – Input correctionField – measured residence time

** Ouput Rate Ratio error is the difference between the output Rate Ratio field and the measured Rate Ratio at the time the output Rate Ratio is transmitted.

rateRatio – actual rate ratio when a Sync message is transmitted

Where rateRatio is calculated from the cumulativeScaledRateOffset in the Sync message or related Follow_Up message

*** Output Rate Ratio inverse error is

rateRatio - $\frac{1}{actual\ rate\ ratio\ at\ upstream\ node\ when\ a\ Sync\ message\ is\ transmitted}$

Where rateRatio is calculated from the cumulativeScaledRateOffset in the Sync message or related Follow_Up message

This is used because increasing the fractional frequency offset of the Local Clock at the upstream PTP Relay instance while the Input Rate Ratio field remains zero is similar to decreasing the fractional frequency offset of the Local Clock at the current PTP Relay instance. See Annex C for more information.

Table 13 shows the required limits on error generation at a timeReceiver instance when its maximum absolute value of rate of change of fractional frequency offset for LocalClock is ≤0,1 ppm/s.

Table 13 – Error generation limits for PTP End Instance

Topic	Value
Time error* when • Maximum absolute value of rate of change of fractional frequency offset for LocalClock at the Grandmaster is ≤0,1 ppm/s (Origin Timestamp) • Input Rate Ratio field is zero. • Correction field is zero. • Maximum absolute value of rate of change of fractional frequency offset for LocalClock at upstream node is ≤0,1 ppm/s (determining pDelayResp, from which NRR is calculated, but not affecting Input Rate Ratio field)	Mean 0 ns +/- 2 ns Standard deviation ≤ 3 ns
Time error* when • Maximum absolute value of rate of change of fractional frequency offset for LocalClock at the Grandmaster is ≤0,1 ppm/s (determining Input Origin Timestamp) • Input Rate Ratio field increasing at 2 ppm/s with each input field including a noise component with uniform distribution between -1 ppm/s and + 1 ppm/s. • Correction field is zero. • Maximum absolute value of rate of change of fractional frequency offset for LocalClock at upstream node is ≤0,1 ppm/s (determining pDelayResp, from which NRR is calculated, but not affecting Input Rate Ratio field)	Mean 0 ns +/- 2 ns Standard deviation ≤ 5 ns
Time error* when • Maximum absolute value of rate of change of fractional frequency offset for LocalClock at the Grandmaster is ≤0,1 ppm/s (determining Input Origin Timestamp) • Input Rate Ratio field is zero. • Correction field is zero. • Maximum absolute value of rate of change of fractional frequency offset for LocalClock at upstream node is increasing at 2 ppm/s with each input field including a noise component with uniform distribution between -1 ppm/s and + 1 ppm/s. (determining pDelayResp, from which NRR is calculated, but not affecting Input Rate Ratio field)	Mean 0 ns +/- 2 ns Standard deviation ≤ 4 ns

*Time error is the difference between the time of the Clock used to generate the preciseOriginTimestamp fields of the incoming Sync messages, for either Working Clock or Global Time domain, and the output of the Working Clock or Global Time domain respectively at the PTP End Instance.

6.2.4 Clock states

ITU G.781.1:2022, Table 8-10 defines the clock states used in this document:

a) Acquiring,

b) Free-run,

c) Locked, and

d) Holdover

The state machine is specified in G.781.1:2022, 8.3.1.1 and Figure 8-11.

6.2.5 Grandmaster PTP Instance requirements

A ClockSource coupled to a ClockMaster of a Grandmaster PTP Instance ensures that its behavior allows a controlled/disciplined ClockTarget to stay in the above stated ranges. This includes the cases in which the ClockSource is controlled (effect of rate and offset compensation) by another ClockSource, for example, a GPS time source..

NOTE A Grandmaster can lose and regain its source of time, leading to large discontinuities in the value of grandmaster time. In such situations, the application can decouple from the grandmaster (see Figure 12). After the grandmaster has regained a source of time, the decision to re-couple to the grandmaster is an application decision.

Figure 12 shows an example of additional factors influencing the maximum rate of change of fractional frequency offset.

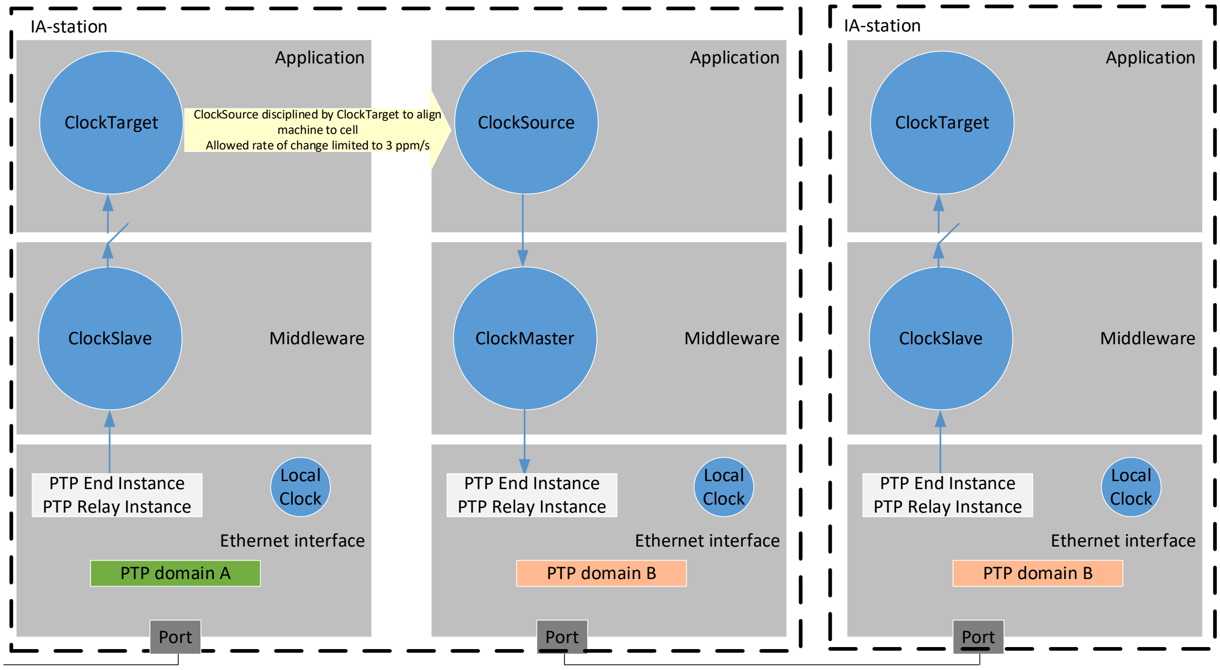


Figure 12 – Externally controlled ClockSource of a Grandmaster

Coupled machines, for example newspaper printing machines, use multiple PTP domains to allow different combinations over time without influencing the main production path. This is done by application coupling between PTP domain A and B as shown in the left-hand IA-station in Figure 12. In this IA-station, time is transferred from the ClockTarget of PTP domain A to the ClockSource of PTP domain B outside of gPTP.

6.2.6 Application framework

Any step change in the time of a ClockSource or ClockTarget whose absolute value exceeds a user-defined threshold (for example 1 µs) leads to action being taken by the application or by a higher-layer entity.

If the change is in Global Time, it is desirable that all consumers of that time be made aware of this change (i.e., a jump in Global Time from the value A to the value B), so that the actual time interval between the time corresponding to A and the time corresponding to B can be evaluated.

In the case of Working Clock time, a time change that exceeds the user-defined threshold (for example 1 µs) ought to be avoided to protect assets and prevent damage. Thus, the ClockSource or ClockTarget ought to be decoupled (see Figure 14) from the PTP-maintained clock when such a time change occurs.

In Figure 14, two ClockTargets are traceable to a reliable source of time, which should be synchronized to Global Time or Working Clock.

The status of a ClockSource, ClockTarget, ClockMaster or ClockSlave is given by the state of the clock (see 6.2.4) as shown in Figure 13. When timestamps are provided to the application, the current ClockSource or ClockTarget state is also provided to the application.

Editor's note: Make sure that the clock states are added to .1AS / .1ASdm.

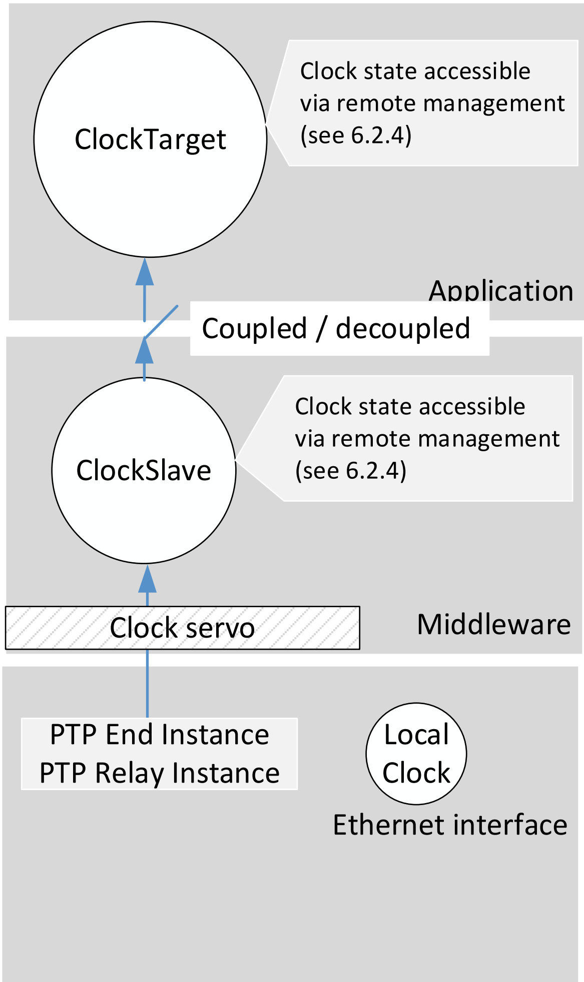


Figure 13 – Clock states

The ClockSlave is controlled by a clock servo (see Figure 13) applying the requirements from 6.2.2 and 6.2.3.

6.2.7 Working Clock domain framework

The gPTP domainNumber of a Working Clock domain is assigned by the CNC. In industrial applications, when stepsRemoved, as specified in IEEE Std 802.1AS-2020, between the Grandmaster PTP Instance and any PTP End Instance, as determined by the Best Master Clock Algorithm, is less than or equal to 64, max|TE_R| of the synchronized time of any ClockTarget, relative to the Grandmaster ClockSource, is expected to be less than or equal to 1 µs (see error budget A in Figure 16). Thus it is incumbent upon any PTP Instance to ensure that the requirements specified in 5.5.3, 6.2.2, and 6.2.3 are met.

NOTE While a minimum stepsRemoved of 64 represents the system requirement, it is desirable to be able to support up to 100 for stepsRemoved while maintaining a max|TE_R| of the synchronized time, relative to the Grandmaster, Clock of less than or equal to 1 μs.

Editor's note: The statement that max|TE sub R| is expected to be 1 μs must be confirmed via simulations. Depending on the simulation results, additional requirements will be needed, for example, on bandwidth and gain peaking of the filter in the PTP End Instance, method of measuring the rateRatio of the LocalClock relative to the Grandmaster, etc. When the simulation work is completed, it should either be described in an informative annex or referenced informatively in the Bibliography (or both)

Editor's note: More work is needed to understand the ramifications of this goal for low data rates (i.e., 10 Mb/s).

6.2.8 Global Time domain framework

The gPTP domainNumber of a Global Time domain is assigned by the CNC. In industrial applications, when stepsRemoved, as specified in IEEE Std 802.1AS-2020, between the Grandmaster PTP Instance and any PTP End Instance, as determined by the Best Master Clock Algorithm, is less than or equal to 100, max|TE_R| of the synchronized time of any ClockTarget, relative to the Grandmaster ClockSource, is expected to be less than or equal to 100 μs (see error budget A in Figure 16). Thus it is incumbent upon any PTP Instance to ensure that the requirements specified in 5.5.3, 6.2.2, and 6.2.3 are met.

Contributions regarding the requirement from the source for Global Time to the GM are requested.

6.2.9 IA-station model for clocks

Industrial automation applications (see 4.1) require synchronized time that is traceable to a known source (i.e., Global Time) and a source of time synchronized to the Working Clock. Figure 14 and Figure 15 show examples of the IA-station internal model for clocks, with the two PTP Instances needed to ensure the availability of a traceable time. In an IA-station, it is possible for the ClockSource or ClockTarget to start decoupled or become decoupled from the ClockSlave or ClockMaster of a PTP Instance; the ClockSource or ClockTarget will run independently of the availability of the network or a Grandmaster. For example, if the PTP Instance enters a clock state other than locked mode, the application might choose to decouple its clock from the PTP Instance and continue to run on its internal clock. If the PTP Instance reenters locked mode, the application can choose to again synchronize to the PTP Instance.

Figure 14 shows the IA-station internal model for clocks, with the two PTP instances used as ClockSlave/ClockTarget.

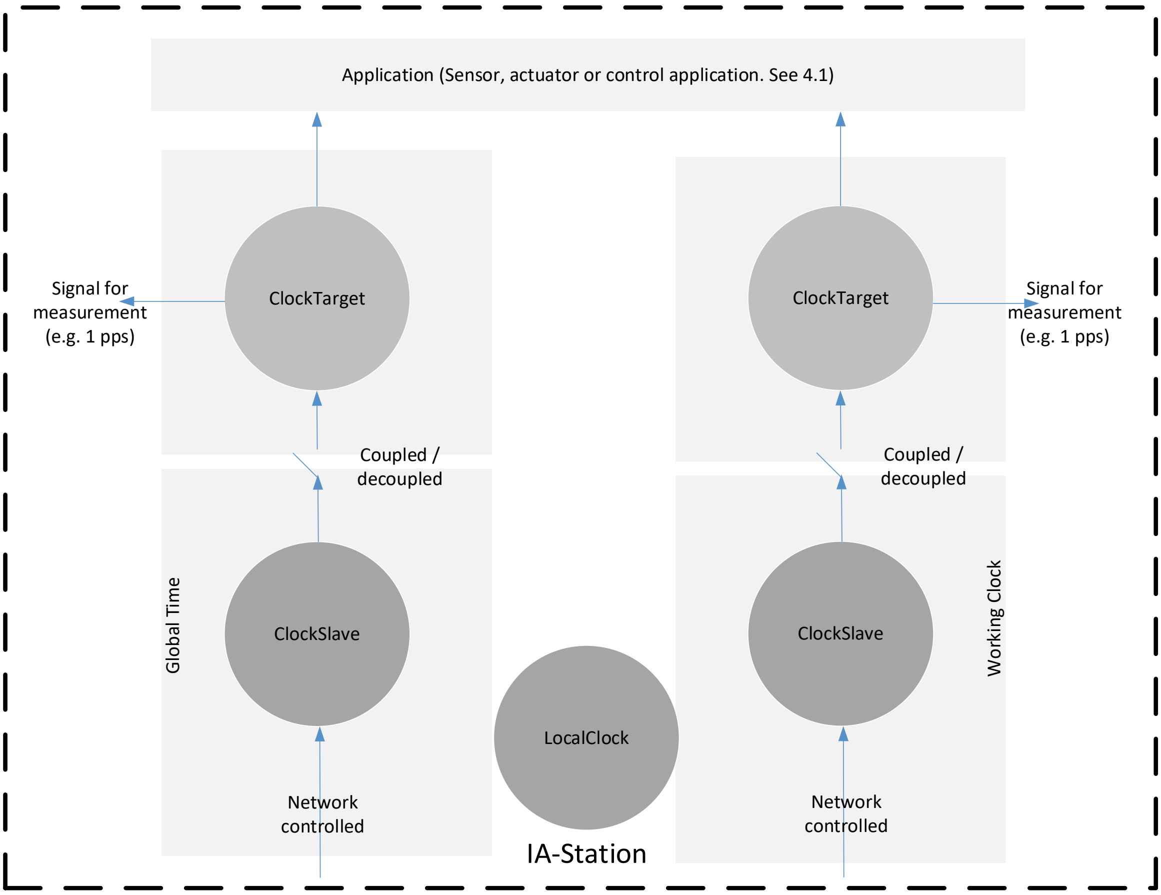


Figure 14 – Example clock usage principles for PTP End Instances

Figure 15 shows the IA-station internal model for clocks, with the two PTP instances used as Grandmaster.

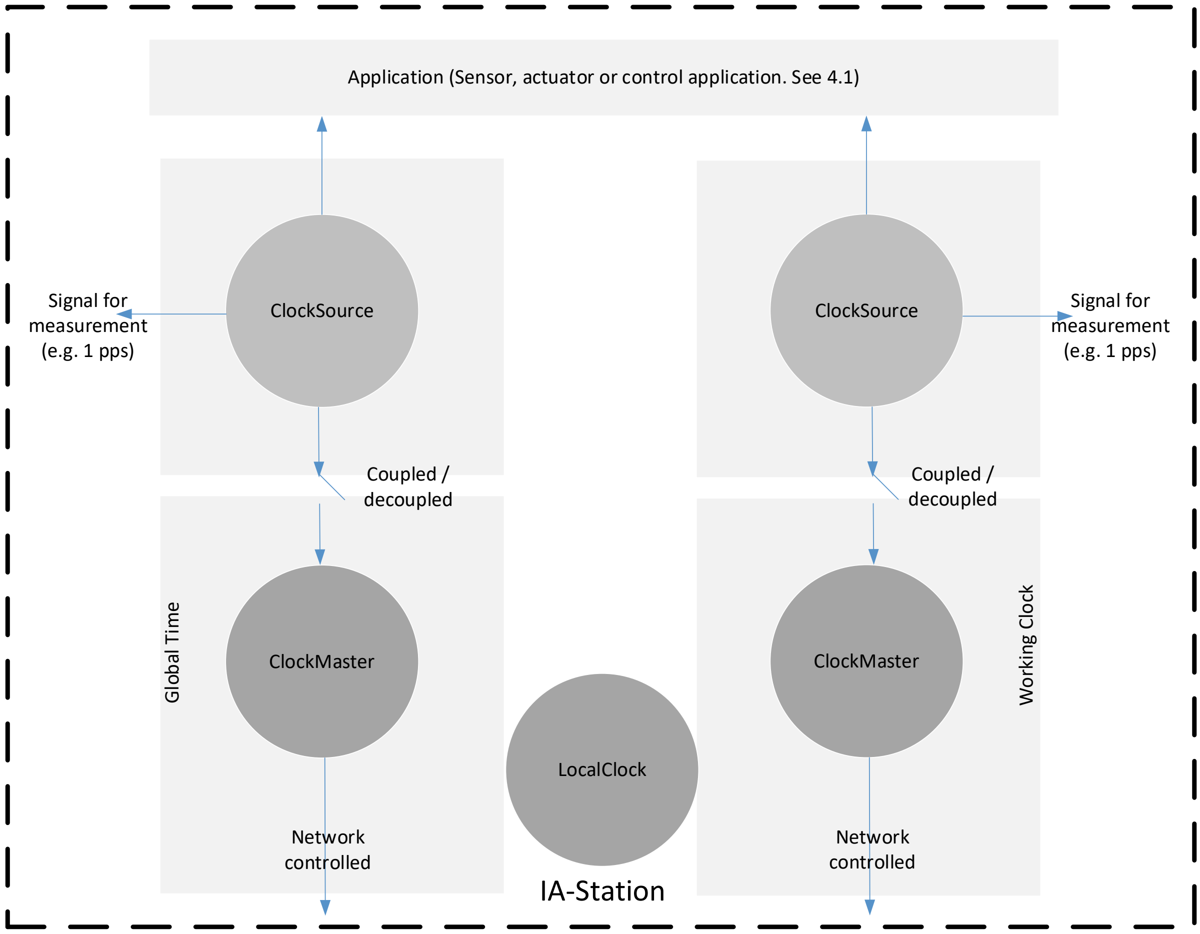


Figure 15 – Example clock usage principles for Grandmaster PTP Instances

6.2.10 Clock usage for the Ethernet interface

6.2.10.1 Time-aware offset control

Time-aware offset control needs an assigned source of time and a definition when to start or to stop, which are dependent on the clock state.

The used clock is the ClockTarget or, in the case of a Grandmaster PTP Instance, the ClockSource.

IA time-aware streams are only transmitted while the chosen ClockSource or ClockTarget is in clock state Locked (see 6.2.4).

Thus, changes of the clock state directly influence the transmission of frames.

6.2.10.2 Gating cycle

Gating cycle control needs an assigned source of time and a definition when to start or to stop, which are dependent on the clock state.

The used clock is the ClockTarget or, in the case of a Grandmaster PTP Instance, the ClockSource.

The gating cycle is running using the chosen ClockSource or ClockTarget in all clock states (see 6.2.4).

6.2.11 Error model

Synchronization needs to be transported over the entire path, from the Grandmaster PTP Instance to the PTP End Instance, through the intermediate PTP Relay Instances. All time errors, cTE and dTE, are accumulated during this process.

Time error can arise in the following processes:

a) the transporting of time in PTP Instances and via PTP Links that connect PTP Instances,

b) the providing of time to the Grandmaster PTP Instance, from the ClockSource entity via the ClockMaster entity, and

c) the providing of time to a ClockTarget entity (end application) via the ClockSlave entity.

NOTE Item a) includes time error introduced in a PTP End Instance between the slave port and the ClockSlave entity, and between the ClockMaster entity and a master port.

An output synchronization signal (for example, 1 pulse per second (PPS)) synchronized to the Working Clock as shown in Figure 14 and Figure 15, at any PTP Instance, is used to measure the time error between the ClockSource of the Grandmaster and the ClockTarget of a PTP Instance that is not the Grandmaster. The additional error introduced by implementation of the output synchronization signal is expected to be in the range of -10 ns to +10 ns. Figure 16 shows the error budget principle used. These budgets do not include any deviation from the PTP timescale. Representative budgets are provided in Annex C.

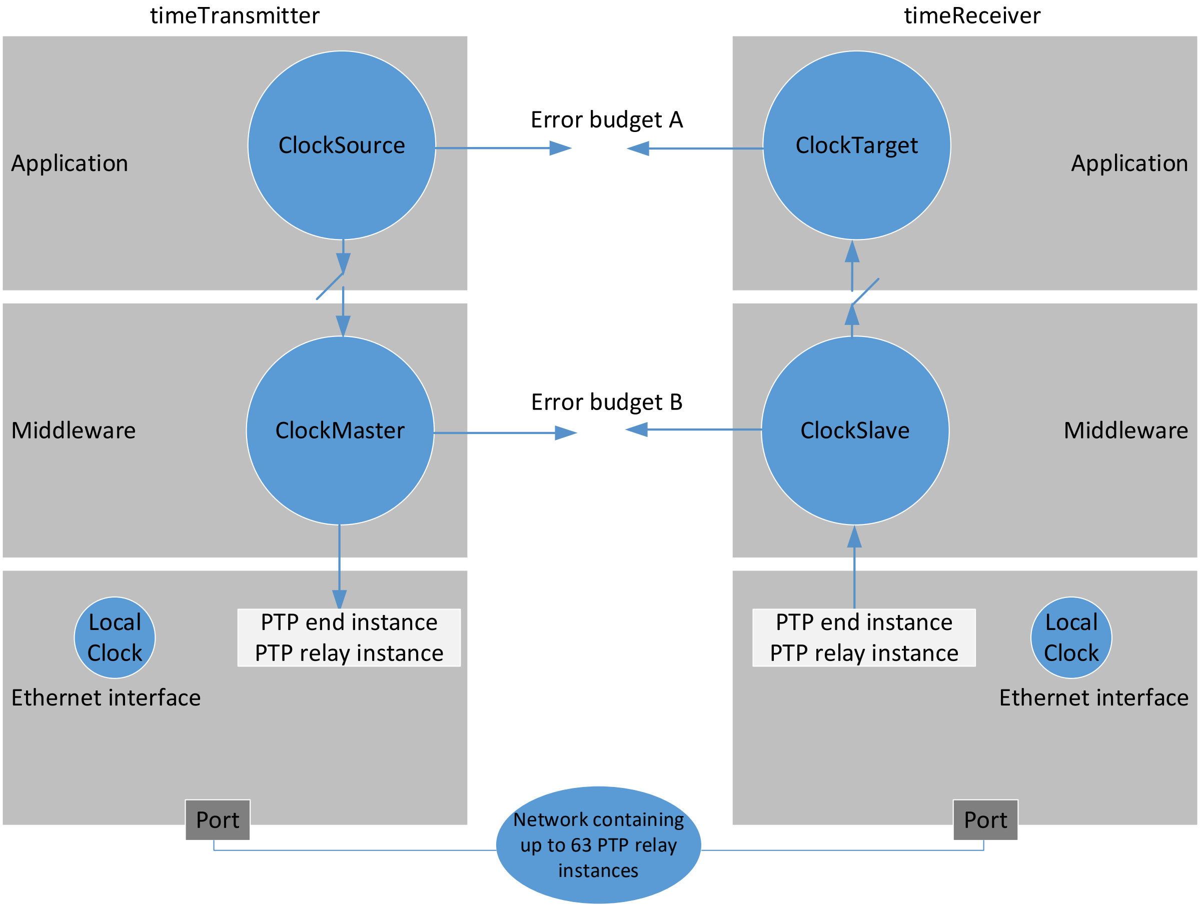


Figure 16 – Error budget scheme

Table 14 shows example values for the splitting of the available error budgets (see Figure 16).

Table 14 – Error budget

Domain	Error budget A	Error budget B
Working Clock	1 µs	900 ns
Global Time	100 µs	99,9 µs

Global time is often used for tracking events in industrial applications (i.e., sequence of events). Any usage of Global time for time stamping of application events is allowed an error budget of 1 ms.

6.2.12 gPTP domains and PTP Instances

Any gPTP domain numbers can be used. The IEEE Std 1588-2019 attribute descriptionDS.userDescription shall be used according to Table 15. One gPTP domain can be used for both Working Clock and Global Time. If only one domain is used, then the requirements for the Working Clock apply (see 6.2.7).

Additionally, the linking between the PTP Instance and the IETF interface is done by referring from the descriptionDS.userDescription to InterfaceName (see 4.6.2).

Table 15 – gPTP domains

gPTP Domain	descriptionDS.userDescription
Working Clock	String contains “WorkingClock” and, if the Working Clock is assigned to an end station interface, the InterfaceName (IETF interface-list entry)
Global Time	String contains “GlobalTime” and, if Global Time is assigned to an end station interface, the InterfaceName (IETF interface-list entry)

6.2.13 Split and combine cases for a PTP domain

Modular machines or production cells allow the splitting and combining of machines if this is required by the production process. To minimize the production disruption, the second machine is connected to the first machine during operation.

Combining the machines does not disturb the first machine, which keeps producing goods. Thus, the Grandmaster of the first machine needs to be the Grandmaster of the combined PTP domain.

Splitting the machines does not disturb the first machine, which keeps producing goods. The Grandmaster of the second machine starts after splitting to allow standalone production for the second machine.

Figure 17 shows the split and combine use case while using BMCA. Jumps in synchronization shall be avoided.

- Splitting:
  - Grandmaster of machine 2 controls machine 2 and Grandmaster of machine 1 controls machine 1.
  - Machine 1 and machine 2 are separated. Machine 1 continues production. The Grandmaster located in Machine 1 provides synchronization.
  - Machine 2 may be moved to a different location or just used stand alone to produce some goods. The Grandmaster in machine 2 provides synchronization for machine 2.
- Combining:
  - Grandmaster of machine 2 needs to follow the Grandmaster from machine 1.
  - Machine 2 is done with its production process and is combined with machine 1 again. Machine 1 may still be producing while machine 2 is combined with machine 1 again.

- Machine 1 is undisturbed and machine 2 is starting to use the Grandmaster from machine 1.

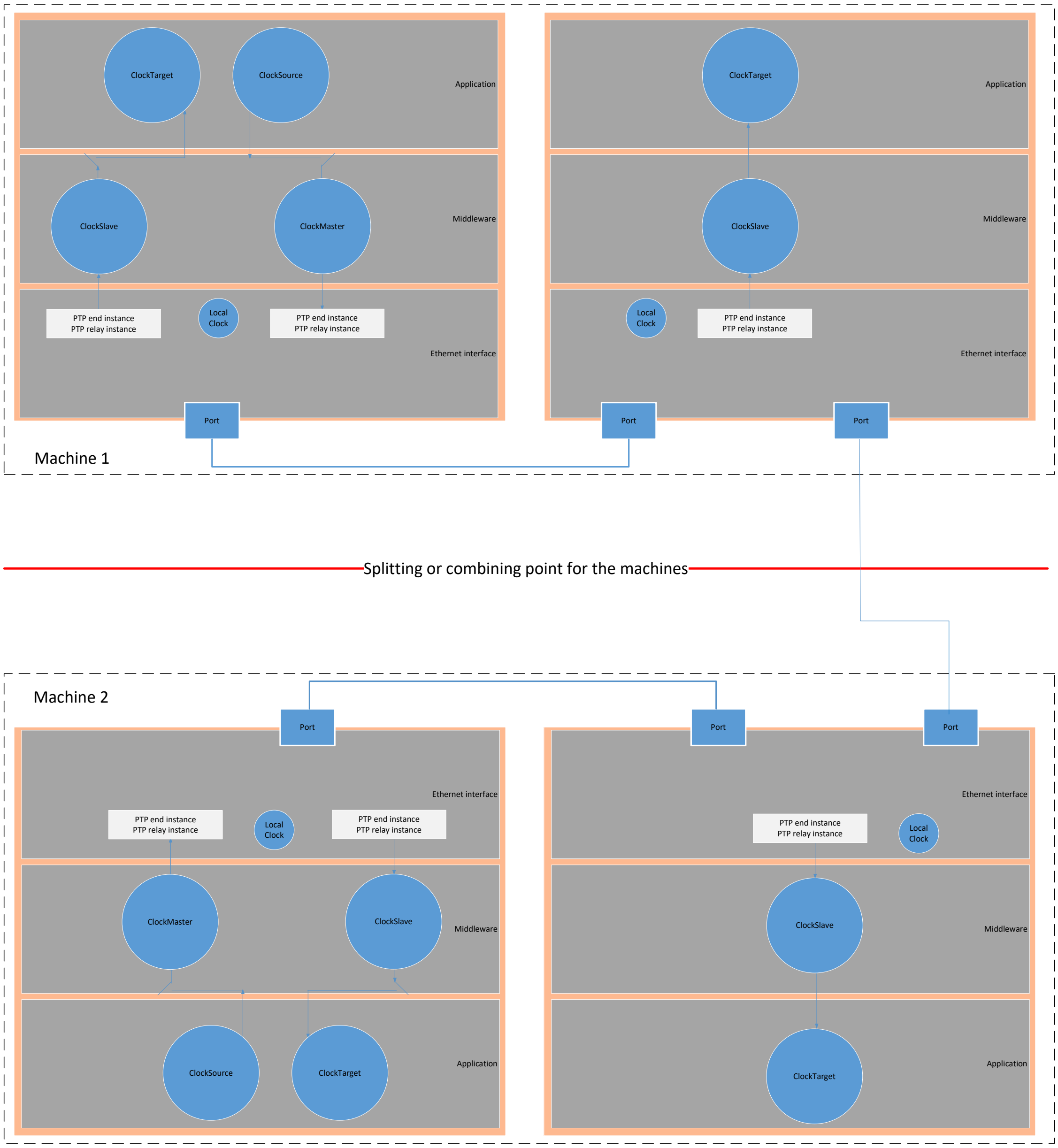


Figure 17 – Split and combine using BMCA

Figure 18 shows the split and combine use case while using Hot standby. Jumps in synchronization shall be avoided.

- Splitting:
  - Grandmaster of machine 2 controls machine 2 and Grandmaster of machine 1 controls machine 1.
  - Machine 1 and machine 2 are separated. Machine 1 continues production. The Grandmaster located in Machine 1 provides synchronization.
  - Machine 2 may be moved to a different location or just used stand alone to produce some goods. The Grandmaster in machine 2 provides synchronization for machine 2.
- Combining:
  - Grandmaster of machine 2 needs to follow the Grandmaster from machine 1.

- Machine 2 is done with its production process and is combined with machine 1 again. Machine 1 may still be producing while machine 2 is combined with machine 1 again.
- Machine 1 is undisturbed and machine 2 is starting to use the Grandmaster from machine 1.

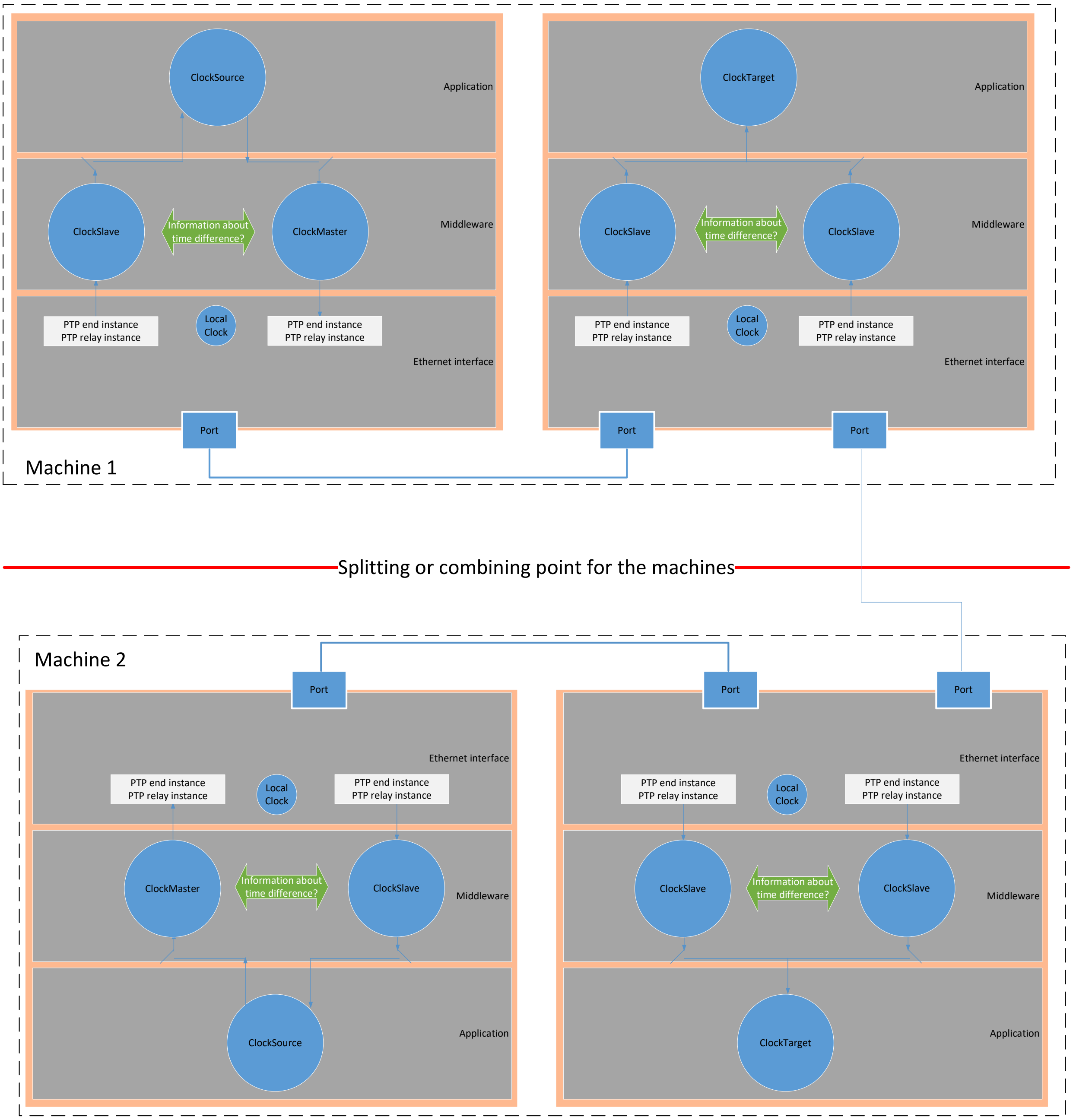


Figure 18 – Split and combine using hot standby

6.3 Security model

6.3.1 General

Subclause 6.3 specifies the security model starting with NETCONF/YANG. It describes the security functionality, the security objects in factory default state, the imprinting of Configuration

Domain-specific security objects and the secure configuration based on Configuration Domain-specific security objects.

NOTE Securing the transport of time synchronization is not covered in this document. Techniques for securing time synchronization exist; however, the user should be aware that such techniques can have performance ramifications.

6.3.2 Security functionality

6.3.2.1 Message exchange protection

6.3.2.1.1 General

Network configuration with NETCONF/YANG shall be protected by NETCONF-over-TLS according to IETF RFC 7589. NETCONF-over-SSH according to IETF RFC 6242 shall not be used. The to-be-configured IA-stations shall act in the NETCONF server role.

NOTE This document selects TLS as a secure transport for NETCONF since TLS is the better match for the case of configuration clients that rely upon unattended or automated operation. This case is dominant in industrial automation. To avoid complexity, the TSN Profile for Industrial Automation deselects SSH as a secure transport for NETCONF.

6.3.2.1.2 TLS profile

TLS shall be used for NETCONF/YANG according to the following profile:

a) TLS protocol version 1.2 according to IETF RFC 5246 shall be used with mutual authentication.

NOTE Mutual authentication includes checking the TLS client and server identity. This is described in subclauses 6.3.4 and 6.3.5 in conjunction with the IDevID and LDevID-NETCONF credentials.

b) The cipher suite TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 shall be supported. The cipher suites TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 and TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 may be supported.

c) IETF RFC 7589 implicitly mandates the cipher suite TLS_RSA_WITH_AES_128_CBC_SHA by referring to IETF RFC 5246. This cipher suite shall not be supported because it requires excessive asymmetric key lengths, it is not an Authenticated Encryption with Associated Data (AEAD) scheme, and it does not provide perfect forward secrecy.

d) Elliptic curve Curve25519 according to IETF RFC 7748 and P-256 according to NIST FIPS 186-4 Digital Signature Standard (DSS) shall be supported. Curve448 according to IETF RFC 7748 and P-521 according to NIST FIPS 186-4 Digital Signature Standard (DSS) may be supported.

e) The TLS Certificate message from the TLS client and server shall contain the self-signed root certificate. This approach allows to simplify/flatten the PKI hierarchy on base of the current TLS client certificate to NETCONF username mapping algorithm in IETF RFC 7589. Implementations shall support TLS Certificate message with at least 2 certificates objects.

f) Elliptic curve Curve25519 according to IETF RFC 7748 and P-256 according to NIST FIPS 186-4 Digital Signature Standard (DSS) shall be supported. Curve448 according to IETF RFC 7748 and P-521 according to NIST FIPS 186-4 Digital Signature Standard (DSS) may be supported.

g) TLS extensions according IETF RFC 6066 and 6961 shall not be used.

6.3.2.1.3 Certificate-to-name mapping

The certificate-to-name mapping procedure in IETF RFC 7589 shall be done as follows.

NOTE IETF RFC 7589, Clause 7, requires NETCONF servers to map client certificates to “NETCONF usernames” and specifies a concrete mapping procedure for this purpose. This mapping is represented by the YANG module ietf-x509-cert-to-name.

The list of mapping entries has a single element containing:

- fingerprint: the fingerprint of the trust anchor for the Configuration Domain
- map_type: ext-60802-roles

The mapping entry provides the assigned role names for the NETCONF client. This list is extracted from the id-60802-pe-roles certificate extension of the client’s TLS-authenticated END ENTITY certificate.

6.3.2.1.4 Role extension

The id-60802-pe-roles extension in LDevID-NETCONF END ENTITY certificates shall be constructed as follows:

a) Extension field extnID

The extnID shall provide the following OBJECT IDENTIFIER to identify the id-60802-pe-roles extension:

```
id-60802 OBJECT IDENTIFIER ::= { <tba> }

id-60802-pe OBJECT IDENTIFIER ::= { id-60802  1 }

id-60802-pe-roles OBJECT IDENTIFIER ::= { id-60802-pe  1 }
```

b) Extension field critical

The id-60802-pe-roles extension shall not be marked as critical (critical:= FALSE).

c) Extension field extnValue

```
60802RoleNamesSyntax ::= SEQUENCE SIZE (1..MAX) OF 60802RoleName

60802RoleName  ::= ENUMERATED {
                    TruststoreAdminRole (0),
                    KeystoreAdminRole (1),
                    UserMappingAdminRole (2)}
```

NOTE The extnValue provides an OCTET STRING that contains the DER-encoded 60802RoleNamesSyntax value. The output of the certificate-to-name mapping is the list of UTF8String values inside this OCTET STRING. This list of assigned role names represents the input for checking access permissions with NACM.

6.3.2.2 Resource access authorization

Access control to NETCONF/YANG resources shall be protected by NACM according to IETF RFC 8341.

NACM specifies a YANG data model (ietf-netconf-acm) for expressing rules to control access to NETCONF/YANG resources. This document profiles NACM to deliver an RBAC model.

NOTE 1 NACM does not natively deliver a role-based access control model but can be geared towards a role-based model by profiling.

This role-based model for security resources shall be applied as follows:

– The set of NETCONF/YANG resources of an IA-station is partitioned according to its YANG modules. This document specifies a permission-to-role assignment for the following YANG modules.

NOTE 2 NACM recognizes following “access-operations": create, read, update, delete, exec and uses the term write access for the access operations "create", "delete", and "update". This document uses the terms read, write and exec access.

- YANG module ietf-truststore, truststore container:
  - – Read access: Authenticated entities
  - – Write access (Configuration Domain-specific trust anchors): Authenticated entities with TruststoreAdminRole
  - – Write access (IDevID trust anchor): not allowed
  - – Exec access: n.a.
- YANG module ietf-keystore, keystore container:

  - Read access (private keys): not allowed
  - Read access (END ENTITY and intermediate certificates): Authenticated entities
  - Write access (Configuration Domain-specific credentials): Authenticated entities with KeystoreAdminRole
  - Write access (IDevID credential): not allowed
  - Exec access: Authenticated entities with KeystoreAdminRole
- YANG module ietf-x509-cert-to-name, x509c2n container:
  - Read access: Authenticated entities
  - Write access: Authenticated entities with UserMappingAdminRole
  - Exec access: n.a.
- YANG module ietf-netconf-acm, nacm container:
  - Read access: Authenticated entities
  - Write access: not allowed
  - Exec access: n.a.

This document does not specify the assignment of role names to actual system entities. This is a duty of system owners or operators.

Editor's note: Elaboration on resource access authorization for further YANG modules is deferred to a later version. This also concerns the behaviour of authorization during the life cycle of IA-station.

6.3.3 IDevID Profile

6.3.3.1 General

IA-stations shall possess IDevID credentials according to the profile in 6.3. CNCs shall contain trust anchors for validating IDevID credentials.

6.3.3.2 Object Contents

6.3.3.2.1 General

The IDevID credential contents shall comply to IEEE Std 802.1AR and the profile in 6.3.

6.3.3.2.2 IA-Station Identity

Any IDevID EE certificate of an IA-station shall take one of the following forms:

- raw form: the IDevID EE certificate complies to IEEE Std 802.1AR
- extended form: the IDevID EE certificate complies to IEEE Std 802.1AR and the requirements provided in 6.3

The extended form of an IDevID EE certificate shall be constructed as follows:

- the verifiable device identity shall appear as a URN in a GeneralName of type uniformResourceIdentifier in the subjectAltName extension
- the URN value shall be constructed according to IETF RFC 8141 and as follows:
  - namespace identifier: ieee (see IETF RFC 8069)
  - namespace-specific string: iec-ieee-60802#verifiable-device-identity
  - q-component (see IETF RFC 8141, 2.3.2) to parameterize the named resource: an ampersand-separated list of keyword=value tuples with following keywords and values. These tuples can appear in any order inside the q-component.
    - The keywords: description, hardware-rev, serial-num, mfg-name, model-name.

- Their corresponding values from the single ‘component’ list entry in the ietf-hardware YANG module that represents the management entity of the IA-station respectively from its pre-material form in percent-encoding (see IETF RFC 3986).

NOTE 1 These are the items with the YANG property config-false from the ‘component’ list entry that represents the management entity of the IA-station. The config-false items firmware-rev and software-rev are excluded to avoid IDevID credential updates in case of FW or SW updates.

NOTE 2 An object looks like urn:ieee:iec-ieee-60802#verifiable-device-identity?=mfg-name=<mfg-name>&model-name=<model-name>&hardware-rev=<hardware-rev>&serial-num=<serial-num>&description=<description>

NOTE 3 One IDevID EE certificate can have one subjectAltName extension which can have one or more GeneralName entries. In particular: there can be one or more GeneralName entries of type uniformResourceIdentifier. This allows other organizations e.g., middleware and application consortia or individual manufacturers to also represent their perception of verifiable device identity in addition to the perception of this document.

6.3.3.2.3 Signature Suites

An IDevID shall utilize the following signature suite:

– ECDSA P-256/SHA-256 according to IEEE Std 802.1AR-2018, 9.2

An IDevID may utilize the following signature suites:

- ECDSA P-521/SHA-512 according to NIST FIPS 186-5/180-4 and using the algorithm identifiers according to IETF RFC 5480
- EdDSA instance Ed25519 according to IETF RFC 8032 using Curve25519 according to IETF RFC 7748 and using the algorithm identifiers according to IETF RFC 8410
- EdDSA instance Ed448 according to IETF RFC 8032 using Curve448 according to IETF RFC 7748 and using the algorithm identifiers according to IETF RFC 8410

6.3.3.3 Information Model

6.3.3.3.1 General

The information model for IDevID credentials and trust anchors shall comply to YANG and NMDA, in particular the YANG modules ietf-keystore and ietf-truststore, as well as the profile in 6.3.3.3.

6.3.3.3.2 Entries

IDevID credentials shall be provided in form of built-in keys of an IA-station by its manufacturer. In YANG, they are modeled as config-false nodes and are represented in the ‘keystore’ container that is instantiated by the YANG module ietf-keystore. The private key shall use the private-key-type choice hidden-private-key i.e., the IDevID private key is not presented in NETCONF/YANG. The details of storing and protecting IDevID private keys as well as using them for signing purposes are implementation-specific.

Trust anchors for IDevID credentials are CNC user-configured data objects: these objects shall be available as applied configuration (IETF RFC 8342) upon CNCs. In YANG, they are modeled as config-true nodes and are represented in the ‘truststore’ container that is instantiated by the YANG module ietf-truststore.

NOTE IA-station built-in trust anchors for use cases such as FW/SW update are out-of-scope in IEC/IEEE 60802.

6.3.3.3.3 Entry Manifoldness

An IA-station shall possess one IDevID credential with a certification path plus trust anchor information issued under the required signature suite according to 6.3.3.2.3 as part of its factory default state.

If an IA-station supports an optional signature suite according to 6.3.3.2.3, it shall possess in addition one IDevID credential with a certification path plus trust anchor information issued under the optional signature suite as part of its factory default state.

An IA-station may have additional IDevID credential(s) with a certification path plus trust anchor information issued under a combination of any required or any supported optional DevID signature suites.

If an IA-station possesses multiple IDevID credentials, then they shall be issued by the same organization (the IA-station manufacturer). Their EE certificates shall contain the same device identity information.

A CNC shall support at least one trust anchor for IDevID credentials per supported IA-station manufacturer.

6.3.3.3.4 Entry Naming

IDevID credentials shall be present in an 'asymmetric-key' entry that is identified as follows:

- /ietf-keystore:keystore/asymmetric-keys/asymmetric-key/name= IDevID-<SignatureSuiteName>-<CertificateSerialNumberOfEECertificate>
- IDevID trust anchors shall be present in 'certificate' entries that are identified as follows:
- /ietf-truststore:truststore/certificate-bags/certificate-bag/certificate/name= IDevID-<SignatureSuiteName>-<CertificateSerialNumberOfCACertificate>
- Such entries shall be present underneath a 'certificate-bag' entry that is identified as follows.
- /ietf-truststore:truststore/certificate-bags/certificate-bag/name=IDevID

6.3.3.4 Processing Model

6.3.3.4.1 General

The processing model for IDevID credentials and trust anchors shall comply to IEEE Std 802.1AR as well as the profile in 6.3.

6.3.3.4.2 Credentials

6.3.3.4.2.1 General

IDevID credentials are used in following use cases:

- NETCONF/YANG security setup from factory default; the number of such events scales with the number of factory resets i.e., this use case is performed sporadically. It is conducted by CNCs and encompasses a device identity verification.
- Device identity verification happens as a subtask during NETCONF/YANG security setup from factory default. It may also happen additionally according to CNC user discretion. The details of device identity verification are also subject to given policy.

In these use cases, IA-stations act in claimant role and CNCs act in verifier role:

- IA-stations shall present the certification path of and prove private key possession for an IDevID credential.
- CNCs shall validate the certification path, check the proof-of-possession for the private key, and verify the obtained device identity information.

6.3.3.4.2.2 Creation

IA-station manufacturers select the form factor for representing verifiable device identity in IDevID credentials: raw or extended form. The details of the IDevID credential issuance process are manufacturer-specific and out-of-scope for this document.

IA-station manufacturers are not required to offer an update feature for IDevID credentials.

6.3.3.4.2.3 Distribution

IA-stations shall supply IDevID credentials in form of built-in keys, see 6.3.3.3.

6.3.3.4.2.4 Use

Verifiers (CNCs) shall perform the following checks when they challenge claimants (IA-stations) to authenticate themselves by means of an IDevID credential.

- IDevID certification path validation according to IETF RFC 5280. Whether this validation happens with or without revocation checks is at the discretion of the CNC user.

  - It is the responsibility of the CNC user to supply a trust anchor configuration (set of trusted certificates or trusted public keys), a revocation check instruction (Boolean) and optionally CRL objects to CNCs.

NOTE 1 The certification path validation is passed if and only if the IDevID EE certificate is the leaf of a valid certification path that ends with a CA certificate which is signed by a configured trust anchor and which is not revoked (if revocation check is enabled).

- Proof-of-possession checking for the private key according to IETF RFC 7589 and 5246.

NOTE 2 The proof-of-possession check is passed if and only if the IA-station possesses the private key which matches the public key in the IDevID EE certificate.

- Device identity verification:
  - It is the responsibility of the CNC user to establish and supply to CNCs: a device identity verification policy which determines the verifiable device identity subset that shall be checked by the CNC for the IA-stations in a configuration domain. This is a subset of {description, hardware-rev, serial-num, mfg-name, model-name}. The empty subset (“no-identity-check”) as well as the whole set are allowed.
  - The device identity verification for an IA-station instance shall behave as follows:
    - If this subset is empty, then the device identity check is passed.
    - If this subset is non-empty, then the CNC performs following expected vs. actual check for each verifiable device identity item in this subset:
      - The check for any item in this subset is passed if the expected value (from ietf-hardware YANG module) matches the actual value (from the verifiable device identity URN value for this document in the subjectAltName extension of the IDevID EE certificate).

NOTE 3 This check fails if the IDevID has raw form.

      - The device identity check is passed if it is passed for all items in the subset.

IDevIDs in raw form (without verifiable device identity URN) may be used if the device identity verification setting option “no-identity-check” is employed. This allows to perform the NETCONF/YANG security setup from factory default for IA-stations with IDevID credentials in raw form. From CNC perspective these IA-stations remain anonymous.

NOTE 4 This document does not specify a mechanism for device identity verification for IDevIDs in raw form. Whether and how device identity checks for such IA-stations are done in an offline mode is at the discretion of CNC users.

6.3.3.4.2.5 Storage

IDevID credentials shall be stored persistently upon an IA-station. The details for implementing this persisted storage are IA-station manufacturer-specific and out-of-scope of this document.

6.3.3.4.2.6 Revocation

It is the responsibility of IA-station manufacturers to report revocation for the IDevID credentials issued by them in form of X.509 CRL objects. These objects are made available in a form that allows relying parties i.e., CNC users to retrieve them at their own discretion.

CNC users decide whether they support IDevID certification path validation with or without revocation:

- if revocation checks are disabled, then certificate path validation shall be performed according to IETF RFC 5280, 6.1 Basic Path Validation
- if revocation checks are enabled, then certificate path validation shall be performed according to IETF RFC 5280, 6.1 Basic Path Validation and 6.3 CRL Validation

NOTE It is the responsibility of CNC users to obtain up-to-date X.509 CRL objects from manufactures and make them locally available for verifiers.

6.3.3.4.3 Trust Anchors

6.3.3.4.3.1 General

Trust anchors are input arguments for certification path validation according to IETF RFC 5280, 6.1.1 input argument (d). Relying parties decide about these input arguments in a discretionary fashion i.e., these objects are not created and distributed as literal trust anchor objects but in a pre-material form of self-signed certificate objects.

NOTE The digital signature in self-signed certificates do not vouch for authenticity of this object: Actor X can issue self-signed certificates featuring the name of actor A that cannot be distinguished from self-signed certificates issued by A. Out-of-band mechanisms are needed to verify the authenticity of self-signed certificates.

The trust anchors for use cases where IA-stations act in claimant role are determined by CNC users.

6.3.3.4.3.2 Creation

The details of the issuance and update processes for self-signed root certificates for validation of IDevID credentials are out-of-scope for this document.

6.3.3.4.3.3 Distribution

With respect to use cases where IA-stations act in claimant role e.g., NETCONF/YANG security setup and device identity verification the following model applies:

- issuers (IA-station manufacturers) create and distribute self-signed root certificates. Issuers also provide out-of-band means that allow relying parties to check the authenticity of these objects.
- relying parties (CNC users) check the authenticity of self-signed root certificates by out-of-band means and decide about their acceptance as trust anchors for certification path validation in a discretional manner and configure their verifiers (CNCs) accordingly.

Specifying details of out-of-band distribution and validation of self-signed root certificates is out-of-scope for this document.

6.3.3.4.3.4 Use

Trust anchors for IDevID credentials are used for certification path validation according to IETF RFC 5280. This concerns CNCs with respect to the use cases NETCONF/YANG security setup from factory default, device identity verification.

6.3.3.4.3.5 Storage

Trust anchors for IDevID credentials shall be stored persistently upon CNCs. The details for implementing this persisted storage are out-of-scope for this document.

6.3.3.4.3.6 Revocation

IA-station manufacturers are not required to support an authority revocation feature for IDevID credential certification authorities.

6.3.4 Security setup based on IDevID

6.3.4.1 General

IA-stations in factory default state shall conduct a security setup sequence for the Configuration Domain. This sequence consists of the following steps, each step described in 6.3.4:

- imprintTrustAnchor: imprint of a Configuration Domain specific trust anchor to an IA-station that allows to validate LDevID-NETCONF certificates presented by communication partners.
- imprintCredential: imprint of a Configuration Domain specific credential to an IA-station, i.e., a private key and the corresponding X.509v3 end entity certificate (plus intermediate CA certificates, if applicable) plus self-signed root CA certificate that serves as own LDevID-NETCONF credential.
- imprintCertToNameMapping: imprint a Configuration Domain specific certificate-to-name mapping to an IA-station

6.3.4.2 imprintTrustAnchor

IA-stations in factory default state shall expect the imprinting of a single Configuration Domain specific trust anchor via NETCONF-over-TLS according to a procedure called “provisional accept of client certificate", which uses an IDevID credential on NETCONF and TLS server side and a LDevID-NETCONF credential on NETCONF and TLS client side and operates as follows at the NETCONF and TLS server:

a) Challenge the client for TLS client authentication according to IETF RFC 7589 by sending a CertificateRequest message according to IETF RFC 5246 with an empty certificate_authorities entry.
b) Perform certification path validation according to IETF RFC 5280 for the contents of the client's Certificate message. This certification path validation fails due to a missing trust anchor for the LDevID-NETCONF credential.
c) Provisionally accept the failing certification path validation when the reason is "no matching trust anchor" (and only this reason) and proceed with the TLS exchange.
d) Expect the client to send a trust anchor for LDevID-NETCONF over the provisionally accepted TLS session (no other object type).
e) If the trust anchor in the NETCONF application payload was accepted, then redo the priorly failing certification path validation using this trust anchor, see step b).
f) If this certification path revalidation is successful, then keep the TLS session alive and send an <rpc-reply> with success. The client then is expected to perform the NETCONF exchanges for imprintCredential (described in 6.3.4.3) and for imprintCertToNameMapping (described in 6.3.4.4) via the already established TLS session.
g) If this certification path revalidation is not successful, then terminate the TLS session. The usual NETCONF/YANG hygiene applies. This is expected to remove the entry in the ietf-truststore that was created in step d).

NOTE This "provisional accept of client certificate" is a mirrored version of the "provisional accept of server cert" in IETF RFC 8995.

The "provisional accept of client cert" in factory default state shall skip the certificate-to-name mapping and shall use the NACM recovery session, i.e., skip permission checking. In this model all authenticated clients are accepted as authorized for doing the first imprinting of the LDevID-NETCONF credential and the corresponding trust anchor. Only contextual checks such as "once only when being in factory default state" are feasible. This model is also known as "trust on first use" (TOFU).

The imprinting NETCONF client should check the actual server identity that is stated by the IA-station on TLS level by matching against:

- End entity certificate contents:
  - A list of accepted (or blocked) manufacturers.
- A list of accepted (or blocked) product instances by their product serial number per accepted manufacturer.
- End entity certificate object as a whole: a list of pinned certificates.

Details of how this matching happens depend on the implementation of the client that performs this imprinting.

The LDevID-NETCONF trust anchor certificate shall be imprinted using the truststore container of the ietf-truststore module with:

- /ts:truststore/ts:certificate-bags/ts:certificate-bag/ts:name = IEC60802,
- /ts:truststore/ts:certificate-bags/ts:certificate-bag/[ts:name=IEC60802]/
- ts:certificate/ts:name = IEC60802-LDevID
- ts:certificate/ts:cert-data containing the IEC60802-LDevID trust anchor certificate data object of type trust-anchor-cert-cms according to ietf-crypto-types, i.e., enveloped in Base64-encoded CMS SignedData in degenerated form "certs-only" (no signature value).

Editor's note: Contribution on generalizing the security list entry naming scheme is welcome.

- The imprintTrustAnchor step shall use the NETCONF operation <edit-config> according to IETF RFC 6241 for the truststore container. The NETCONF operation <commit> shall not yet be applied, but rather after successful completion of all security setup sequence steps.

6.3.4.3 imprintCredential

6.3.4.3.1 General

The LDevID-NETCONF end entity certificate shall be provided as X.509v3 public key certificate according to IETF RFC 5280 with the following criteria:

- Contains the FQDN of the NETCONF server in its subjectAltName extension according to IETF RFC 7589 and IETF RFC 6125
- Contains an ECDSA public key and shall be signed with ECDSA according to the selected cryptographic algorithm
- Contains a digitalSignature in its keyUsage extension
- Has a finite validity period

NOTE The actual length of the validity period is at the discretion of the user of the Configuration Domain.

Dependent on the key generation capabilities, different steps are applied to this keystore container.

6.3.4.3.2 Internal key generation

For IA-station with internal key generation capabilities, two NETCONF exchanges are performed. Processing steps for the first NETCONF exchange shall be applied as follows at the NETCONF server:

a) Receive and process the NETCONF request message with action <generate-csr> and input values
   - /ks:keystore/ks:asymmetric-keys/ks:asymmetric-key/[ks:name=LDevID_NETCONF]/ks:generate-csr/ks:input/ks:csr-format containing identity p10-csr according to ietf-crypto-types
   - /ks:keystore/ks:asymmetric-keys/ks:asymmetric-key/[ks:name=LDevID_NETCONF]/ks:generate-csr/ks:input/ks:csr-info containing a Base64-encoded PKCS#10 CertificationRequestInfo according to IETF RFC 2986.
b) Base64-decode the <csr-info> value and parse it as a PKCS#10 CertificationRequestInfo object.
c) Extract the algorithm information from the child element SubjectPublicKeyInfo of CertificationRequestInfo and randomly generate a key pair for the specified algorithm.
d) Internally store the private key together with its metadata for example, algorithm information, <name> value in a secure manner.
e) Put the public key into the (parsed) PKCS#10 CertificationRequestInfo.
f) Serialize the PKCS#10 CertificationRequestInfo (including the public key).
g) Use the private key to create signature value for the (serialized) PKCS#10 CertificationRequestInfo (including the public key).
h) Create a NETCONF reply message with /ks:keystore/ks:asymmetric-keys/ks:asymmetric-key/[ks:name=LDevID-NETCONF]/ks:generate-csr/ks:output/ks:p10-csr containing the data object of the previous step.

In the second NETCONF exchange, the LDevID-NETCONF end entity certificate (plus intermediate CA certificates) shall be imprinted using the keystore container of the ietf-keystore module with:

- /ks:keystore/ks:asymmetric-keys/ks:asymmetric-key/ks:name = LDevID-NETCONF

- /ks:keystore/ks:asymmetric-keys/ks:asymmetric-key/[ks:name=LDevID-NETCONF]/
- ks:certificates/ks:certificate/ks:name = LDevID-NETCONF
- ks:certificates/ks:certificate/ks:cert-data containing the certificate chain LDevID-NETCONF end entity certificate (plus intermediate CA certificates, if applicable) plus self-signed root CA certificate as data object of type end-entity-cert-cms according to ietf-crypto-types

The imprintCredential step shall use the NETCONF operation <edit-config> according to IETF RFC 6241 for the keystore container. The NETCONF operation <commit> shall not yet be applied, but rather after successful completion of all security setup sequence steps.

6.3.4.3.3 External key generation

For IA-stations without internal key generation capability, external key generation may be used. For external key generation, one NETCONF exchange is performed.

The LDevID-NETCONF private key and end entity certificate (plus intermediate CA certificates) shall be imprinted using the keystore container of the ietf-keystore module with:

- /ks:keystore/ks:asymmetric-keys/ks:asymmetric-key/ks:name = LDevID-NETCONF
- /ks:keystore/ks:asymmetric-keys/ks:asymmetric-key/[ks:name=LDevID-NETCONF]/
- ks:certificates/ks:certificate/ks:name = LDevID-NETCONF
- ks:certificates/ks:certificate/ks:public-key-format describing the encoding of the public key of the selected cryptographic algorithm according to ietf-crypto-types
- ks:certificates/ks:certificate/ks:public-key containing the public key value in the selected public-key-format
- ks:certificates/ks:certificate/ks:private-key-format describing the encoding of the private key of the selected cryptographic algorithm according to ietf-crypto-types
- ks:certificates/ks:certificate/ks:cleartext-private-key containing the private key value in the selected private-key-format

NOTE The option <cleartext-private-key> was picked to make the first description as simple as possible. This is not meant as the recommended or preferred form.

- ks:certificates/ks:certificate/ks:name = LDevID-NETCONF
- ks:certificates/ks:certificate/ks:cert-data containing the certificate chain LDevID-NETCONF end entity certificate (plus intermediate CA certificates, if applicable) plus self-signed root CA certificate as data object of type end-entity-cert-cms according to ietf-crypto-types

The imprintCredential step shall use the NETCONF operation <edit-config> according to IETF RFC 6241 for the keystore container. The NETCONF operation <commit> shall not yet be applied, but rather after successful completion of all security setup sequence steps.

External key generation can introduce security vulnerabilities during the generation and loading process. Ensuring those processes are secure is the responsibility of the user and outside the scope of this document.

6.3.4.4 imprintCertToNameMapping

The Configuration Domain specific certificate-to-name mapping shall be imprinted using the x509c2n container in the ietf-x509-cert-to-name module with:

- x509c2n:cert-to-name/
- id = 1
- x509c2n:tls-fingerprint containing the Configuration Domain specific fingerprint of the LDevID-NETCONF trust anchor
- x509c2n:map-type <xmlns=" urn:ieee:std:60802:security”> = ext-60802-roles

NOTE The application of this map-type is described in 6.3.4.2, steps e) and f).

The imprintCertToNameMapping step shall use the NETCONF operation <edit-config> according to IETF RFC 6241 for the x509c2n container. Afterwards the NETCONF operation <commit> shall be applied to finalize the security setup sequence steps and to leave the factory default state.

6.3.5 Secure configuration based on LDevID-NETCONF

Configuration by NETCONF/YANG is protected by NETCONF-over-TLS as described in 6.3.2.1 and NACM as described in 6.3.2.2. The NETCONF/YANG servers and clients shall use LDevID-NETCONF credentials for authentication.

The procedure called “provisional accept of client certificate” as described in 6.3.4.2 shall not be applied anymore if the IA-station has left the factory default state. Instead, after successful establishment of a TLS session according to IETF RFC 7589, the NETCONF server shall perform a certificate-to-name mapping and authorization check as follows:

a) Compare the fingerprint of the trust anchor of the NETCONF client’s certification path with the fingerprint contained in cert-to-name list entries of the x509c2n container for equal values.

b) If no cert-name list entry match is found, then terminate the TLS session.

c) If a cert-to-name list entry match is found, then verify if the map-type is equal to ext-60802-roles.

d) If the map-type does not match, then terminate the TLS session.

e) If the map-type value matches, then extract the role values from the id-60802-pe-roles certificate extension of the NETCONF client’s TLS-authenticated end entity certificate. The output is a list of string values from the enumeration of defined role names according to this document.

f) The list of role name string values is provided as input to NACM for permission checking. The access to the requested resource is checked according to the rules configured in the nacm container of the ietf-netconf-acm YANG module.

The NETCONF client checks if the expected identity to address the NETCONF server (IP address or DNS name) matches to the actual server identity that is stated by the IA-station on TLS level. This shall be done by comparing the expected identity with the subjectAltName extension of the TLS authenticated LDevID-NETCONF end entity server certificate.

6.4 Bridge delay Requirements

Editor’s note: Contribution requested.

6.5 Bridge FDB requirements

The For IA time-aware streams, IA streams, and IA traffic engineered non-streams, the FDB shall be configured as follows:

a) Learning disabled.

b) Independent VLAN Learning enabled.

c) Default forwarding rule is drop.

For IA non-streams, the FDB shall be configured as follows:

a) Learning enabled.

b) Shared VLAN learning enabled.

c) Default forwarding rule is flooding.

NOTE Configuration of the FDB is the responsibility of the user.

6.6 Bridge reporting requirements

This clause will identify the parameters which bridge, and end station vendors are required to report. These values will be included in the PCS Proforma and therefore used for conformance testing. Specific guidance regarding values for these parameters will be provided in an informative annex.

A contribution identifying these parameters and providing the guidance for these parameters is forthcoming.

6.7 Management

Editor's note: IEEE802.1Q Clause 12.1 should be reviewed to ensure this clause is consistent with management requirements for bridges.

6.7.1 General

Subclause 6.7 describes a model for configuration, deployment, and management of an industrial automation network.

Editor's note: Some of the mechanisms described in the clause may be generic to TSN configuration and more appropriately dealt with in the P802.1Qdj PAR or a separate project.

6.7.2 IA-station management model

6.7.2.1 General

The management model of IA-stations covers simple end station IA-stations as well as combined IA-stations as described in 4.3. The IA-station management model is applied for topology discovery, network provisioning and stream establishment.

6.7.2.2 IEEE 802.1Q management model

In industrial automation both Bridge and end station components make use of IEEE 802.1Q defined functionality (for example, traffic classes, gate control). Thus, the IEEE 802.1Q management model is the basic management model to be applied to all IA-stations. Figure 19 shows the implementation of the IEEE Std 802.1Q Bridge model in YANG as specified in IEEE Std 802.1Qcp-2018. The IETF Interface Management YANG model is specified in IETF RFC 8343.

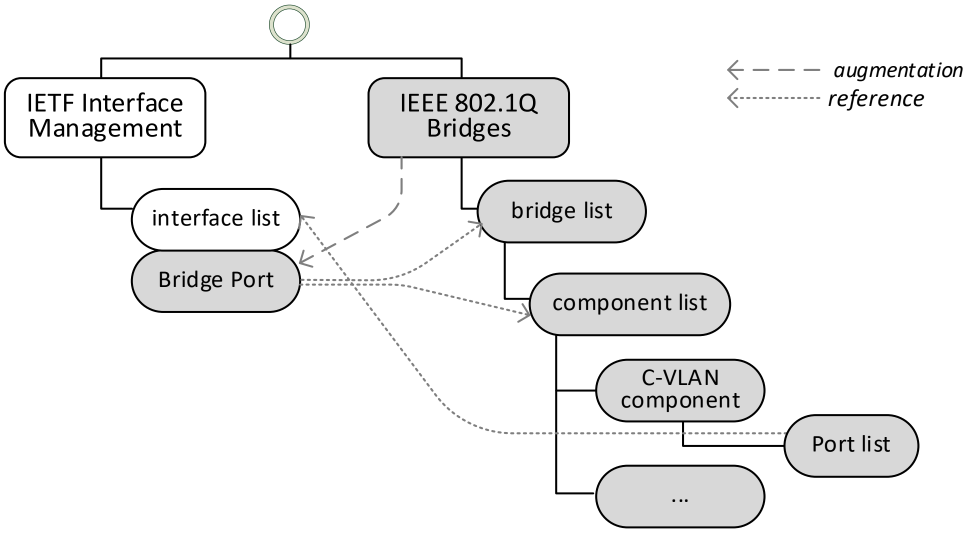


Figure 19 – Generic IEEE 802.1Q YANG Bridge management model

The IEEE 802.1Q Bridge model is organized as a bridge list where each bridge includes an underlying component list (for example, C-VLAN components). Each component has a Port list attached with references to the representation of the ports in the IETF interface list. The managed data of the ports is defined as Bridge Port augmentation to the IETF interface model. Each Bridge Port includes a reference to its bridge and component instances in the IEEE 802.1Q Bridge model.

This YANG model is applied to IA-stations:

- Each functional unit of an IA-station is modeled as bridge entry in the bridge list.
- Each Bridge and end station component of an IA-station is modeled as C-VLAN component.
- The IA-station components belonging to a common functional unit are added to the component list of this functional unit's bridge entry.
- Each IA-station external or internal port is modeled as Bridge Port.

The IA-station ports belonging to a common component are added to the Port list of the related component list entry.

Further YANG models which are relevant for IA-stations are described in 6.7.9.

6.7.2.3 Internal LAN connection model

The modeling of internal connections between C-VLAN components within an IA-station is aligned to IEEE Std 802.1Q, 17.3.2.2. Figure 20 shows the usage of this model with an additional I-LAN IETF interface object together with appropriate `higher-layer-if` and `lower-layer-if` reference objects to describe the internal connection.

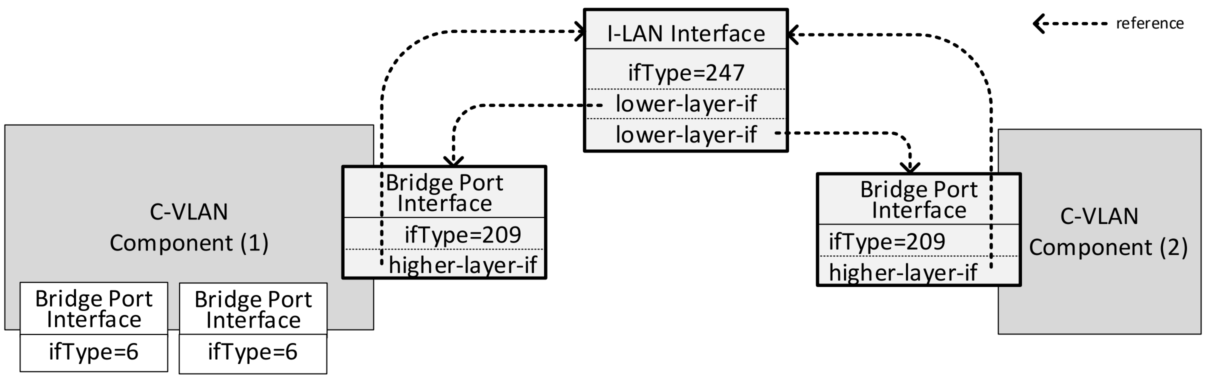


Figure 20 – Internal LAN connection management model

This internal LAN connection model comprises three configuration steps:

- The internal Ports of the C-VLAN components are modeled as IETF interfaces of type bridge with Bridge Port augmentation.
- An additional I-LAN IETF interface of type ilan is created.
- The I-LAN interface references the internal Bridge Port interfaces of the connected C-VLAN components as lower-layer-if, and
- the internal Bridge Port interfaces of the connected C-VLAN components reference the I-LAN interface as higher-layer-if.

Figure 21 shows the application of this model to the example IA-station of Figure 20.

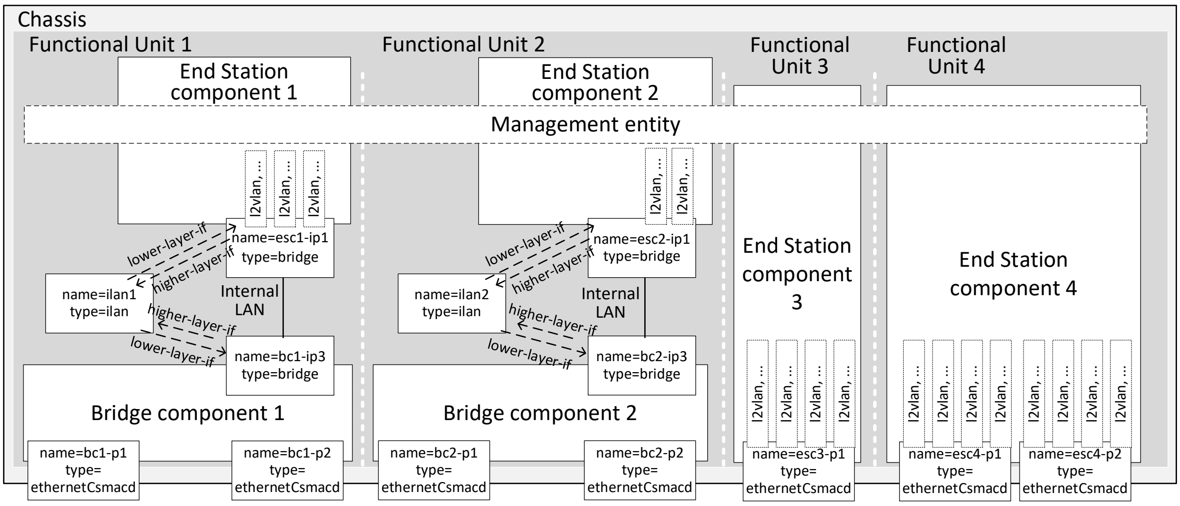


Figure 21 – IA-station example with IETF interfaces

NOTE Figure 21 represents an abstract model and is not intended to imply a particular implementation or partitioning

Figure 21 also shows the IETF Interfaces of type l2vlan which allow late binding of IA-station applications to the configured VLANs and priorities. The l2vlan interfaces of end station components are described in 6.7.2.5.

6.7.2.4 Spanning Tree, VLAN and TE-MSTID configuration

C-VLAN C-VLAN Bridge components of IA-stations shall support:

- the Common and Internal Spanning Tree (CIST) calculated by the Multiple Spanning Tree Algorithm and Protocol (MSTP), and
- the Traffic Engineering Multiple Spanning Tree Instance Identifier (TE-MSTID) as specified in IEEE Std 802.1Q-2022, 5.5.2.

The MSTP configuration is either default or accomplished by IA-station specific means.

Editor's note: There is no MSTP YANG available yet.

CNCs configure VLANs in the vlan list in the bridge-vlan container of the ieee802-dot1q-bridge YANG module. Ports are assigned to a vlan as static-filtering-entries in a filtering-database.

NOTE vlan, in lowercase, refers to a YANG element.

VLANs are assigned to filtering databases in the vid-to-fid list of the bridge-vlan container. The filtering databases, and in consequence the VLANs, are by default assigned to the MSTP calculated Internal Spanning Tree and may be assigned to the TE-MSTID by management.

TE-MSTID assignment is accomplished via the bridge-mst container of the ieee802-dot1q-bridge YANG module.

The configured VLAN names shall conform to the scheme defined in 6.7.2.4 to support the required translations for VLAN-ID and PCP values as described in 4.3 and 6.7.2.5. The length of a VLAN name is restricted to a maximum of 32 characters so that a compact name scheme is selected:

VLAN name	60802-[<TrafficTypeCode><PCP>]{1,6}-<VID>[R]

- <TrafficTypeCode> values are described in the Traffic type code column of Table 7.
- <PCP> values are in the range of [0..7].
- <VID> values are in the range of [1..4094].
- There may be 1 to 6 [<TrafficTypeCode><PCP>] tuples in a VLAN name.
- VLANs with the optional [R] suffix represent VLANs which are used for redundant stream transmission. The VLAN which is associated to a redundant VLAN is identified by the VLAN name without the [R] suffix, with identical <TrafficTypeCode><PCP> tuple values.

VLAN name examples:

– 60802-H7-101	– VID 101 is used for isochronous traffic, which is mapped to PCP 7.
– 60802-H7-102R	– VID 102 is used for the redundant traffic of VID 101.
– 60802-A0B1-100	– VID 100 is used for best effort low traffic applying PCP 0, and best effort high traffic applying PCP 1.

The following example shows the VID/FID/MSTID configuration of an IA-station’s C-VLAN bridge component, which supports three VLANs in three Forwarding Databases (VID 100 in FID 1, VID 101 in FID 2 and VID 102 in FID 3). FID 2 and FID 3 – and in consequence VID 101 and VID 102 - are assigned to the TE-MSTID. FID 1 – and in consequence VID 100 - is not assigned to a MSTID and thus, is implicitly assigned to the Internal Spanning Tree (IST).

Figure 22 shows the representation of this example configuration in the MST Configuration Table)

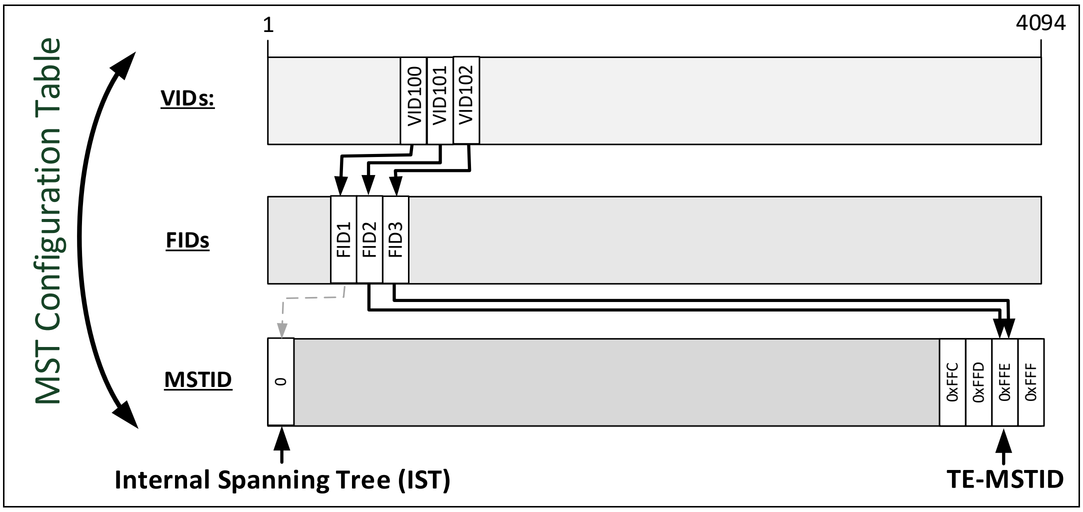


Figure 22 – VID/FID/MSTID example

The YANG-based configuration of this example is shown as YANG instance data snippet of the ieee802-dot1q-bridge YANG module. Herein the MST configuration table is included in component “bridge-component-x”, which is part of bridge “functional-unit-x”.

```
<ieee802-dot1q-bridge xmlns="urn:ietf:params:xml:ns:yang:ieee802-dot1q-bridge">
    <bridges>
        <bridge> <!-- list -->
            <name>functional-unit-x</name>
            ...
```

```
            <component> <!-- list -->
                <name>bridge-component-x</name>
                ...
                <bridge-vlan>
                    <version>2</version> <!-- MST supported -->
                    ...
                    <vlan>
                      <vid>100</vid>
                      <name>60802-A0B1-100</name> <!-- best effor high and low -->
                    </vlan>
                    <vlan>
                      <vid>101</vid>
                      <name>60802-H7-101</name> <!-- isochronous -->
                    </vlan>
                    <vlan>
                      <vid>102</vid>
                      <name>60802-H7-102R</name> <!-- isochronous -->
                    </vlan>
                    ...
                    <vid-to-fid>
                        <vid>100</vid>
                        <fid>1</fid>
                    </vid-to-fid>
                    <vid-to-fid>
                        <vid>101</vid>
                        <fid>2</fid>
                    </vid-to-fid>
                    <vid-to-fid>
                        <vid>102</vid>
                        <fid>3</fid>
                    </vid-to-fid>
                </bridge-vlan>
                ...
                <bridge-mst>
                    ...
                    <fid-to-mstid>  <!-- list -->
                        <!-- fid 1 is implicitly assigned to mstid 0 -->
                        <fid>2</fid>
                        <mstid>4094</mstid>  <!-- TE-MSTID -->
                    </fid-to-mstid>
                    <fid-to-mstid>  <!-- list -->
                        <fid>3</fid>
                        <mstid>4094</mstid>  <!-- TE-MSTID -->
                    </fid-to-mstid>
                </bridge-mst>
                ...
            </component>
        </bridge>
    </bridges>
</ieee802-dot1q-bridge>
```

6.7.2.5 l2vlan type interfaces

Figure 21 shows the IETF Interfaces of type l2vlan in the end station components, which allow late binding of IA-station middlewares and applications to the configured VLANs and priorities.

The CNC/NPE configures the VLANs using the Bridge Component YANG module (ieee802-dot1q-bridge) as shown in 6.7.2.4 with VLAN names describing the usage of PCP/VID values for various traffic types.

The CNC/NPE configures additionally for every member port of the VLAN the l2vlan interfaces with names composed of the VLAN names appended with the port interface name. The lower-layer-if reference can be set by the IA-stations internally to the end station component port interface if required by the end station component.

NOTE The CNC cannot configure the lower-layer-if reference because it is defined read-only in the ietf-interfaces YANG module.

The l2vlan interface names shall conform to the scheme defined in 6.7.2.5 to allow the required translations for VLAN-ID and PCP values as described in 4.6.

VLAN name	as defined in 6.7.2.4
l2vlan interface name	<VLAN name>-<PortIfName>

<PortIfName> is the name of the end station component Port interface in the interface table.

l2vlan name examples:

60802-H7-101-ESC1-IP1	Isochronous traffic on interface ESC1-IP1 is mapped to PCP 7 and VID 101.
60802-H7-102R-ESC1-IP1	Redundant isochronous traffic on interface ESC1-IP1 is mapped to PCP 7 and VID 102.
60802-A0B1-100-ESC1-IP1	Best effort low traffic applying PCP 0, and best effort high traffic applying PCP 1 are both mapped to VID 100 on interface ESC1-IP1.

6.7.3 Discovery of IA-station internal structure

LLDP provides information about the external connectivity of IA-stations. To identify the internal structure of complex IA-stations (see 4.3) the IEEE 802.1Q management model (see 6.7.2.2) and the IETF Interface management model are applied:

- The functional units of an IA-station are represented as bridge entries in the bridge-list.
- The components of a functional unit are represented as component entries in the associated bridge entry’s component-list.
- Internal LAN connections between components of a functional unit are identified by I-LAN entries in the IETF interface list (6.7.2.3).

6.7.4 Network engineering model

To understand the requirements for network configuration, deployment and management, an engineering model covering industrial use cases is required. The “fully centralized model” described in IEEE Std 802.1Qcc-2018, 46.1.3.3 includes two functional entities: the CUC and the CNC. The roles of the CUC and CNC remain as specified in IEEE Std 802.1Qcc-2018, this document only elaborates them further for industrial automation. A conceptual block diagram of a CNC is shown in Figure 23, which adds further details to the CNC specified in IEEE Std 802.1Qcc-2018 to serve the industrial automation use case. The following functional entities are introduced:

a) The Topology Discovery Entity (TDE)
The topology discovery entity is responsible for the topology discovery (i.e., bridge component and end station component discovery). The TDE also performs a topology verification in cases where an expected topology is provided by the engineering tool. The resulting topology information is used by the CNC. The TDE detects added or removed IA-stations, including internal structure and connectivity. Thus, the CNC becomes aware of them. Overall, the TDE discovers and maintains an inventory of the devices, including their capabilities and the topology they form.

b) The Path Entity (PE)
The PE computes, establishes and maintains the forwarding paths for the IA time-aware stream and IA stream traffic type categories according to 4.7.3.

c) The Sync Tree Entity (STE)
The STE computes, establishes and maintains the sync trees. For example, for Working Clock and Global Time.

d) The Resource Allocation Entity (RAE)
The RAE is responsible for the allocation of the resources that are necessary for all traffic

type categories, according to 4.7.3, to meet their requirements via their forwarding paths. For example, frame buffers at egress ports and FDB entries.

e) The Network Provisioning Entity (NPE)
The NPE applies a network policy provided by the Engineering Tool to the IA-stations within the Configuration Domain. It uses the information discovered by the TDE to create a network configuration based upon this policy which is then applied to all IA-stations. The CNC uses the chosen network configuration together with the discovered IA-stations and their capabilities as input for its stream calculation and deployment.

A CNC includes these functional entities. The implementation of these functional entities and the CNC can vary. The means of communication among these functional entities is implementation dependent.

If there are multiple CNCs in one Configuration Domain, then it is ensured by some means that, at most, a single CNC is in charge at any time in the given Configuration Domain. (The means to ensure a single CNC being in charge in a Configuration Domain is beyond the scope of this release of this document.)

The CNC can be in a dedicated station or integrated into any IA-controller or IA-device. Generally, its engineering tool interface is user-specific and can only work with the compatible engineering tools. The definition of this interface is outside the scope of this document. The user or a CNC can provide traffic requirements and topology information in a standardized file format. A CNC can provide a user-specific way to read this information.

The CUC can be in a dedicated station or integrated into any IA-controller or IA-device. Generally, the CUC is user-specific. In industrial automation use cases, an IA-controller integrated CUC is very likely.

For stream establishment, the UNI of the CNC component is exposed.

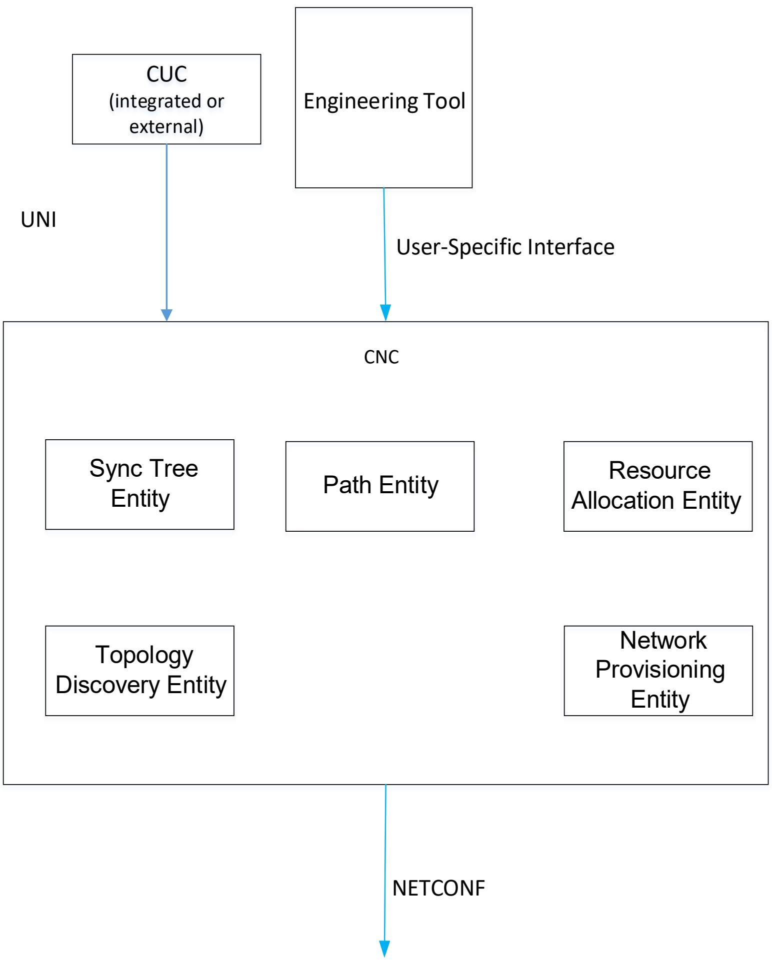


Figure 23 – Structure and interfaces of a CNC

Figure 24 shows an example of the structure of an IA-Station which the CNC might discover and manage.

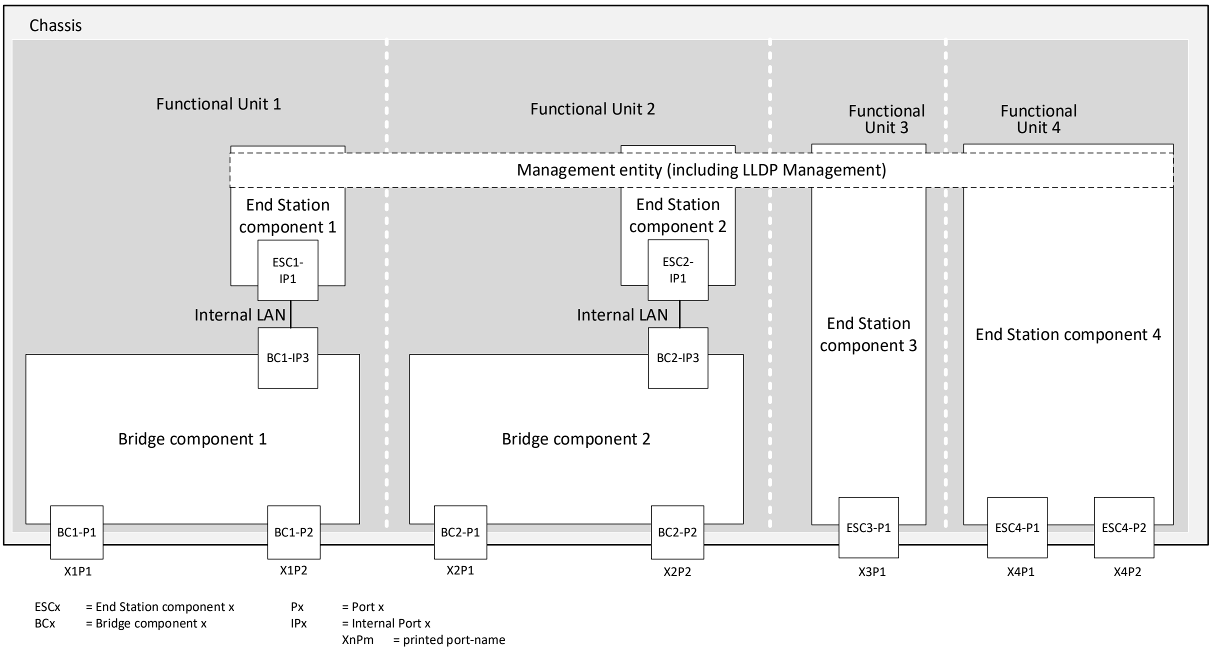


Figure 24 – IA-station structure example

Figure 25 shows the interaction of bridges and end stations with the CNC.

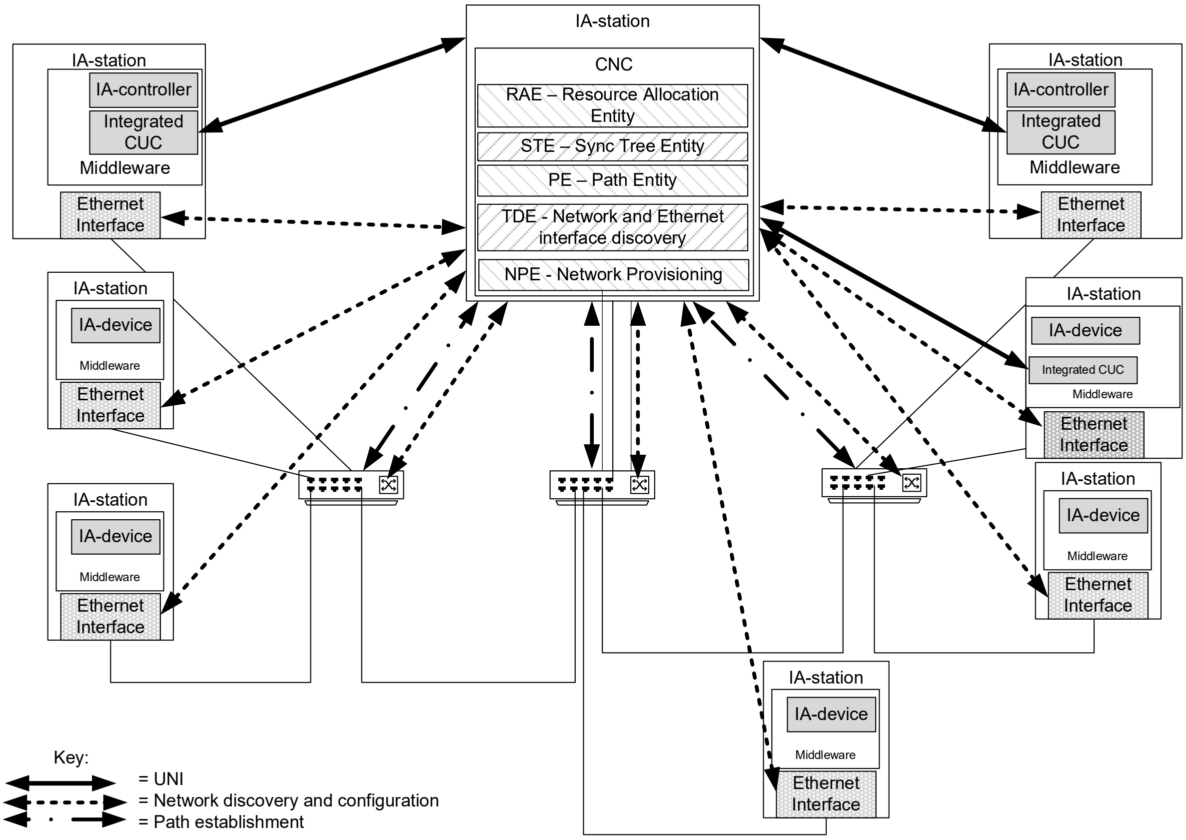


Figure 25 – CNC interaction

6.7.5 Operation

6.7.5.1 General

A representative model for network configuration is shown in Figure 26. This diagram maintains the traditional role of the IA-controller and the IA-device in an industrial automation network. It should be pointed out that IA-devices and IA-controllers will require configuration from engineering tools (refer to engineering tools A, B, D, and E). These tools and associated interfaces are out of scope for this profile. In this example, engineering tool C communicates directly with the CNC to provide traffic requirements for the network. The protocols that the engineering tool uses for communication with end stations are specific to the user application.

The UNI is the interface to the CNC which is serviced by NETCONF over TLS. The UNI service recognizes that industrial automation communications are typically connection oriented. There is a communication initiator, typically in a IA-controller, which is responsible for establishing those connections, determining what data is of interest and providing the required update rate. So, while an application/middleware of an IA-station (for example a Drive) understands what information it can produce and the maximum rate at which that information can be provided, until an IA-controller establishes a connection with that device, it does not know where that information needs to go and what update rate is required to close the control loop. The IA-controller gets this information from its engineering tool. There can be multiple IA-controllers in each Configuration Domain. The CNC uses the topology, the device capabilities, the device configuration, and the traffic specifications from the user to calculate a path for each Talker/Listener pair. The UNI then provides stream identification (VLAN, DMAC, etc.) to the Middleware.

The operational management model, see Figure 26, reflects the current and traditional model used in industrial automation. Figure 26 shows an active CNC managing multiple IA-stations. Each station can wholly incorporate a CUC and interact with the CNC directly.

Security requirements (see 6.3) are an important consideration for these networks and are integrated into the design, configuration, and deployment of any management model.

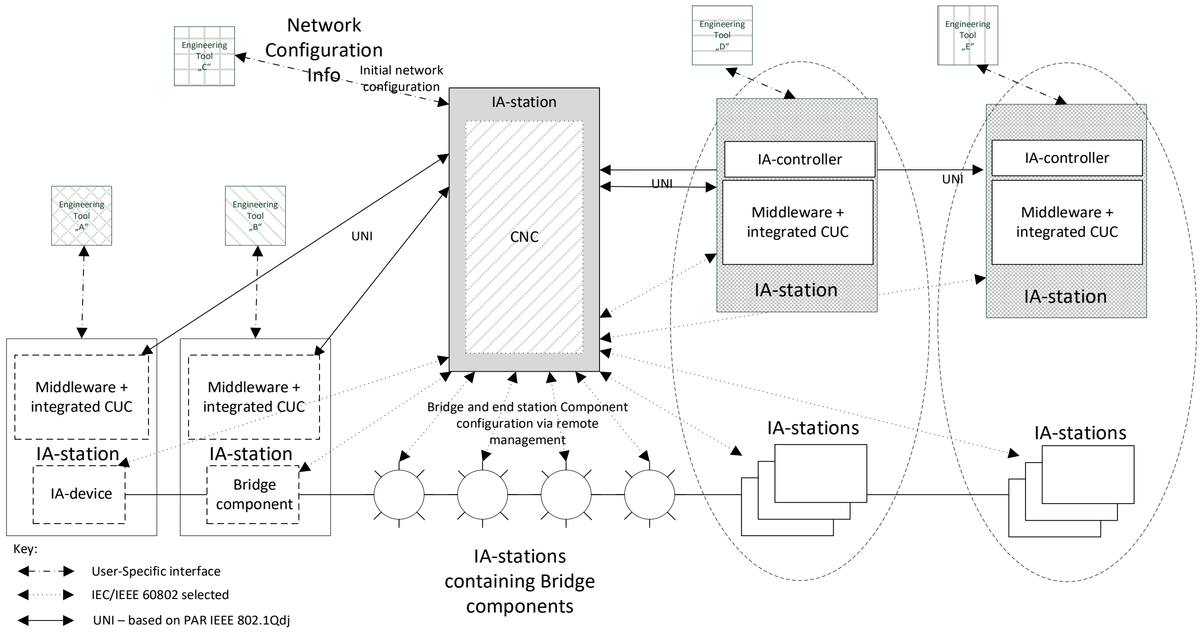


Figure 26 – Operational management model

Figure 27 shows the steps that are typically performed in the scope of the CUC-CNC interaction.

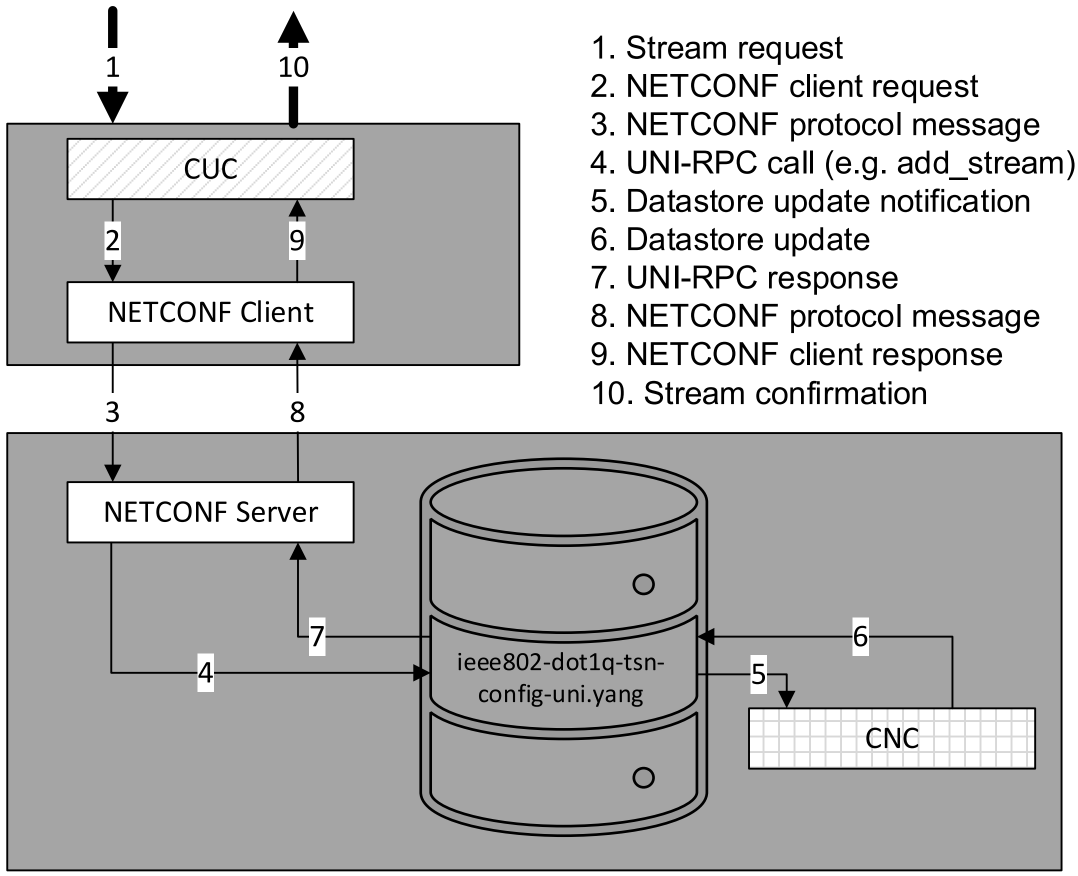


Figure 27 – UNI service model

After the computation of the paths and the scheduling and/or shaping configuration has been done, the CNC configures the IA-stations via NETCONF client. The typical steps that are performed in this process are shown in Figure 28 below.

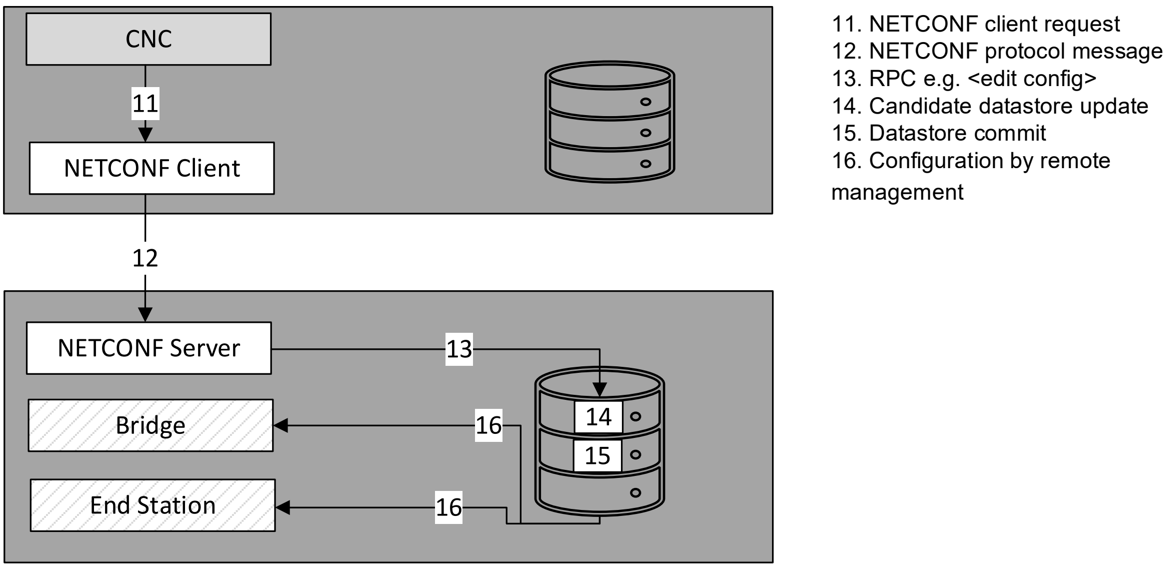


Figure 28 – CNC southbound

Instances of NETCONF servers and clients within a Configuration Domain are shown in Figure 29. IA-stations that contain a CNC and/or CUC entity contain both a NETCONF server and a NETCONF client. All other IA-stations contain a NETCONF server. A NETCONF client at the CUC side is needed for the UNI. NETCONF server at the CNC side is needed to accommodate the UNI as well as remote network management of the end stations and bridges that are contained in the same chassis as the CNC entity. The NETCONF client on the CNC side is needed for the southbound interface of the CNC i.e., for the remote management of the bridges and end stations in the scope of stream configuration. All IA-stations have a NETCONF server to make remote management possible. The NETCONF server used by the CNC serves multiple NETCONF Clients (CUCs) within a single Configuration Domain whose requests clients can occur simultaneously.

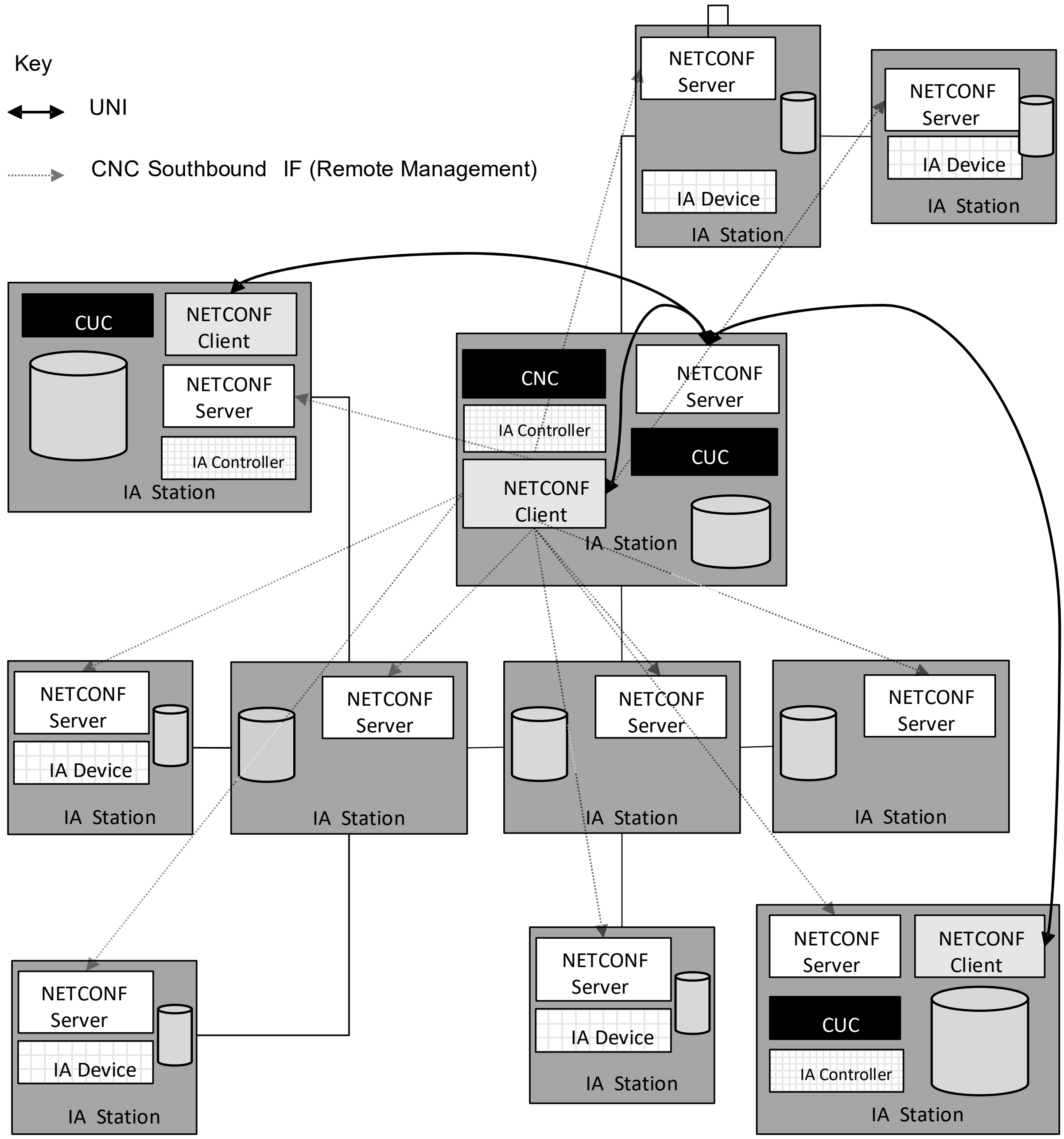


Figure 29 – NETCONF usage in a configuration domain

6.7.5.2 Domain port states

A CNC manages available network resources and assigns them to the IA-stations. Management of the network resources is only possible if the CNC owns these resources. Thus, no connected station is allowed to make use of network resources that are not granted by the CNC. The security configuration of a connected station allows remote access for the CNC.

Protection of the network resources is done by managing the ports (see Figure 30) at the boundary of the Configuration Domain. The state of any newly connected station is unknown. The CNC is responsible for determining if the newly connected station is added to the Configuration Domain and configuring the IA-station appropriately.

This port state model avoids any assumptions about configuration of added stations or network portions.

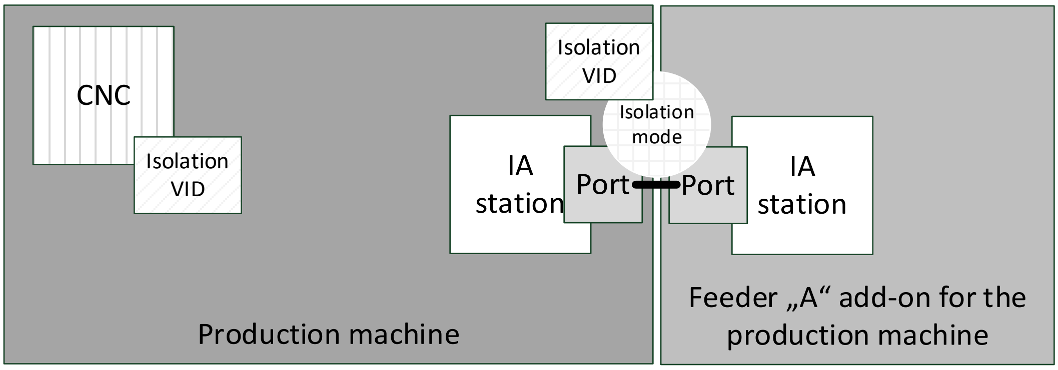


Figure 30 – Boundary port model

Ports of an IA-station that is a member of a Configuration Domain have different states:

- Isolated – a station connected via this port can only be accessed by a CNC. In the isolated state:
  - the port gets to or remains in isolated state in case of a link down event, e.g., when nothing is connected, or no link is established;
  - the port gets to or remains in isolated state in case of a link up event;
  - the port stays in isolated state as long as the neighbor is unknown, not able to enter Boundary state.
- Boundary – a station connected via this port is not part of the Configuration Domain, but is allowed to access devices inside the Configuration Domain and to pass traffic through the Configuration Domain
- Inside – a station connected via this port is part of the Configuration Domain

The determination of whether a given port of an IA-station remains in the Isolated state or transitions to the Boundary or Inside state is performed by the CNC using remote management. A port acts as a domain boundary if it is in the Isolated or Boundary state.

For example, a port could be configured as follows:

- Isolated state
  - Port is IST boundary
  - Port is not part of a sync tree
  - Port uses VLAN stripping for egress
  - Port uses VLAN assignment and priority regeneration to assign all traffic to an isolated VLAN
  - Port uses an ingress rate limiter to control the amount of traffic for the Configuration Domain
- Boundary state

  - Port is part of IST
  - Port is part of a sync tree
  - Port uses VLAN stripping for egress
  - Port uses VLAN assignment and priority regeneration to assign all traffic to a default VLAN
  - Port uses an ingress rate limiter to control the amount of traffic for the Configuration Domain
- Inside state
  - Port is part of IST
  - Port is part of a sync tree
  - Port is part of the active topology for stream and non-stream traffic

An example workflow includes the following steps executed by the CNC:

a) Topology discovery
   1) Case A: Link down / Port not connected
      i) Set port to isolated state
      ii) Configure a NETCONF subscription “on data change” to the port state leaf
   2) Case B: Neighbor is not a Configuration Domain member
      i) Set port to boundary state
      ii) Configure a NETCONF subscription “on data change” to the port state leaf
   3) Case C: Neighbor is not a Configuration Domain member – but part of expected topology
      i) Set port to boundary state
      ii) Configure the neighbor station as Configuration Domain member
      iii) Set port to inside state
b) NETCONF subscription trigger

   Issued to the CNC upon change of subscribed YANG data.

6.7.5.3 Engineered network

For an offline engineered (based on the available Digital data sheets of the used IA-stations) centralized approach with fixed topology, fixed stations and fixed paths, the user provides traffic requirements, path information, topology information and expected network configuration to the CNC. The CNC then uses the TDE, RAE and the NPE to perform the calculation of paths, resources, and stream schedules necessary to meet the specified traffic requirements and deploys the result of these calculations via remote management. The CNC also provides these results to the CUC via the UNI. The CUC then configures the end stations using the User-to-User interface (see Figure 3).

The workflow for this example consists of the following steps:

a) The user determines:
   1) the expected network topology
   2) the expected stations and its capabilities, value ranges and quantities
   3) the expected paths and resources
   4) the required streams
   5) the requirements for IA non-stream traffic.

This step focuses on network capabilities including the Ethernet interface of the end stations. For example, if the end station is a sensor, the user needs to consider the Ethernet interface capabilities of the sensor as they apply to the physical world.

b) Engineering Tool provides this information to the CNC via a user-specific interface.

Although the communication between the CNC and any Engineering Tool is user-specific, the CNC needs to obtain all information needed by the integrated TDE and NPE.

c) The CNC uses the TDE to discover the topology and checks it against the expected topology. The NPE is used to configure the IA-stations of the Configuration Domain.
d) The CNC uses STE and NPE to setup, validate, and monitors synchronization configuration in the Configuration Domain.
e) The CNC uses the information from engineering item a), steps 1 to 4, above to respond to requests from Middleware (with integrated CUC) using UNI. These requests are handled using the already established stream paths received from the user.

If the CNC is not required after commissioning, then the CNC can be removed after setting up the IA-stations. That requires that all IA-stations have a persistent storage for the data provided by the CNC.

6.7.5.4 Dynamic topology

6.7.5.4.1 General

For a centralized approach with a dynamic topology and dynamic paths, the user provides the network policy to the CNC. The TDE performs topology discovery including IA-station capabilities (YANG representation of the Digital Data Sheet) and the NPE performs network configuration for the CNC. IA-stations then provide traffic requirements via the Middleware to the CNC via the UNI. The CNC then uses the TDE, RAE, and NPE to perform the calculation of paths, resources, and stream schedules necessary to meet the specified traffic requirements and deploys the result of these calculations via remote management. The CNC also provides these results to the CUC via the UNI. The CUC then configures the end stations using the User-to-User interface (see Figure 3).

The workflow for this example consists of the following steps:

a) The user determines the network policy and provides it to the CNC.
b) The TDE continuously discovers the physical network topology and station capabilities of each station using remote management.
c) The NPE uses the information gathered in steps a) to b) to configure the stations in the Configuration Domain.
d) The CNC uses STE and NPE to setup, validate and monitor synchronization configuration in the Configuration Domain.

The CNC uses the information from steps a) to d) to respond to requests from Middleware using UNI. The CNC establishes streams in the bridges via a remote management protocol.

6.7.5.4.2 Adding an IA-station

Each station added to the Configuration Domain will be discovered by the TDE and receive the network configuration from the NPE (for an example workflow, see 6.7.5.2). After this, the Middleware can request stream establishment.

When an IA-station is added to the network, it is isolated until the CNC determines that its traffic requirements can be accommodated without disrupting other traffic (see 6.7.5.2).

6.7.5.4.3 Removing an IA-station

Each station removed from the Configuration Domain will be discovered by the TDE (for an example workflow, see 6.7.5.2). A neighboring station can receive an updated network configuration by the NPE. After this, the removed IA-station is no longer part of the Configuration Domain.

6.7.5.4.4 Replacing an IA-station

In the simplest case, replacing an IA-station is simply the sequence of removing an IA-station (6.7.5.4.3) and adding an IA-station (6.7.5.4.2). In more complex cases, other precautions or user actions can be needed following deployment.

6.7.5.5 Engineered network extended by dynamic topology

Modular machines, robot tool changers or more general plug & produce can add or remove modules. The basic machine is handled as engineered network. Additional modules or removed modules are handled dynamically.

6.7.6 Engineered time-synchronization spanning tree

6.7.6.1 General

Engineered time-synchronization spanning tree (sync tree) for a given gPTP domain refers to the usage of external port configuration instead of BMCA for the construction of a desired sync tree with the Grandmaster PTP Instance as the root (see IEEE Std 802.1AS-2020, 10.3.1).

One of the advantages of engineered sync trees is to enable a planned, deterministic, and stable configuration of the IEEE Std 802.1AS-2020 sync tree for a given gPTP domain. For example, this approach prevents sync tree changes in case of IA-station addition or removal from the network. Working Clock (see 3.3.13) and hot standby (see P802.1ASdm) are use cases of engineered sync tree.

The Grandmaster PTP Instance might reside in a dedicated grandmaster-capable IA-station or integrated into a grandmaster-capable IA-controller.

6.7.6.2 Sync tree requirements

Sync tree requirements for all participating PTP Instances in a gPTP domain are specified in 5.5.3. In addition, 5.6.2 item b) is required for all participating PTP Relay Instances.

6.7.6.3 STE phases

6.7.6.3.1 General

The STE should follow the logical sequence described in 6.7.6.3 if an engineered sync tree is utilized in a gPTP domain. Each STE phase describes an externally observable behavior of the participating PTP Instances in a gPTP domain.

6.7.6.3.2 Discovery phase

In discovery phase, STE utilize the topology discovered by the TDE to verify the capabilities and status of participating IA-stations via a diagnostics entity (see 6.7.7.1) by reading the following managed objects:

- The status of oper-status parameter is up (see IETF RFC 8343) for all participating Ethernet links.
- The status of isMeasuringDelay (see IEEE Std 802.1AS-2020, 14.16.4) is TRUE for all PTP Ports.
- The status of asCapable (see IEEE Std 802.1AS-2020, 14.8.7) is TRUE for all PTP Ports.
- The status of asCapableAcrossDomains (see IEEE Std 802.1AS-2020, 14.16.5) is TRUE for all LinkPorts.
- The status of gmCapable (see IEEE Std 802.1AS-2020, 14.2.7) is TRUE, only applicable to the Grandmaster PTP Instance.

STE should use the information collected via managed objects and the discovered topology to verify the constraints on the gPTP domain, for example:

- Verify that the number of PTP Relay Instances (hops) between the Grandmaster PTP Instance and any given Slave PTP End Instance is within the limit prescribed by for example, CNC.
- Verify per PTP link that the value of meanLinkDelay (see IEEE Std 802.1AS-2020, 14.16.6) is less than or equal to meanLinkDelayThresh (see IEEE Std 802.1AS-2020, 14.16.7 and IEEE Std 802.1AS-2020, Table 11-1) value to detect for example, anomaly in propagation delay.

NOTE Even if neighboring PTP Instances do report asCapable, It can be that a link between asCapable neighboring PTP Instances is not asCapable due to for example, wrong setting of meanLinkDelayThresh value. The meanLinkDelayThresh value reflects estimated propagation delay of the installed link.

6.7.6.3.3 Provisioning phase

In provisioning phase, STE should apply the desired configuration to all participating PTP Instances, for example:

- The desiredState of all PTP ports of the Grandmaster PTP Instance is set to MasterPort.
- The desiredState of exactly one PTP port of all the other PTP Instances is set to SlavePort.
- The desiredState of remaining PTP ports that are part of sync tree in non-Grandmaster PTP Relay Instances is set to MasterPort.
- The desiredState of all other PTP ports is set to PassivePort.

Then STE should validate, for example:

- The syncLocked (see IEEE Std 802.1AS-2020, 14.8.52) parameter is TRUE for all PTP ports of PTP Relay Instances that are in MasterPort state.

6.7.6.3.4 Monitoring phase

6.7.6.3.4.1 General

In monitoring phase, STE in combination with for example, TDE and diagnostics entity (see 6.7.7.1) should monitor the status and the performance of the gPTP domain by reading the relevant managed objects.

6.7.6.3.4.2 Status monitoring

The STE in combination with for example, TDE and diagnostics entity (see 6.7.7.1) should monitor the status of the gPTP domain by reading the following managed objects:

- The status of oper-status parameter is up (see IETF RFC 8343) for all participating Ethernet links.
- Verify the existence of at least a single Grandmaster PTP Instance across gPTP domain, i.e., grandmasterIdentity (see IEEE Std 802.1AS-2020, 14.4.4).

Editor's note: Adding a managed object for gmPresent is under consideration in IEEE P802.1ASdm. The corresponding YANG variable is a subject of IEEE P802.1ASdn.

- Detect each addition (see 6.7.7.4) and removal (see 6.7.7.5) of a PTP Instance.
- Verify that the number of PTP Relay Instances (hops) between the Grandmaster PTP Instance and any given Slave PTP End Instance is within the limit prescribed by for example, CNC.

6.7.6.3.4.3 Performance monitoring

The STE in combination with the TDE detects the change of status of the gPTP instances within the Configuration Domain by monitoring the following managed objects:

- Verify that the PTP Instances are in SYNCED state (see P802.1ASdm), i.e., time is synchronized according to the requirements of this document.

Editor's note: It is expected that Asdm will provide managed objects which reflect this state

- Verify that the clockQuality of Grandmaster PTP Instance (see - IEEE Std 802.1AS-2020, 14.2.4) is within the requirements of this document.
- Detect any change in phase or frequency of the Grandmaster PTP Instance, i.e., lastGmPhaseChange (IEEE Std 802.1AS-2020, 14.3.4), lastGmFreqChange (IEEE Std 802.1AS-2020, 14.3.5).
- Verify per PTP link that the value of meanLinkDelay (see IEEE Std 802.1AS-2020, 14.16.6) is less than or equal to meanLinkDelayThresh (see IEEE Std 802.1AS-2020, 14.16.7 and IEEE Std 802.1AS-2020, Table 11-1) value to detect for example, anomaly in propagation delay.
- Verify that the PTP messages timeout events, syncReceiptTimeoutCount (see IEEE Std 802.1AS-2020, 14.10.10) and announceReceiptTimeoutCount (see IEEE Std 802.1AS-2020, 14.10.11) are negligible with respect to the requirements of this document.
- Verify that the RateRatio value (see 6.2.3) is within the expected range (see Table 11 and Table 12) per PTP link.

Any deviation detected by a PTP Instance can be conveyed to the STE via, for example, notification.

6.7.6.4 Adding an IA-station

Each IA-station added to the gPTP domain will be discovered by STE via TDE. It is the responsibility of the CNC to on-board this newly added station. IA-stations can receive an updated gPTP configuration via STE.

A newly installed IA-station can disrupt the operation of a gPTP domain. The extent of disruption is dependent on the location of the IA-station in the gPTP domain and the type of PTP Instance running on that IA-station. For example, if PTP Instances are arranged in a daisy-chain formation and if a IA-station with a non-Grandmaster Relay Instance is installed in the middle of a daisy-chain then this change will disrupt for example, the operation of downstream PTP Instances.

6.7.6.5 Removing an IA-station

The removal of a station from the gPTP domain will be detected by STE via TDE. IA-stations can receive an updated gPTP configuration via STE.

A newly installed IA-station can disrupt the operation of a gPTP domain. It is the responsibility of the CNC to take the steps necessary to ensure the removal of the station does not disrupt the network. For example, if PTP Instances are arranged in a daisy-chain formation and if a IA-station that is running a non-Grandmaster Relay Instance is removed from the middle of a daisy-chain then this change will disrupt for example, the operation of downstream PTP Instances.

6.7.6.6 Replacing an IA-station

A IA-station replacement follows the sequence of removing a IA-station according to 6.7.7.5 and adding a IA-station according to 6.7.7.4.

6.7.7 Diagnostics

6.7.7.1 General

Diagnosis for an IA-station is done by monitoring YANG representation of the IA-station’s local database.

A vendor can implement an observer in a diagnostics entity, which could reside in the CNC. This diagnostics entity uses the information provided by remote management to define the monitored objects and set up fitting notifications.

6.7.7.2 Observer model

A diagnostic entity can select any objects described via YANG and observe them via NETCONF. The NETCONF binding is specified in RFC 8640, and the subscription model in RFC 8641. NETCONF messages can be pipelined, i.e., a client can invoke multiple RPCs without having to wait for RPC result messages first. RPC messages are defined in RFC 6241 and notification messages are defined in RFC 5277. To reduce the load on the diagnostic entity caused by the many IA-stations, it configures the objects to be monitored and the associated notifications on the IA-station.

Figure 31 shows the model of a diagnostic observer.

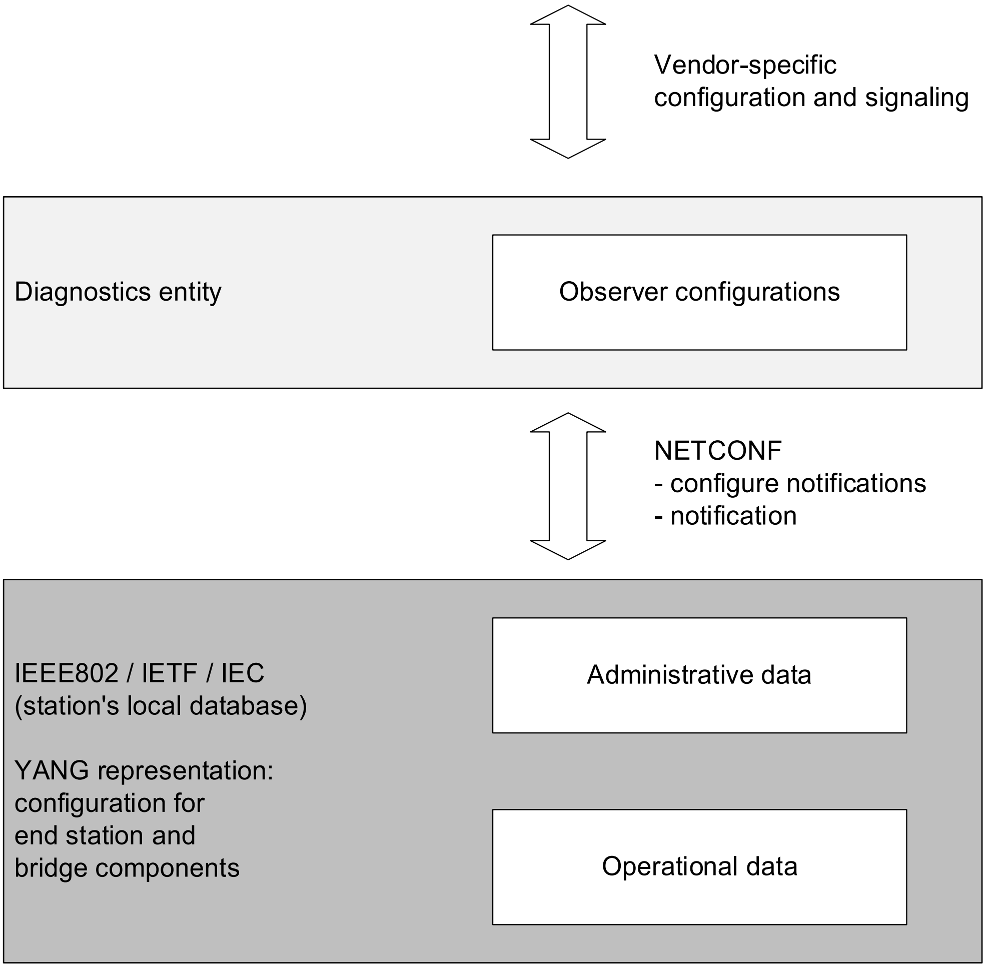


Figure 31 – Observer model

6.7.7.3 Usage of YANG Push

IA-station diagnostics shall be implemented by YANG-Push subscriptions as defined in IETF RFC 8641 (YANG Push) and IETF RFC 8639 (Subscribed Notifications).

IA-stations shall support the “subtree” selection filter as defined in IETF RFC 8041, 3.6

6.7.7.4 Mandatory RPCs

An IA-station shall support following RPCs as defined in IETF RFC 8641:

a) establish-subscription
b) modify-subscription
c) delete-subscription
d) kill-subscription

6.7.7.5 Mandatory notifications

An IA-station shall support following notifications as defined in IETF RFC 8641

a) subscription-resumed
b) subscription-modified
c) subscription-terminated
d) subscription-suspended
e) push-update
f) push-change-update

6.7.7.6 Mandatory diagnostics data nodes

An IA-station shall provide following data nodes for diagnostic purpose:

Data to be provided as “On-change” subscription:

a) Change of link-status
b) Change of MAU-type
c) Change of sync-status

Data to be provided as periodic time-aligned subscriptions:

a) dropped frames statistic counters for external ports
b) VLAN specific counters

Editor’s note: detailed location of nodes in YANG tree to be inserted

6.7.7.7 Usage of NETCONF notifications

IA-stations shall implement the binding of a stream of events according to IETF RFC 8640 (NETCONF Notifications) using the “encode-xml” feature and the “NETCONF” event stream of IETF RFC 8639.

An IA-station shall support dynamic subscriptions as defined in IETF RFC 8640 Clauses 5, 6 and 7.

6.7.8 Data sheet

6.7.8.1 General

The user requires data sheets containing the capabilities, value ranges and quantities of IA-stations. See Annex B for example quantities in a representative Configuration Domain. Data sheets need to be available for offline and online (plug & produce) engineering.

Online datasheets are modeled using YANG. YANG modeling can also be used for the offline data sheet to keep the offline and online format the same.

6.7.8.2 Digital data sheet of an IA-station

Both engineering models, offline via an engineering tool and online with plug & produce by the CNC, require information about the capabilities of an IA-station, for example, states, configurations, supported features, etc.

This data is extracted from the implemented YANG modules, which are available in the local database of the IA-station.

The data from the implemented YANG modules is also available offline in the form of a Digital Data Sheet of an IA-station as an DigitalDataSheet file.

The Digital Data Sheet of an IA-station provides a collection of all instantiated data nodes of all YANG modules that are present in the local database of the IA-station. This includes all YANG modules required by this profile, as well as all additional modules that have been added by the manufacturer.

The Digital Data Sheet does not contain any additional information that is not modeled by the YANG modules that exist in the local database of the IA-station.

The data sheet contains a single instance data set. It carries complete configuration and state data of each YANG module that is present in the local database of the IA-station.

The identity of the datastore with which the instance data set is associated is reported as defined in IETF RFC 9195. The format of the YANG instance data set is defined in IETF RFC 9195. The file format is based on the XML encoding. It is created by applying the respective XML encoding rules for the YANG structure of the YANG module mentioned above.

A user uses the information from the Digital Data Sheet to understand the quantities and capabilities of an IA-station, which is required for successful offline engineering of the network.

The features of a CNC need to be available for offline and online engineering or diagnostics. For this purpose, YANG modules are used that allow structured access to the local database of the CNC according to 6.7.9.2.6.12.

Any IA-station can include a CNC entity in which case the collection of YANG modules of such IA-station would include all CNC specific YANG modules for example, the ieee802-dot1q-tsn-config-uni YANG module. Since all IA-stations meet the requirements from 5.5.5, the CNC related YANG instance data is automatically included in the digital data sheet of the IA-station that hosts the CNC as described in 6.7.9.2.

Editor's note: It is not clear if the currently available YANG modules provide enough information for the creation of a Digital Twin.

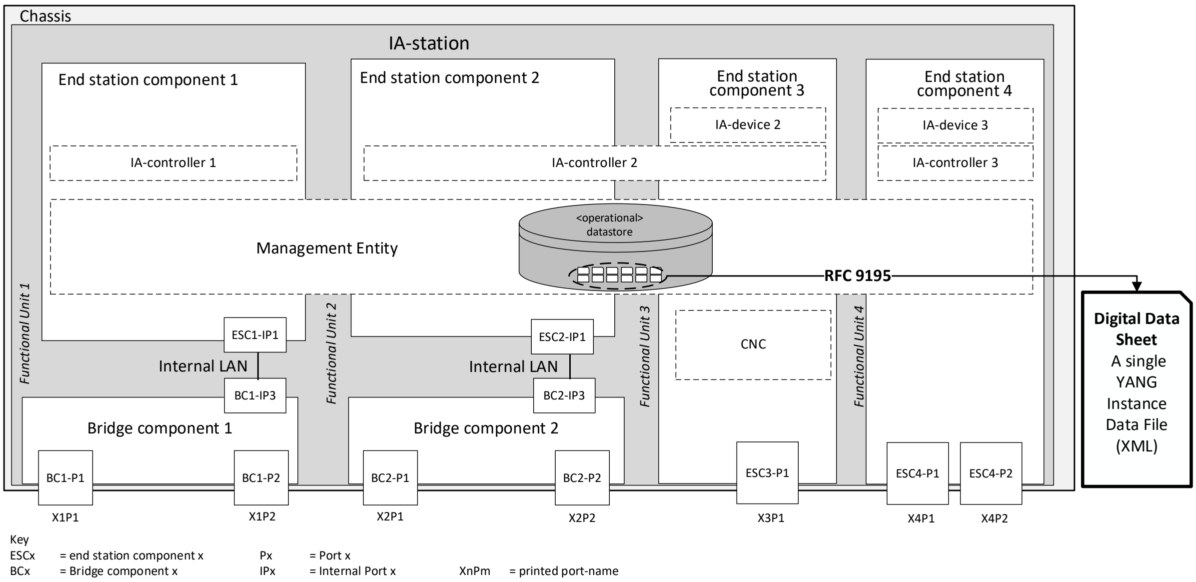


Figure 32 – Creation of the digital data sheet of an IA-station

6.7.8.3 Traffic requirements description

Digital twins allow the simulation of the network. For this purpose, the properties of the IA-stations, the CNC and the required traffic is known.

The digital data sheets for the CNC and IA-stations provide a vendor-independent means to gather the information needed for simulation. However, a description of the generated communication load or bandwidth usage is missing.

The generated communication load, bandwidth usage, required latencies and traffic classes need to be described offline.

This allows a digital twin to be created and the network to be simulated.

Editor's note: Traffic requirements Description structure will be based upon an upcoming contribution.

6.7.9 YANG representation of managed objects

6.7.9.1 General

All managed objects shall be represented in the YANG 1.1 format as described in IETF RFC 7950.

6.7.9.2 Common YANG modules, features and leaves

6.7.9.2.1 General

The YANG modules, features and leaves in 6.7.9.2 shall be supported by all IA-stations.

6.7.9.2.2 IEEE standard for Ethernet

IA-stations shall support the ieee802-ethernet-interface YANG module according to IEEE Std 802.3.2-2019 with the following leaves:

- `/ietf-interfaces/interface/ethernet/duplex`
- `/ietf-interfaces/interface/ethernet/speed`

- /ietf-interfaces/interface/ethernet/flow-control/pause/direction (if the feature "ethernet-pause" is supported)

6.7.9.2.3 Station and media access control connectivity discovery

IA-stations shall support the following leaves from the ieee802-dot1ab-lldp YANG module according to IEEE Std 802.1ABcu-2021 with values and value ranges according to 6.8.

- /ieee802-dot1ab-lldp/lldp/message-fast-tx
- /ieee802-dot1ab-lldp/lldp/message-tx-hold-multiplier
- /ieee802-dot1ab-lldp/lldp/message-tx-interval
- /ieee802-dot1ab-lldp/lldp/reinit-delay
- /ieee802-dot1ab-lldp/lldp/tx-credit-max
- /ieee802-dot1ab-lldp/lldp/tx-fast-init
- /ieee802-dot1ab-lldp/lldp/notification-interval
- /ieee802-dot1ab-lldp/lldp/remote-statistics
- /ieee802-dot1ab-lldp/lldp/local-system-data
- /ieee802-dot1ab-lldp/lldp/port
- /ieee802-dot1ab-lldp/lldp/remote-statistics/last-change-time
- /ieee802-dot1ab-lldp/lldp/remote-statistics/remote-inserts
- /ieee802-dot1ab-lldp/lldp/remote-statistics/remote-deletes
- /ieee802-dot1ab-lldp/lldp/remote-statistics/remote-drops
- /ieee802-dot1ab-lldp/lldp/remote-statistics/remote-ageouts
- /ieee802-dot1ab-lldp/lldp/local-system-data/chassis-id-subtype
- /ieee802-dot1ab-lldp/lldp/local-system-data/chassis-id
- /ieee802-dot1ab-lldp/lldp/local-system-data/system-name
- /ieee802-dot1ab-lldp/lldp/local-system-data/system-description
- /ieee802-dot1ab-lldp/lldp/local-system-data/system-capabilities-supported
- /ieee802-dot1ab-lldp/lldp/local-system-data/system-capabilities-enabled
- /ieee802-dot1ab-lldp/lldp/port/name
- /ieee802-dot1ab-lldp/lldp/port/dest-mac-address
- /ieee802-dot1ab-lldp/lldp/port/admin-status
- /ieee802-dot1ab-lldp/lldp/port/notification-enable
- /ieee802-dot1ab-lldp/lldp/port/tlvs-tx-enable
- /ieee802-dot1ab-lldp/lldp/port/message-fast-tx
- /ieee802-dot1ab-lldp/lldp/port/message-tx-hold-multiplier
- /ieee802-dot1ab-lldp/lldp/port/message-tx-interval
- /ieee802-dot1ab-lldp/lldp/port/reinit-delay
- /ieee802-dot1ab-lldp/lldp/port/tx-credit-max
- /ieee802-dot1ab-lldp/lldp/port/tx-fast-init
- /ieee802-dot1ab-lldp/lldp/port/notification-interval
- /ieee802-dot1ab-lldp/lldp/port/management-address-tx-port

- /ieee802-dot1ab-lldp/lldp/port/port-id-subtype
- /ieee802-dot1ab-lldp/lldp/port/port-id
- /ieee802-dot1ab-lldp/lldp/port/port-desc
- /ieee802-dot1ab-lldp/lldp/port/remote-systems-data

6.7.9.2.4 Synchronization

6.7.9.2.4.1 Timesync

IA-stations shall support the ieee1588-ptp YANG module according to IEEE P1588e with the following features:

- cmlds (Common Mean Link Delay Service)
- external-port-config

IA-stations shall support the ieee1588-ptp YANG module according to IEEE P1588e with the following leaves:

- /ieee1588-ptp/ptp/instances/instance/instance-index
- /ieee1588-ptp/ptp/instances/instance/default-ds/clock-identity
- /ieee1588-ptp/ptp/instances/instance/default-ds/number-ports
- /ieee1588-ptp/ptp/instances/instance/default-ds/domain-number
- /ieee1588-ptp/ptp/instances/instance/default-ds/slave-only
- /ieee1588-ptp/ptp/instances/instance/default-ds/sdo-id
- /ieee1588-ptp/ptp/instances/instance/default-ds/instance-enable
- /ieee1588-ptp/ptp/instances/instance/default-ds/external-port-config-enable
- /ieee1588-ptp/ptp/instances/instance/default-ds/instance-type
- /ieee1588-ptp/ptp/instances/instance/description-ds/user-description
- /ieee1588-ptp/ptp/instances/ports/port/port-index
- /ieee1588-ptp/ptp/instances/ports/port/underlying-interface
- /ieee1588-ptp/ptp/instances/ports/port/port-ds/port-state
- /ieee1588-ptp/ptp/instances/ports/port/port-ds/delay-mechanism
- /ieee1588-ptp/ptp/instances/ports/port/port-ds/port-enable
- /ieee1588-ptp/ptp/instances/ports/port/external-port-config-port-ds/desired-state
- /ieee1588-ptp/ptp/common-services/cmlds/default-ds/clock-identity
- /ieee1588-ptp/ptp/common-services/cmlds/default-ds/number-link-ports
- /ieee1588-ptp/ptp/common-services/cmlds/ports/port/port-index
- /ieee1588-ptp/ptp/common-services/cmlds/ports/port/underlying-interface
- /ieee1588-ptp/ptp/common-services/cmlds/ports/port/link-port-ds/port-identity/clock-identity
- /ieee1588-ptp/ptp/common-services/cmlds/ports/port/link-port-ds/port-identity/port-number
- /ieee1588-ptp/ptp/common-services/cmlds/ports/port/link-port-ds/domain-number

- /ieee1588-ptp/ptp/common-services/cmlds/ports/port/link-port-ds/service-measurement-valid
- /ieee1588-ptp/ptp/common-services/cmlds/ports/port/link-port-ds/mean-link-delay
- /ieee1588-ptp/ptp/common-services/cmlds/ports/port/link-port-ds/scaled-neighbor-rate-ratio
- /ieee1588-ptp/ptp/common-services/cmlds/ports/port/link-port-ds/log-min-pdelay-req-interval
- /ieee1588-ptp/ptp/common-services/cmlds/ports/port/link-port-ds/version-number
- /ieee1588-ptp/ptp/common-services/cmlds/ports/port/link-port-ds/minor-version-number
- /ieee1588-ptp/ptp/common-services/cmlds/ports/port/link-port-ds/delay-asymetry

6.7.9.2.4.2 Timesync (draft ieee802-dot1as-ptp)

IA-stations shall support the ieee802-dot1as-ptp YANG module according to IEEE P802.1ASdn with the following leaves:

- /ieee802-dot1as-ptp/ptp/instances/instance/default-ds/gm-capable
- /ieee802-dot1as-ptp/ptp/instances/instance/default-ds/current-utc-offset-valid
- /ieee802-dot1as-ptp/ptp/instances/instance/default-ds/ptp-timescale
- /ieee802-dot1as-ptp/ptp/instances/ports/port/port-ds/sync-receipt-timeout
- /ieee802-dot1as-ptp/ptp/instances/ports/port/port-ds/current-one-step-tx-oper
- /ieee802-dot1as-ptp/ptp/instances/ports/port/port-ds/use-mgt-one-step-tx-oper
- /ieee802-dot1as-ptp/ptp/instances/ports/port/port-ds/mgt-one-step-tx-oper
- /ieee802-dot1as-ptp/ptp/instances/ports/port/port-ds/sync-locked
- /ieee1588-ptp/ptp/common-services/cmlds/ports/port/link-port-ds/cmlds-link-port-enabled
- /ieee1588-ptp/ptp/common-services/cmlds/ports/port/link-port-ds/is-measuring-delay
- /ieee1588-ptp/ptp/common-services/cmlds/ports/port/link-port-ds/as-capable-across-domains
- /ieee1588-ptp/ptp/common-services/cmlds/ports/port/link-port-ds/mean-link-delay-thresh
- /ieee1588-ptp/ptp/common-services/cmlds/ports/port/link-port-ds/current-log-pdelay-req-interval
- /ieee1588-ptp/ptp/common-services/cmlds/ports/port/link-port-ds/use-mgt-log-pdelay-req-interval
- /ieee1588-ptp/ptp/common-services/cmlds/ports/port/link-port-ds/mgt-log-pdelay-req-interval
- /ieee1588-ptp/ptp/common-services/cmlds/ports/port/link-port-ds/current-compute-rate-ratio

- `/ieee1588-ptp/ptp/common-services/cmlds/ports/port/link-port-ds/use-mgt-compute-rate-ratio`
- `/ieee1588-ptp/ptp/common-services/cmlds/ports/port/link-port-ds/mgt-compute-rate-ratio`
- `/ieee1588-ptp/ptp/common-services/cmlds/ports/port/link-port-ds/current-compute-mean-link-delay`
- `/ieee1588-ptp/ptp/common-services/cmlds/ports/port/link-port-ds/use-mgt-compute-mean-link-delay`
- `/ieee1588-ptp/ptp/common-services/cmlds/ports/port/link-port-ds/mgt-compute-mean-link-delay`
- `/ieee1588-ptp/ptp/common-services/cmlds/ports/port/link-port-ds/allowed-lost-responses`
- `/ieee1588-ptp/ptp/common-services/cmlds/ports/port/link-port-ds/allowed-faults`

6.7.9.2.4.3 Timesync (iecieee60802)

IA-stations shall support the iecieee60802 YANG module according to this standard with the following leaves:

- `/iecieee60802/ptp/max-ptp-instances`
- `/iecieee60802/ptp/max-hot-standby-systems`
- `/iecieee60802/ptp/clock-source/arb-supported`
- `/iecieee60802/ptp/clock-source/ptp-supported`
- `/iecieee60802/ptp/clock-source/identity`
- `/iecieee60802/ptp/clock-target/arb-supported`
- `/iecieee60802/ptp/clock-target/ptp-supported`
- `/iecieee60802/ptp/clock-target/identity`
- `/iecieee60802/ptp/instances/instance/default-ds/application-clock/clock-state`
- `/iecieee60802/ptp/instances/instance/default-ds/application-clock/identity`

NOTE: the existence of /iecieee60802/ptp/clock-source implies that the IA station is GM capable.

6.7.9.2.5 Security configuration modules

6.7.9.2.5.1 YANG module for a keystore

IA-stations shall support the ietf-keystore YANG module according to draft-ietf-netconf-keystore-2x with the following features:

- central-keystore-supported
- asymmetric-keys

IA-stations shall support the ietf-keystore YANG module according to draft-ietf-netconf-keystore-2x with the following leaves:

- `/ietf-keystore/keystore/asymmetric-keys/asymmetric-key/name`

- `/ietf-keystore/keystore/asymmetric-keys/asymmetric-key/public-key-format`
- `/ietf-keystore/keystore/asymmetric-keys/asymmetric-key/public-key`
- `/ietf-keystore/keystore/asymmetric-keys/asymmetric-key/private-key-format`
- `/ietf-keystore/keystore/asymmetric-keys/asymmetric-key/hidden-private-key`
- `/ietf-keystore/certificates/certificate/name`
- `/ietf-keystore/certificates/certificate/cert-data`
- `/ietf-keystore/certificates/certificate/expiration-date`
- `/ietf-keystore/certificates/certificate/csr-info`
- `/ietf-keystore/certificates/certificate/certificate-signing-request`

6.7.9.2.5.2 Network configuration access control

IA-stations shall support the ietf-netconf-acm YANG module according to IETF RFC 8341 with the following leaves:

Editor's note: The to be supported features and leaves have to be worked out.

6.7.9.2.5.3 A YANG data module for a truststore

IA-stations shall support the ietf-truststore YANG module according to draft-ietf-netconf-trust-anchors-2x with the following features:

- central-keystore-supported
- certificates

IA-stations shall support the ietf-truststore YANG module according to draft-ietf-netconf-trust-anchors-12x with the following leaves:

- `/ietf-truststore/truststore/certificate-bags/certificate-bag/name`
- `/ietf-truststore/truststore/certificate-bags/certificate-bag/certicicate/name`
- `/ietf-truststore/truststore/certificate-bags/certificate-bag/certicicate/cert-data`
- `/ietf-truststore/truststore/certificate-bags/certificate-bag/certicicate/expiration-date`

6.7.9.2.6 IA-station management

6.7.9.2.6.1 System capabilities

IA-stations shall support the ietf-system-capabilities YANG module according to IETF RFC 9196 with the following leaves:

- `/ietf-system-capabilities/datastore-capabilities/datastore`
- `/ietf-system-capabilities/datastore-capabilities/per-node-capabilities`
- `/ietf-system-capabilities/subscription-capabilities/on-change-supported`

6.7.9.2.6.2 YANG library

IA-stations shall support the ietf-yang-library YANG module according to IETF RFC 8525 with the following leaves:

- `/ietf-yang-library/yang-library/module-set [list]`
- `/ietf-yang-library/yang-library/schema [list]`
- `/ietf-yang-library/yang-library/datastore [list]`
- `/ietf-yang-library/yang-library/content-id`

6.7.9.2.6.3 NETCONF extensions to support the network management datastore architecture

IA-stations shall support the ietf-netconf-nmda YANG module according to IETF RFC 8526 with the following leaves:

Editor's note: The to be supported features and leaves have to be worked out.

6.7.9.2.6.4 YANG push

IA-stations shall support the ietf-yang-push YANG module according to IETF RFC 8641 with the following feature:

- on-change

IA-stations shall support the ietf-yang-push YANG module according to IETF RFC 8641 with the following leaves:

Editor's note: The to be supported leaves have to be worked out.

6.7.9.2.6.5 YANG notification capabilities

IA-stations shall support the ietf-notification-capabilities YANG module according to IETF RFC 9196 with the following leaves:

Editor's note: The to be supported features and leaves have to be worked out.

6.7.9.2.6.6 YANG notifications

IA-stations shall support the ietf-subscribed-notifications YANG module according to IETF RFC 8639 with the following features:

- `configured`
- `encode-xml`
- `subtree`

IA-stations shall support the ietf-subscribed-notifications YANG module according to IETF RFC 8639 with the following leaves:

- `/ietf-subscribed-notifications/streams/stream/name`
- `/ietf-subscribed-notifications/streams/stream/description`
- `/ietf-subscribed-notifications/streams/stream/replay-support`

- `/ietf-subscribed-notifications/streams/stream/replay-log-creation-time`
- `/ietf-subscribed-notifications/streams/stream/replay-log-aged-time`
- `/ietf-subscribed-notifications/filters/stream-filter/name`
- `/ietf-subscribed-notifications/filters/stream-filter/filter-spec`
- `/ietf-subscribed-notifications/subscriptions/subscription/id`
- `/ietf-subscribed-notifications/subscriptions/subscription/target`
- `/ietf-subscribed-notifications/subscriptions/subscription/stop-time`
- `/ietf-subscribed-notifications/subscriptions/subscription/dscp`
- `/ietf-subscribed-notifications/subscriptions/subscription/weighting`
- `/ietf-subscribed-notifications/subscriptions/subscription/dependency`
- `/ietf-subscribed-notifications/subscriptions/subscription/transport`
- `/ietf-subscribed-notifications/subscriptions/subscription/encoding`
- `/ietf-subscribed-notifications/subscriptions/subscription/purpose`
- `/ietf-subscribed-notifications/subscriptions/subscription/notification-message-origin`
- `/ietf-subscribed-notifications/subscriptions/subscription/configured-subscription-state`
- `/ietf-subscribed-notifications/subscriptions/subscription/receivers`

6.7.9.2.6.7 NETCONF monitoring

IA-stations shall support the ietf-netconf-monitoring YANG module according to IETF RFC 6022 with the following leaves:

Editor's note: The to be supported features and leaves have to be worked out.

6.7.9.2.6.8 System management

IA-stations shall support the ietf-system YANG module according to IETF RFC 7317 with the following leaves:

- `/ietf-system/system/contact`
- `/ietf-system/system/hostname`
- `/ietf-system/system/location`

6.7.9.2.6.9 Hardware management

IA-stations shall support the ietf-hardware YANG module according to IETF RFC 8348 with the following leaves:

- `/ietf-hardware/component/name`
- `/ietf-hardware/component/class`
- `/ietf-hardware/component/description`
- `/ietf-hardware/component/hardware-rev`
- `/ietf-hardware/component/software-rev`

- `/ietf-hardware/component/serial-num`
- `/ietf-hardware/component/mfg-name`
- `/ietf-hardware/component/model-name`

An IA-station shall provide exactly one /ietf-hardware/component with class “chassis” and may provide further components with other classes.

The following leaves of the “chassis” component shall be used for verifiable IA-station identity (see 6.3.3.2.2):

- `/ietf-hardware/component/description`
- `/ietf-hardware/component/hardware-rev`
- `/ietf-hardware/component/serial-num`
- `/ietf-hardware/component/mfg-name`
- `/ietf-hardware/component/model-name`

6.7.9.2.6.10 Interface management

IA-stations shall support the ietf-interfaces YANG module according to IETF RFC 8343 with the following leaves:

- `/ietf-interfaces/interface/name`
- `/ietf-interfaces/interface/description`
- `/ietf-interfaces/interface/type`
- `/ietf-interfaces/interface/enabled`
- `/ietf-interfaces/interface/oper-status`
- `/ietf-interfaces/interface/phys-address`
- `/ietf-interfaces/interface/higher-layer-if`
- `/ietf-interfaces/interface/lower-layer-if`
- `/ietf-interfaces/interface/speed`
- `/ietf-interfaces/interface/statistics/discontinuity-time`
- `/ietf-interfaces/interface/statistics/in-octets`
- `/ietf-interfaces/interface/statistics/in-discards`
- `/ietf-interfaces/interface/statistics/in-errors`
- `/ietf-interfaces/interface/statistics/out-octets`
- `/ietf-interfaces/interface/statistics/out-discards`
- `/ietf-interfaces/interface/statistics/out-errors`

6.7.9.2.6.11 Bridge component

IA-stations shall support the ieee802-dot1q-bridge YANG module according to IEEE Std 802.1Qcp-2018 as amended by IEEE P802.1Qcw with the following feature:

ingress-filtering

IA-stations shall support the ieee802-dot1q-bridge YANG module according to IEEE Std 802.1Qcp-2018 as amended by IEEE P802.1Qcw with the following leaves:

- `/ietf-interfaces/interface/bridge-port/bridge-name`

- /ietf-interfaces/interface/bridge-port/component-name
- /ietf-interfaces/interface/bridge-port/port-type
- /ietf-interfaces/interface/bridge-port/pvid
- /ietf-interfaces/interface/bridge-port/default-priority
- /ietf-interfaces/interface/bridge-port/traffic-class
- /ietf-interfaces/interface/bridge-port/statistics
- /ieee802-dot1q-bridge/bridges/bridge/name
- /ieee802-dot1q-bridge/bridges/bridge/address
- /ieee802-dot1q-bridge/bridges/bridge/bridge-type
- /ieee802-dot1q-bridge/bridges/bridge/ports
- /ieee802-dot1q-bridge/bridges/bridge/components
- /ieee802-dot1q-bridge/bridges/bridge/component/name
- /ieee802-dot1q-bridge/bridges/bridge/component/id
- /ieee802-dot1q-bridge/bridges/bridge/component/type
- /ieee802-dot1q-bridge/bridges/bridge/component/traffic-class-enabled
- /ieee802-dot1q-bridge/bridges/bridge/component/ports
- /ieee802-dot1q-bridge/bridges/bridge/component/bridge-port
- /ieee802-dot1q-bridge/bridges/bridge/component/capabilities
- /ieee802-dot1q-bridge/bridges/bridge/component/filtering-database
- /ieee802-dot1q-bridge/bridges/bridge/component/permanent-database
- /ieee802-dot1q-bridge/bridges/bridge/component/bridge-vlan
- /ieee802-dot1q-bridge/bridges/bridge/component/bridge-mst
- /ieee802-dot1q-bridge/bridges/bridge/component/capabilities/extended-filtering
- /ieee802-dot1q-bridge/bridges/bridge/component/capabilities/traffic-classes
- /ieee802-dot1q-bridge/bridges/bridge/component/capabilities/static-entry-individual-port
- /ieee802-dot1q-bridge/bridges/bridge/component/capabilities/ivl-capable
- /ieee802-dot1q-bridge/bridges/bridge/component/capabilities/svl-capable
- /ieee802-dot1q-bridge/bridges/bridge/component/capabilities/hybrid-capable
- /ieee802-dot1q-bridge/bridges/bridge/component/capabilities/configurable-pvid-tagging
- /ieee802-dot1q-bridge/bridges/bridge/component/capabilities/local-vlan-capable
- /ieee802-dot1q-bridge/bridges/bridge/component/filtering-database/aging-time
- /ieee802-dot1q-bridge/bridges/bridge/component/filtering-database/size

- `/ieee802-dot1q-bridge/bridges/bridge/component/filtering-database/static-entries`
- `/ieee802-dot1q-bridge/bridges/bridge/component/filtering-database/dynamic-entries`
- `/ieee802-dot1q-bridge/bridges/bridge/component/filtering-database/static-vlan-registration-entries`
- `/ieee802-dot1q-bridge/bridges/bridge/component/filtering-database/dynamic-vlan-registration-entries`
- `/ieee802-dot1q-bridge/bridges/bridge/component/filtering-database/mac-address-registration-entries`
- `/ieee802-dot1q-bridge/bridges/bridge/component/filtering-database/filtering-entry`
- `/ieee802-dot1q-bridge/bridges/bridge/component/filtering-database/vlan-registration-entry`
- `/ieee802-dot1q-bridge/bridges/bridge/component/permanent-database/size`
- `/ieee802-dot1q-bridge/bridges/bridge/component/permanent-database/static-entries`
- `/ieee802-dot1q-bridge/bridges/bridge/component/permanent-database/static-vlan-registration-entries`
- `/ieee802-dot1q-bridge/bridges/bridge/component/permanent-database/filtering-entry`
- `/ieee802-dot1q-bridge/bridges/bridge/component/bridge-vlan/version`
- `/ieee802-dot1q-bridge/bridges/bridge/component/bridge-vlan/max-vids`
- `/ieee802-dot1q-bridge/bridges/bridge/component/bridge-vlan/override-default-pvid`
- `/ieee802-dot1q-bridge/bridges/bridge/component/bridge-vlan/max-msti`
- `/ieee802-dot1q-bridge/bridges/bridge/component/bridge-vlan/vlan`
- `/ieee802-dot1q-bridge/bridges/bridge/component/bridge-vlan/vid-to-fid-allocation`
- `/ieee802-dot1q-bridge/bridges/bridge/component/bridge-vlan/fid-to-vid-allocation`
- `/ieee802-dot1q-bridge/bridges/bridge/component/bridge-vlan/vid-to-fid`
- `/ieee802-dot1q-bridge/bridges/bridge/component/bridge-mst/mstid`
- `/ieee802-dot1q-bridge/bridges/bridge/component/bridge-mst/fid-to-mstid`
- `/ieee802-dot1q-bridge/bridges/bridge/component/bridge-mst/fid-to-mstid-allocation`

6.7.9.2.6.12 IEC/IEEE 60802 YANG module

IA-stations with CNC functionality shall support the iecieee60802 YANG module according to this document with the following features:

- cnc

IA-stations with CUC functionality shall support the iecieee60802 YANG module according to this document with the following features:

- cuc

IA-stations shall support the iecieee60802 YANG module according to this document with the following nodes:

Editor's note: The required nodes are to be defined.

6.7.9.2.6.13 NETCONF Client

IA-stations with CNC and/or CUC functionality shall support the ietf-netconf-client YANG module according to draft-ietf-netconf-client-server with the following features:

- tls-initiate
- tls-listen
- central-netconf-client-supported

IA-stations with CNC and/or CUC functionality shall support the ietf-netconf-client YANG module according to draft-ietf-netconf-client-server with the following nodes:

- `/ietf-netconf-client/netconf-client/listen/idle-timeout`
- `/ietf-netconf-client/netconf-client/listen/endpoint/transport/tls/tls-client-parameters`
- `/ietf-netconf-client/netconf-client/initiate/netconf-server/name`
- `/ietf-netconf-client/netconf-client/initiate/netconf-server/endpoints/endpoint/name`
- `/ietf-netconf-client/netconf-client/initiate/netconf-server/endpoints/endpoint/transport/tls/tls-client-parameters`

6.7.9.2.6.14 NETCONF Server

IA-stations shall support the ietf-netconf-server YANG module according to draft-ietf-netconf-client-server with the following features:

- tls-call-home
- central-netconf-server-supported

IA-stations shall support the ietf-netconf-server YANG module according to draft-ietf-netconf-client-server with the following nodes:

- `/ietf-netconf-server/netconf-server/listen/idle-timeout`
- `/ietf-netconf-server/netconf-server/listen/endpoint/name`
- `/ietf-netconf-server/netconf-server/listen/endpoint/transport/tls/netconf-server-parameters`
- `/ietf-netconf-server/netconf-server/listen/endpoint/transport/tls/tls-server-parameters`
- `/ietf-netconf-server/netconf-server/call-home/netconf-client/name`
- `/ietf-netconf-server/netconf-server/call-home/netconf-client/endpoints/endpoint/name`
- `/ietf-netconf-server/netconf-server/call-home/netconf-client/endpoints/endpoint/transport/tls/netconf-server-parameters`
- `/ietf-netconf-server/netconf-server/call-home/netconf-client/endpoints/endpoint/transport/tls/tls-server-parameters`

6.7.9.2.7 YANG Module for TSN UNI

IA-stations with CNC functionality shall support the ieee802-dot1q-tsn-config-uni YANG module according to P802.1Qdj with the following nodes:

– /ieee802-dot1q-tsn-config/tsn-uni

6.7.9.3 Optional YANG models, features and leaves

6.7.9.3.1 General

The following YANG modules, features and leaves shall be supported by IA-stations if the base functionality they describe is included.

6.7.9.3.2 Scheduled traffic

IA-stations supporting the enhancements for scheduled traffic shall support the ieee802-dot1q-sched YANG module according to IEEE P802.1Qcw with the following feature:

scheduled-traffic

IA-stations supporting the enhancements for scheduled traffic shall support the ieee802-dot1q-sched YANG module according to IEEE P802.1Qcw with the following leaves:

- `ietf-interfaces/interface/bridge-port/gate-parameter-table/queue-max-sdu-table`
- `ietf-interfaces/interface/bridge-port/gate-parameter-table/gate-enabled`
- `ietf-interfaces/interface/bridge-port/gate-parameter-table/admin-gate-states`
- `ietf-interfaces/interface/bridge-port/gate-parameter-table/oper-gate-states`
- `ietf-interfaces/interface/bridge-port/gate-parameter-table/admin-control-list`
- `ietf-interfaces/interface/bridge-port/gate-parameter-table/oper-control-list`
- `ietf-interfaces/interface/bridge-port/gate-parameter-table/admin-cycle-time`
- `ietf-interfaces/interface/bridge-port/gate-parameter-table/oper-cycle-time`
- `ietf-interfaces/interface/bridge-port/gate-parameter-table/admin-cycle-time-extension`
- `ietf-interfaces/interface/bridge-port/gate-parameter-table/oper-cycle-time-extension`
- `ietf-interfaces/interface/bridge-port/gate-parameter-table/admin-base-time`
- `ietf-interfaces/interface/bridge-port/gate-parameter-table/oper-base-time`
- `ietf-interfaces/interface/bridge-port/gate-parameter-table/config-change`
- `ietf-interfaces/interface/bridge-port/gate-parameter-table/config-change-time`
- `ietf-interfaces/interface/bridge-port/gate-parameter-table/tick-granularity`
- `ietf-interfaces/interface/bridge-port/gate-parameter-table/current-time`

- `ietf-interfaces/interface/bridge-port/gate-parameter-table/config-pending`
- `ietf-interfaces/interface/bridge-port/gate-parameter-table/config-change-error`
- `ietf-interfaces/interface/bridge-port/gate-parameter-table/supported-list-max`
- `ietf-interfaces/interface/bridge-port/gate-parameter-table/supported-cycle-max`
- `ietf-interfaces/interface/bridge-port/gate-parameter-table/supported-interval-max`

6.7.9.3.3 Frame preemption

IA-stations supporting frame preemption according to IEEE Std 802.1Q-2018, 5.4.1 ad), shall support the ieee802-dot1q-preemption YANG module according to IEEE P802.1Qcw with the following feature:

frame-preemption

IA-stations supporting frame preemption according to IEEE Std 802.1Q-2018, 5.4.1 ad), shall support the ieee802-dot1q-preemption YANG module according to IEEE P802.1Qcw with the following leaves:

- `/ietf-interfaces/interface/bridge-port/frame-preemption-parameters/frame-preemption-status-table`
- `/ietf-interfaces/interface/bridge-port/frame-preemption-parameters/preemption-active`

6.7.9.3.4 Credit-based shaper

Editor's note: This YANG module is currently undefined.

6.8 Topology discovery and verification

6.8.1 Topology discovery and verification requirements

Electrical engineering of machines with multiple IA-stations includes the definition of the machine internal network topology (i.e., the engineered topology).

The machine internal network topology includes type specific data of IA-stations (for example model name or manufacturer name) as well as instance specific data (for example IP addresses or DNS names).

The electrical engineering data of the network topology is used:

- During commissioning to ensure that machine planning and installation are identical.
- By the TDE during operation to verify that the actual topology of the Configuration Domain matches the engineered topology.
- By maintenance staff during repair to easily identify failed IA-stations, ports, or links to be replaced.

Repair and replacement of an IA-station does not require verification for the updated engineered topology. Otherwise, the TDE produces a verification error.

IA-stations do not need to be pre-configured when they are repaired or replaced. IA-stations report type and instance data as described in 6.8.3.

6.8.2 Topology discovery overview

6.8.2.1 General

LLDP enables the discovery of IA-stations, their external ports, and their external connectivity. A Topology Discovery Entity can query LLDP data by remote management to derive the physical network topology.

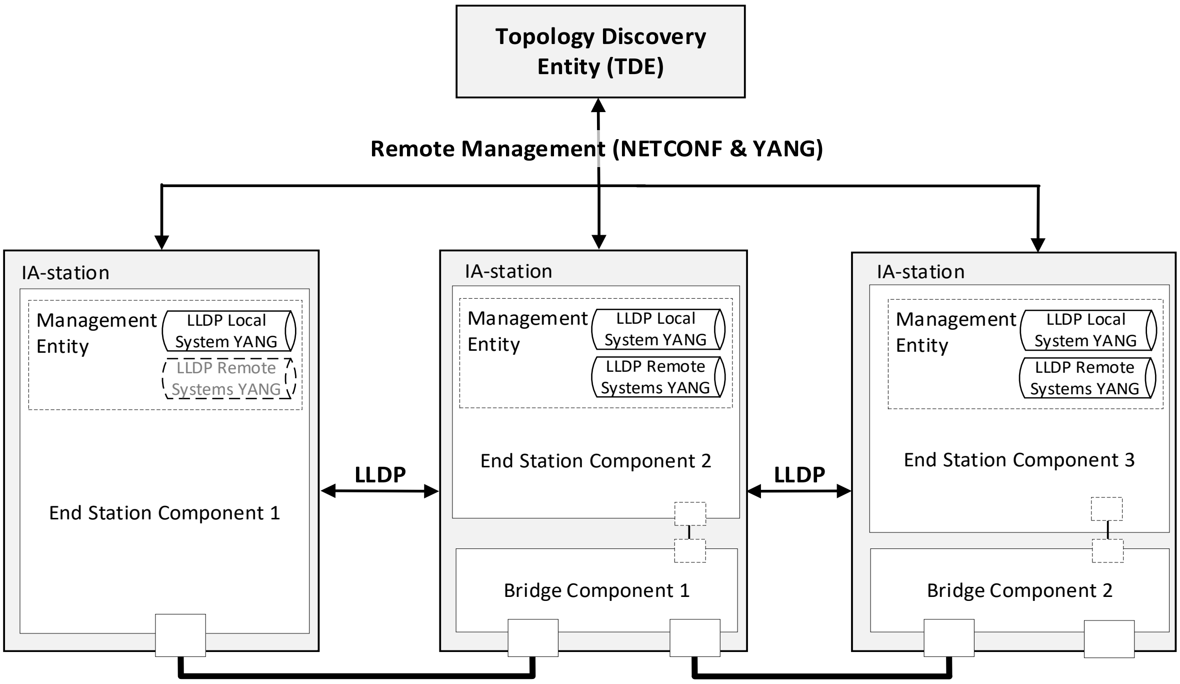


Figure 33 – Usage example of LLDP

Figure 33 illustrates a network showing the LLDP agent implementations in an IA-station consisting of a single end station component and two IA-stations with end station and Bridge components (see 4.3). The LLDP protocol is used to convey neighborhood information among peers, and NETCONF is used between the TDE and the IA-stations to query this neighborhood information from the IA-stations. This information allows the TDE to discover IA-stations and the physical network topology.

NOTE A Topology Discovery Entity (TDE) can be run from anywhere in the network with reachability to the to-be-discovered devices.

IA-stations announce themselves via LLDP to support discovery by the TDE. Announcements contain the management address (see 6.8.2.4.6) and system capabilities (see 6.8.2.4.5) for the discovery operation. The announced system capabilities information enables the TDE to identify IA-stations with multiple end station and Bridge components. The TDE can use the definitions in 6.7.3 for the discovery of the internal structure of such IA-stations.

To allow for adaptability of the operational behavior and exchanged information, IA-stations support the local system YANG (see 6.7.9.2.3). IA-stations that include a Bridge component additionally support the processing of received LLDP messages and support the remote systems YANG (see 6.7.9.2.3).

6.8.2.2 LLDP operational control parameters

LLDP defines several operational parameters that control the protocol behavior (see IEEE Std 802.1AB-2016, 10.5.1). These parameter definitions apply to all external ports of an IA-station.

NOTE According to IEEE Std 802.1AB-2016, 9.1.1 c), changes to the local system that impact information exchanged via LLDP immediately trigger the transmission of an LLDPDU to communicate the local changes as quickly as possible to any neighboring systems.

An IA-station shall support LLDP transmit mode (adminStatus enabledTxOnly) on an external end station component port and may support transmit and receive mode (adminStatus enabledRxTx) on that port (see IEEE Std 802.1AB-2016, 10.5.1).

An IA-station shall support LLDP transmit and receive mode (adminStatus enabledRxTx) on an external Bridge component port (see IEEE Std 802.1AB-2016, 10.5.1).

6.8.2.3 LLDPDU transmission, reception, and addressing

The destination address to be used for LLDPDU transmission (dest-mac-address) shall be the nearest bridge group MAC address, i.e., 01-80-C2-00-00-0E, on all ports to limit the scope of LLDPDU propagation to a single physical link (see IEEE Std 802.1AB-2016, 7.1 item a).

NOTE IEEE Std 802.1AB-2016 defines LLDPDUs to be transmitted untagged, i.e., frames do not carry priority information for traffic class selection. At the same time, IEEE Std 802.1AB-2016 neither specifies a well-defined device-internal priority nor management capabilities for the configuration of the traffic class to be used for the transmission of LLDPDUs. It is the user’s responsibility to ensure that LLDPDUs do not interfere with the transmission of time-critical control data.

6.8.2.4 LLDP TLV selection

6.8.2.4.1 General

An IA-station transmitting LLDPDUs shall include the LLDP TLVs selected in 6.8.2.4 and may include additional TLVs (tlvs-tx-enable). An IA-station receiving LLDPDUs shall process LLDPDUs.

Each LLDPDU shall contain the following LLDP TLVs specified in IEEE Std 802.1AB-2016, 8.5:

- Exactly one Chassis ID TLV according to 6.8.2.4.2,
- Exactly one Port ID TLV according to 6.8.2.4.3,
- Exactly one Time To Live TLV according to 6.8.2.4.4,
- Exactly one System Capabilities TLV according to 6.8.2.4.5, and
- One or more Management Address TLVs according to 6.8.2.4.6.

NOTE The concatenation of the Chassis ID and Port ID fields enables the recipient of an LLDPDU to identify the sending LLDP agent/port.

6.8.2.4.2 Chassis ID TLV

The Chassis ID field shall contain the same value for all transmitted LLDPDUs independent from the transmitting port of the IA-station, i.e., be a non-volatile identifier which is unique within the context of the administrative domain.

The Chassis ID subtype field (chassis-id-subtype) should contain subtype 4, indicating that the Chassis ID field (chassis-id) contains a MAC address to achieve the Chassis ID's desired uniqueness. For IA-stations with multiple unique MAC addresses, any one of the IA-station’s MAC addresses may be used and shall be the same for all external ports of that IA-station.

6.8.2.4.3 Port ID TLV

The Port ID field shall contain the same value for all transmitted LLDPDUs for a given external port, i.e., be a non-volatile, IA-station-unique identifier of the LLDPDU-transmitting port.

The Port ID subtype field (port-id-subtype) should contain subtype 5, indicating that the Port ID field contains the port interface name (name) according to IETF RFC 8343.

IA-stations should restrict the system-defined port interfaces to read-only access and a maximum name length of 255 characters. The names should match the imprinted port names on the chassis.

6.8.2.4.4 Time To Live TLV

The Time To Live value shall be set according to IEEE Std 802.1AB-2016, 8.5.4 (message-tx-interval * message-tx-hold-multiplier + 1).

Editor's note: The default value specified in IEEE 802.1AB-2016 is 30*4+1=121s

6.8.2.4.5 System capabilities TLV

An IA-station consisting of a single end station component shall set the system capabilities and enabled capabilities fields (system-capabilities-supported, system-capabilities-enabled) to Station Only (i.e., bit 8 set to 1) for all transmitted LLDPDUs.

An IA-station consisting of at least one End Station Component and at least one Bridge Component shall set the system capabilities and enabled capabilities fields to Station Only (i.e., bit 8 set to “1”) and C-VLAN component (i.e., bit 9 set to “1”) for all transmitted LLDPDUs.

NOTE The combination of the Station Only and C-VLAN component flags is used as a marker indicating to the TDE that the internal structure of the IA-station consists of multiple components. This is a deliberate deviation from IEEE Std 802.1AB-2016, Table 8-4, which states in a footnote: "The Station Only capability is intended for devices that implement only an end station capability, and for which none of the other capabilities in the table apply. Bit 8 should therefore not be set in conjunction with any other bits."

6.8.2.4.6 Management address TLV

An IA-station shall announce at least one IPv4 address by which its Management entity (see 4.3) can be reached (management-address-tx-port).

6.8.2.5 LLDP remote systems data

An IA-station supporting the remote systems YANG shall be able to store information from at least one neighbor per external port.

Receiving LLDPDUs from more neighbors than supported on a given port shall result in the last one received being saved to the remote systems YANG as described in IEEE Std 802.1AB-2016, 9.2.7.7.5.

6.8.3 Topology verification overview

Topology verification checks discovered topologies against engineered topologies. Topology verification data includes for every IA-station:

- model name,
- manufacturer name,
- management address.

Topology verification data includes for every external port of an IA-station:

- port name,
- remote connection (i.e., management address and port name of connected IA-station).

To support topology verification IA-stations shall support LLDP YANG data as defined in 6.7.9.2.3 and Hardware Management YANG data as defined in 6.7.9.2.6.9.

IA-station hardware instance specific data like MAC addresses or serial numbers are not considered for topology verification. This kind of data changes after a repair and replacement operation and thus, would induce a topology verification error.

6.9 CNC

6.9.1 General

Subclause 6.9 describes stream destination MAC address handling at the CNC.

6.9.2 Stream destination MAC address range

A CNC manages the destination MAC address for requested streams. This destination MAC address together with the VID identifies the path used for these streams. Thus, a stream destination MAC address needs to be unique together with the VID in a configuration domain.

Preferably, a CNC uses a contiguous address range for managing the stream addresses to support hardware optimization.

Figure 34 shows the possible selections of a CNC for a contiguous address range. The CNC selects an OUI and an offset of the address range for the stream destination MAC addresses.

An address range of 2048 stream destination MAC addresses allows together with a VID the usage of 2048 streams. Each additional VID used for streams allow additional 2048 streams.

EXAMPLE

CNC selected OUI := 00-80-C2

CNC selected address range := 0..2047

CNC selected VID := 101

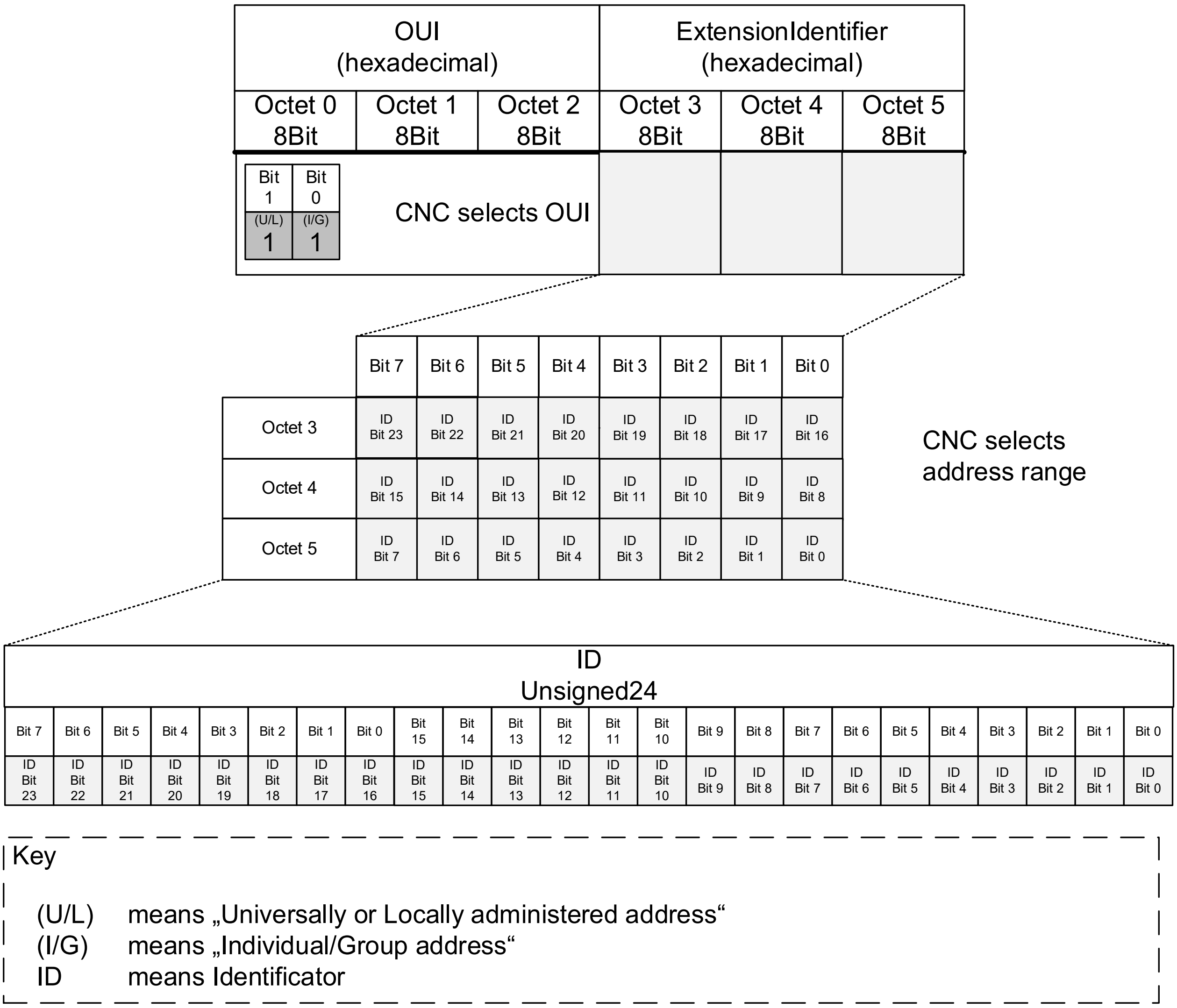


Figure 34 – Stream Destination MAC Address

Annex A
(normative)

PCS proforma – Time-sensitive networking profile for industrial automation

A.1 General

The supplier of an implementation that is claimed to conform to the profile specified in this document shall complete the corresponding Profile Conformance Statement (PCS) proforma, which is presented in a tabular format based on the format used for Protocol Implementation Conformance Statement (PICS) proformas.

The tables do not contain an exhaustive list of all requirements that are stated in the referenced standards; for example, if a row in a table asks whether the implementation is conformant to Standard X, and the answer “Yes” is chosen, then it is assumed that it is possible, for that implementation, to fill out the PCS proforma defined in Standard X to show that the implementation is conformant; however, the tables in this document will only further refine those elements of conformance to Standard X where particular answers are required for the profiles specified here.

A completed PCS proforma is the PCS for the implementation in question. The PCS is a statement of which capabilities and options of the protocol have been implemented. The PCS can have a number of uses, including use by the following:

c) Protocol implementer, as a checklist to reduce the risk of failure to conform to the document through oversight.

d) Supplier and acquirer, or potential acquirer, of the implementation, as a detailed indication of the capabilities of the implementation, stated relative to the common basis for understanding provided by the standard PCS proforma.

e) User, or potential user, of the implementation, as a basis for initially checking the possibility of interworking with another implementation.

NOTE While interworking can never be guaranteed, failure to interwork can often be predicted from incompatible PCS.

f) Protocol tester, as the basis for selecting appropriate tests against which to assess the claim for conformance of the implementation.

g) The user, to verify whether the IA-station, as described by the PCS, fulfills use-case requirements.

A.2 Abbreviations and special symbols

A.2.1 Status symbols

M: mandatory

O: optional

O.n: optional, but support of at least one of the group of options labeled by the same numeral n is required

X: prohibited

pred: conditional-item symbol, including predicate identification: see A.3.4

¬ logical negation, applied to a conditional item’s predicate

A.2.2 General abbreviations

N/A: not applicable

PCS: Profile Conformance Statement

A.3 Instructions for completing the PCS proforma

A.3.1 General structure of the PCS proforma

The first part of the PCS proforma, implementation identification and protocol summary, is to be completed as indicated with the information necessary to identify fully both the supplier and the implementation.

The main part of the PCS proforma is a fixed-format questionnaire, divided into several subclauses, each containing a number of individual items. Answers to the questionnaire items are to be provided in the rightmost column, either by simply marking an answer to indicate a restricted choice (usually Yes or No) or by entering a value or a set or range of values. There are some items where two or more choices from a set of possible answers can apply; all relevant choices are to be marked. Each item is identified by an item reference in the first column. The second column contains the question to be answered; the third column records the status of the item—whether support is mandatory, optional, or conditional; see also A.3.4. The fourth column contains the reference or references to the material that specifies the item in the main body of this document, and the fifth column provides the space for the answers.

The PCS indicates support of one of the conformance classes, ccA or ccB, specified in this profile.

A supplier may also provide (or be required to provide) further information, categorized as either Additional Information or Exception Information. When present, each kind of further information is to be provided in a further subclause of items labeled Ai or Xi, respectively, for cross-referencing purposes, where (i) is any unambiguous identification for the item (for example, simply a numeral). There are no other restrictions on its format and presentation.

A completed PCS proforma, including any Additional Information and Exception Information, is the Protocol Implementation Conformation Statement for the implementation in question.

NOTE Where an implementation is capable of being configured in more than one way, a single PCS may be able to describe all such configurations. However, the supplier has the choice of providing more than one PCS, each covering some subset of the implementation’s configuration capabilities, in case that makes for easier and clearer presentation of the information.

A.3.2 Additional information

Items of Additional Information allow a supplier to provide further information intended to assist the interpretation of the PCS. It is not intended or expected that a large quantity will be supplied, and a PCS can be considered complete without any such information. Examples might be an outline of the ways in which a (single) implementation can be set up to operate in a variety of environments and configurations, or information about aspects of the implementation that are outside the scope of this document but that have a bearing on the answers to some items.

References to items of Additional Information may be entered next to any answer in the questionnaire and may be included in items of Exception Information.

A.3.3 Exception information

It may occasionally happen that a supplier will wish to answer an item with mandatory status (after any conditions have been applied) in a way that conflicts with the indicated requirement. No preprinted answer will be found in the Support column for this item. Instead, the supplier shall write the missing answer into the Support column, together with an Xi reference to an item of Exception Information, and shall provide the appropriate rationale in the Exception item itself.

An implementation for which an Exception item is required in this way does not conform to this document.

NOTE A possible reason for the situation described previously is that a defect in this document has been reported, a correction for which is expected to change the requirement not met by the implementation.

A.3.4 Conditional status

A.3.4.1 Conditional items

The PCS proforma contains a number of conditional items. These are items for which both the applicability of the item itself, and its status if it does apply (mandatory or optional) are dependent on whether certain other items are supported.

Where a group of items is subject to the same condition for applicability, a separate preliminary question about the condition appears at the head of the group, with an instruction to skip to a later point in the questionnaire if the “Not Applicable” (N/A) answer is selected. Otherwise, individual conditional items are indicated by a conditional symbol in the Status column.

A conditional symbol is of the form “pred: S” where pred is a predicate as described in A.3.4.2, and S is a status symbol, M or O.

If the value of the predicate is true (see A.3.4.2), the conditional item is applicable, and its status is indicated by the status symbol following the predicate: The answer column is to be marked in the usual way. If the value of the predicate is false, the “Not Applicable” (N/A) answer is to be marked.

A.3.4.2 Predicates

A predicate is one of the following:

h) An item-reference for an item in the PCS proforma: The value of the predicate is true if the item is marked as supported and is false otherwise.

   1) A predicate-name, for a predicate defined as a Boolean expression constructed by combining item-references using the Boolean operator OR: The value of the predicate is true if one or more of the items is marked as supported.

   2) The logical negation symbol “¬” prefixed to an item-reference or predicate-name: The value of the predicate is true if the value of the predicate formed by omitting the “¬” symbol is false, and vice versa.

Each item whose reference is used in a predicate or predicate definition, or in a preliminary question for grouped conditional items, is indicated by an asterisk in the Item column.

A.3.4.3 References to other standards

The following shorthand notation is used in the References columns of the profile tables:

<standard abbreviation>:<Clause-number/sub-clause-number>

where standard abbreviation is one of the following:

Q: IEEE Std 802.1Q-2018

AS: IEEE Std 802.1AS-2020

Dot3: IEEE Std 802.3-2022

Hence, a reference to “IEEE Std 802.1Q-2018, 5.4.2” would be abbreviated to “Q:5.4.2”.

This profile refers to and selects from more standards than listed above. Thus, this list is incomplete. The list must be complete prior to CDV and SA ballot. It may be necessary to develop a different reference scheme for reference to RFCs.

A.3.5 Electronic datasheet

A provider of a device shall provide the PCS values in a standardized electronic format as data sheet of the product.

Editor’s note: A standard format for an electronic datasheet must be selected. YANG is one possibility.

A.4 Common requirements

A.4.1 Implementation identification

The entire PCS pro forma is a form that shall be filled out by a supplier according to Table A.1.

Table A.1 – Implementation identification template

Supplier	
Contact point for queries about the PCS	
Implementation Name(s) and Version(s)	
Other information necessary for full identification, for example, name(s) and version(s) of machines and/or operating system names	

Only the first three items are required for all implementations; other information may be completed as appropriate in meeting the requirement for full identification.

NOTE The terms "Name" and "Version" should be interpreted appropriately to correspond with a supplier's terminology (for example, Type, Series, Model).

A.4.2 Profile summary, IEC/IEEE 60802

Table A.2 shows the profile summary template.

Table A.2 – Profile summary template

Identification of profile specification	**IEC/IEEE 60802 - Time-Sensitive Networking Profile for Industrial Automation**			
Identification of amendments and corrigenda to the PCS proforma that have been completed as part of the PCS	Amd. Amd.	: :	Corr. Corr.	: :
Have any Exception items been required? (See A.3.3: the answer "Yes" means that the implementation does not conform to IEC/IEEE 60802)	No	[ ]	Yes	[ ]
Date of Statement				

A.4.3 Implementation type

The form in Table A.3 is used to indicate the type of system that the PCS describes.

Table A.3 – Implementation type template

Item	Feature	Status	References	Support	
BGE	Does the IA-station contain a Bridge component?	O.1		Yes [ ]	No [ ]
TLK	Does the IA-station contain an end station component?	O.1		Yes [ ]	No [ ]

NOTE A single IA-station can incorporate the functionality of one or more of the functions listed in this table. For example, an IA-station could have both an end station component and a Bridge component.

Editor's note: Further definition of the PCS Proforma will be deferred pending agreement on requirements for conformance classes. The PCS Proforma will be completed prior to Sponsor Ballot.

Annex B
(informative)

Representative Configuration Domain

The quantities listed are examples and may not be consistent with the profile as requirements evolve. The examples outlined in Annex B will be reconciled to the requirements in the draft prior to CDV/SA Ballot.

The following quantities are representative of what could be supported in a single Configuration Domain:

IA-stations: 1 024

Network diameter: 64

Streams per IA-Controller for IA-Controller to IA-device (C2D) communication:

- 512 Talker and >= 512 Listener streams.
- 1 024 Talker and >= 1 024 Listener streams in case of seamless redundancy.

Streams per IA-Controller for IA-Controller to IA-Controller (C2C) communication:

- 64 Talker and >= 64 Listener streams.
- 128 Talker and >= 128 Listener streams in case of seamless redundancy.

Streams per IA-device for IA-device-to-IA-device (D2D) communication:

- 2 Talker and 2 Listener streams.
- 4 Talker and 4 Listener streams in case of seamless redundancy.

Example calculation of data flow quantities for eight PLCs – without seamless redundancy:

- 8 x 512 x 2 = 8 192 streams for C2D communication, plus
- 8 x 64 x 2 = 1 024 streams for C2C communication
- (8 192 + 1 024) * 2 000 = 18 432 000 Bytes data of all streams

Annex C
(informative)

Error model

C.1 General

Synchronization needs to handle the whole path, from the Grandmaster PTP Instance to the PTP End Instance, through the intermediate PTP Relay Instances.

All time errors, cTE and dTE, are accumulated during this process.

Time error can arise in the following processes:

a) the transporting of time in a PTP Instance and via PTP Links that connect PTP Instances,

b) the providing of time to the Grandmaster PTP Instance, from the ClockSource entity via the ClockMaster entity, and

c) the providing of time to a ClockTarget entity (end application) via the ClockSlave entity.

NOTE Item a) includes time error introduced in a PTP End Instance between the slave port and the ClockSlave entity, and between the ClockMaster entity and a master port.

C.2 Time error components due to relaying of time

Both the PTP Instances and the gPTP communication paths contribute to time error. The error components are either cTE (for example static link delay error due to asymmetry, PHY delay error) or dTE (for example, LocalClock phase noise, timestamp error due to timestamp granularity, timestamp error due to error in reading the timestamping clock when the timestamp is taken).

cTE is either positive or negative. cTE components at different PTP Instances or PTP Links might have different signs and thus cancel each other in full or in part; however, in the worst case the cTE components would have the same sign and add linearly. The distribution of dTE is generally assumed to be either Gaussian (for clock phase noise) or uniform (for timestamp granularity). The combination of cTE and dTE accumulation via a PTP chain is limited, as shown below, to avoid $\max|TE_R|$ exceeding the respective limit (see 6.2.5 and 6.2.6).

The requirements for cTE are:

- for a PTP Link, cTE shall be in the range of -10 ns to +10 ns
- for a PTP Instance cTE shall be in the range of -5 ns to +5 ns

The requirements for dTE are:

- For a PTP Link, dTE is assumed to be zero.
- For a PTP Instance, dTE shall be in the range of -50 ns to +50 ns.

Editor's note: It must be verified via simulation that this requirement on dTE can be met with non-zero timestamp granularity, non-zero dynamic timestamp error, and clock stability. The simulations will either be described in an informative annex or referenced informatively in the Bibliography. Note that these simulations are separate from the simulations that verify time error performance over multiple (for example, 64 or 100) hops; these simulations are for a single PTP Instance. An informative annex that describes how dTE for a single PTP Instance is measured will be added.

Editor's note: Simulations to date have produced a significantly smaller budget for cTE than is specified above (see: https://www.ieee802.org/1/files/public/docs2021/60802-garner-further-analysis-of-cTE-budgeting-based-on-mult-replic-dTE-simul-0621-v01.pdf)

Editor's note: The prescribed values for cTE and dTE may be difficult to meet due to the sampling error of the gPTP timestamp (see: http://www.ieee802.org/1/files/public/docs2020/60802-Rodrigues-Sampling-error-of-gPTP-timestamp-04-20-v00.pdf)

C.3 Time error components due to providing time to the Grandmaster or to an end application

Both the Grandmaster PTP Instance and the PTP Instance that provides timing to the end application contribute to time error. The error components are either cTE (for example, due to uncompensated link asymmetry) or dTE.

For the transfer of time from the ClockSource entity to the ClockMaster entity, excluding the error introduced at the input to the ClockMaster entity:

- cTE shall be in the range of -10 ns to +10 ns.
- dTE shall be in the range -20 ns to +20 ns.

For the transfer of time from the ClockSlave entity of a PTP Instance that is not the Grandmaster PTP Instance, to the ClockTarget entity:

- cTE shall be in the range of -10 ns to +10 ns
- dTE shall be in the range -20 ns to +20 ns.

For an output synchronization signal (for example, 1 pulse per second (PPS) synchronized to the working clock as shown in Figure 14 and Figure 15) at any PTP Instance, used to measure the time error between the Grandmaster ClockSource and the ClockTarget of a PTP Instance that is not the Grandmaster, the additional error introduced by implementation of the output synchronization signal is expected to be in the range of -10 ns to +10 ns.

Annex D
(informative)

Description of Clock Control System

D.1 Introduction

This Annex provides an introductory discussion of a basic clock control system. For more detailed information, see the Bibliography References for this Annex.

Figure D.1 shows a basic control system model that uses a proportional plus integral (PI) controller. This is meant to be reference model, i.e., it is not meant to specify an implementation. Requirements for the clock control system can be expressed using parameters (e.g., 3dB bandwidth, gain peaking, frequency response) that are based on this reference model. Any implementation whose parameters are within the requirements is considered to be acceptable. For example, the model of Figure D.1 is expressed in the analog domain (i.e., s-domain), and will be shown shortly to be second order. An actual implementation can be digital, and can be higher order, as long as it meets the respective requirements.

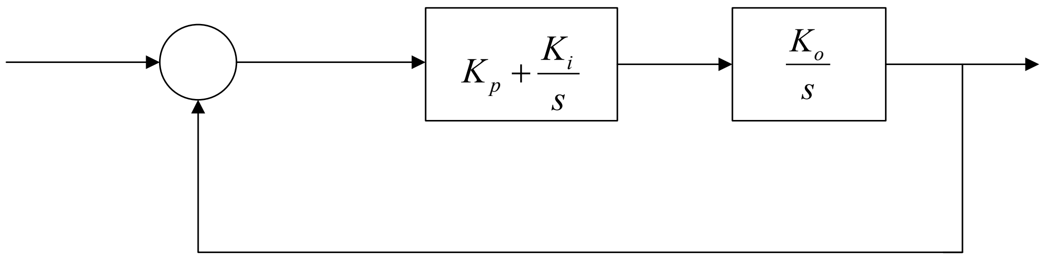


Figure D.1 – Reference model for clock control system

In Figure D.1, the plant, i.e., the entity being controlled, represents the clock oscillator. It is desired that the phase output, Y(t) of the oscillator follow the phase input, U(t), as closely as possible (the signals are shown in the frequency domain in Figure D.1; however, they can equivalently be expressed in the time domain, with t representing time). Because of this behavior, this control system is also referred to as a phase-locked loop (PLL). The parameter Ko is the oscillator gain; the oscillator frequency is equal to the oscillator input multiplied by Ko. In some implementations the input signal to the oscillator is a voltage, and the oscillator is referred to as a voltage-controlled oscillator (VCO). However, other implementations are possible, e.g., digital implementations, where the oscillator is a digital controlled oscillator (DCO). Since the input to the oscillator depends on the implementation, it is not labeled in Figure D.1.

The control system of Figure D.1 uses negative feedback to enable the phase output to follow the phase input. The phase detector computes the difference between the input and output signals to produce the error signal E(s). The error signal is then filtered by the PI filter to produce the input to the oscillator. The filter is referred to as a PI filter because its output is the sum of the proportional gain, Kp, multiplied by the error signal and the integral gain, Ki, multiplied by the integral of the error signal. The gains Ko, Kp, and Ki must be chosen such that the performance of the control system is acceptable, i.e., the time-domain behavior of the output with respect to the input is acceptable. However, an alternative set of parameters, which are more convenient, can be defined in terms of Ko, Kp, and Ki; this is done in the next section.

D.2 Transfer function for control system

From the block diagram of Figure D.1, the input and output are related by:

$$Y(s) = \left(K_p + \frac{K_i}{s}\right)\left(\frac{K_o}{s}\right)\left(U(s) - Y(s)\right) \tag{D.1}$$

or

$$Y(s) = \frac{\left(K_p + \frac{K_i}{s}\right)\left(\frac{K_o}{s}\right)}{1 + \left(K_p + \frac{K_i}{s}\right)\left(\frac{K_o}{s}\right)} U(s) \tag{D.2}$$

This can be simplified by multiplying the numerator and denominator by s^2 to produce:

$$Y(s) = H(s)U(s) \tag{D.3}$$

where the transfer function *H(s)* is given by:

$$H(s) = \frac{K_p K_o s + K_i K_o}{s^2 + K_p K_o s + K_i K_o} \tag{D.4}$$

In equation (D.4), the parameter K_o does not appear independently of K_p and K_i; rather, only the products K_pK_o and K_iK_o appear. The plant and PI filter could have been combined in the model of Figure D.1; this is consistent with the fact that the exact nature of the signal between the PI filter and plant is unimportant in this reference model. The units of K_pK_o are (time)$^{-1}$ and the units of K_iK_o are (time)$^{-2}$. The frequency units need to be the same as the units of *s*, e.g., if *s* has units rad/s, then K_pK_o has units rad/s and K_iK_o has units (rad/s)^2. The integration operation in the plant results in the transfer function being dimensionless, which is consistent with the fact that the input and output of the control system both have units of phase.

The transfer function can be expressed in an equivalent form by defining the undamped natural frequency, ω_n, and damping ratio, ζ:

$$H(s) = \frac{2\zeta\omega_n s + \omega_n^2}{s^2 + 2\zeta\omega_n s + \omega_n^2} \tag{D.5}$$

where

$$\omega_n = \sqrt{K_i K_o}$$
$$\varsigma = \frac{K_p K_o}{2\sqrt{K_i K_o}} = \frac{K_p}{2}\sqrt{\frac{K_i}{K_o}} \qquad \text{(D.6)}$$

In the equation for ζ, the first form shows explicitly that ζ depends only on the products $K_p K_o$ and $K_i K_o$.

D.3 Frequency response for control system

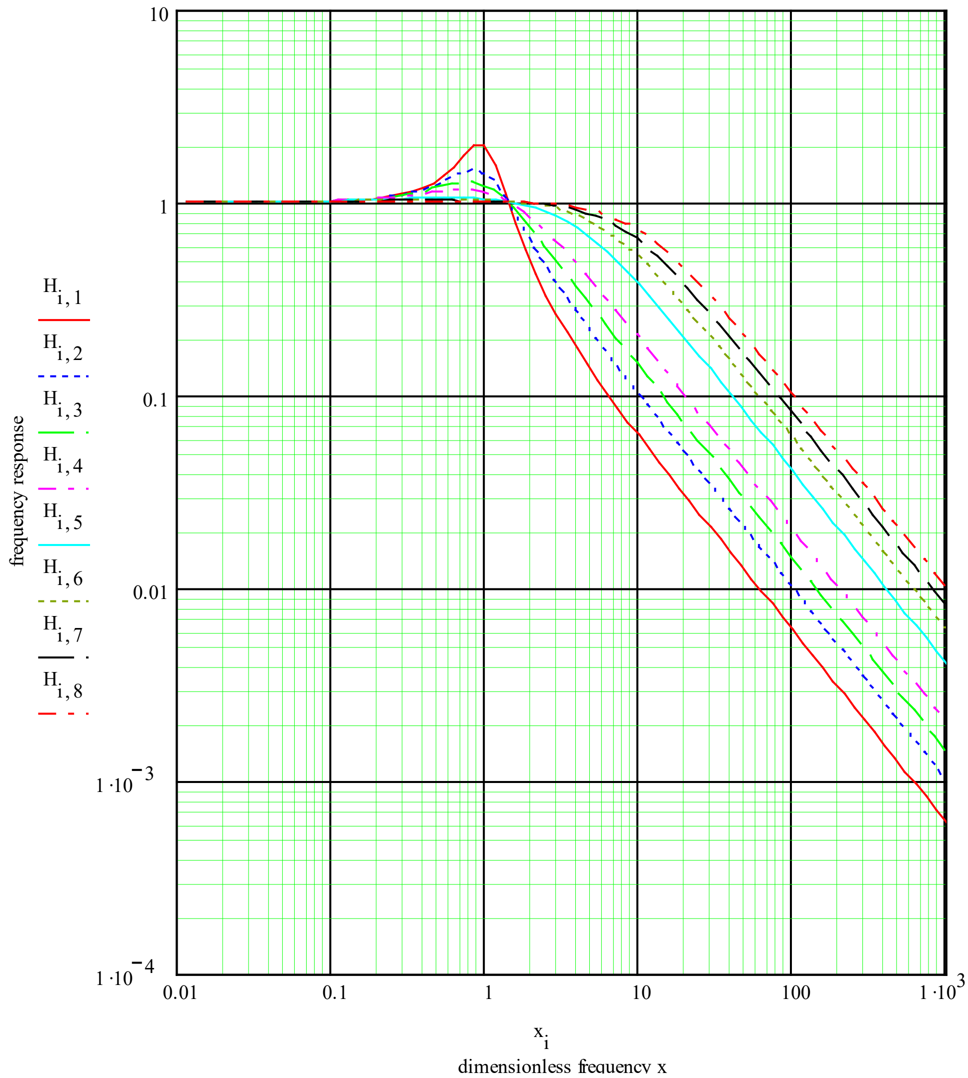
The frequency response is obtained by setting $s = j\omega$ in equation (D.5) and taking the absolute value (here j rather than i is used for $\sqrt{-1}$ to avoid confusion with other uses of i), where ω is the frequency in rad/s. The result is:

$$\left|H(j\omega)\right| = \left|\frac{2\varsigma\omega_n\omega j + \omega_n^2}{-\omega^2 + \omega_n^2 + 2\varsigma\omega_n\omega j}\right| = \left(\frac{4\varsigma^2\omega_n^2\omega^2 + \omega_n^4}{\left(\omega_n^2 - \omega^2\right)^2 + 4\varsigma^2\omega_n^2\omega^2}\right)^{1/2} \qquad \text{(D.7)}$$

Dividing the numerator and denominator of equation (D.7) by ω_n^4 and defining the dimensionless frequency $x = \omega/\omega_n$ produces:

$$\left|H(j\omega)\right| = \left(\frac{4\varsigma^2 x^2 + 1}{\left(1 - x^2\right)^2 + 4\varsigma^2 x^2}\right)^{1/2} \qquad \text{(D.8)}$$

Figure D.2 contains plots of frequency response (equation (D.8)) versus dimensionless frequency x, on a log-log scale, for damping ratio ζ equal to 0,3, 0,5, 0,707, 1,0, 2,0, 3,0, 4,0, and 5,0. It is seen that the frequency response is very close to 1 for values of dimensionless frequency much less than 1 (i.e., for $\omega \ll \omega_n$). The frequency response increases as the frequency approaches the undamped natural frequency (i.e., as dimensionless frequency approaches 1) and reaches a peak for dimensionless frequency slightly less than 1. The frequency response then decreases, eventually having a slope (i.e., roll-off) of 20 dB/decade (i.e., frequency response decreases by a factor of 10 for every factor of 10 increase in x for x >> 1). Figure D.3 shows the detail of frequency response for x in the range 0,1 to 10.



4258

4259 **Figure D.2 – Frequency response for the control system of Figure D.1, for damping ratio**
4260 **equal to 0,3, 0,5, 0,707, 1,0, 2,0, 3,0, 4,0, and 5,0**

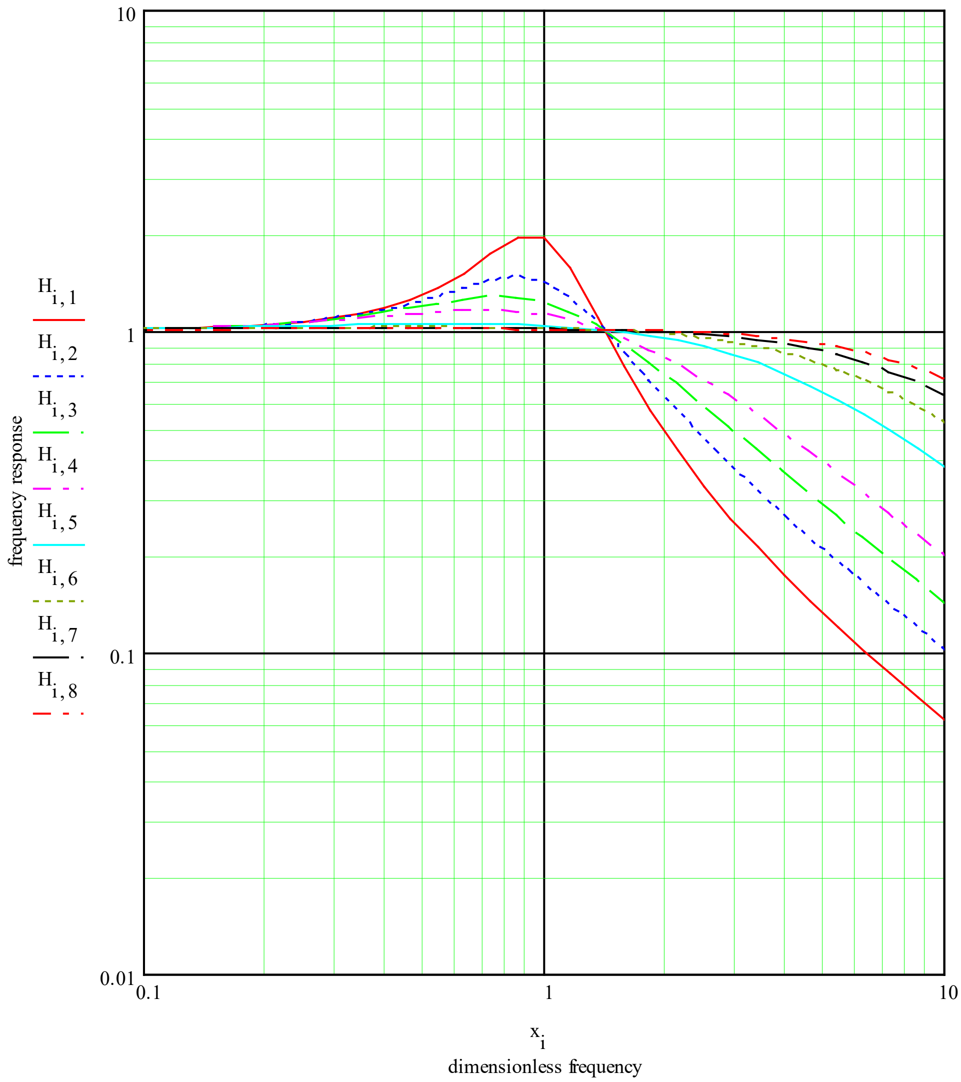


Figure D.3 – Detail of frequency response for the control system of Figure D.1 for dimensionless frequency in the range 0,1 to 10

In addition to undamped natural frequency ω_n and damping ratio ζ, the parameters 3dB bandwidth and gain peaking are often used when specifying clock performance. The 3dB bandwidth is defined as the value of frequency for which the frequency response is equal to –3dB. Since dB is given by 10 multiplied by the logarithm to base 10 of the power ratio, which is 20 multiplied by the logarithm to base 10 of the amplitude ratio, –3dB corresponds to the value $10^{-3/20}$. The 3dB bandwidth can be computed by setting equation (D.8) equal to $10^{-3/20}$ and solving for x in terms of ζ. This is equivalent to setting the quantity in parentheses (i.e., inside the square root) in equation (D.8) equal to $10^{-3/10}$ and solving for x. Now, $10^{-3/10}$ is approximately equal to 0,5012, i.e., it is very close to ½. Then the 3dB bandwidth can be obtained by solving the following equation for x in terms of ζ:

$$\frac{4\varsigma^2 x^2 + 1}{\left(1 - x^2\right)^2 + 4\varsigma^2 x^2} = \frac{1}{2} \qquad \text{(D.9)}$$

or

$$x^4 - 2\left(2\varsigma^2 + 1\right)x^2 - 1 = 0 \tag{D.10}$$

The result is:

$$x = \left[2\varsigma^2 + 1 + \sqrt{(2\varsigma^2 + 1)^2 + 1}\right]^{1/2} \tag{D.11}$$

or

$$\omega_{3\mathrm{dB}} = \omega_n \left[2\varsigma^2 + 1 + \sqrt{(2\varsigma^2 + 1)^2 + 1}\right]^{1/2} \tag{D.12}$$

The gain peaking is the maximum value of the frequency response, in dB. It is computed by differentiating equation (D.8) with respect to *x*, setting the result to zero, solving for *x*, and then substituting this value of *x* into equation (D.8) to obtain the maximum. The result is:

$$H_p = \left[1 - 2\alpha - 2\alpha^2 + 2\alpha\left(2\alpha + \alpha^2\right)^{1/2}\right]^{-1/2} \tag{D.13}$$

where α is related to damping ratio by:

$$\alpha = \frac{1}{4\varsigma^2} \tag{D.14}$$

and H_p is the gain peaking expressed as a pure fraction. The gain peaking in dB is equal to $20 \cdot \log_{10} H_p$. In some cases, it is necessary to compute damping ratio from gain peaking. The result for this is:

$$\alpha = \frac{(1-q)\left(1+\sqrt{1-q}\right)}{2q} \tag{D.15}$$

where

$$q = \frac{1}{H_p^2} \tag{D.16}$$

Damping ratio is obtained from α using equation (D.14).

If 3dB bandwidth and gain peaking are given, damping ratio can be obtained using equations (D.14) through (D.16). Undamped natural frequency can then be obtained using equation (D.12).

Figure D.4 shows gain peaking, expressed as a pure fraction, as a function of damping ratio. Figure D.5 shows gain peaking in dB as a function of damping ratio.

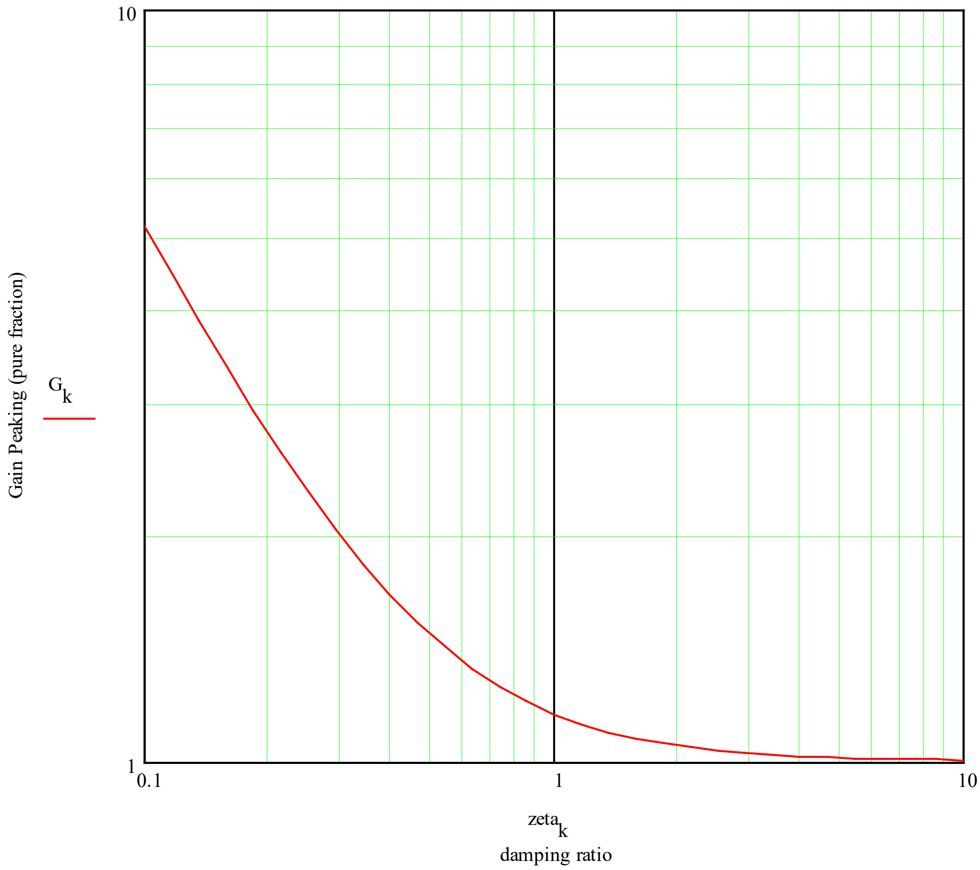


Figure D.4 – Gain peaking, expressed as a pure fraction, as a function of damping ratio

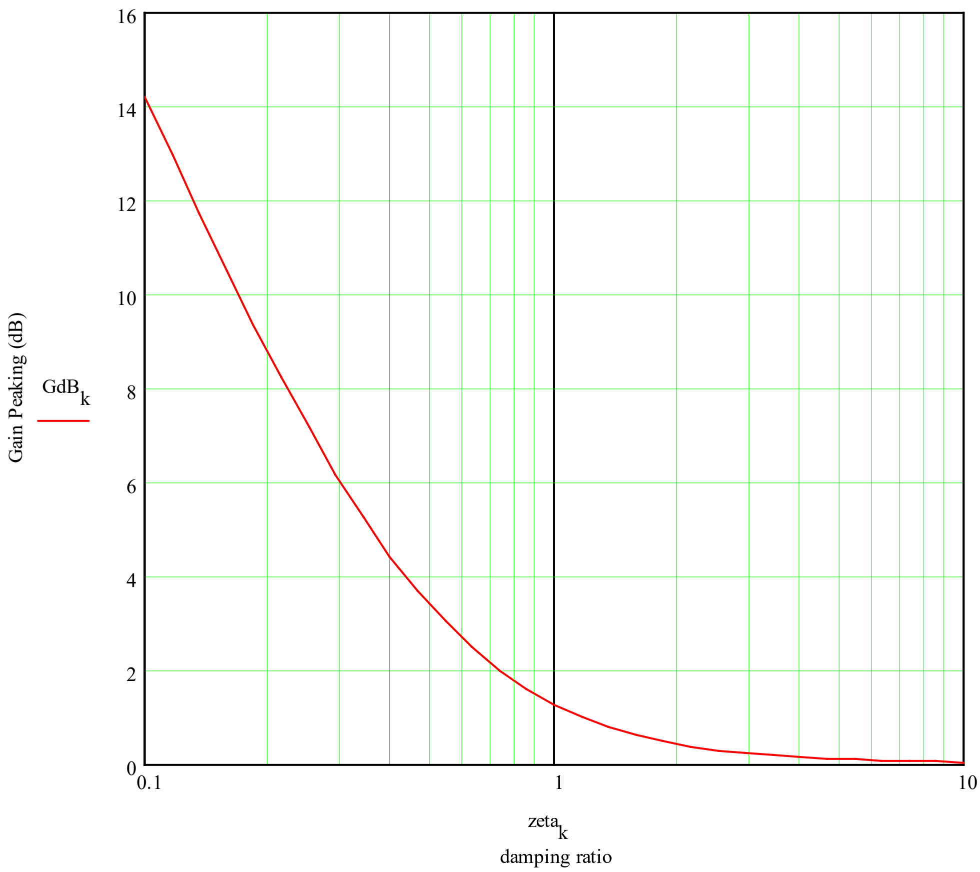


Figure D.5 – Gain peaking in dB as a function of damping ratio

The performance requirements for the clock can be specified using the frequency response. Specifically, the requirement can be stated as:

a) Maximum 3dB bandwidth in Hz,

b) Maximum gain peaking in dB, and

c) Frequency response plot (mask) corresponding to (a) and (b) that is not to be exceeded.

D.4 Example

[Editor's note: This example is based on the clock parameter values in use at the time the initial draft of this annex was prepared. If the values change as a result of later analyses or simulations, the example needs to be changed to reflect that.]

Consider a clock control system with K_pK_o = 11 rad/s and K_iK_o = 65 (rad/s)^2. The undamped natural frequency and damping ratio are:

$$\begin{aligned} \omega_n &= \sqrt{K_iK_o} = \sqrt{65\ (\text{rad/s})^2} = 8.06226\ \text{rad/s} \\ \varsigma &= \frac{K_pK_o}{2\sqrt{K_iK_o}} = \frac{11\ \text{rad/s}}{2\sqrt{65\ (\text{rad/s})^2}} = 0.68219 \end{aligned} \tag{D.17}$$

The gain peaking is obtained from:

$$\alpha = \frac{1}{4(0.68219)^2} = 0.53719$$

$$H_p \text{ (purefraction)} = \left[1 - 2(0.53719) - 2(0.53719)^2 + 2(0.53719)\sqrt{2(0.53719) + (0.53719)^2}\right]^{-1/2} = 1.28803 \quad \text{(D.18)}$$

$$H_p \text{ (dB)} = 20\log_{10}(1.28803) \text{ dB} = 2.1985 \text{ dB}$$

The 3dB bandwidth is:

$$\begin{aligned} f_{3\text{dB}} \text{ (Hz)} &= \frac{\omega_n}{2\pi}\left[1 + 2\varsigma^2 + \sqrt{\left(1 + 2\varsigma^2\right)^2 + 1}\right]^{1/2} \\ &= \frac{8.06226}{2\pi}\left[1 + 2\left(0.68219\right)^2 + \sqrt{\left(1 + 2\left(0.68219\right)^2\right)^2 + 1}\right]^{1/2} \\ &= 2.5998 \text{ Hz} \approx 2.6 \text{ Hz} \end{aligned} \quad \text{(D.19)}$$

The frequency response is shown in Figure D.6.

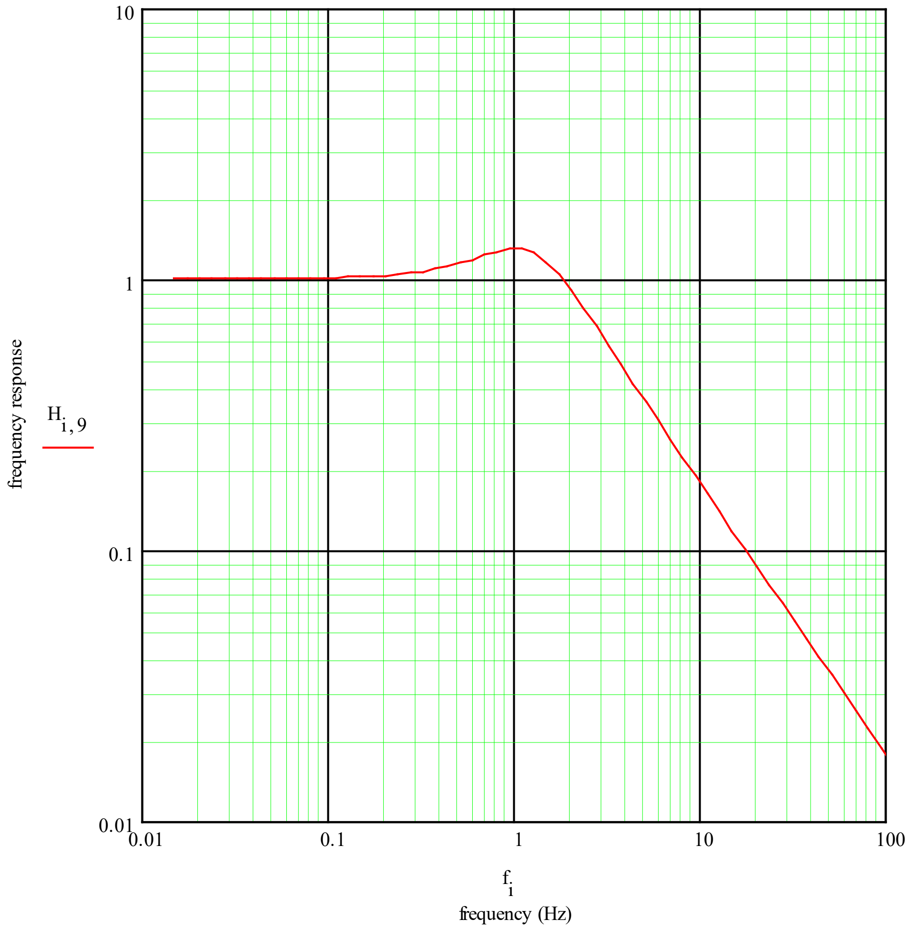


Figure D.6 – Example Frequency response

Annex Z
(informative)

Gaps

Z.1 Gaps for Release 1:

1) Security
   a) Device Identity (802.1AR) needs to be clarified, is there a secured device identity and an unsecured device identity? https://www.ieee802.org/1/files/public/docs2021/60802-Pfaff-et-al-Background-for-802-1AR-Adoption-1121-v01.pdf
      i) Second presentation coming
      ii) Is a self-signed certificate allowable?
   b) Device Discovery needs to include both identity and topology to secure a device.
   c) x509 v3 certificates- Identify and specify the extensions needed from a 60802 point of view. Which mandatory and optional fields are mandatory for 60802?
   d) UNI access model and access control (working w/ Qdj participants to address)
   e) Need to obtain an OID for 60802 extensions to x509 v3 certificates. This may be 802.1 centric if the requirements are common. Need to add a placeholder for the OID in the draft.

2) Time Sync
   a) Clock Status: 60802 needs to define a specific algorithm to determine when an IA-station is in-sync and not in-sync. A contribution is needed.
   b) The result of this algorithm needs to be available via management and hooks are needed in 802.1AS to allow state machines to make use of this algorithm which may differ from the corresponding algorithm in .1AS. Comments with proposed solutions to this effect are needed during ASdm balloting.
   c) 60802 YANG modules need to add management variables to report the state of ClockTarget and ClockSource.
   d) https://www.ieee802.org/1/files/public/docs2021/60802-Steindl-ClockTarget-and-ClockSource-1121-v05.pdf
   e) Gap analysis of YANG Module being defined in 802.1ASdn and 802.1ASdm.
   f) Parameter Selection for time sync through simulation and modeling https://www.ieee802.org/1/files/public/docs2021/60802-McCall-Stanton-Time-Sync-Error-Model-and-Analysis-2021-11-v02.pdf

3) Remote Management (e.g. Discovery)
   a) YANG model for .3 MAUTypes is a gap
   b) MSTP YANG Model is a gap
   c) NETCONF with multiple clients has an issue with locking.
   d) YANG module selection of optional parameters for alignment (Contribution from Martin)
   e) Trust/keystore YANG modules RFC will be finalized in 2022

4) Data Sheets
   a) IA-Device Description
      i) What parameters
      ii) Add Value Ranges

        iii) Add Quantities

    b) Add detail to Traffic Patterns (could this be deferred to Edition 2?)

    c) Complete YANG models augmented by missing quantities and value/range information needs to be able to be exported in a file. This includes for devices (IA-Device Description) and CNC’s (Traffic Patterns). Bring this question to YANGSTERS.

5) CNC

    a) Qdj terms and definitions

        i) gap analysis

        ii) UNI/YANG Module Definition

            1) Multiple NETCONF client concurrent connections

            2) Network Management Datastore Architecture

            3) Network Management Access Control

    b) Conformance Criteria for a CNC

Z.2 Topics for Edition 2:

- Securing 802.1AS-2020 operation is a known gap that will not be filled for 60802 R1. Security considerations, for example gPTP message security, is deffered; but, if implemented, then it should follow the IEEE1588-2019 message security model, or the new amendment being developed by IEEE 1588 WG (P1588d)
- Network Access Control? 802.1X? Auto-protection with 802.1Q based blocking? Isolate or deprioritize "untrusted" devices?
- MacSec? 802.1AE?
- distributed configuration
- Merging outputs from multiple CNC's into one running system
- Security: protection for discovering neighborhood relations
- Security: Security: protection for discovering neighborhood relations

Bibliography

1) Best, Roland E., Phase-Locked Loops, Design, Simulation, and Applications, Fifth Edition, 2003.
2) Gardner, Floyd M., Phaselock Techniques, Second Edition, 1979.
3) IEC 61784-2 (all parts), *Industrial networks - Profiles - Part 2: Additional real-time fieldbus profiles based on ISO/IEC/IEEE 8802-3*
4) IEEE Std 1588-2019, *IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems*
5) IEEE Std 802-2014, *IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture*
6) IETF RFC 4949, Shirey, R., *Internet Security Glossary, Version 2*, August 2007, available at https://www.rfc-editor.org/info/rfc4949
7) IETF RFC 5890, Klensin, J., *Internationalized Domain Names for Applications (IDNA): Definitions and Document Framework*, August 2010, available at https://www.rfc-editor.org/info/rfc5890
8) IETF RFC 5891, Klensin, J., *Internationalized Domain Names in Applications (IDNA): Protocol*, August 2010, available at https://www.rfc-editor.org/info/rfc5891
9) IETF RFC 8995, Pritikin, M., Richardson, M., Eckert, T., Behringer, M., and Watsen, K., *Bootstrapping Remote Secure Key Infrastructure (BRSKI)*, May 2021, available at https://www.rfc-editor.org/info/rfc8995
10) ITU-T Series G Supplement 65, Simulations of transport of time over packet networks, Geneva, October 2018.
11) Ogata, Katsuhiko, Modern Control Engineering, Second Edition, Prentice Hall, 1990.
12) Rogers, John, Plett, Calvin, Dai, Foster, Integrated Circuit Design for High-Speed Frequency Synthesis, Artech House, 2006.
13) Wolaver, Dan H., Phase-Locked Loop Circuit Design, Prentice Hall, 1991.