

Initial SA ballot of Draft 3.0 of the

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

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

NOTE – This page is not subject to ballot comments.

CONTENTS

3	FOREWORD.....	9
4	INTRODUCTION.....	11
5	1 Scope.....	12
6	2 Normative References	12
7	3 Terms, definitions, symbols, abbreviated terms and conventions	15
8	3.1 General.....	15
9	3.2 List of terms, abbreviated terms and definitions given in various standards.....	16
10	3.3 Terms defined in this document.....	18
11	3.4 Abbreviated terms and acronyms.....	19
12	3.5 Conventions.....	22
13	3.5.1 Convention for capitalizations.....	22
14	3.5.2 Unit conventions	22
15	3.5.3 Conventions for YANG contents	23
16	3.5.4 Conventions for YANG selection / Digital Data Sheet	23
17	4 Overview of TSN in industrial automation	23
18	4.1 Industrial application operation	23
19	4.2 Industrial applications	25
20	4.2.1 General	25
21	4.2.2 Control loop tasks	27
22	4.2.3 Start of control loop tasks.....	28
23	4.3 IA-stations	28
24	4.4 Ethernet interface.....	29
25	4.5 Mechanisms that can be used to meet control loop latency requirements.....	30
26	4.6 Translation between middleware and network provisioning.....	30
27	4.6.1 Interfaces of type I2vlan	30
28	4.6.2 PTP Instances	32
29	4.7 Industrial traffic types	33
30	4.7.1 General	33
31	4.7.2 Traffic type characteristics	33
32	4.7.3 Traffic type categories.....	34
33	4.7.4 Traffic types.....	35
34	4.8 Security for TSN-IA	37
35	4.8.1 General	37
36	4.8.2 Security configuration model	37
37	4.8.3 NETCONF/YANG processing.....	38
38	4.8.4 NETCONF/YANG access control	39
39	4.8.5 Identity checking	40
40	4.8.6 Secure device identity	40
41	5 Conformance	43
42	5.1 General.....	43
43	5.2 Requirements terminology	43
44	5.3 Profile conformance statement (PCS)	43
45	5.4 Conformance classes	43
46	5.5 IA-station requirements	44
47	5.5.1 IA-station PHY and MAC requirements for external ports	44

48	5.5.2	IA-station topology discovery requirements	45
49	5.5.3	IA-station requirements for time synchronization	45
50	5.5.4	IA-station requirements for management	46
51	5.6	IA-station options	47
52	5.6.1	IA-station PHY and MAC options for external ports	47
53	5.6.2	IA-station options for time synchronization	47
54	5.6.3	IA-station options for management	48
55	5.7	Bridge component requirements	48
56	5.7.1	Common Bridge component requirements	48
57	5.7.2	ccA Bridge component requirements	49
58	5.7.3	ccB Bridge component requirements	50
59	5.8	Bridge component options	50
60	5.8.1	Common Bridge component options	50
61	5.8.2	ccA Bridge component options	50
62	5.8.3	ccB Bridge component options	50
63	5.9	End station component requirements	51
64	5.9.1	Common end station Component requirements	51
65	5.9.2	ccA end station component requirements	51
66	5.9.3	ccB end station component requirements	52
67	5.10	End station component options	52
68	5.10.1	Common end station component options	52
69	5.10.2	ccA end station component options	52
70	5.10.3	ccB end station component options	53
71	5.11	CNC requirements	53
72	5.12	CNC options	54
73	5.13	CUC requirements	54
74	5.14	CUC options	54
75	6	Required functions for an industrial network	54
76	6.1	General	54
77	6.2	Synchronization	54
78	6.2.1	General	54
79	6.2.2	PTP Instance requirements	54
80	6.2.3	PTP protocol requirements	55
81	6.2.4	Clock Control System requirements for PTP End Instances	56
82	6.2.5	Error Generation Limits	56
83	6.2.6	Clock states	59
84	6.2.7	Application framework	59
85	6.2.8	Working Clock domain framework	60
86	6.2.9	Global Time domain framework	60
87	6.2.10	IA-station model for clocks	60
88	6.2.11	Clock usage for the Ethernet interface	62
89	6.2.12	Error model	62
90	6.2.13	gPTP domains and PTP Instances	63
91	6.3	Security model	64
92	6.3.1	General	64
93	6.3.2	Security functionality	64
94	6.3.3	IDevID Profile	67
95	6.3.4	Security setup based on IDevID	71
96	6.3.5	Secure configuration based on LDevID-NETCONF	75

97	6.4 Management	75
98	6.4.1 General	75
99	6.4.2 IA-station management model	75
100	6.4.3 Discovery of IA-station internal structure	81
101	6.4.4 Network engineering model	81
102	6.4.5 Operation.....	85
103	6.4.6 Engineered time-synchronization spanning tree	91
104	6.4.7 Diagnostics.....	92
105	6.4.8 Data sheet.....	95
106	6.4.9 YANG representation of managed objects and nodes ,	96
107	6.4.10 YANG Data Model.....	114
108	6.5 Topology discovery and verification	147
109	6.5.1 Topology discovery and verification requirements	147
110	6.5.2 Topology discovery overview.....	147
111	6.5.3 Topology verification overview.....	150
112	6.6 CNC	150
113	6.6.1 General	150
114	6.6.2 Stream destination MAC address range	150
115	Annex A (normative) PCS proforma – Time-sensitive networking profile for industrial	
116	automation	152
117	A.1 General	152
118	A.2 Abbreviations and special symbols	152
119	A.2.1 Status symbols	152
120	A.2.2 General abbreviations	153
121	A.3 Instructions for completing the PCS proforma	153
122	A.3.1 General structure of the PCS proforma	153
123	A.3.2 Additional information	153
124	A.3.3 Exception information.....	153
125	A.3.4 Conditional status	154
126	A.4 Common requirements	154
127	A.4.1 Instructions	154
128	A.4.2 Implementation identification	154
129	A.4.3 Profile summary, IEC/IEEE 60802	155
130	A.4.4 Implementation summary	155
131	A.5 IA-station Requirements and Options.....	155
132	A.5.1 Instructions	155
133	A.5.2 IA-station requirements	155
134	A.5.3 IA-station PHY and MAC options for external ports	156
135	A.5.4 IA-station options for time synchronization.....	156
136	A.5.5 IA-station secure management exchange options	156
137	A.5.6 CNC Requirements	157
138	A.5.7 CUC Requirements	157
139	A.6 Bridge Component	158
140	A.6.1 Instructions	158
141	A.6.2 Bridge Component Requirements	158
142	A.6.3 Common Bridge Component Options	158
143	A.6.4 ccA Bridge Component Options	158
144	A.6.5 ccB Bridge Component Options	158
145	A.7 End Station Component.....	160

146	A.7.1	Instructions	160
147	A.7.2	Common End Station Component Requirements	160
148	A.7.3	Common End Station Component Options	160
149	A.7.4	ccA End Station Component Options	160
150	A.7.5	ccB End Station Component Options	160
151	Annex B (informative)	Representative Configuration Domain	162
152	Annex C (informative)	Description of Clock Control System	163
153	C.1	Clock control system introduction	163
154	C.2	Transfer function for control system.....	164
155	C.3	Frequency response for control system.....	165
156	C.4	Example	170
157	Annex D (informative)	Time Synchronization Annex.....	172
158	D.1	Overview	172
159	D.2	Principles of Operation	173
160	D.2.1	General	173
161	D.2.2	Grandmaster PTP Instance Implementation	174
162	D.2.3	Splitting, Joining and Aligning Time Domains.....	175
163	D.2.4	PTP Link Characteristics	176
164	D.3	Notes on Normative Requirements	176
165	D.3.1	Oscillator Requirements	176
166	D.3.2	Timestamp Granularity Error	176
167	D.3.3	Dynamic Timestamp Error	177
168	D.3.4	Grandmaster PTP Instance Error Generation	177
169	D.3.5	PTP Relay Instance Error Generation	177
170	D.3.6	PTP End Instance Error Generation.....	179
171	D.4	Approach to Testing Normative Requirements.....	180
172	D.4.1	General	180
173	D.4.2	Testing Grandmaster PTP Instance	180
174	D.4.3	Testing PTP Relay Instance	181
175	D.4.4	Testing PTP End Instance	183
176	D.5	Example Algorithms	184
177	D.5.1	General	184
178	D.5.2	Algorithm for Tracking NRR Drift	184
179	D.5.3	Algorithm to Compensate for Errors in measured NRR due to Clock Drift	186
180	D.5.4	Algorithm for Tracking RR Drift.....	188
181	D.5.5	Algorithm to Compensate for Errors in measured RR due to Clock Drift.....	189
182	D.5.6	Algorithm to Compensate for Errors in measured RR due to Clock Drift at PTP End Instance	191
183	D.5.7	Mean Link Delay Averaging	192
184	Bibliography	194
185			
186			
187	Figure 1 – Data flow in a control loop	24	
188	Figure 2 – IA-station interaction with CNC – Transmit path	26	
189	Figure 3 – IA-station interaction with CNC – Receive path	27	
190	Figure 4 – IA-station example	28	
191	Figure 5 – Model for cycles	29	
192	Figure 6 – Traffic type translation example	31	
193	Figure 7 – IETF Interfaces used for Traffic Type Translation	31	

194	Figure 8 – PTP Instance Translation Example	32
195	Figure 9 – descriptionDS.userDescription used for PTP Instance Translation	33
196	Figure 10 – NETCONF/YANG security processing steps	38
197	Figure 11 – IA-station conformance model.....	44
198	Figure 12 – Clock model	60
199	Figure 13 – Example clock usage principles for PTP End Instances	61
200	Figure 14 – Example clock usage principles for Grandmaster PTP Instances	61
201	Figure 15 – Error budget scheme	63
202	Figure 16 – Generic IEEE 802.1Q YANG Bridge management model	76
203	Figure 17 – Internal LAN connection management model.....	77
204	Figure 18 – IA-station example with IETF interfaces	77
205	Figure 19 – VID/FID/MSTID example.....	79
206	Figure 20 – Structure and interfaces of a CNC.....	83
207	Figure 21 – IA-station structure example	84
208	Figure 22 – CNC interaction	84
209	Figure 23 – Operational management model	85
210	Figure 24 – UNI service model	86
211	Figure 25 – CNC southbound	86
212	Figure 26 – NETCONF usage in a Configuration Domain	87
213	Figure 27 – Boundary port model	88
214	Figure 28 – Observer model.....	93
215	Figure 29 – Creation of the digital data sheet of an IA-station	96
216	Figure 30 – Module iecieee60802-ethernet-interface.....	120
217	Figure 31 – Module iecieee60802-bridge	121
218	Figure 32 – Module iecieee60802-dot1-sched-bridge	122
219	Figure 33 – Module iecieee60802-subscribed-notifications.....	122
220	Figure 34 – Module iecieee60802-ia-station	122
221	Figure 35 – Module iecieee60802-tsn-config-uni	123
222	Figure 36 – Usage example of LLDP	148
223	Figure 37 – Stream Destination MAC Address	151
224	Figure C.1 – Reference model for clock control system	163
225	Figure C.2 – Frequency response for the control system of Figure C.1	166
226	Figure C.3 – Detail of frequency response for the control system of Figure C.1 for dimensionless frequency in the range 0,1 to 10	167
228	Figure C.4 – Gain peaking (pure fraction) as a function of damping ratio	169
229	Figure C.5 – Gain peaking in dB as a function of damping ratio.....	169
230	Figure C.6 – Example Frequency response	171
231	Figure D.1 – Approach to Testing Normative Requirements for Grandmaster PTP Instance	180
233	Figure D.2 – Approach to Testing Normative Requirements for PTP Relay Instance - 1	181
234	Figure D.3 – Approach to Testing Normative Requirements for PTP Relay Instance - 2	182
235	Figure D.4 – Approach to Testing Normative Requirements for PTP Relay Instance - 3	182
236	Figure D.5 – Approach to Testing Normative Requirements for PTP End Instance	183

237	Figure D.6 – RR Drift Tracking and Error Compensation Calculations – PTP Relay Instance	189
239	Figure D.7 – RR Drift Tracking and Error Compensation Calculations – PTP End Instance	191
241	Figure D.8 – Signals and timestamps to measure path delay	192
242		
243	Table 1 – List of terms	16
244	Table 2 – Traffic type characteristics	33
245	Table 3 – IA time-aware stream characteristics.....	34
246	Table 4 – IA stream characteristics	34
247	Table 5 – IA traffic engineered non-stream characteristics	35
248	Table 6 – IA non-stream characteristics.....	35
249	Table 7 – Industrial automation traffic types summary.....	35
250	Table 8 – Example traffic class to traffic type mapping.....	37
251	Table 9 – Required values	55
252	Table 10 – Protocol settings.....	55
253	Table 11 – Clock Control System requirements	56
254	Table 12 – Error generation limits for Grandmaster PTP Instance	56
255	Table 13 – Error generation limits for PTP Relay Instance	57
256	Table 14 – Error generation limits for PTP End Instance	58
257	Table 15 – Error budget	63
258	Table 16 – descriptionDS.userDescription of gPTP Domains.....	63
259	Table 17 – VLAN name examples.....	78
260	Table 18 – I2vlan name examples	80
261	Table 19 – Map of traffic type code to traffic type	81
262	Table 20 – Summary of the YANG modules	124
263	Table A.1 – Implementation identification template	154
264	Table A.2 – Profile summary template	155
265	Table A.3 – Implementation type	155
266	Table A.4 – IA-station requirements	155
267	Table A.5 – IA-station PHY and MAC options	156
268	Table A.6 – IA-station time synchronization options	156
269	Table A.7 – IA-station secure management exchange options.....	157
270	Table A.8 – CNC Requirements	157
271	Table A.9 – CUC Requirements	157
272	Table A.10 –Bridge Component Requirements.....	158
273	Table A.11 – Common Bridge Component Options	158
274	Table A.12 – ccA Bridge Component Options	158
275	Table A.13 – ccB Bridge Component Options	159
276	Table A.14 – Common End Station Component Requirements	160
277	Table A.15 – Common End Station Component Options.....	160
278	Table A.16 – ccA End Station Component Options.....	160
279	Table A.17 – ccB End Station Component Options.....	161
280	Table D.1 – Time Synchronisation Error Budget	172

281	Table D.2 – Protocol configurations & other measures to achieve dTE budget.....	173
282	Table D.3 – Protocol configurations & other measures to achieve dTE budget.....	177
283	Table D.4 – Protocol configurations & other measures to achieve dTE budget.....	178
284	Table D.5 – Protocol configurations & other measures to achieve dTE budget.....	179
285		
286		
287		

288 Time-sensitive networking profile for industrial automation

289

290

291

292

FOREWORD

- 293 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising
294 all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international
295 co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and
296 in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports,
297 Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC document(s)"). Their
298 preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with
299 may participate in this preparatory work. International, governmental and non-governmental organizations liaising
300 with the IEC also participate in this preparation.
- 301 IEEE Standards documents are developed within IEEE Societies and Standards Coordinating Committees of the
302 IEEE Standards Association (IEEE SA) Standards Board. IEEE develops its standards through a consensus
303 development process, approved by the American National Standards Institute, which brings together volunteers
304 representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members
305 of IEEE and serve without compensation. While IEEE administers the process and establishes rules to promote
306 fairness in the consensus development process, IEEE does not independently evaluate, test, or verify the
307 accuracy of any of the information contained in its standards. Use of IEEE Standards documents is wholly
308 voluntary. *IEEE documents are made available for use subject to important notices and legal disclaimers (see*
309 <https://standards.ieee.org/ipr/disclaimers.html> *for more information).*
- 310 IEC collaborates closely with IEEE in accordance with conditions determined by agreement between the two
311 organizations. This Dual Logo International Standard was jointly developed by the IEC and IEEE under the terms
312 of that agreement.
- 313 2) The formal decisions of IEC on technical matters express, as nearly as possible, an international consensus of
314 opinion on the relevant subjects since each technical committee has representation from all interested IEC
315 National Committees. The formal decisions of IEEE on technical matters, once consensus within IEEE Societies
316 and Standards Coordinating Committees has been reached, is determined by a balanced ballot of materially
317 interested parties who indicate interest in reviewing the proposed standard. Final approval of the IEEE standards
318 document is given by the IEEE Standards Association (IEEE SA) Standards Board.
- 319 3) IEC/IEEE Publications have the form of recommendations for international use and are accepted by IEC National
320 Committees/IEEE Societies in that sense. While all reasonable efforts are made to ensure that the technical
321 content of IEC/IEEE Publications is accurate, IEC or IEEE cannot be held responsible for the way in which they
322 are used or for any misinterpretation by any end user.
- 323 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications
324 (including IEC/IEEE Publications) transparently to the maximum extent possible in their national and regional
325 publications. Any divergence between any IEC/IEEE Publication and the corresponding national or regional
326 publication shall be clearly indicated in the latter.
- 327 5) IEC and IEEE do not provide any attestation of conformity. Independent certification bodies provide conformity
328 assessment services and, in some areas, access to IEC marks of conformity. IEC and IEEE are not responsible
329 for any services carried out by independent certification bodies.
- 330 6) All users should ensure that they have the latest edition of this publication.
- 331 7) No liability shall attach to IEC or IEEE or their directors, employees, servants or agents including individual
332 experts and members of technical committees and IEC National Committees, or volunteers of IEEE Societies and
333 the Standards Coordinating Committees of the IEEE Standards Association (IEEE SA) Standards Board, for any
334 personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for
335 costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC/IEEE
336 Publication or any other IEC or IEEE Publications.
- 337 8) Attention is drawn to the normative references cited in this publication. Use of the referenced publications is
338 indispensable for the correct application of this publication.
- 339 9) Attention is drawn to the possibility that implementation of this IEC/IEEE Publication may require use of material
340 covered by patent rights. By publication of this standard, no position is taken with respect to the existence or
341 validity of any patent rights in connection therewith. IEC or IEEE shall not be held responsible for identifying
342 Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or
343 scope of Patent Claims or determining whether any licensing terms or conditions provided in connection with
344 submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory.
345 Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk
346 of infringement of such rights, is entirely their own responsibility.
- 347
- 348 IEC/IEEE 60802 was prepared by subcommittee 65C: Industrial networks, of IEC technical
349 committee 65: Industrial-process measurement, control and automation, in cooperation with
350 IEEE 802.1: Higher Layer LAN Protocols Working Group of IEEE 802: LAN/MAN Standards
351 Committee of the IEEE computer society, under the IEC/IEEE Dual Logo Agreement between
352 IEC and IEEE. It is an International Standard.

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

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

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

355
356 Full information on the voting for its approval can be found in the report on voting indicated in
357 the above table.

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

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

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

- 365 • reconfirmed,
366 • withdrawn, or
367 • revised.

368
**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.**

369

370

371

372

373

INTRODUCTION

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

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

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

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

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

395

396 Time-sensitive networking profile for industrial automation

397

398 1 Scope

399 This document defines time-sensitive networking profiles for industrial automation. The profiles
400 select features, options, configurations, defaults, protocols, and procedures of bridges, end
401 stations, and LANs to build industrial automation networks. This document also specifies YANG
402 modules defining read-only information available online and offline as a digital data sheet. This
403 document also specifies YANG modules for remote procedure calls and actions to address
404 requirements arising from industrial automation networks.

405 2 Normative References

406 The following documents are referred to in the text in such a way that some or all of their content
407 constitutes requirements of this document. For dated references, only the edition cited applies.
408 For undated references, the latest edition of the referenced document (including any
409 amendments) applies.

410 IEEE Draft Std P1588e¹, *Standard for a Precision Clock Synchronization Protocol for*
411 *Networked Measurement and Control Systems Amendment: MIB and YANG Data Models*

412 IEEE Std 802.1AB-2016², *IEEE Standard for Local and Metropolitan Area Networks: Station*
413 *and Media Access Control Connectivity Discovery*

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

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

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

420 IEEE Draft Std P802.1ASdm, *IEEE Standard for Local and Metropolitan Area Networks: Timing*
421 *and Synchronization for Time-Sensitive Applications Amendment: Hot Standby*

422 IEEE Draft Std P802.1ASdn, *IEEE Standard for Local and Metropolitan Area Networks: Timing*
423 *and Synchronization for Time-Sensitive Applications Amendment: YANG Data Model*

424 IEEE Std 802.1ASdr-2024, *IEEE Standard for Local and Metropolitan Area Networks: Timing*
425 *and Synchronization for Time-Sensitive Applications Amendment: Inclusive Terminology*

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

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

431 IEEE Std 802.1CBdb-2021, *IEEE Standard for Local and Metropolitan Area Networks: Frame*
432 *Replication and Elimination for Reliability — Amendment 2: Extended Stream Identification*
433 *Functions*

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

- 434 IEEE Std 802.1Q-2022, *IEEE Standard for Local and Metropolitan Area Network: Bridges and*
435 *Bridged Networks*
- 436 IEEE Std 802.1Qcw-2023, *Standard for Local and Metropolitan Area Networks: Bridges and*
437 *Bridged Networks, Amendment: YANG Data Models for Scheduled Traffic, Frame Preemption,*
438 *and Per-Stream Filtering and Policing*
- 439 IEEE Draft Std P802.1Qdj, *Draft Standard for Local and Metropolitan Area Networks: Bridges and*
440 *Bridged Networks, Amendment: Configuration Enhancements for Time-Sensitive*
441 *Networking*
- 442 IEEE Draft Std P802.1Qdx, *Draft Standard for Local and Metropolitan Area Networks: Bridges and*
443 *Bridged Networks, Amendment: YANG Data Models for the Credit-Based Shaper*
- 444 IEEE Std 802.3-2022, *IEEE Standard for Ethernet*
- 445 IEEE Std 802.3.2-2019, *IEEE Standard for Ethernet YANG Data Model Definitions*
- 446 IEEE Std 802.3de-2022, *Standard for Ethernet Amendment 6: Enhancements to MAC Merge*
447 *and Time Synchronization Service Interface for Point-to-Point 10 Mb/s Single-Pair Ethernet*
- 448 IETF RFC 2131, Droms, R., *Dynamic Host Configuration Protocol*, March 1997, available at
449 <https://www.rfc-editor.org/info/rfc2131>
- 450 IETF RFC 2986, Nystrom, M. and Kaliski, B., *PKCS #10: Certification Request Syntax*
451 *Specification Version 1.7*, November 2000, available at <https://www.rfc-editor.org/info/rfc2986>
- 452 IETF RFC 3986, Berners-Lee, T., Fielding, R., and Masinter, L., *Uniform Resource Identifier*
453 *(URI): Generic Syntax*, January 2005, available at <https://www.rfc-editor.org/info/rfc3986>
- 454 IETF RFC 4836, Beili, E., *Definitions of Managed Objects for IEEE 802.3 Medium Attachment*
455 *Units (MAUs)*, April 2007, available at <https://www.rfc-editor.org/info/rfc4836>
- 456 IETF RFC 5246, Dierks, T. and Rescorla, E., *The Transport Layer Security (TLS) Protocol*,
457 August 2008, available at <https://www.rfc-editor.org/info/rfc5246>
- 458 IETF RFC 5277, Chisholm, S. and Trevino, H., *NETCONF Event Notification*, July 2008,
459 available at <https://www.rfc-editor.org/info/rfc5277>
- 460 IETF RFC 5280, Turner, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and Polk, W.,
461 *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL)*
462 *Profile*, May 2008, available at <https://www.rfc-editor.org/info/rfc5280>
- 463 IETF RFC 5289, Rescorla, E., *TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES*
464 *Galois Counter Mode (GCM)*, August 2008, available at <https://www.rfc-editor.org/info/rfc5289>
- 465 IETF RFC 5480, Cooper, S., Brown, D., Yiu, K., Housley, R., and Polk, T., *Elliptic Curve*
466 *Cryptography Subject Public Key Information*, March 2009, available at <https://www.rfc->
467 [editor.org/info/rfc5480](https://www.rfc-editor.org/info/rfc5480)
- 468 IETF RFC 6022, Scott, M. and Bjorklund, M., *YANG Module for NETCONF Monitoring*, October
469 2010, available at <https://www.rfc-editor.org/info/rfc6022>
- 470 IETF RFC 6024, Reddy, R. and Wallace, C., *Trust Anchor Management Requirements*, October
471 2010, available at <https://www.rfc-editor.org/info/rfc6024>
- 472 IETF RFC 6125, Saint-Andre, P. and Hodges, J., *Representation and Verification of Domain-*
473 *Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX)*
474 *Certificates in the Context of Transport Layer Security (TLS)*, March 2011, available at
475 <https://www.rfc-editor.org/info/rfc6125>
- 476 IETF RFC 6241, Enns, R., Bjorklund, M., Schoenwaelder, J. and Bierman, A., *Network*
477 *Configuration Protocol (NETCONF)*, June 2011, available at <https://www.rfc->
478 [editor.org/info/rfc6241](https://www.rfc-editor.org/info/rfc6241)

- 479 IETF RFC 7317, Bierman, A. and Bjorklund, M., *A YANG Data Model for System Management*,
480 August 2014, available at <https://www.rfc-editor.org/info/rfc7317>
- 481 IETF RFC 7589, Badra, M., Luchuk, A. and Schoenwaelder, J., *Using the NETCONF Protocol*
482 over Transport Layer Security (TLS) with Mutual X.509 Authentication, June 2015, available at
483 <https://www.rfc-editor.org/info/rfc7589>
- 484 IETF RFC 7748, Langley, A., Hamburg, M., and Turner, S., *Elliptic Curves for Security*, January
485 2016, available at <https://www.rfc-editor.org/info/rfc7748>
- 486 IETF RFC 7905, Langley, A., Chang, W., Mavrogiannopoulos, N., Strombergson, J., and
487 Josefsson, S., *ChaCha20-Poly1305 Cipher Suites for Transport Layer Security (TLS)*, June
488 2016, available at <https://www.rfc-editor.org/info/rfc7905>
- 489 IETF RFC 7950, Bjorklund, M., *The YANG 1.1 Data Modeling Language*, August 2016, available
490 at <https://www.rfc-editor.org/info/rfc7950>
- 491 IETF RFC 8032, Josefsson, S., and Liusvaara, I., *Edwards-Curve Digital Signature Algorithm*
492 (*EdDSA*), January 2017, available at <https://www.rfc-editor.org/info/rfc8032>
- 493 IETF RFC 8069, Thomas, A., *URN Namespace for IEEE*, February 2017, available at
494 <https://www.rfc-editor.org/info/rfc8069>
- 495 IETF RFC 8141, Sainbt-Andre, P., and Klensin, J., *Uniform Resource Names (URNs)*, April
496 2017, available at <https://www.rfc-editor.org/info/rfc8141>
- 497 IETF RFC 8340, Bjorklund, M. and Berger, L., *YANG Tree Diagrams*, March 2018, available at
498 <https://www.rfc-editor.org/info/rfc8340>
- 499 IETF RFC 8341, Bierman, A. and Bjorklund, M., *Network Configuration Access Control Model*,
500 March 2018, available at <https://www.rfc-editor.org/info/rfc8341>
- 501 IETF RFC 8342, Bjorklund, M., Schoenwaelder, J., Shafer, P., Watsen, K. and Wilton, R.,
502 *Network Management Datastore Architecture (NMDA)*, March 2018, available at
503 <https://www.rfc-editor.org/info/rfc8342>
- 504 IETF RFC 8343, Bjorklund, M., *YANG Data Model for Interface Management*, March 2018,
505 available at <https://www.rfc-editor.org/info/rfc8343>
- 506 IETF RFC 8348, Bierman, A., Bjorklund, M., Dong, J., and Romascanu, D., *A YANG Data Model*
507 for *Hardware Management*, March 2018, available at <https://www.rfc-editor.org/info/rfc8348>
- 508 IETF RFC 8410, Josefsson, S., and Schaad, J., *Algorithm Identifiers for Ed25519, Ed448,*
509 *X25519, and X448 for Use in the Internet X.509 Public Key Infrastructure*, August 2018,
510 available at <https://www.rfc-editor.org/info/rfc8410>
- 511 IETF RFC 8446, Rescorla, E., *The Transport Layer Security (TLS) Protocol Version 1.3*, August
512 2018, available at <https://www.rfc-editor.org/info/rfc8446>
- 513 IETF RFC 8525, Bierman, A., Bjorklund, M., Schoenwaelder, J., Watsen, K. and Wilton, R.,
514 *YANG Library*, March 2019, available at <https://www.rfc-editor.org/info/rfc8525>
- 515 IETF RFC 8526, Bierman, A., Bjorklund, M., Schoenwaelder, J., Shafer, P., Watsen, K. and
516 Wilton, R., *NETCONF Extensions to Support the Network Management Datastore Architecture*,
517 March 2019, available at <https://www.rfc-editor.org/info/rfc8526>
- 518 IETF RFC 8639, Voit, E., Clemm, A., Gonzalez Prieto, A., Nilsen-Nygaard, E., and Tripathy, A.,
519 *Subscription to YANG Notifications*, September 2019, available at [https://www.rfc-editor.org/info/rfc8639](https://www.rfc-
520 editor.org/info/rfc8639)
- 521 IETF RFC 8640, Voit, E., Clemm, A., Gonzalez Prieto, A., Nilsen-Nygaard, E. and Tripathy, A.,
522 *Dynamic Subscription to YANG Events and Datastores over NETCONF*, September 2019,
523 available at <https://www.rfc-editor.org/info/rfc8640>

- 524 IETF RFC 8641, Clemm, A. and Voit, E., *Subscription to YANG Notifications for Datastore*
525 *Updates*, September 2019, available at <https://www.rfc-editor.org/info/rfc8641>
- 526 IETF RFC 8808, Wu, Q., Lengyel, B., and Niu, Y., *A YANG Data Model for Factory Default*
527 *Settings*, August 2020, available at <https://www.rfc-editor.org/info/rfc8808>
- 528 IETF RFC 9195, Lengyel, B. and Claise, B., *A File Format for YANG Instance Data*, February
529 2022, available at <https://www.rfc-editor.org/info/rfc9195>
- 530 IETF RFC 9196, Lengyel, B., Clemm, A. and Claise, B., *YANG Modules Describing Capabilities*
531 *for Systems and Datastore Update Notifications*, February 2022, available at <https://www.rfc->
532 [editor.org/info/rfc9196](https://www.rfc-editor.org/info/rfc9196)

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

- 536 IETF RFC „Internet-Draft (I-D)“, Turner, S., and Housley, R., *Updates to Using the NETCONF*
537 *Protocol over Transport Layer Security (TLS) with Mutual X.509 Authentication* (draft-ietf-
538 *netconf-over-tls13*), Internet Draft, Work in Progress by NETCONF WG, available at
539 <https://datatracker.ietf.org/doc/draft-ietf-netconf-over-tls13/>
- 540 IETF RFC „Internet-Draft (I-D)“, Watsen, K., *A YANG Data Model for a Truststore* (draft-ietf-
541 *netconf-trust-anchors*), Internet Draft, Work in Progress by NETCONF WG, available at
542 <https://datatracker.ietf.org/doc/draft-ietf-netconf-trust-anchors/>
- 543 IETF RFC „Internet-Draft (I-D)“, Watsen, K., *A YANG Data Model for a Keystore* (draft-ietf-
544 *netconf-keystore*), Internet Draft, Work in Progress by NETCONF WG, available at
545 <https://datatracker.ietf.org/doc/draft-ietf-netconf-keystore/>
- 546 IETF RFC „Internet-Draft (I-D)“, Watsen, K., *NETCONF Client and Server Models* (draft-ietf-
547 *netconf-client-server*), Internet Draft, Work in Progress by NETCONF WG, available at
548 <https://datatracker.ietf.org/doc/html/draft-ietf-netconf-client-server-31>
- 549 IETF RFC „Internet-Draft (I-D)“, Watsen, K., *YANG Data Types and Groupings for Cryptography*
550 (draft-ietf-netconf-crypto-types), Internet Draft, Work in Progress by NETCONF WG, available
551 at <https://datatracker.ietf.org/doc/draft-ietf-netconf-crypto-types/>
- 552 ISO/IEC 9594-8:2020, *Information technology — Open systems interconnection — Part 8: The*
553 *Directory: Public-key and attribute certificate frameworks*, available at:
554 <https://www.iso.org/obp/ui/#iso:std:iso-iec:9594:-8:en>
- 555 NIST FIPS 180-4, *Secure Hash Standard (SHS)*, August 2015, available at
556 <https://csrc.nist.gov/publications/detail/fips/180/4/final>
- 557 NIST FIPS 186-5, *Digital Signature Standard (DSS)*, February 2023, available at
558 <https://csrc.nist.gov/publications/detail/fips/186/5/final>
- 559 NIST SP 800-186, *Recommendations for Discrete Logarithm-based Cryptography: Elliptic*
560 *Curve Domain Parameters*, February 2023, available at
561 <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-186.pdf>

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

564 **3 Terms, definitions, symbols, abbreviated terms and conventions**

565 **3.1 General**

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

- 569 • IEC Electropedia: available at <https://www.electropedia.org/>
 570 • ISO Online browsing platform: available at <https://www.iso.org/obp>
 571 • IEEE Standards Dictionary Online: available at <https://dictionary.ieee.org>
 572 • ITU-T Terms and Definitions database: available at https://www.itu.int/br_tsbs/#/

573
 574 NOTE Definitions in IEC 60050 can be found in the Electropedia link above.

575 **3.2 List of terms, abbreviated terms and definitions given in various standards**

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

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

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

581 **Table 1 – List of terms**

Term	Source
BTCA	IEEE Std 802.1AS-2020 as amended by IEEE Std 802.1ASdr-2024
Bridge	IEEE Std 802.1Q-2022
Bridge Port	IEEE Std 802.1Q-2022
CFM	IEEE Std 802.1Q-2022
Clock	IEEE Std 802.1AS-2020
ClockTimeTransmitter	IEEE Std 802.1AS-2020 as amended by IEEE Std 802.1ASdr-2024
ClockTimeReceiver	IEEE Std 802.1AS-2020 as amended by IEEE Std 802.1ASdr-2024
ClockSource	IEEE Std 802.1AS-2020
ClockTarget	IEEE Std 802.1AS-2020
CNC	IEEE Std 802.1Q-2022
Configuration Domain	IEEE Draft Std P802.1Qdj
constant time error (cTE)	ITU-T G.8260
Customer Virtual Local Area Network (C-VLAN) component	IEEE Std 802.1Q-2022
CUC	IEEE Std 802.1Q-2022
device	IEEE Std 802.1AR-2018
DLL	IEEE Std 802-2014
DTE	IEEE Std 802.3-2022
dynamic time error (dTE)	ITU-T G.8260
end entity (EE)	NIST Special Publication 800-57 Part 2, Revision 1
end station	IEEE Std 802-2014
Ethernet	IEEE Std 802.3-2022
FDB	IEEE Std 802.1Q-2022
FID	IEEE Std 802.1Q-2022
fingerprint	IETF RFC 7589
FQTSS	IEEE Std 802.1Q-2022
fractional frequency offset	IEEE Std 802.1AS-2020
frame	IEEE Std 802.1Q-2022
frame preemption	IEEE Std 802.1Q-2022
FRER	IEEE Std 802.1CB-2017

Term	Source
gating cycle	IEEE Std 802.1Q-2022
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-2022
IST	IEEE Std 802.1Q-2022
LAN	IEEE Std 802-2014
latency	IEEE Std 802.1Q-2022
Listener	IEEE Std 802.1Q-2022
LLDP	IEEE Std 802.1AB-2016
LLDPDU	IEEE Std 802.1AB-2016
local clock	IEEE Std 802.1AS-2020
LocalClock	IEEE Std 802.1AS-2020
logical link	IEEE Std 802-2014
LPI	IEEE Std 802.3-2022
MAC	IEEE Std 802-2014
MMRP	IEEE Std 802.1Q-2022
MST	IEEE Std 802.1Q-2022
MVRP	IEEE Std 802.1Q-2022
NETCONF	IETF RFC 6241
PCP	IEEE Std 802.1Q-2022
PDU	IEEE Std 802.1Q-2022
PHY	IEEE Std 802.3-2022
PLS	IEEE Std 802.3-2022
Port	IEEE Std 802.1Q-2022
preciseOriginTimestamp	IEEE Std 802.1AS-2020
primary domain	IEEE Draft Std P802.1ASdm
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-2022
redundancy	IEC 60050-192
residence time	IEEE Std 802.1AS-2020
secondary domain	IEEE Draft Std P802.1ASdm
signature suite	IEEE Std 802.1AR-2018
station	IEEE Std 802-2014
stream	IEEE Std 802.1Q-2022
synchronized time	IEEE Std 802.1AS-2020
Talker	IEEE Std 802.1Q-2022
time error	ITU-T G.8260

Term	Source
time-sensitive stream	IEEE Std 802.1Q-2022
traffic class	IEEE Std 802.1Q-2022
TLV	IEEE Std 802.3-2022
UNI	IEEE Std 802.1Q-2022
VID	IEEE Std 802.1Q-2022
VLAN	IEEE Std 802.1Q-2022
X.509	ISO/IEC 9594-8:2020
YANG	IETF RFC 6020

582

583 **3.3 Terms defined in this document**584 **3.3.1****application clock**

585 clock used by the application to time events

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

588 **3.3.2****Bridge component**

589 Customer Virtual Local Area Network (C-VLAN) component as specified in IEEE Std 802.1Q-591 2022

592 **3.3.3****control latency**

593 time delay between the input to a sensor application and the output from an actuator application

595 Note 1 to entry: For the purposes of this document, control latency does not include latencies in the sensor, 596 actuator, or the physical system in a process.

597 **3.3.4****deadline**

599 application defined reference point that represents a time when data is required by the 600 application

601 **3.3.5****digital data sheet**

603 information about the capabilities of an IA-station, for example, states, configurations, and 604 supported features

605 **3.3.6****end station component**

607 end station entity as specified in IEEE Std 802-2014

608 **3.3.7****Global Time**

609 synchronized time, derived from a gPTP domain, that is traceable to the PTP timescale

611 **3.3.8****IA-controller**

613 industrial automation function, consisting of a comparing element and a controlling element, 614 that performs a specified control function

615 Note 1 to entry: An IA-controller exchanges data with several IA-devices or other IA-controllers for the purpose of 616 control of a system.

617 Note 2 to entry: The primary categories of IA-controllers are distributed control systems (DCS), programmable logic 618 controllers (PLCs), and programmable automation controllers (PACs).

3.3.9**IA-device**

621 industrial automation function, consisting of sensor and/or actuator elements to read and/or
622 write process data

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

3.3.10**IA-station**

627 material element or assembly of one or more end station components, and zero, one or more
628 bridge components

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

3.3.11**imprinting**

632 <security> equipping IA-stations with an LDevID credential as specified in IEEE Std 802.1AR-
633 2018, corresponding trust anchor as specified in IETF RFC 6024, and certificate-to-name
634 mapping instructions as specified in IETF RFC 7589, Clause 7

3.3.12**management entity**

637 IA-station function responsible for configuration of Bridge components, end station components
638 and ports

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

3.3.13**network diameter**

642 number of links in the longest of all the calculated shortest paths between each pair of nodes
643 in the network

3.3.14**network provisioning**

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

3.3.15**nominal frequency**

649 ideal frequency with zero uncertainty

650 Note 1 to entry: The nominal frequency of the PTP timescale is further explained in IEEE Std 1588-2019, 7.2.1,
651 7.2.2, and Annex B.

3.3.16**ppm**

654 $\mu\text{Hz}/\text{Hz}$

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

3.3.17**Working Clock**

659 synchronized time, derived from a gPTP domain, that is traceable to the PTP timescale, or to
660 an ARB timescale that is continuous

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

663

3.4 Abbreviated terms and acronyms

AEAD Authenticated Encryption with Associated Data

AES Advanced Encryption Standard

ARB Arbitrary

ASCII American Standard Code for Information Interchange

ASN	Abstract Syntax Notation
BTCA	Best timeTransmitter Clock Algorithm
CA	Certification Authority
CBC	Cipher Block Chaining
ccA	Conformance Class A
ccB	Conformance Class B
CFM	Connectivity Fault Management
CMLDS	Common Mean Link Delay Service
CMS	Cryptographic Message Syntax
CN	Common Name
CNC	Centralized Network Configuration
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
ECDSA	Elliptic Curve Digital Signature Algorithm
EdDSA	Edwards-Curve Digital Signature Algorithm
EE	End Entity
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 Reliability
GCM	Galois Counter Mode
gPTP	generalized Precision Time Protocol
HMAC	Keyed-Hashing for Message Authentication Code
HW	HardWare
IA	Industrial Automation
IDevID	Initial Secure Device Identifier
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers

I-LAN	Internal Local Area Network
ISO	International Organization for Standardization
ISS	Internal Sublayer Service
IST	Internal Spanning Tree
IT	Information Technology
ITU	International Telecommunication Union
IVL	Independent Virtual Local Area Network Learning
LDevID	Locally Significant Secure 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
NRR	Neighbor Rate Ratio
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OMG®	Object Management Group
OT	Operations Technology
OUI	Organizationally Unique 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
PPS	Pulse Per Second
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
UML®	Unified Modeling Language™
UNI	User/Network Interface
URL	Uniform Resource Locator
URN	Uniform Resource Name
VID	VLAN Identifier
VLAN	Virtual Local Area Network
YANG	Yet Another Next Generation data modeling language

665 NOTE OMG®, UML® and Unified Modeling Language™ are either registered trademarks or trademarks of a product
666 supplied by the Object Management Group, Inc. in the United States and/or other countries. This information is given
667 for the convenience of users of this document and does not constitute an endorsement by IEEE or IEC of the product
668 named. Equivalent products may be used if they can be shown to lead to the same results.

669

670 **3.5 Conventions**

671 **3.5.1 Convention for capitalizations**

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

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

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

679

680 **3.5.2 Unit conventions**

681 This document uses:

- 682 • Gb/s for gigabits per second,
683 • Mb/s for megabits per second and,
684 • kb/s for kilobits per second.

685

686 **3.5.3 Conventions for YANG contents**

687 YANG modules and XML instance data for YANG shown in this document use the following
 688 style:

689 Text style higher-layer-if text style

690 Contents of a YANG module use the following style:

```
691 <ieee802-dot1q-bridge xmlns="urn:ietf:params:xml:ns:yang:ieee802-dot1q-bridge">
692   <brides>
693     <bridge> <!-- list -->
694       <name>functional-unit-x</name>
695       ...

```

696 **3.5.4 Conventions for YANG selection / Digital Data Sheet**

697 The digital data sheet expresses device capabilities and therefore, not all nodes in a YANG
 698 module need be included in the digital data sheet. YANG nodes in 6.4.9 marked with [m], are
 699 mandatory nodes in the digital data sheet, nodes marked with [c] are conditional mandatory if
 700 the IA-station supports the corresponding optional functionality. Nodes marked with [o] are
 701 optional nodes in the digital data sheet. These marking in no way affect whether the feature
 702 and associated YANG module is required for the IA-station. Please refer to Clause 5 for
 703 conformance criteria for the IA-station.

704 YANG node selections in 6.4.9 of parent nodes implicitly include all subsidiary child nodes.

705 **4 Overview of TSN in industrial automation**706 **4.1 Industrial application operation**

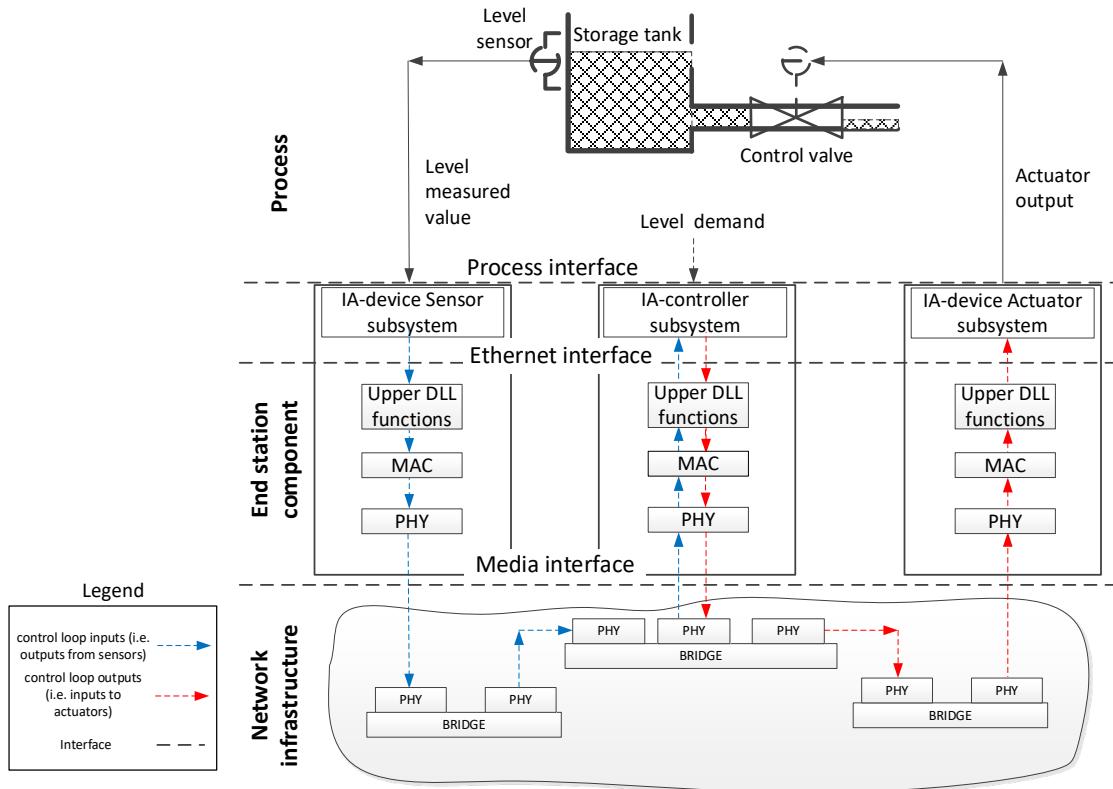
707 Industrial network applications are based on three main types of building blocks, which can be
 708 combined in one IA-controller or provided as a combination of an IA-controller and IA-devices
 709 interconnected through a suitable communication network.

710 These basic building blocks are:

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

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

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



727

728

Figure 1 – Data flow in a control loop

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

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

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

742 Control latency is a critical factor in all types of control and needs to be bounded. Components
 743 contributing to the control latency time are shown in Figure 1.

- 744 • Application time for sampling, computation, and processing within each IA-controller and IA-
 745 device. These are specific to the IA-device and IA-controller and known to the IA-device or
 746 IA-controller makers.
- 747 • The time for data transfer through the upper DLL functions, MAC and PHY layers within
 748 each IA-controller and IA-device. This time depends on the implementation of these
 749 components, their situation-dependent load and performance, and configuration elements
 750 related to QoS supported by these components.
- 751 • The End Station and Bridge schedule and transfer time through the network. These are
 752 influenced by the configuration process, which allocates available bandwidth and priorities
 753 to various types of application messages.

754 Offline engineering of the network is possible, including the calculation of the control latency
 755 time. During system operation, management services are provided for diagnostics and checking
 756 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 include:

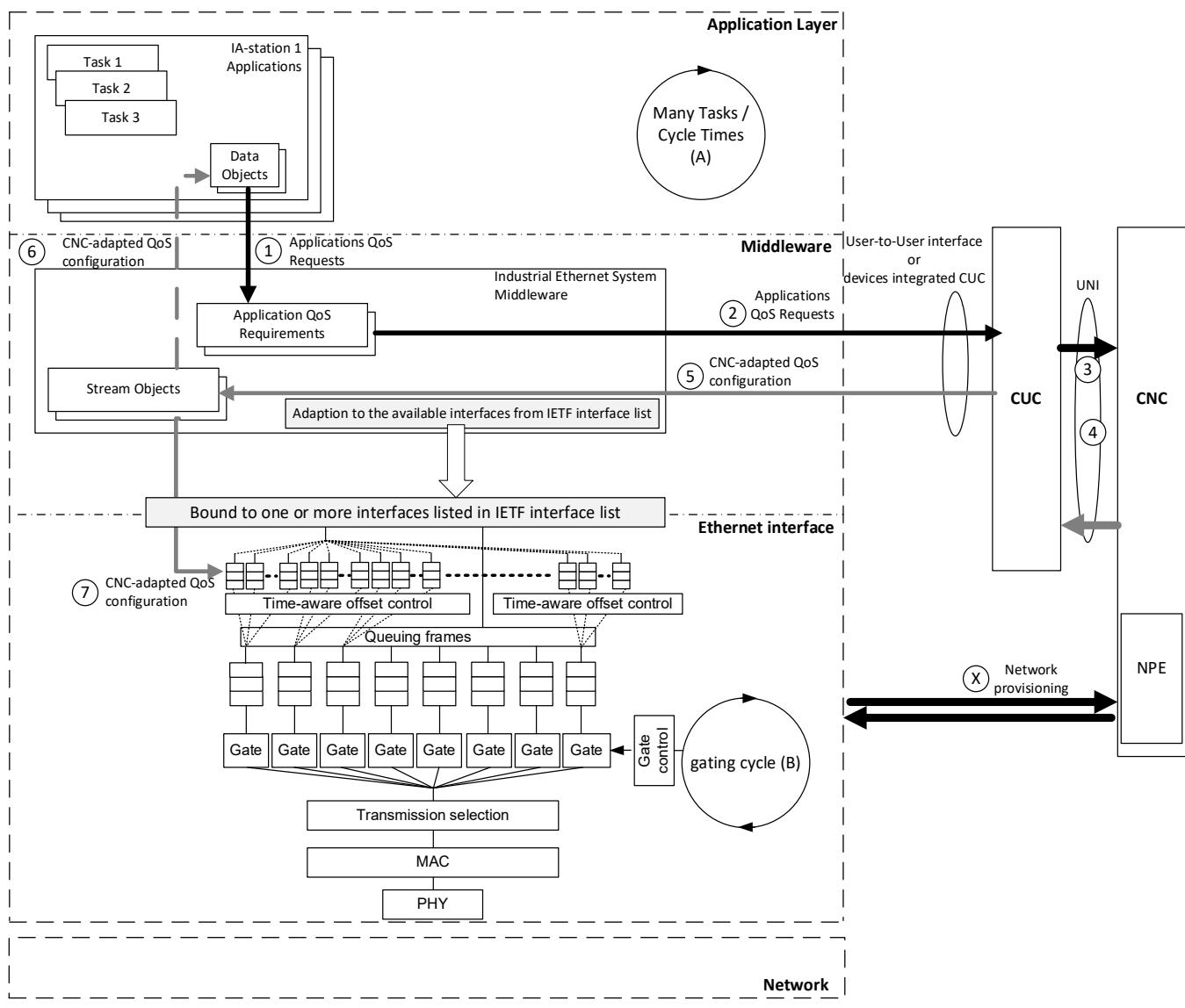
- Background tasks, which are executed when no other task is running. There can be zero, one, or more such tasks in an industrial application.
- Main task which executes periodically. The start and execution of this task is often based upon the ARB timescale. There can be zero or one such task, in an industrial application.
- Global Time tasks. The start and execution of these tasks is often based upon Global Time (for example, at noon every day or at noon every Friday). 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, or a process fault occurs). 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.

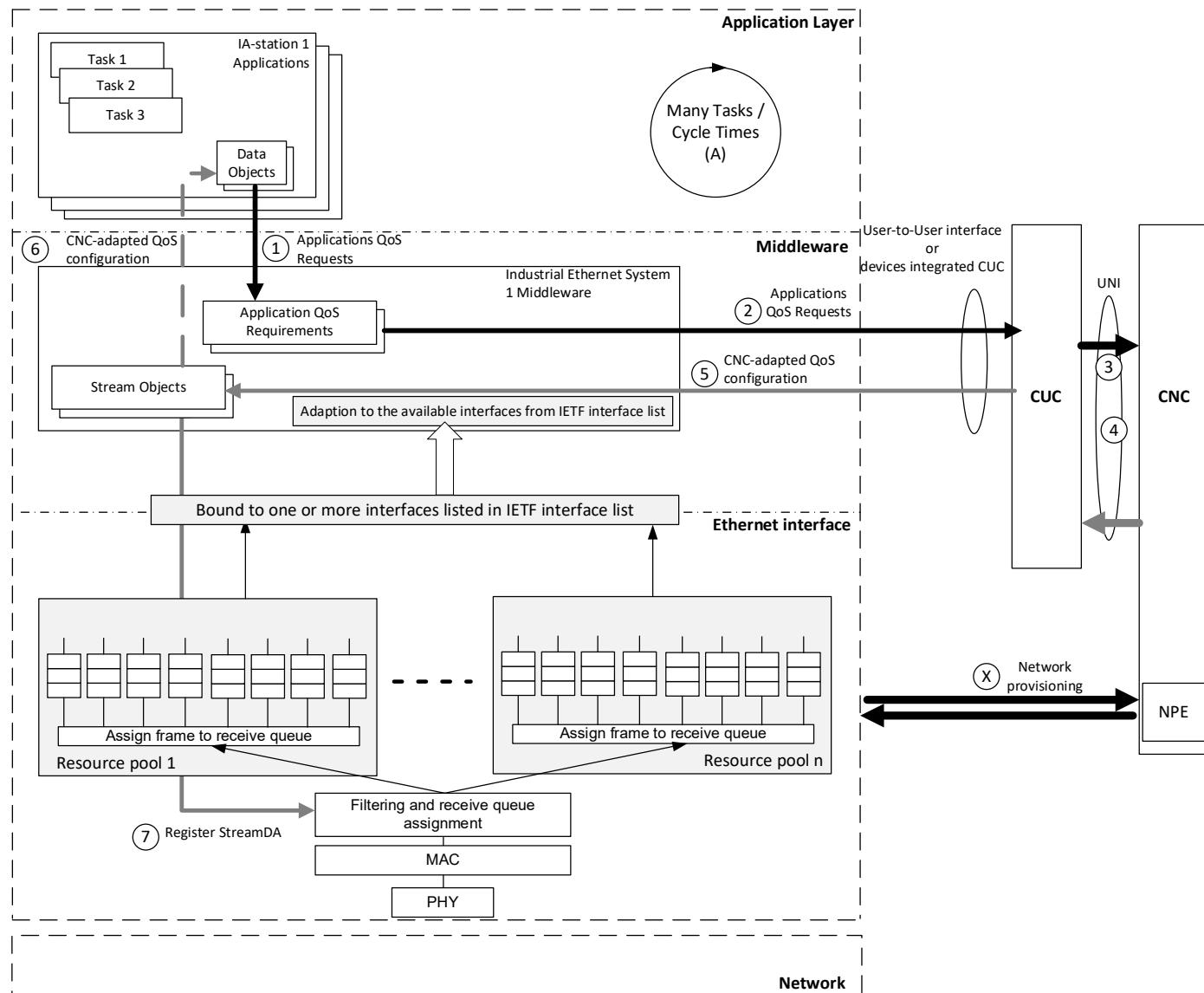
A user defines the required automation tasks along with the data objects required as output and input for these tasks and the end station which hosts these tasks. Thus, these tasks are bound to data objects, which need to be exchanged between end stations per the user's definition. Many of these tasks 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 Std 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.

790

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



793
794 **Figure 3 – IA-station interaction with CNC – Receive path**
795

796 **4.2.2 Control loop tasks**

797 Multiple control loop tasks can be implemented and run in parallel in their automation devices.
798 For example, this behavior can be implemented by using a common Working Clock, a common
799 starting point relative to the Working Clock and a common duration for this control loop task at
800 the involved IA-devices and IA-controllers. The data objects associated with the control loop
801 share common values for some attributes (for example, the same values for
802 DataObject_Update_Interval and DataObject_Deadline). Multiple control loop tasks can be
803 implemented and run in parallel in their 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 units of 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 four 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. Functional unit 4 includes a single end station component with two external ports.

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, IA-device 3, IA-controller 3) or in multiple end station components (IA-controller 2, management entity).

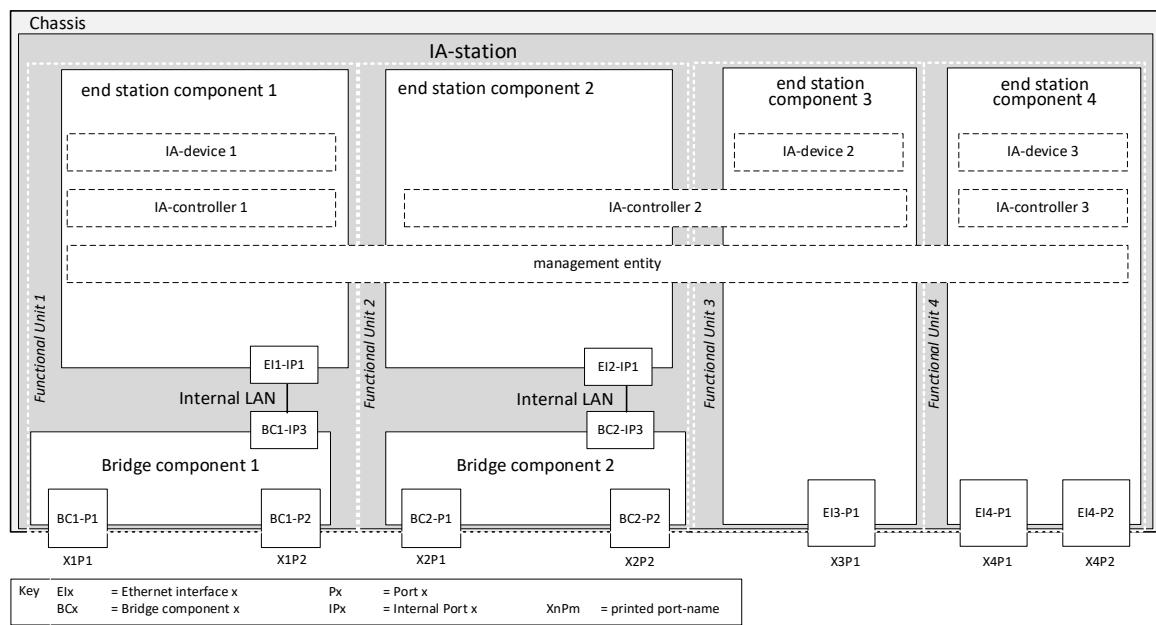


Figure 4 – IA-station example

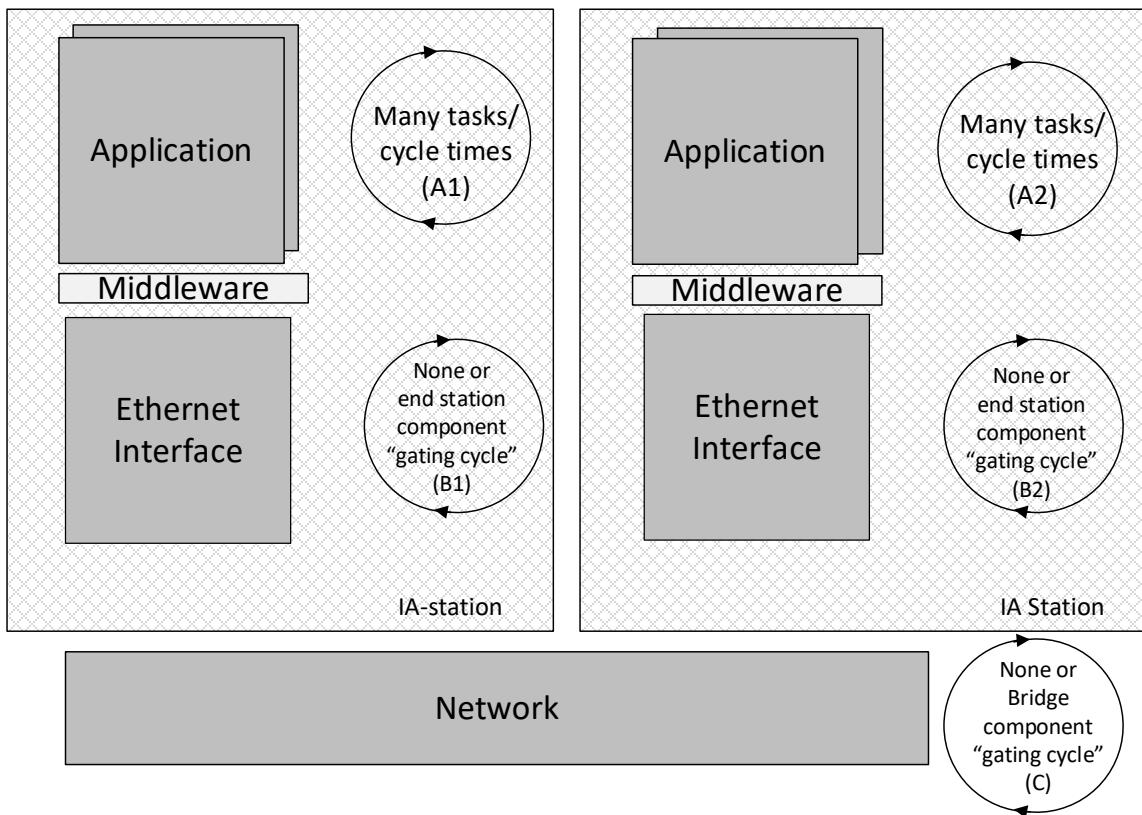
836 4.4 Ethernet interface

837 One or more middleware components act as a layer between applications and the Ethernet
 838 interface. Figure 2 and Figure 3 show the relation between applications, middleware, Ethernet
 839 interface and the network. Various applications can run in parallel on an automation device.
 840 Data objects represent the information exchanged between applications running in different end
 841 stations. The application requirements contained in these data objects are translated by the
 842 middleware into stream requirements for use by the CUC. This translation can be accomplished
 843 in one or both of the following ways:

- 844 a) The user defines the data objects and translates them into stream requirements and end-
 845 station communication-configurations. A user-specific mechanism is used to configure the
 846 network components, establish paths, and the time-aware offset control.
- 847 b) The user defines the data objects and associates them with QoS requirements for each
 848 stream (application QoS requirements). These can be forwarded as stream requirement
 849 requests by a CUC to a CNC. The CNC responds by providing a stream configuration
 850 response. The request and response are specified in IEEE Draft Std P802.1Qdjj. This
 851 information is used to configure the time-aware offset control, which utilizes per-stream
 852 queues. The CUC can be integrated into the end station or can be accessed via a user-to-
 853 user protocol. The middleware uses this information for configuring Talkers and Listeners.
 854 This information is also used to add additional timing information to the data objects for
 855 application usage.

856 Time-aware offset control utilizes per-stream queues (see IEEE Std 802.1Q-2022, Figure 34-1)
 857 and the traffic specification of the streams, including transmission offsets, provided by the CNC
 858 to ensure the order of stream transmission.

859



860
 861 **Figure 5 – Model for cycles**

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

865 4.5 Mechanisms that can be used to meet control loop latency requirements

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

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

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

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

881 Reserving time on the network for certain traffic types can be done through enhancements for
882 scheduled traffic according to IEEE Std 802.1Q-2022, 8.6.8.4. An aligned gating cycle needs
883 to be defined for this method to work. Once a gating cycle is defined, portions of a cycle time
884 can either be allocated to streams or classes of streams.

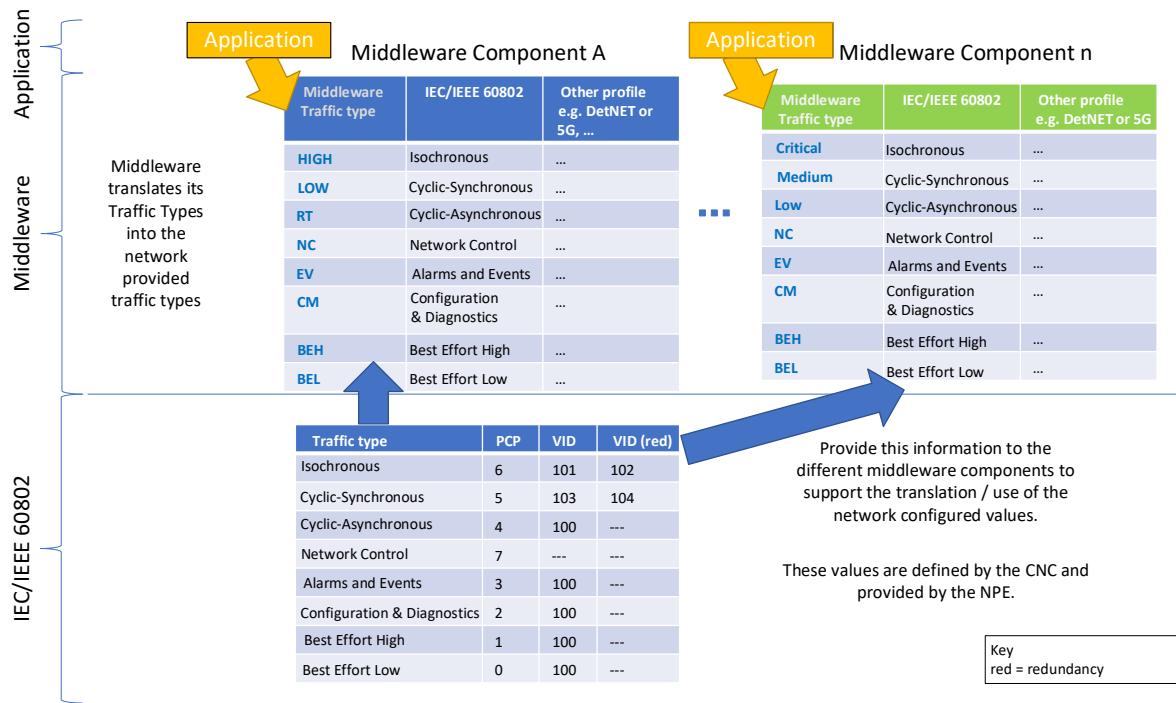
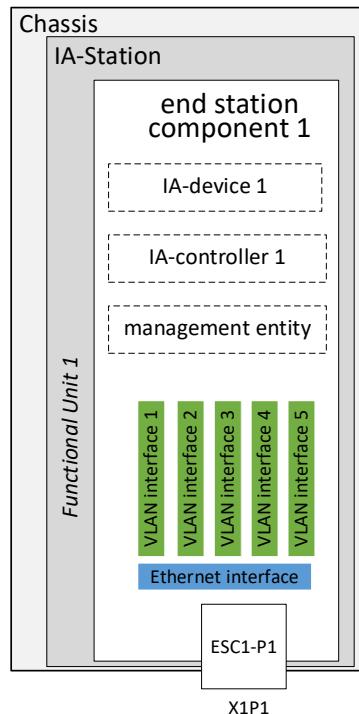
885 Multiple Talker/Listener(s) pairs can be used for streams between end stations. Engineered
886 time-triggered transmit can be used to coordinate transmission of all the traffic that shares a
887 network to meet application requirements.

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

890 4.6 Translation between middleware and network provisioning**891 4.6.1 Interfaces of type l2vlan**

892 Application engineering can be done without knowledge of the network provisioning. Since the
893 application is not aware of the network provisioning, it cannot directly map to the network
894 configuration, for example, the use of PCP or VID as configured in the network. This problem
895 is solved by providing a translation table, in the form of a YANG module definition, to the
896 middleware. The IA-station's local YANG datastore contains this information.

897 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 (IETF RFC 7224) can be used to provide the required mapping information to all installed middleware and applications.

907 The name string of the I2vlan interfaces can provide the vlan-id, the assigned traffic types with
 908 their PCP values and redundancy information (see 6.4.2.5).

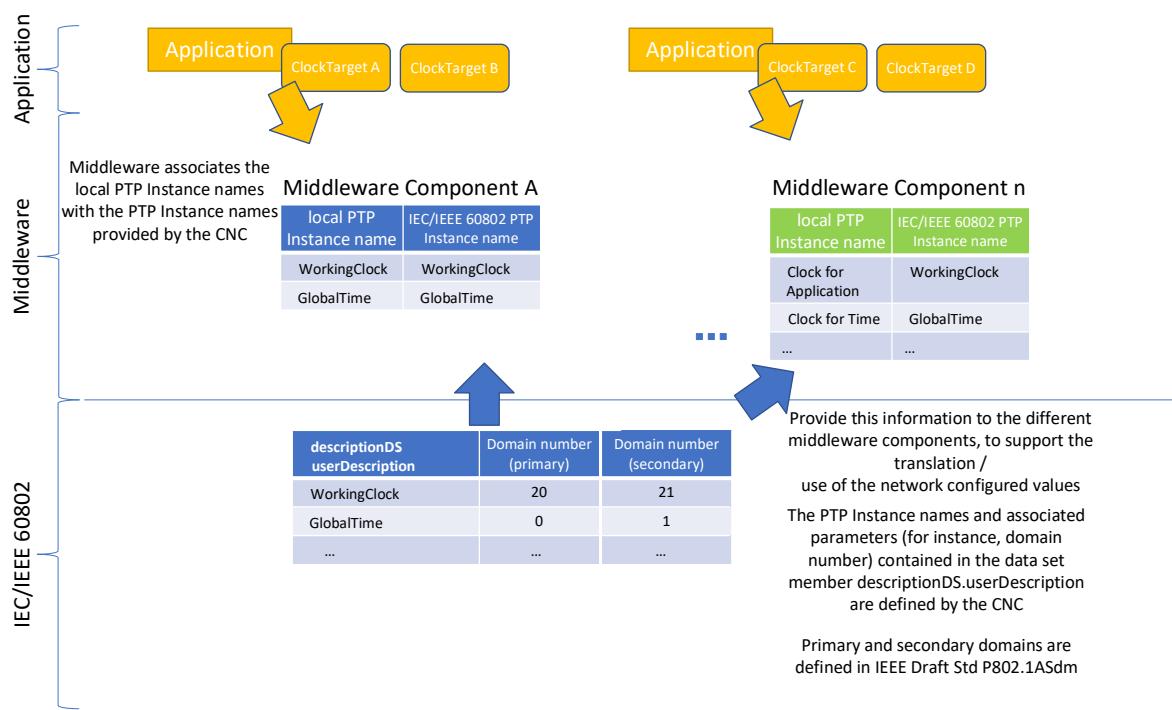
909

910 4.6.2 PTP Instances

911 PTP domain numbers are also configured during network provisioning. The middleware needs
 912 to know which PTP domain is assigned to which target clock. This is done by providing
 913 descriptionDS.userDescription names according to IEEE Std 1588-2019, 8.2.5.5 to create a
 914 translation table.

915 descriptionDS.userDescription names allow the support of multiple middleware components at
 916 one IA-station using the same PTP Instances (see 6.2.13). An IA-station's local database stores
 917 this information.

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

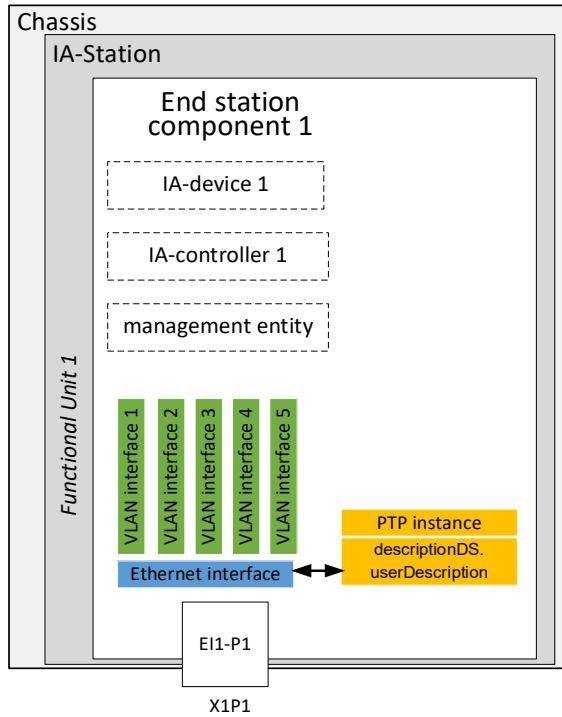


919

920

921

Figure 8 – PTP Instance Translation Example



922

923 **Figure 9 – descriptionDS.userDescription used for PTP Instance Translation**

924

925 The userDescription contains the clock type (i.e., WorkingClock, GlobalTime, or both). This
 926 information is used by the middleware to align to the intended ClockTarget or ClockSource (see
 927 6.2.13).

928 **4.7 Industrial traffic types**929 **4.7.1 General**

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

- 934 a) First define characteristics of generic traffic types (traffic-type-categories) and
 935 b) Second define instances of the generic traffic types, i.e., the traffic types.

936

937 **4.7.2 Traffic type characteristics**

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

940 **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: <ul style="list-style-type: none"> • Required: traffic frames are transmitted cyclically • Optional: Implementation of cyclic traffic is at the discretion of the user.

Characteristic	Description
Data delivery requirements	<p>Denotes the delivery constraints for the traffic. Four options are specified:</p> <ul style="list-style-type: none"> • 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	<p>Talker data transmission occurs at a specific point in time based upon the Working Clock. Available selections are:</p> <ul style="list-style-type: none"> • Required • Optional: Implementation of time-triggered transmission is at the discretion of the user. <p>Enhancements of scheduled traffic is only one means of achieving time-triggered transmission. Other, application-based, methods are possible</p>

941

942 **4.7.3 Traffic type categories**

943 **4.7.3.1 General**

944 The two-step approach described in 4.7.1 allows a clear differentiation between characteristics
 945 as seen from the “network” point of view and “application” point of view. Traffic-type-categories
 946 allow different IEEE 802 feature selections to achieve the goals of a specific network
 947 deployment. Four traffic-type-categories are identified in industrial automation systems:

- 948 a) IA time-aware stream,
 949 b) IA stream,
 950 c) IA traffic engineered non-stream,
 951 d) IA non-stream.

952

953 **4.7.3.2 IA time-aware stream**

954 The characteristics of this traffic type category are shown in Table 3.

955 **Table 3 – IA time-aware stream characteristics**

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

956

957 **4.7.3.3 IA stream**

958 The characteristics of this traffic type category are shown in Table 4.

959 **Table 4 – IA stream characteristics**

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

960 **4.7.3.4 IA traffic engineered non-stream**

961 The characteristics of this traffic type category are shown in Table 5.

962

Table 5 – IA traffic engineered non-stream characteristics

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

963 **4.7.3.5 IA non-stream**

964 The characteristics of this traffic type category are shown in Table 6.

965

Table 6 – IA non-stream characteristics

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

966

967 **4.7.4 Traffic types**968 **4.7.4.1 General**969 Table 7 summarizes relevant industrial automation traffic types and their associated
970 characteristics. In an industrial automation system, other applications, such as audio or video,
971 utilizes one of these traffic types. Traffic Type codes are needed for the VLAN naming scheme
972 specified in this document. See 6.4.2.4 for more information.

973

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
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

974

975 **4.7.4.2 Isochronous**976 A type of IA time-aware stream traffic. This type of traffic is transmitted cyclically using time-
977 triggered transmission. Listeners have individual deadline requirements. Cycle times are
978 typically in the range of microseconds to tens of milliseconds. Frame size is typically below 500
979 octets. Talker-Listener pairs are synchronized to the Working Clock. The network is configured
980 by the CNC to provide zero congestion loss for this traffic type. This type of traffic is normally
981 used in control loop tasks.

982 **4.7.4.3 Cyclic-synchronous**

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

989 **4.7.4.4 Cyclic-asynchronous**

990 A type of IA stream traffic. This type of traffic is transmitted cyclically with latency requirements
991 bounded by the interval as specified in IEEE Std 802.1Q-2022, 46.2.3.5.1. Talker-Listener pairs
992 have individual latency requirements. Cycle times are typically in the range of milliseconds to
993 seconds. Frame size is unconstrained except as indicated in 5.5.1. Data exchanges between
994 Talker-Listener pairs are typically not dependent on the Working Clock. This traffic type typically
995 tolerates limited congestion loss. The network is configured by the CNC to handle this traffic
996 type without loss, up to a certain number of frames or data size.

997 **4.7.4.5 Alarms and events**

998 A type of IA traffic engineered non-stream. This type of traffic is transmitted cyclically or
999 acyclically. This traffic expects bounded latency including time for retransmission in the range
1000 of milliseconds to hundreds of milliseconds. The source of the alarm or event typically limits the
1001 bandwidth allocated to this traffic. Frame size is unconstrained except as indicated in 5.5.1.
1002 Congestion loss can occur. Retransmission to mitigate frame loss is expected. The network is
1003 configured by the CNC to handle these frames, including bursts of frames, up to a certain
1004 number of frames or data size over a defined period.

1005 **4.7.4.6 Configuration and diagnostics**

1006 A type of IA traffic engineered non-stream. This type of traffic is transmitted cyclically or
1007 acyclically. This traffic expects bounded latency, up to seconds, including time for
1008 retransmission. The source of configuration or diagnostics frames typically limits the bandwidth
1009 allocated to this traffic. Frame size is unconstrained except as indicated in 5.5.1. Congestion
1010 loss can occur. Retransmission to mitigate frame loss is expected. The network is configured
1011 by the CNC to handle these frames, including bursts of frames, up to a certain number of frames
1012 or data size over a defined period.

1013 **4.7.4.7 Network control**

1014 A type of IA traffic engineered non-stream. This type of traffic can be transmitted cyclically or
1015 acyclically. This traffic expects bounded latency including time for retransmission. Frame size
1016 is unconstrained except as indicated in 5.5.1. The network is configured by the CNC to handle
1017 these frames, including bursts of frames, up to a certain number of frames or data size over a
1018 defined period. If these limits are exceeded congestion loss can occur. Network control is
1019 comprised of services required to maintain network operation. Examples include time
1020 synchronization, loop prevention, and topology detection.

1021 **4.7.4.8 Best effort**

1022 A type of IA non-stream. The network is configured by the CNC so that these frames do not
1023 interfere with other traffic types. These frames are forwarded when resources are available.
1024 Congestion loss resulting in frame drop can occur. It is sometimes desirable to have more than
1025 one traffic class for best effort traffic (see Table 8).

1027 **4.7.4.9 Traffic class to traffic type mapping**

1028 Table 8 provides an example for the usage of traffic classes based on the traffic type:

1029 **Table 8 – Example traffic class to traffic type mapping**

Traffic class	PCP (8 Queues)	PCP (4 Queues)	Traffic Type
7	6	2	Isochronous
6	5	1	Cyclic-Synchronous
5	4	1	Cyclic-Asynchronous
4	7	3	Network Control
3	3	0	Alarms and Events
2	2	0	Configuration & Diagnostics
1	1	0	Best Effort High
0	0	0	Best Effort Low

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

1030
1031 The traffic-type-categories definition allows different IEEE 802 feature selections to achieve
1032 specified goals. Moreover it helps in identification of the traffic protection mechanisms.
1033 Adherence to this example of a common mapping helps minimize potential conflicts between
1034 traffic types.

1035
1036 **4.8 Security for TSN-IA**

1037 **4.8.1 General**

1038 Subclause 4.8 describes selected aspects of TSN-IA security. Protecting the management of
1039 industrial communication is the main objective of TSN-IA security. The protection of
1040 communications that use industrial traffic types is not addressed by this document.

1041
1042 **4.8.2 Security configuration model**

1043 Security configuration is a part of system engineering and configuration. The security
1044 configuration in this document does not encompass the supply of configuration objects for
1045 middleware and application security. Security configuration settles the prerequisites for
1046 protecting the establishment and management of communications that use industrial traffic
1047 types (see 4.7). It ensures that the security features of IA-stations (including CNCs) can be
1048 used for protecting message exchanges and authorizing the resource accesses during stream
1049 establishment and management. This security configuration supplies deployment-specific
1050 configuration objects to IA-stations. They encompass:

- 1051 • Instructions about cryptographic algorithms,
- 1052 • Credentials and trust anchors,
- 1053 • Instructions to interpret the outcome of peer entity authentication while enforcing resource
1054 access controls, and
- 1055 • Access control rules and permissions

1056 This security configuration uses NETCONF/YANG request/response exchanges:

- 1057 • The to-be-configured IA-stations act in NETCONF server role with respect to their security
1058 configuration.
- 1059 • A NETCONF client is responsible for setting-up IA-stations for security. This NETCONF
1060 client possesses information about the security relationship to be established during security
1061 configuration or about the expectations on the IA-stations in a Configuration Domain. It can

be implemented as part of an interactive or automated process (for example an engineering tool, or CNC operation). 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 (see IETF RFC 4210, 3.1.1).

- The security configuration exchanges supply deployment-specific objects (trust anchors, credentials etc.) to IA-stations and manages them. 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 (for example, NETCONF sessions or managed objects) on NETCONF servers is specified by IETF RFC 6241 (NETCONF). Therefore, message exchange protection between NETCONF clients and servers as well as resource access authorization by NETCONF servers is needed:

- IETF RFC 7589 and draft-ietf-netconf-over-tls13 (NETCONF-over-TLS) specify 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 security as shown in Figure 10. The processing steps are executed upon the current configuration of the NETCONF server's YANG modules.

1086

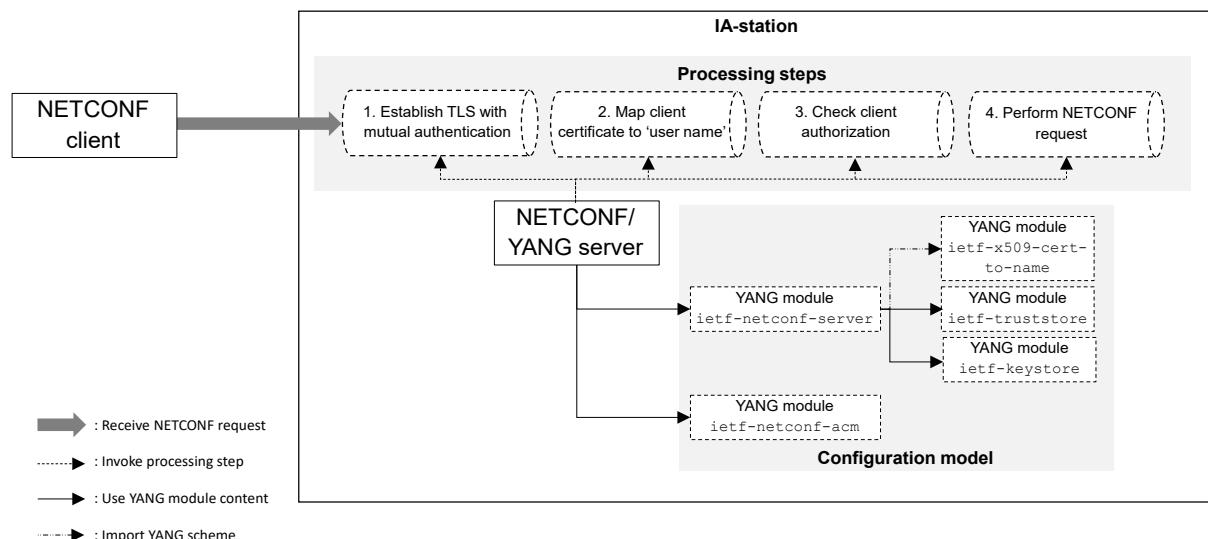


Figure 10 – NETCONF/YANG security processing steps

The processing steps on the side of NETCONF servers are:

- Establish a TLS connection with mutual authentication: The NETCONF server acts as TLS server and awaits connection requests of NETCONF clients (TLS clients). At the beginning of the TLS handshake, the TLS client and server negotiate the TLS protocol version to be used. 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

- 1097 verifies its authentication by trust anchors in its ietf-truststore YANG module according
 1098 to 6.3.4. A successful mutual authentication is a prerequisite for proceeding to the next
 1099 step.
- 1100 2) Map the client certificate to a username: The NETCONF server maps the authenticated
 1101 TLS client certificate to a “NETCONF username”³ by applying an ordered list of mapping
 1102 instructions. These instructions are provided in its ietf-x509-cert-to-name YANG module.
 1103 The applicable list item is identified by matching its configured fingerprint (according to
 1104 IETF RFC 7589, Clause 7) against the certification path that was used for TLS client
 1105 authentication (an end entity certificate or a CA certificate). According to the map type
 1106 of the identified list item, the NETCONF server determines the “NETCONF username”.
 1107 This can be done by extracting information from the end entity certificate of the
 1108 NETCONF client. A successful certificate-to-“NETCONF username” mapping is a
 1109 prerequisite for proceeding to the next step.
- 1110 3) Check client authorization: The NETCONF server checks if the NETCONF client has the
 1111 permission to access the requested NETCONF/YANG resource based on its “NETCONF
 1112 username” and the access control rules available in its ietf-netconf-acm YANG module.
 1113 See 4.8.4 for more information about NETCONF/YANG access control. A successful
 1114 authorization is a prerequisite for proceeding to the next step.
- 1115 4) Perform NETCONF request: If all preceding steps succeeded, the NETCONF server
 1116 performs the NETCONF request.

1117 **4.8.4 NETCONF/YANG access control**

1118 NACM defines a YANG information model for describing permitted/denied access operations.
 1119 NETCONF servers are responsible for enforcing access control to their resources according to
 1120 the information in their ietf-netconf-acm YANG modules. NACM allows the description of
 1121 access-controlled resources in terms of NETCONF protocol operations, nodes in YANG
 1122 datastores and/or types of notification events. NACM uses character strings to represent the
 1123 subject actors i.e., NETCONF clients. These character strings are known as “NETCONF
 1124 username”. The NACM access control information of a NETCONF server is created, updated,
 1125 and deleted per IA-station. The management of this information happens along the IA-station
 1126 lifecycle for example, manufacturing, bootstrapping, operation, maintaining, re-owning,
 1127 destructing. Moreover, the management of the NACM access control information itself is subject
 1128 to NACM access control.

1129 This document employs multiple YANG data models for fulfilling its purposes. This extends
 1130 beyond the above identified YANG modules (see 4.8.3). The NETCONF server on an IA-station
 1131 enforces access control for NETCONF/YANG resources. To meet this objective, the NETCONF
 1132 server on an IA-station is supplied with access control information for the used
 1133 NETCONF/YANG resources. NACM is employed for this purpose and profiles default access
 1134 control information for the NETCONF/YANG resources (see 6.3.2.2). This relieves other
 1135 organizations or individuals for example, manufacturers, integrators, operators, owners from
 1136 being responsible to create NACM access control information for the respective
 1137 NETCONF/YANG resources.

1138 NACM relies on character strings (known as “NETCONF username”) to refer to clients. NACM
 1139 access control information as specified in this document, populates the “NETCONF username”
 1140 character strings in NACM with role names specified in 6.3.2.1.4, c). This allows to create
 1141 default NACM information without knowing actual names of individual entities. A role name can
 1142 refer to 0, 1 or more individual entities. It is the responsibility of users to assign role names to
 1143 individual entities. This happens by binding the assigned role names to the credentials of
 1144 individual entities. The current form to express this binding is a role extension in the identity
 1145 certificates of end entities defined in this document. These are NETCONF clients, i.e., these
 1146 role extensions appear in the end entity certificates of LDevID credentials for NETCONF clients.

1147 As initial step NACM maps the NETCONF username to a set of groups. The set of groups
 1148 determines the set of rules to be applied for access-controlled resources.

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

4.8.5 Identity checking

IETF RFC 7589 (NETCONF-over-TLS) specifies that NETCONF clients check the identity of NETCONF servers (IETF RFC 7589, Clause 6) and that NETCONF servers verify the identity of NETCONF clients (IETF RFC 7589, Clause 7).

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, Clause 6, for the details of retrieving the actual and comparing it against the 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 `ietf-netconf-acm` and `ietf-x509-cert-to-name` YANG modules.

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-2018. It matches the term IA-station in this document.

The device identity refers to a set of information items about a device 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.

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, Clause 3 and 7.1).

4.8.6.2 Verifiable Device Identity

Certain aspects of device identity are verified 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. Verification of the responder's identity helps defeat DNS spoofing, component impersonation and man-in-the-middle attacks. This is

1194 specified by IETF RFC 7589 and described in IETF RFC 6125, Clause 6. Passing this check
1195 is a prerequisite before NETCONF application exchanges can happen.

- 1196 • mfg-name values in instances of the ietf-hardware YANG module. These values make
1197 claims about the IA-station manufacturer. Their verification is a means to protect against
1198 counterfeiting.

1199 The verification of IA-station identity happens according to a model that is fully specified by this
1200 document. That verification can be done in a manufacturer-agnostic manner. This verification
1201 is important before supplying locally significant credentials especially LDevID to IA-stations that
1202 are in factory-default state.

1203 **4.8.6.3 Verification Support Mechanisms**

1204 **4.8.6.3.1 General**

1205 Subclause 4.8.6.3 considers mechanisms that support device identity verification during online
1206 interactions with IA-stations.

1207 **4.8.6.3.2 Secure Transports**

1208 Sending information in plain form over a protected channel, e.g., ietf-hardware YANG module
1209 contents via NETCONF-over-TLS protects the transferred information during its transit through
1210 the network but does not vouch for the correctness of the received information e.g., the mfg-
1211 name value.

1212 **4.8.6.3.3 Secure Information**

1213 Protecting information objects by means of a cryptographic authentication code or digital
1214 signature enables verification of the authenticity and integrity of that information. These
1215 cryptographic authentication codes can use symmetric or asymmetric schemes. In case of
1216 asymmetric schemes, raw and self-signed public keys need to be distinguished from CA-signed
1217 public keys.

1218 Asymmetric schemes with CA-signed public keys are preferable for the verifiable device identity
1219 use case: claimants and verifiers share a public key; the claimant possesses the corresponding
1220 private key. The establishment and storage of the shared public keys uses public key
1221 certificates. For this approach self-signed CA certificates are to be established in an authentic
1222 manner. The number of self-signed CA certificates is independent from the number of verifiers
1223 (NCNs) as well as claimants (IA-stations).

1224 **4.8.6.3.4 IDevID and LDevID Credentials**

1225 IDevID and LDevID credentials are specified by IEEE Std 802.1AR-2018. These objects are
1226 comprised of a certification path and a private key. The certification path encompasses an end
1227 entity certificate which contains verifiable device identity in a CA-signed form. The device
1228 identity verification happens after validating the certification path (IETF RFC 5280, Clause 6)
1229 and checking the proof-of-possession for the private key. The certification path validation
1230 demands trust anchors as input arguments (IETF RFC 5280, 6.1.1 input argument (d)).

1231 Two types of credentials are distinguished by IEEE Std 802.1AR-2018:

- 1232 • IDevIDs are issued by device manufacturers. They represent an initial identity as it is known
1233 at device production-time. The initial device identity is not locally significant: it cannot
1234 contain deployment-specific information such as DNS names or IP addresses.
- 1235 • LDevIDs are issued by other actors e.g., a device user. They represent a locally significant
1236 device identity: they can contain deployment-specific information e.g., DNS names or IP
1237 addresses.

1238 IEEE Std 802.1AR-2018, Clause 6, uses signature suites to describe the subject public key and
1239 the signature fields in IDevID and LDevID certification paths. This notion is different from TLS
1240 cipher suites.

1241 NOTE IDevID and LDevID credentials also serve purposes beyond secure device identity, for instance the
1242 realization of secure transports. This facilitates the use case of NETCONF/YANG security setup from factory default
1243 state.

4.8.6.3.5 IDevID Items beyond IEEE Std 802.1AR-2018

IEEE Std 802.1AR-2018 allows verification of the following identity items:

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

NOTE 1 IEEE Std 802.1AR-2018 represents the initial device identity as an optional serialNumber attribute (OID 2.5.4.5) in the subject field of the EE certificate. This value is unique within the domain of significance of the EE certificate issuer.

NOTE 2 This verification can happen after certification path validation and the proof-of-possession checking for the private key.

The following bullet points describe options beyond IEEE Std 802.1AR-2018 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, and
- 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, and
- 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 (see 6.3.3.2.2 for more information) 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 can also bind initial device identity information.
- Items that encode device naming information appear in the subjectAltName extension.

NOTE This is specified in IETF RFC 5280, 4.2.1.6. It is further explained in 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-2018) and,
 - the hostname of the NETCONF/YANG server in LDevID credentials (IETF RFC 6125, Clause 6).
 - 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 can be provided by the device itself or by a device-external source, and

- 1293 • If it is provided in form of an unprotected information object, then the reference object
1294 that is embedded to EE certificates includes a digest value.

1295 **5 Conformance**

1296 **5.1 General**

1297 A claim of conformance to this document is a claim that the behavior of an implementation of
1298 an IA-station (see 5.5, 5.6) with its Bridge components (see 5.7, 5.8) and end station
1299 components (see 5.9, 5.10) meets the mandatory requirements of this document and may
1300 support options identified in this document. Furthermore this document includes conformance
1301 requirements for CNC and CUC implementations (see 5.11, 5.13).

1302 **5.2 Requirements terminology**

1303 The verbal forms for required expressions of provisions follow the conventions:

- 1304 a) Requirements terminology is provided in the ISO/IEC Directives Part 2:2021, Clause 7. This
1305 document can be found at www.iec.ch/members_experts/refdocs.
- 1306 b) The Profile Conformance Statement (PCS) proformas (see Annex A) reflect the occurrences
1307 of the words “shall,” “may,” and “should” within this document.
- 1308 c) This document avoids needless repetition and apparent duplication of its formal
1309 requirements by using is, is not, are, and are not for definitions and the logical
1310 consequences of conformant behavior. Behavior that is permitted but is neither always
1311 required nor directly controlled by an implementer or administrator, or whose conformance
1312 requirement is detailed elsewhere, is described by can. Behavior that never occurs in a
1313 conformant implementation or system of conformant implementations is described by
1314 cannot. The word allow is used as a replacement for the phrase “Support the ability for,”
1315 and the word capability means “can be configured to.”

1316 **5.3 Profile conformance statement (PCS)⁴**

1317 The supplier of an implementation that is claimed to conform to this document shall provide the
1318 information necessary to identify both the supplier and the implementation and shall complete
1319 a copy of the PCS proforma provided in Annex A.

1320 **5.4 Conformance classes**

1321 This document includes conformance requirements and options that are related to an entire
1322 station, as well as conformance requirements and options that are related to single Bridge or
1323 end station components within an IA-station. Figure 11 illustrates this conformance model.

4 Copyright release for the PCS: Users of this document may freely reproduce the PCS contained in this document so that it can be used for its intended purpose.

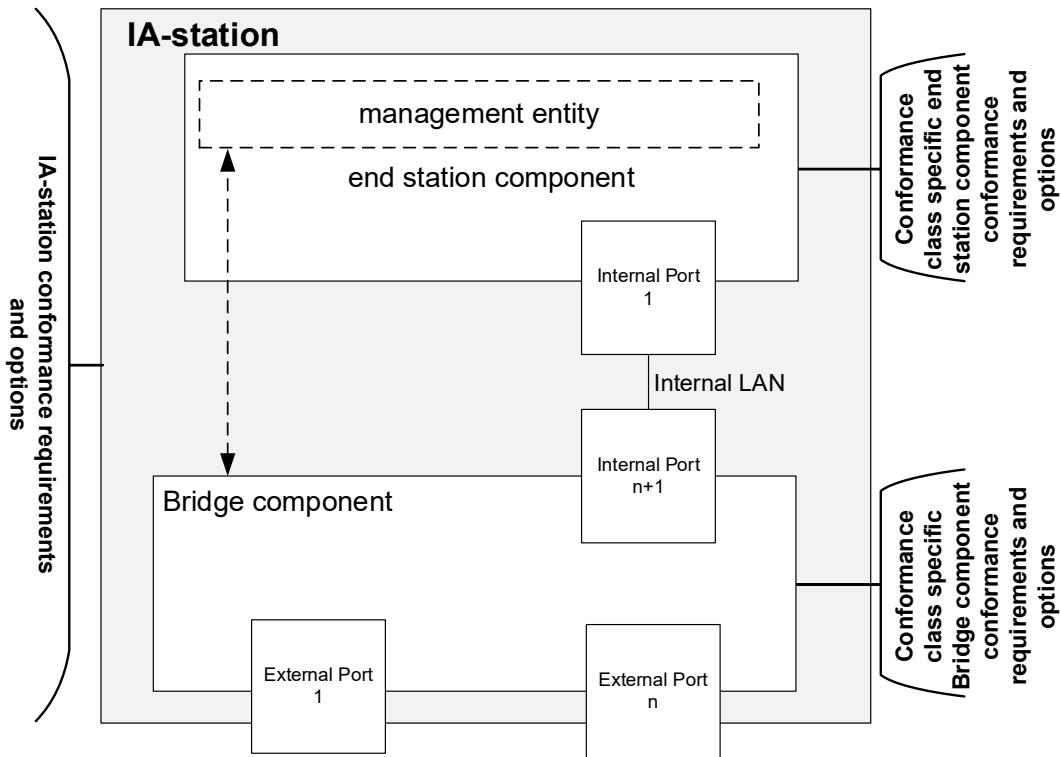


Figure 11 – IA-station conformance model

This document 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 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 list of requirements for external ports.

- 1345 a) Media Access Control (MAC) service specification according to IEEE Std 802.3-2022, Clause 2.
- 1347 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).
- 1350 c) Layer Management according to IEEE Std 802.3-2022, 5.2.4.
- 1351 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, 5 Gb/s, or 10 Gb/s together with the corresponding managed objects:

- 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 and,
 - 9) 1000BASE-T1 MAU type according to IEEE Std 802.3-2022, Clause 97.
- e) Support the YANG features and nodes of the ieee802-ethernet-interface module according to 6.4.9.2.1.
 - f) Ethernet support for time synchronization protocols according to IEEE Std 802.3-2022, Clause 90.

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

1375

1376 **5.5.2 IA-station topology discovery requirements**

1377 IA-stations for which a claim of conformance to this document is made shall support the
1378 following list of requirements.

- 1379 a) The required capabilities according to IEEE Std 802.1AB-2016, 5.3 and IEEE Std
1380 802.1ABCu-2021, 5.3.
- 1381 b) Topology discovery and verification according to 6.5.
- 1382 c) The YANG features and nodes of the ieee802-dot1ab-lldp module according to 6.4.9.2.2.

1383 **5.5.3 IA-station requirements for time synchronization**

1385 These requirements are related to the entire IA-station with all its PTP Instances and PTP Ports.
1386 IA-stations for which a claim of conformance to this document is made shall support the
1387 following list of requirements.

- 1388 a) PTP Instance requirements according to IEEE Std 802.1AS-2020, 5.4.1 items a) through i).
1389 NOTE A gPTP domain in a PTP End Instance can be used for Global Time, Working Clock, or both.
- 1390 b) Timing and synchronization management according to IEEE Std 802.1AS-2020, 5.4.2 items
1391 j) and k).
- 1392 c) PTP Instance requirements according to 6.2.2.
- 1393 d) PTP Protocol requirements according to 6.2.3.
- 1394 e) Error generation limits according to 6.2.4.
- 1395 f) PtplInstanceSyncStatus state machine according to 6.2.6.
- 1396 g) The transmission of the Drift_Tracking TLV according to IEEE Draft Std P802.1ASdm, 5.4.2
1397 item n).
- 1398 h) External port configuration capability according to IEEE Std 802.1AS-2020, 5.4.2 item g).
- 1399 i) MAC-specific timing and synchronization methods for IEEE Std 802.3 full-duplex links
1400 according to IEEE Std 802.1AS-2020, 5.5 items a) through c) and item h).
- 1401 j) The YANG features and nodes of the:

- 1402 i) ieee1588-ptp module according to 6.4.9.2.3.1,
1403 ii) ieee802-dot1as-ptp module according to 6.4.9.2.3.2, and
1404 iii) ieee802-dot1as-hs module according to 6.4.9.2.3.3.
1405 k) The message timestamp point according to IEEE Std 802.1AS-2020, 11.3.9.
1406 l) The Common Mean Link Delay Service (CMLDS) according to IEEE Std 802.1AS-2020,
1407 11.2.17.
1408 m) The descriptionDS according to IEEE Std 1588-2019, 8.2.5.

1410 **Editor's Note:** The numbering of some items referenced in IEEE Std 802.1AS-2020 may be
1411 affected by IEEE Draft Std 802.1ASdm. Renumbering of these items is deferred until this
1412 amendment is through SA ballot.

1414 **5.5.4 IA-station requirements for management**

1415 **5.5.4.1 General**

1416 These requirements are related to the secured management of an entire IA-station independent
1417 of the internal component structure.

1418 **5.5.4.2 Secure management exchanges**

1419 IA-stations for which a claim of conformance to this document is made shall support the
1420 following list of requirements.

- 1421 a) NETCONF server functionality according to IETF RFC 6241 including:
1422 1) Candidate configuration capability as described in IETF RFC 6241, 8.3,
1423 2) Rollback-on-Error capability as described in IETF RFC 6241, 8.5, and
1424 3) Validate capability as described in IETF RFC 6241, 8.6.
1425 b) NETCONF-over-TLS server according to 6.3.2.1 and 6.3.4.
1426 c) Secure Device Identity according to 6.3.3 and IEEE Std 802.1AR-2018, 5.3 a) using the
1427 signature suite in IEEE Std 802.1AR-2018 9.2, 5.3 d), and 5.3 i).
1428 d) PKIX according to 6.3.2.1.4 and IETF RFC 5280, 4.1, 4.2.1.1-3, 4.2.1.6, 6.1, 6.2.
1429 e) NACM (IETF RFC 8341) supporting four different roles according to 6.3.2.1.4 c).
1430 f) The YANG features and nodes of the:
1431 1) ietf-keystore module according to 6.4.9.2.4.1,
1432 2) ietf-netconf-acm module according to 6.4.9.2.4.2 and,
1433 3) ietf-truststore according to 6.4.9.2.4.3.
1434 g) NETCONF Event Notifications according to IETF RFC 5277 including operations according
1435 to IETF RFC 5277, Clause 2.
1436 h) Support of Dynamic Subscriptions to YANG Events and Datastores over NETCONF
1437 according to 6.4.7.7.
1438 i) NETCONF Extensions to support the Network Management Datastore Architecture (NMDA)
1439 as described in IETF RFC 8526.
1440 j) DHCP client according to IETF RFC 2131, 4.1, 4.2, and 4.4.
1441 k) Support at least one of the following asymmetric key pair generation methods.
1442 1) Component-internal generation according to 6.3.4.3.
1443 2) Component-external generation according to 6.3.4.3.
1444 l) Support storage of at least one IDevID credential according to 6.3.4.1 and one LDevID-
1445 NETCONF credential according to 6.3.3.4.2.5.

1446 IA-stations for which a claim of conformance to this document is made should support internal
1447 key generation according to 6.3.4.3.2.

1448 **5.5.4.3 IA-station management YANG modules**

1449 IA-stations for which a claim of conformance to this document is made shall support the YANG
1450 features and nodes for IA-station management of the:

- 1451 a) ietf-system-capabilities module according to 6.4.9.2.5.1,
- 1452 b) ietf-yang-library module as according to 6.4.9.2.5.2,
- 1453 c) ietf-yang-push module according to and 6.4.9.2.5.3,
- 1454 d) ietf-notification-capabilities module according to 6.4.9.2.5.4,
- 1455 e) ietf-subscribed-notifications module according to 6.4.9.2.5.5,
- 1456 f) Diagnostics using YANG-Push subscriptions according to 6.4.7,
- 1457 g) ietf-netconf-monitoring module according to 6.4.9.2.5.6,
- 1458 h) ietf-system module according to 6.4.9.2.5.7,
- 1459 i) ietf-hardware module according to 6.4.9.2.5.8,
- 1460 j) ietf-interfaces module according to 6.4.9.2.5.9,
- 1461 k) ieee802-dot1q-bridge module according to 6.4.9.2.5.10,
- 1462 l) iecieee60802-ethernet-interface module according to 6.4.9.2.5.11 and,
- 1463 m) ietf-netconf-server according to 6.4.9.2.5.12.
- 1464 n) iecieee60802-bridge according to 6.4.9.2.5.11.
- 1465 o) ietf-subscribed-notifications according to 6.4.9.2.5.13.
- 1466 p) iecieee60802-subscribed-notifications according to 6.4.9.2.5.13.
- 1467 q) iecieee60802-ia-station according to 6.4.9.2.5.11.

1468

1469 **5.5.4.4 Digital data sheet**

1470 IA-stations for which a claim of conformance to this document is made shall provide a 60802
1471 instance data file according to 6.4.8. The instance data file shall contain at least the YANG
1472 nodes of 6.4.9 that are marked with [m]. Nodes marked with [c] shall be included if the
1473 associated feature is supported.

1474 NOTE It is the user's responsibility to ensure that the filename is unique by using a standardized mechanism (for
1475 example, GUID, URL, or ReverseDomainName).

1476 **5.6 IA-station options**

1477 **5.6.1 IA-station PHY and MAC options for external ports**

1478 IA-stations for which a claim of conformance to this document is made may support the following
1479 list of requirements.

- 1480 a) Power over Ethernet (PoE) over 2 Pairs according to IEEE Std 802.3-2022, Clause 33.
- 1481 b) Power Interfaces according to IEEE Std 802.3-2022, Clause 104.
- 1482 c) Power over Ethernet according to IEEE Std 802.3-2022 Clause 145.

1483

1484 **5.6.2 IA-station options for time synchronization**

1485 IA-stations for which a claim of conformance to this document is made may support the following
1486 list of requirements.

- 1487 a) The media-independent timeTransmitter capability according to IEEE Std 802.1AS-2020,
1488 5.4.2 item b) as amended by IEEE Std 802.1ASdr-2024.
- 1489 b) Grandmaster PTP Instance capability according to IEEE Std 802.1AS-2020, 5.4.2 item c).

- 1490 c) More than one PTP port as a PTP Relay Instance according to IEEE Std 802.1AS-2020,
1491 5.4.2 item d).
1492 d) Transmit of the Signaling message according to IEEE Std 802.1AS-2020, 5.4.2 item e).
1493 e) The SyncIntervalSetting state machine according to IEEE Std 802.1AS-2020, 5.4.2 item h).
1494 f) One or more application interfaces according to IEEE Std 802.1AS-2020, 5.4.2 item i).
1495 g) Hot standby redundancy requirements according to IEEE Draft Std P802.1ASdm, 5.4.2, item
1496 m).

1497

1498 **5.6.3 IA-station options for management**

1499 IA-stations for which a claim of conformance to this document is made may support the following
1500 list of requirements.

- 1501 a) Writable-Running capability according to IETF RFC 6241, 8.2.
1502 b) Confirmed Commit capability according to IETF RFC 6241, 8.4.
1503 c) Distinct Startup capability according to IETF RFC 6241, 8.7.
1504 d) URL capability according to IETF RFC 6241, 8.8.
1505 e) XPath capability according to IETF RFC 6241, 8.9.
1506 f) NETCONF-over-TLS server supporting TLS version 1.2, according to IETF RFC 7589,
1507 6.3.2.1 and 6.3.4.
1508 g) NETCONF-over-TLS server supporting TLS version 1.3, according to IETF RFC 7589 and
1509 draft-ietf-netconf-over-tls13, with one or more of the following cipher suites according to
1510 IETF RFC 8446, 9.1:
1511 • TLS_AES_128_GCM_SHA256,
1512 • TLS_AES_256_GCM_SHA384, and
1513 • TLS_CHACHA20_POLY1305_SHA256.
1514 and one or more of the following signature schemes:
1515 • ecdsa_secp256r1_sha256 according to NIST FIPS 186-5 and NIST SP 800-186, 3.2.1.3,
1516 • ecdsa_secp521r1_sha512 according to NIST FIPS 186-5 and NIST SP 800-186, 3.2.1.5,
1517 • ed25519 according to IETF RFC 8032, 5.1, and
1518 • ed448 according to IETF RFC 8032, 5.2.
1519 h) PKIX according to IETF RFC 5280, 4.2.1.13, Clause 5, and 6.3.
1520

1521 **5.7 Bridge component requirements**1522 **5.7.1 Common Bridge component requirements**

1523 A Bridge component implementation of any conformance class for which a claim of conformance
1524 to this document is made shall support the following list of requirements.

- 1525 a) C-VLAN component requirements according to IEEE Std 802.1Q-2022, 5.5 and 5.4 except
1526 item o) in IEEE Std 802.1Q-2022, 5.4.
1527 b) The use of Customer VLAN Identifiers (C-VID).
1528 c) FDB to contain Static and Dynamic VLAN Registration Entries for a minimum of 10 VIDs
1529 according to IEEE Std 802.1Q-2022, 8.8.
1530 NOTE 1 An example use case for 10 VIDs: 2 VIDs for IA time-aware stream or IA stream traffic, 2 VIDs for IA
1531 time-aware stream or IA stream redundancy, 4 VIDs for IA traffic engineered non-stream or IA non-stream traffic,
1532 1 isolation VID, and 1 default VID (see 6.4.5.2).
1533 d) Translation of VIDs through support of the VID Translation Table or through support of both
1534 the VID Translation Table and Egress VID translation table on one or more Bridge Ports
1535 according to IEEE Std 802.1Q-2022, 6.9.

- 1536 e) The strict priority algorithm for transmission selection on each port for each traffic class
1537 according to IEEE Std 802.1Q-2022, 8.6.8.1.
- 1538 f) The capability to disable Priority-based flow control if it is implemented according to IEEE
1539 Std 802.1Q-2022, Clause 36.
- 1540 g) The Priority Regeneration requirements according to IEEE Std 802.1Q-2022, 5.4.1, item o).
- 1541 h) MST according to IEEE Std 802.1Q-2022, 5.4.1.1 a) to i) and k) to o) and 6.4.2.4.
- 1542 i) TE-MSTID according to IEEE Std 802.1Q-2022, 8.6. and 8.8 and IEEE Std 802.1Q-2022,
1543 5.5.2.
- 1544 j) Spanning tree, VLAN, and TE-MSTID configuration according to 6.4.2.4.
- 1545 k) The I2vlan interface types per 6.4.2.5.
- 1546 l) Flow meters including support of at least 3 flow meters per port, according to IEEE Std
1547 802.1Q-2022 8.6.5.3 items a), b), and f) and 8.6.5.5 items a) through c). A flow meter should
1548 set following IEEE Std 802.1Q-2022, 8.6.5.5 parameters to values:
1549 • Item d) Excess Information Rate (EIR) = 0,
1550 • Item e) Excess burst size (EBS) = 0, and
1551 • Item g) Color mode (CM) = color_blind.

1552 NOTE 1 When CM = color_blind, DropOnYellow (IEEE Std 802.1Q-2022, 8.6.5.5, item h), MarkAllFramesRed
1553 (IEEE Std 802.1Q-2022, 8.6.5.1.3, item j), and MarkAllFramesRedEnable (IEEE Std 802.1Q-2022, 8.6.5.5, item
1554 i) are not used.

1555 NOTE 2 For example, an implementation could contain one flow meter for broadcast traffic, one flow meter for
1556 multicast traffic and one flow meter for unicast traffic.

- 1557 m) Support the YANG features and nodes for flow meter configuration according to
1558 6.4.9.2.5.14.
- 1559 n) Support stream identification component behaviors according to IEEE Std 802.1CB-2017,
1560 5.3 and IEEE Std 802.1CBdb-2021, 5.5 d).

1561 **5.7.2 ccA Bridge component requirements**

1562 A Bridge component implementation for which a claim of conformance to ccA of this document
1563 is made shall support the following list of requirements.

- 1564 a) Common Bridge component requirements according to 5.7.1.
- 1565 b) At least 2 PTP Instances according to 5.5.3.
- 1566 c) Eight queues according to IEEE Std 802.1Q-2022, 8.6.6.
- 1567 d) Enhancements for scheduled traffic for data rates of 100 Mb/s and 1 Gb/s according to IEEE
1568 Std 802.1Q-2022, 5.4.1 items ab) and ac) including:
1569 1) TickGranularity of less than or equal to 10 ns according to IEEE Std 802.1Q-2022,
1570 8.6.9.4.16 and Table 12-32,
1571 2) the allowable delay between the transmission selection timing point and the on-the-wire
1572 timing point, less any delay for the PHY (IEEE Std 802.1Q-2022, Figure 12-6), of less
1573 than or equal to 10 ns, and
1574 NOTE Transmission selection timing points have a granularity of 1 ns; however, operation is determined by the
1575 precision of the "tick" event.
1576 3) support of the YANG features and nodes of the ieee802-dot1q-sched module according
1577 to 6.4.9.3.2.
1578 4) support of the YANG features and nodes of the iecieee60802-sched-bridge module
1579 according to 6.4.9.3.3.
1580 e) Frame preemption according to IEEE Std 802.1Q-2022, 5.4.1 item ae), for data rates of
1581 100 Mb/s and 1 Gb/s, including:
1582 1) support of Interspersing Express Traffic with preemptable traffic according to IEEE
1583 Std 802.3-2022, Clause 99, including support of the Additional Ethernet Capabilities for
1584 TLV in an LLDPDU to indicate supported functions of frame preemption according to
1585 IEEE Std 802.3-2022, 79.3.7, and

- 1586 2) support of the YANG features and nodes of the ieee802-dot1q-preemption module
1587 according to 6.4.9.3.4.

1588

1589 **5.7.3 ccb Bridge component requirements**

1590 A Bridge component implementation for which a claim of conformance to ccb of this document
1591 is made shall support the following list of requirements.

- 1592 a) Common Bridge component requirements according to 5.7.1.
1593 b) At least 1 PTP Instance according to 5.5.3.
1594 c) At least four queues according to IEEE Std 802.1Q-2022, 8.6.6.

1595

1596 **5.8 Bridge component options**

1597 **5.8.1 Common Bridge component options**

1598 A Bridge component implementation of any conformance class for which a claim of conformance
1599 to this document is made may support the operation of the credit-based shaper algorithm
1600 according to IEEE Std 802.1Q-2022, 8.6.8.2 on all Ports as the transmission selection algorithm
1601 for at least 4 traffic classes including support of the YANG features and nodes of the <ieee-
1602 cbs> module according to 6.4.9.3.5.

1603 **5.8.2 ccA Bridge component options**

1604 A Bridge component implementation for which a claim of conformance to ccA of this document
1605 is made may support the following list of requirements.

- 1606 a) Any or none of the common Bridge component options according to 5.8.1.
1607 b) More than 2 PTP Instances according to 5.5.3.
1608 c) Enhancements for scheduled traffic for data rates of 10 Mb/s, 2,5 Gb/s, 5 Gb/s, and 10 Gb/s
1609 according to IEEE Std 802.1Q-2022, 5.4.1 items ab) and ac) including:
1610 1) TickGranularity of less than or equal to 10 ns according to IEEE Std 802.1Q-2022,
1611 8.6.9.4.16 and Table 12-32,
1612 2) the allowable delay between the transmission selection timing point and the on-the-wire
1613 timing point, less any delay for the PHY (IEEE Std 802.1Q-2022, Figure 12-6), of less
1614 than or equal to 10 ns, and
1615 3) support of the YANG features and nodes of the ieee802-dot1q-sched module according
1616 to 6.4.9.3.2.
1617 4) support of the YANG features and nodes of the iec60802-sched-bridge module
1618 according to 6.4.9.3.3.

- 1619 d) Frame preemption according to IEEE Std 802.1Q-2022, 5.4.1 item ae), for data rates of 10
1620 Mb/s, 2,5 Gb/s, 5 Gb/s, and 10 Gb/s, including:

1621 NOTE IEEE Std 802.3de-2022, 99.1, comprises 10 Mb/s.

- 1622 1) support of Interspersing Express Traffic with preemptable traffic according to IEEE
1623 Std 802.3-2022, Clause 99, including support of the Additional Ethernet Capabilities for
1624 TLV in an LLDPDU to indicate supported functions of frame preemption according to
1625 IEEE Std 802.3-2022, 79.3.7, and

- 1626 2) support of the YANG features and nodes of the ieee802-dot1q-preemption module
1627 according to 6.4.9.3.4.

1628

1629 **5.8.3 ccb Bridge component options**

1630 A Bridge component implementation for which a claim of conformance to ccb of this document
1631 is made may support the following list of requirements.

- 1632 a) Any or none of the common Bridge component options according to 5.8.1.
1633 b) Up to eight queues according to IEEE Std 802.1Q-2022, 8.6.6.

- 1634 c) More than 1 PTP Instance according to 5.5.3.
- 1635 d) Enhancements for scheduled traffic according to IEEE Std 802.1Q-2022, 5.4.1 items ab)
1636 and ac) including:
 - 1637 1) TickGranularity of less than or equal to 10 ns according to IEEE Std 802.1Q-2022,
1638 8.6.9.4.16 and Table 12-32,
 - 1639 2) the allowable delay between the transmission selection timing point and the on-the-wire
1640 timing point, less any delay for the PHY (IEEE Std 802.1Q-2022, Figure 12-6), of less
1641 than or equal to 10 ns, and
 - 1642 3) support of the YANG features and nodes of the ieee802-dot1q-sched module according
1643 to 6.4.9.3.2.
 - 1644 4) support of the YANG features and nodes of the iecieee60802-sched-bridge module
1645 according to 6.4.9.3.3.
- 1646 e) Frame preemption according to IEEE Std 802.1Q-2022, 5.4.1 item ae), including:
 - 1647 1) support of Interspersing Express Traffic with preemptable traffic according to IEEE
1648 Std 802.3-2022, Clause 99 including support of the Additional Ethernet Capabilities for
1649 TLV in an LLDPDU to indicate supported functions of frame preemption according to
1650 IEEE Std 802.3-2022, 79.3.7, and
 - 1651 2) support of the YANG features and nodes of the ieee802-dot1q-preemption module
1652 according to 6.4.9.3.4.

1653

1654 **5.9 End station component requirements**

1655 **5.9.1 Common end station Component requirements**

1656 An end station component implementation of any conformance class for which a claim of
1657 conformance to this document is made shall support the following list of requirements.

- 1658 a) The use of at least one customer VID for IA traffic engineered non-stream or IA non-stream
1659 traffic.
- 1660 b) The use of an additional customer VID for IA time-aware stream traffic if that traffic type
1661 category is supported.
- 1662 c) The use of an additional customer VID for IA stream traffic if that traffic type category is
1663 supported.
- 1664 d) The use of an additional customer VID for IA time-aware stream traffic if redundancy for that
1665 traffic type category is supported.
- 1666 e) The use of an additional customer VID for IA stream traffic if redundancy for that traffic type
1667 category is supported.
- 1668 f) Participate in only a single Configuration Domain.
- 1669 g) The use of an additional customer VID for an isolation VLAN.
- 1670 h) The use of an additional customer VID for a default VLAN

1671

1672 **ccA end station component requirements**

1673 An end station component implementation for which a claim of conformance to ccA of this
1674 document is made shall support the following list of requirements.

- 1675 a) Common end station component requirements according to 5.9.1.
- 1676 b) At least 2 PTP Instances according to 5.5.3.
- 1677 c) End station requirements for enhancements for scheduled traffic according to IEEE Std
1678 802.1Q-2022, 5.25, for data rates of 100 Mb/s and 1 Gb/s including:
 - 1679 1) TickGranularity of less than or equal to 10 ns according to IEEE Std 802.1Q-2022,
1680 8.6.9.4.16 and Table 12-32,

- 1681 2) the allowable delay between the transmission selection timing point and the on-the-wire
1682 timing point, less any delay for the PHY (IEEE Std 802.1Q-2022, Figure 12-6), of less
1683 than or equal to 10 ns, and
- 1684 3) support of the YANG features and nodes of the ieee802-dot1q-sched module according
1685 to 6.4.9.3.2.
- 1686 4) support of the YANG features and nodes of the iecieee60802-sched-bridge module
1687 according to 6.4.9.3.3.
- 1688 d) End station requirements for frame preemption according to IEEE Std 802.1Q-2022, 5.26,
1689 for data rates of 100 Mb/s, and 1 Gb/s, if the IA time-aware stream traffic or the IA stream
1690 traffic type categories are supported, including:
- 1691 1) support of Interspersing Express Traffic according to IEEE Std 802.3-2022, Clause 99,
1692 including support of the Additional Ethernet Capabilities TLV in an LLDPDU to indicate
1693 supported functions of frame preemption according to IEEE Std 802.3-2022, 79.3.7 and
1694 Table 79-8, and
- 1695 2) support of the YANG features and nodes of the ieee802-dot1q-preemption module
1696 according to 6.4.9.3.4.

1698 **5.9.3 ccB end station component requirements**

1699 An end station component implementation for which a claim of conformance to ccB of this
1700 document is made shall support the following list of requirements: Common end station
1701 component requirements according to 5.9.1.

1702 **5.10 End station component options**

1703 **5.10.1 Common end station component options**

1705 An end station component implementation of any conformance class for which a claim of
1706 conformance to this document is made may support the following list of requirements.

- 1707 a) The operation of the credit-based shaper algorithm according to IEEE Std 802.1Q-2022,
1708 8.6.8.2 including support of the YANG features and nodes of the ieee802-dot1q-cbs module
1709 according to 6.4.9.3.5.
- 1710 b) Talker end system behaviors according to IEEE Std 802.1CB-2017, as amended by IEEE
1711 Std 802.1CBdb-2021 and IEEE Std 802.1CBcv-2021, 5.6, and 5.7 c) on one or more ports
1712 and for 1 or more Compound Streams, including support of the ieee802-dot1cb-stream-
1713 identification and ieee802-dot1cb-frer YANG modules according to 6.4.9.3.6.
- 1714 c) Listener end system behaviors according to IEEE Std 802.1CB-2017, as amended by IEEE
1715 Std 802.1CBdb-2021 and IEEE Std 802.1CBcv-2021, 5.9 on one or more ports and for 1 or
1716 more Compound Streams, including support of the ieee802-dot1cb-stream-identification
1717 and ieee802-dot1cb-frer YANG modules according to 6.4.9.3.6.

1719 **5.10.2 ccA end station component options**

1720 An end station component implementation for which a claim of conformance to ccA of this
1721 document is made may support the following list of requirements.

- 1722 a) Common end station options according to 5.10.1
- 1723 b) More than 2 PTP Instances according to 5.5.3.
- 1724 c) End station requirements for enhancements for scheduled traffic according to IEEE Std
1725 802.1Q-2022, 5.25, for data rates of 10 Mb/s, 2,5 Gb/s, 5 Gb/s, and 10 Gb/s including:
- 1726 1) TickGranularity of less than or equal to 10 ns according to IEEE Std 802.1Q-2022,
1727 8.6.9.4.16 and Table 12-32,
- 1728 2) the allowable delay between the transmission selection timing point and the on-the-wire
1729 timing point, less any delay for the PHY (IEEE Std 802.1Q-2022, Figure 12-6), of less
1730 than or equal to 10 ns, and

- 1731 3) support of the YANG features and nodes of the ieee802-dot1q-sched module according
1732 to 6.4.9.3.2.
- 1733 4) support of the YANG features and nodes of the iecieee60802-sched-bridge module
1734 according to 6.4.9.3.3.
- 1735 d) End station requirements for frame preemption according to IEEE Std 802.1Q-2022, 5.26,
1736 for data rates of 10 Mb/s, 2,5 Gb/s, 5 Gb/s, and 10 Gb/s including:
1737 NOTE IEEE Std 802.3de-2022, 99.1, comprises 10 Mb/s.
- 1738 1) support of Interspersing Express Traffic according to IEEE Std 802.3-2022, Clause 99,
1739 and IEEE Std 802.3de, 99.1, including support of the Additional Ethernet Capabilities
1740 TLV in an LLDPDU to indicate supported functions of frame preemption according to
1741 IEEE Std 802.3-2022, 79.3.7 and Table 79-8, and
- 1742 2) support of the YANG features and nodes of the ieee802-dot1q-preemption module
1743 according to 6.4.9.3.4.

1744 **5.10.3 ccb end station component options**

1746 An end station component implementation for which a claim of conformance to ccb of this
1747 document is made may support the following list of requirements.

- 1748 a) Common end station component options according to 5.10.1.
- 1749 b) One or more PTP Instances according to 5.5.3.
- 1750 c) End station requirements for enhancements for scheduled traffic according to IEEE Std
1751 802.1Q-2022, 5.25 including:
- 1752 1) TickGranularity of less than or equal to 10 ns according to IEEE Std 802.1Q-2022,
1753 8.6.9.4.16 and Table 12-32,
- 1754 2) the allowable delay between the transmission selection timing point and the on-the-wire
1755 timing point, less any delay for the PHY (IEEE Std 802.1Q-2022, Figure 12-6), of less
1756 than or equal to 10 ns, and
- 1757 3) support of the YANG features and nodes of the ieee802-dot1q-sched module according
1758 to 6.4.9.3.2.
- 1759 4) support of the YANG features and nodes of the iecieee60802-sched-bridge module
1760 according to 6.4.9.3.3.
- 1761 d) End station requirements for frame preemption according to IEEE Std 802.1Q-2022, 5.26
1762 including:
- 1763 1) support of Interspersing Express Traffic according to IEEE Std 802.3-2022, Clause 99,
1764 and IEEE Std 802.3de, 99.1, including support of the Additional Ethernet Capabilities
1765 TLV in an LLDPDU to indicate supported functions of frame preemption according to
1766 IEEE Std 802.3-2022, 79.3.7 and Table 79-8, and
- 1767 2) support of the YANG features and nodes of the ieee802-dot1q-preemption module
1768 according to 6.4.9.3.4.

1769 **5.11 CNC requirements**

1771 CNCs for which a claim of conformance to this document is made shall support the following
1772 list of requirements.

- 1773 a) TSN CNC station requirements according to IEEE Std 802.1Q-2022, 5.29.
- 1774 b) NETCONF-over-TLS server and related client functionality 5.5.4.2.
- 1775 c) The common YANG modules, features, and nodes according to 6.4.9.2.
- 1776 d) The optional YANG modules, features, and nodes according to 0.
- 1777 e) Be integrated in an IA-station that supports the use of at least one customer VLAN Identifier
1778 for an isolation VLAN and one VLAN identifier for a default VLAN.
- 1779 f) Support CUC/CNC YANG modules, features and nodes according to 6.4.9.4.

1780

1781 5.12 CNC options

1782 There are no optional CNC features.

1783 5.13 CUC requirements

1784 CUCs for which a claim of conformance to this document is made shall support the following
1785 list of requirements.

- 1786 a) Support NETCONF-over-TLS client functionality with client related security requirements
1787 according to 5.5.4.2.
- 1788 b) The TSN UNI YANG module, features, and nodes according to 6.4.9.4.1.
- 1789 c) The ietf-netconf-client module according to 6.4.9.4.1.

1790 5.14 CUC options

1791 There are no optional CUC features.

1792 6 Required functions for an industrial network**1793 6.1 General**

1794 Clause 6 provides requirements specific to this document and the industrial use case.

1795 6.2 Synchronization**1796 6.2.1 General**

1797 An IA-station can contain more than one Grandmaster PTP Instance and PTP End Instance to
1798 support:

- 1799 a) hot-standby use cases, or
- 1800 b) Working Clock or Global Time.

1801 For further explanation of the requirements for time synchronization, refer to Annex D.

1802 6.2.2 PTP Instance requirements

1803 A Grandmaster PTP Instance, a PTP Relay Instance and a PTP End Instance, and the Working
1804 Clock or Global Time clocks connected to them, shall meet the following requirements under
1805 their allowed working conditions and for their lifetime.

- 1806 a) The fractional frequency offset of the LocalClock relative to the nominal frequency shall be
1807 according to Table 9.
- 1808 b) The range of the rate of change of fractional frequency offset of the LocalClock shall be
1809 according to Table 9.
- 1810 c) During operation, the Working Clock and Global Time at Grandmaster PTP Instances and
1811 PTP End Instances shall increase monotonically, where monotonic means that for a time y
1812 that occurs after time x , the ClockTarget's timestamp of y is greater than or equal to the
1813 ClockTarget's timestamp of x .
- 1814 d) The Working Clock and Global Time at a PTP End Instance can be controlled by applying a
1815 frequency change over a period of time. The frequency applied can have a fine resolution
1816 to speed up or slow down the clock smoothly, and it has a total range of frequency
1817 adjustment.
- 1818 e) For the Global Time at a PTP End Instance, the maximum value of frequency adjustment
1819 shall be according to Table 9.
- 1820 f) For the Working Clock at a PTP End Instance, the maximum value of frequency adjustment
1821 shall be according to Table 9.

1822 For Working Clock or Global Time, decoupled from a ClockTarget, a higher maximum value of
1823 frequency adjustment and maximum rate of change of fractional frequency offset are allowed.
1824 As soon as it is coupled (or coupled again) a) to f) apply.

1825

1826

Table 9 – Required values

Topic	Value
Local Clock at non-Grandmaster PTP Instance, range of fractional frequency offset relative to the nominal frequency	± 50 ppm
Local Clock at non-Grandmaster PTP Instance, range of rate of change of fractional frequency offset with respect to the nominal frequency	± 1 ppm/s
Working Clock and Global Time (acting as ClockSource) and Local Clock at Grandmaster PTP Instance, range of fractional frequency offset with respect to the nominal frequency	± 25 ppm
Working Clock and Global Time (acting as ClockSource) and Local Clock at Grandmaster PTP Instance, range of rate of change of fractional frequency offset with respect to the nominal frequency (steady state, see Annex D.2.3)	± 1 ppm/s
Working Clock and Global Time (acting as ClockSource) at Grandmaster PTP Instance, range of rate of change of fractional frequency offset (transient, see Annex D.2.3)	± 3 ppm/s
Working Clock and Global Time at PTP End Instance, maximum value of frequency adjustment	± 250 ppm over any observation interval of 1 ms
NOTE 1 If the Grandmaster PTP Instance implementation is such that its Working Clock and Local Clock are the same or otherwise locked to the same frequency, the normative requirements on the Working Clock take priority over those on the Local Clock.	
NOTE 2 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, the adjustment is expected to be gradual over the defined interval rather than instantaneous.	
NOTE 3 The example algorithms that track clock drift use up to 4 seconds of historical data and can take that length of time to respond to changes in clock drift. The example algorithm has been used for simulating cases where no fast changes in the observed frequency drift rate were observed. In most of the real-life situations, this condition can be satisfied.	

1827

1828

6.2.3 PTP protocol requirements

1830 Table 10 shows the required protocol times.

1831

Table 10 – Protocol settings

Topic	Value
Nominal time between successive Announce messages (announce interval)	1 s
Nominal time between successive Pdelay_Req messages (Pdelay_Req message transmission interval)	125 ms
Range of allowed time between successive Pdelay_Req messages	119 ms to 131 ms
Nominal time between successive Sync messages at the Grandmaster (Sync message transmission interval)	125 ms
Range of allowed time between successive Sync messages at the Grandmaster	119 ms to 131 ms
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 Measured Mean: ≤ 5 ms

Topic	Value
Maximum time between transmission of a Sync message and transmission of the related Follow_Up message	2,5 ms
Time between reception of a Pdelay_Req message and transmission of the subsequent Pdelay_Resp message (i.e. Pdelay turnaround time).	Maximum: 15 ms
NOTE 1 A consequence of having a single allowed value of mean sync interval is that syncLocked mode is achieved. If the timeTransmitter port sync interval is the same as that of the timeReceiver port, syncLocked mode is achieved.	
NOTE 2 The values contained in this table apply to both the Working Clock and Global Time.	

1832

6.2.4 Clock Control System requirements for PTP End Instances

Table 11 shows the required Clock control system characteristics at a PTP End Instance.

1835

Table 11 – Clock Control System requirements

Topic	Value
Maximum Bandwidth (Hz)	1,0 Hz
Minimum Bandwidth (Hz)	0,7 Hz
Maximum Gain Peaking (dB)	2,2 dB
Minimum absolute value of Roll-off	20 dB/decade
NOTE 1 For more information regarding the clock control system see Annex C.	
NOTE 2 The values contained in this table apply to both the Working Clock and Global Time.	

1836

6.2.5 Error Generation Limits

Table 12 shows the required limits on error generation at a Grandmaster PTP instance. A limit on error generation for a Grandmaster PTP Instance is a limit on the amount of error it generates in the output Sync message compared to its Working Clock (acting as ClockSource) and Local Clock. See D.3.4.

1842

Table 12 – Error generation limits for Grandmaster PTP Instance

Topic	Value
(preciseOriginTimestamp + correctionField) in PTP timing message minus Working Clock at Grandmaster when Sync message is transmitted	Allowable range of the measured mean: - 10 ns to + 10 ns Range around the measured mean within which 90% of measurements fall: ± 7 ns Range around the measured mean within which 100% of measurements fall: ± 10 ns
True Rate Ratio between Working Clock at Grandmaster and Local Clock when Sync message is transmitted minus rateRatio field in Follow_Up information TLV	Mean 0 ppm ± 0,1 ppm Standard deviation ≤ 0,1 ppm
syncEgressTimestamp in Drift_Tracking TLV minus Local Clock when Sync message is transmitted	Range around the measured mean within which 90% of measurements fall: ± 7 ns Range around the measured mean within which 100% of measurements fall: ± 10 ns

Topic	Value
Note 1 “Allowable range of the measured mean” specifies limits on constant error. “Range around the measured mean” and “Allowable measured standard deviation around the measured mean” specify limits on dynamic error. A limit on the constant error of syncEgressTimestamp is not specified because constant error in this characteristic is not a source of time synchronization error.	

1843

1844 Table 13 shows the required limits on error generation at a PTP Relay instance. A limit on error
 1845 generation for a PTP Relay Instance is a limit on the amount of error it adds to the output Sync
 1846 message compared to the input Sync message. These requirements are written for the case
 1847 when errors due to change of fractional frequency offset of its Local Clock with respect to the
 1848 nominal frequency and errors in the input Sync message are negligible with respect to the
 1849 specified error generation limits. See D.3.5.

1850

Table 13 – Error generation limits for PTP Relay Instance

Topic	Value
(preciseOriginTimestamp + correctionField) in the PTP timing message transmitted by PTP Relay Instance minus Working Clock at Grandmaster when the Sync message is transmitted, while... <ul style="list-style-type: none"> • Working Clock (acting as ClockSource) at Grandmaster is stable. • Local Clock at upstream PTP Instance is stable • meanLinkDelay between upstream PTP Instance and PTP Relay Instance is negligible 	Allowable range of the measured mean: - 2 ns to + 2 ns Range around the measured mean within which 90% of measurements fall: ± 10 ns Range around the measured mean within which 100% of measurements fall: ± 20 ns
rateRatio field in the Follow_Up information TLV transmitted by PTP Relay Instance minus the Rate Ratio from the PTP Relay Instance's Local Clock to the WorkingClock at the Grandmaster, while... <ul style="list-style-type: none"> • Working Clock (acting as ClockSource) at Grandmaster is stable. • Local Clock at upstream PTP Instance is stable. 	Allowable range of the measured mean: - 0,1 ppm to + 0,1 ppm Allowable measured standard deviation around the measured mean: 0,02 ppm
rateRatio field in the Follow_Up information TLV transmitted by PTP Relay Instance minus the Rate Ratio from the PTP Relay Instance's Local Clock to the WorkingClock at the Grandmaster, while... <ul style="list-style-type: none"> • WorkingClock (acting as ClockSource) at Grandmaster PTP Instance, fractional frequency offset with respect to the nominal frequency is increasing at 1 ppm/s • Local Clock at upstream PTP Instance is stable. 	Allowable range of the measured mean: - 0,1 ppm to + 0,1 ppm Allowable measured standard deviation around the measured mean: 0,08 ppm
rateRatio field in the Follow_Up information TLV transmitted by PTP Relay Instance minus the Rate Ratio from the PTP Relay Instance's Local Clock to the WorkingClock at the Grandmaster, while... <ul style="list-style-type: none"> • WorkingClock (acting as ClockSource) at Grandmaster PTP Instance, fractional frequency offset with respect to the nominal frequency is increasing at 1 ppm/s • Local Clock at upstream PTP Instance, fractional frequency offset with respect to the nominal frequency is increasing at 1 ppm/s 	Allowable range of the measured mean: - 0,1 ppm to + 0,1 ppm Allowable measured standard deviation around the measured mean: 0,08 ppm
rateRatioDrift field in the Drift_Tracking TLV transmitted by PTP Relay Instance minus the Rate Ratio Drift from the PTP Relay Instance's Local Clock to the WorkingClock at the Grandmaster, while... <ul style="list-style-type: none"> • WorkingClock (acting as ClockSource) at Grandmaster is stable. • Local Clock at upstream PTP Instance is stable. 	Allowable range of the measured mean: - 0,1 ppm/s to + 0,1 ppm/s Allowable measured standard deviation around the measured mean: 0,02 ppm/s

Topic	Value
<p>rateRatioDrift field in the Drift_Tracking TLV transmitted by PTP Relay Instance minus the Rate Ratio Drift from the PTP Relay Instance's Local Clock to the WorkingClock at the Grandmaster, while...</p> <ul style="list-style-type: none"> • WorkingClock (acting as ClockSource) at Grandmaster PTP Instance, fractional frequency offset with respect to the nominal frequency is increasing at 1 ppm/s • Local Clock at upstream PTP Instance is stable. 	Allowable range of the measured mean: - 0,1 ppm/s to + 0,1 ppm/s
Allowable measured standard deviation around the measured mean: 0,08 ppm/s	
<p>rateRatioDrift field in the Drift_Tracking TLV transmitted by PTP Relay Instance minus the Rate Ratio Drift from the PTP Relay Instance's Local Clock to the WorkingClock at the Grandmaster, while...</p> <ul style="list-style-type: none"> • WorkingClock (acting as ClockSource) at Grandmaster PTP Instance, fractional frequency offset with respect to the nominal frequency is increasing at 1 ppm/s • Local Clock at upstream PTP Instance, fractional frequency offset with respect to the nominal frequency is increasing at 1 ppm/s 	Allowable range of the measured mean: - 0,1 ppm/s to + 0,1 ppm/s
Allowable measured standard deviation around the measured mean: 0,08 ppm/s	
syncEgressTimestamp in Drift_Tracking TLV minus Local Clock when Sync message is transmitted	Range around the measured mean within which 90% of measurements fall: ± 7 ns
	Maximum difference of any measurement from the measured mean: ± 10 ns
meanLinkDelay measured by the PTP Relay Instance minus the actual path delay	±3 ns
Note 1 “Allowable range of the measured mean” specifies limits on constant error. “Range around the measured mean” and “Allowable measured standard deviation around the measured mean” specify limits on dynamic error. A limit on the constant error of syncEgressTimestamp is not specified because constant error in this characteristic is not a source of time synchronization error.	

1851

1852 Table 14 shows the required limits on error generation at a PTP End Instance. A limit on error
1853 generation for a PTP End Instance is a limit on the amount of error it adds to its Working Clock
1854 (acting as ClockTarget) compared to the input Sync message. These requirements are written
1855 for the case when errors due to change of fractional frequency offset of its Local Clock with
1856 respect to the nominal frequency and errors in the input Sync message are negligible with
1857 respect to the specified error generation limits. See D.3.6.

1858

Table 14 – Error generation limits for PTP End Instance

Topic	Value
<p>Working Clock (acting as ClockTarget) at PTP End Instance minus Working Clock (acting as Clock Source) at Grandmaster, while...</p> <ul style="list-style-type: none"> • WorkingClock (acting as ClockSource) at Grandmaster is stable. • Local Clock at upstream PTP Instance is stable. • meanLinkDelay between upstream PTP Instance and PTP Relay Instance is negligible 	Allowable range of cTE: - 10 ns to + 10 ns Allowable range of dTE: - 15 ns to + 15 ns

Topic	Value
Working Clock (acting as ClockTarget) at PTP End Instance minus Working Clock (acting as Clock Source) at Grandmaster, while... <ul style="list-style-type: none"> • WorkingClock (acting as ClockSource) at Grandmaster PTP Instance, fractional frequency offset with respect to the nominal frequency is increasing at 1 ppm/s • Local Clock at upstream PTP Instance is stable. • meanLinkDelay between upstream PTP Instance and PTP Relay Instance is negligible 	Allowable range of cTE: - 10 ns to + 10 ns Allowable range of dTE: - 230 ns to + 20 ns
Working Clock (acting as ClockTarget) at PTP End Instance minus Working Clock (acting as Clock Source) at Grandmaster, while... <ul style="list-style-type: none"> • WorkingClock (acting as ClockSource) at Grandmaster PTP Instance, fractional frequency offset with respect to the nominal frequency is increasing at 1 ppm/s • Local Clock at upstream PTP Instance, fractional frequency offset with respect to the nominal frequency is increasing at 1 ppm/s • meanLinkDelay between upstream PTP Instance and PTP Relay Instance is negligible 	Allowable range of cTE: - 10 ns to + 10 ns Allowable range of dTE: - 230 ns to + 20 ns
meanLinkDelay measured by the PTP End Instance minus the actual path delay	± 3 ns

1859

1860 6.2.6 Clock states

1861 Industrial automation systems monitor the synchronization status of each PTP Instance to
 1862 determine the viability of operations. This status is obtained from the isSynced global variable
 1863 specified in IEEE Draft Std P802.1ASdm, 18.4.1.

1864 PtInstanceSyncStatus state machine in IEEE Draft Std P802.1ASdm shall be supported
 1865 independent whether hot standby is supported. The interface primitives of 9.3.3, 9.4.3, 9.5.3,
 1866 9.6.2 of IEEE Draft Std P802.1ASdm shall be supported.

1867 6.2.7 Application framework

1868 Any step change in the time of a ClockSource or ClockTarget whose absolute value exceeds a
 1869 user-defined threshold (for example 1 μ s) leads to action being taken by the application or by
 1870 a higher-layer entity.

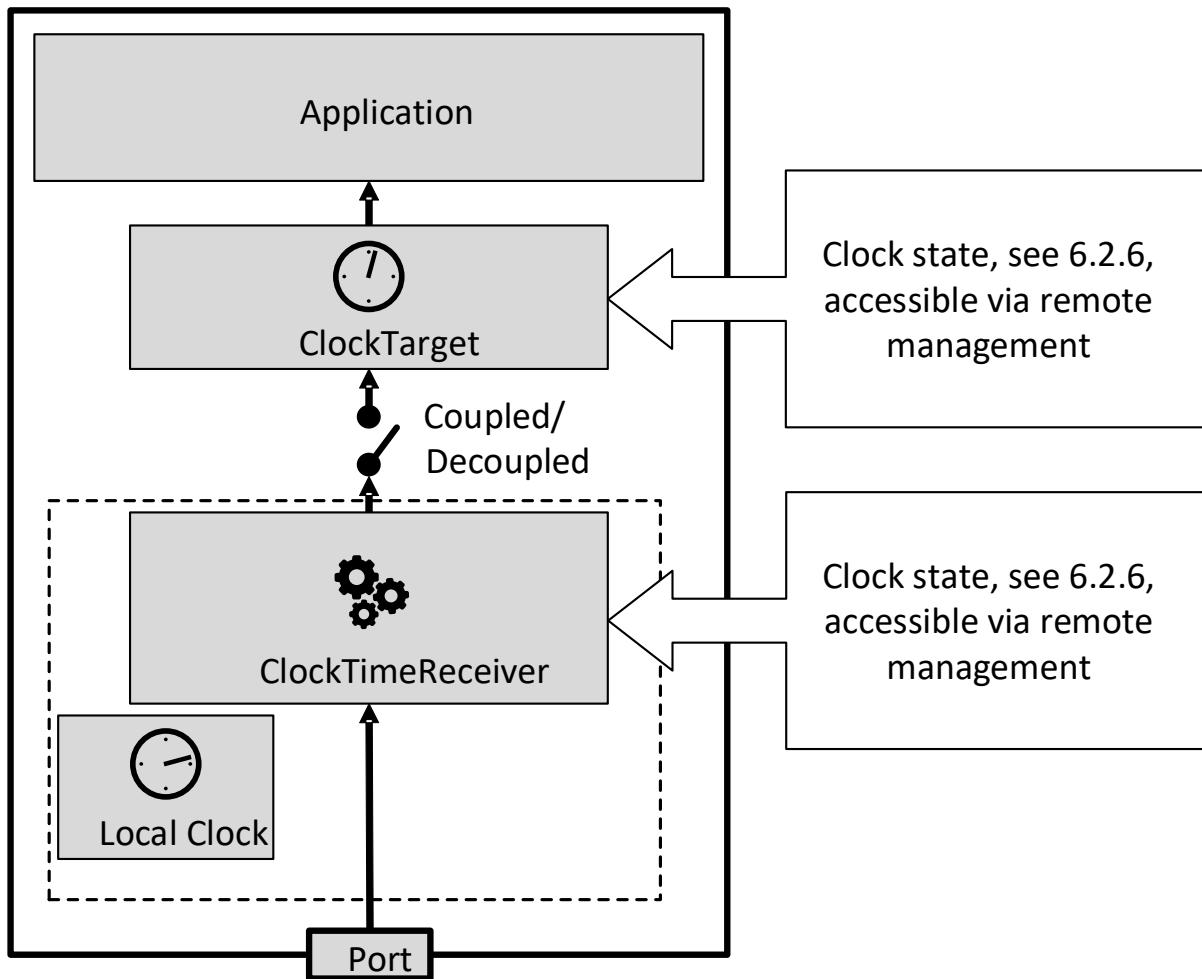
1871 If the change is in Global Time, it is desirable that all consumers of that time be made aware of
 1872 this change (i.e., a jump in Global Time from the value A to the value B), so that the actual time
 1873 interval between the time corresponding to A and the time corresponding to B can be evaluated.

1874 In the case of Working Clock, a time change that exceeds the user-defined threshold (for
 1875 example 1 μ s) is avoided to protect assets and prevent damage. Thus, the ClockSource or
 1876 ClockTarget can be decoupled (see Figure 13) from the PTP-maintained clock when such a
 1877 time change occurs.

1878 In Figure 13, two ClockTargets are traceable to a reliable source of time, which should be
 1879 synchronized to Global Time or Working Clock.

1880 The status of a ClockSource, ClockTarget, ClockTimeTransmitter or ClockTimeReceiver is
 1881 given by the state of the clock (see 6.2.6) as shown in Figure 12. When timestamps are provided
 1882 to the application, the current ClockSource or ClockTarget state can also be provided to the
 1883 application.

1884



1885

1886

Figure 12 – Clock model

1887

1888 **6.2.8 Working Clock domain framework**

1889 The gPTP domainNumber of a Working Clock domain is assigned by the CNC. In industrial
 1890 applications, when the number of PTP Relay Instances between the Grandmaster PTP Instance
 1891 and any PTP End Instance is less than or equal to 99, max|TER| of the synchronized time of
 1892 any ClockTarget, relative to the Grandmaster ClockSource, is less than or equal to 1 μ s (see
 1893 error budget A in Figure 15). Thus it is incumbent upon any PTP Instance to ensure that the
 1894 requirements specified in 5.5.3, 6.2.2, 6.2.3, 6.2.4, and 6.2.5 are met.

1895 **6.2.9 Global Time domain framework**

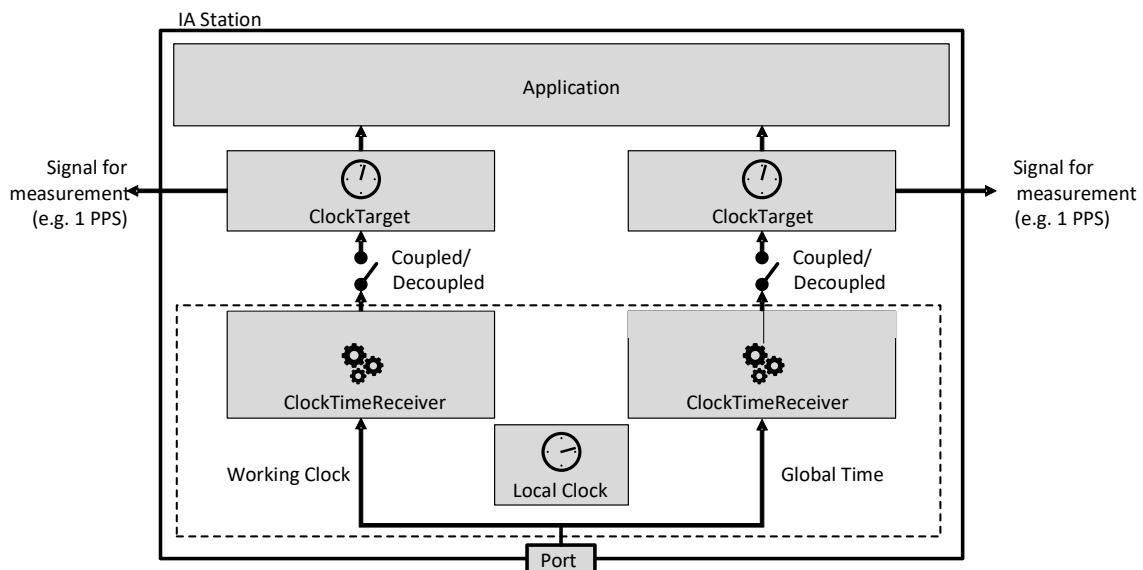
1896 The gPTP domainNumber of a Global Time domain is assigned by the CNC. In industrial
 1897 applications, when the number of PTP Relay Instances between the Grandmaster PTP Instance
 1898 and any PTP End Instance is less than or equal to 99, max|TER| of the synchronized time of
 1899 any ClockTarget, relative to the Grandmaster ClockSource, is less than or equal to 100 μ s (see
 1900 error budget A in Figure 15). Thus it is incumbent upon any PTP Instance to ensure that the
 1901 requirements specified in 5.5.3, 6.2.2, 6.2.3, 6.2.4, and 6.2.5 are met.

1902 **6.2.10 IA-station model for clocks**

1903 Industrial automation applications, as described in 4.1, require synchronized time that is
 1904 traceable to a known source (i.e., Global Time) and a source of time synchronized to the
 1905 Working Clock. Figure 13 and Figure 14 show examples of the IA-station internal model for
 1906 clocks with the two PTP Instances. It is possible for the ClockSource or ClockTarget to start
 1907 decoupled or become decoupled from the ClockTimeTransmitter or ClockTimeReceiver,
 1908 respectively, of a PTP Instance; the ClockSource or ClockTarget runs independently of the

1909 availability of the network or a Grandmaster. For example, if the PTP Instance enters a state
 1910 where `isSynced` is FALSE, the application might choose to decouple its clock from the PTP
 1911 Instance and continue to run on its internal clock. If `isSynced` for the PTP Instance changes to
 1912 TRUE, the application can choose to again synchronize to the PTP Instance.

1913 Figure 13 shows the IA-station internal model for clocks, with the two PTP instances used as
 1914 `ClockTimeReceiver/ClockTarget`.

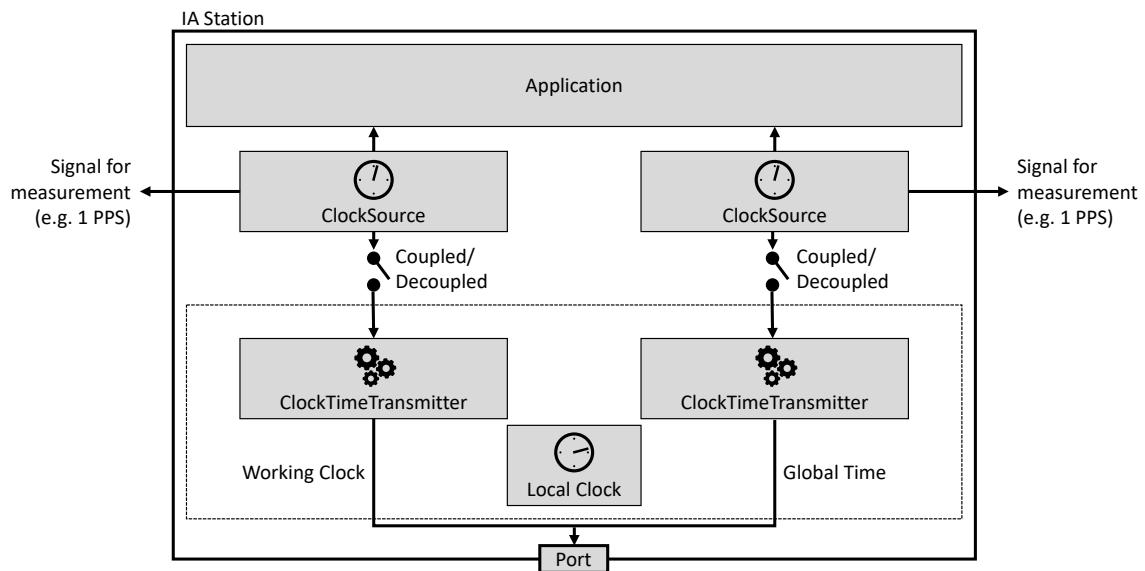


1915

1916

1917 **Figure 13 – Example clock usage principles for PTP End Instances**

1918 Figure 14 shows the IA-station internal model for clocks, with the two PTP instances used as
 1919 Grandmaster.



1920

1921 **Figure 14 – Example clock usage principles for Grandmaster PTP Instances**

1922

6.2.11 Clock usage for the Ethernet interface**6.2.11.1 Time-aware offset control**

Time-aware offset control (see 4.4), if used, needs an assigned source of time and a definition when to start or to stop, which are dependent on the clock state.

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

IA time-aware streams are only transmitted while isSynced for the chosen ClockSource or ClockTarget is TRUE (see 6.2.6).

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

6.2.11.2 Gating cycle

To control the gating cycle, the gate control list needs an assigned source of time. Enabling and disabling the gate control list is dependent on the clock state.

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

The gating cycle is run using the chosen ClockSource or ClockTarget regardless of the value of isSynced (see 6.2.6).

6.2.12 Error model

Synchronization is 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:

- 1944 a) the transporting of time in PTP Instances and via PTP Links that connect PTP Instances,
- 1945 b) the providing of time to the Grandmaster PTP Instance, from the ClockSource entity via the
- 1946 ClockTimeTransmitter entity, and
- 1947 c) the providing of time to a ClockTarget entity (end application) via the ClockTimeReceiver
- 1948 entity.

NOTE Item a) includes time error introduced in a PTP End Instance between the timeReceiver port and the ClockTimeReceiver entity, and between the ClockTimeTransmitter entity and a timeTransmitter port.

1951

1952 An output synchronization signal (for example, 1 pulse per second (PPS)) synchronized to the Working Clock as shown in Figure 13 and Figure 14, 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 in the range of -10 ns to +10 ns. Figure 15 shows the error budget principle used. These budgets do not include any deviation from the PTP timescale. Representative budgets are provided in Annex D.

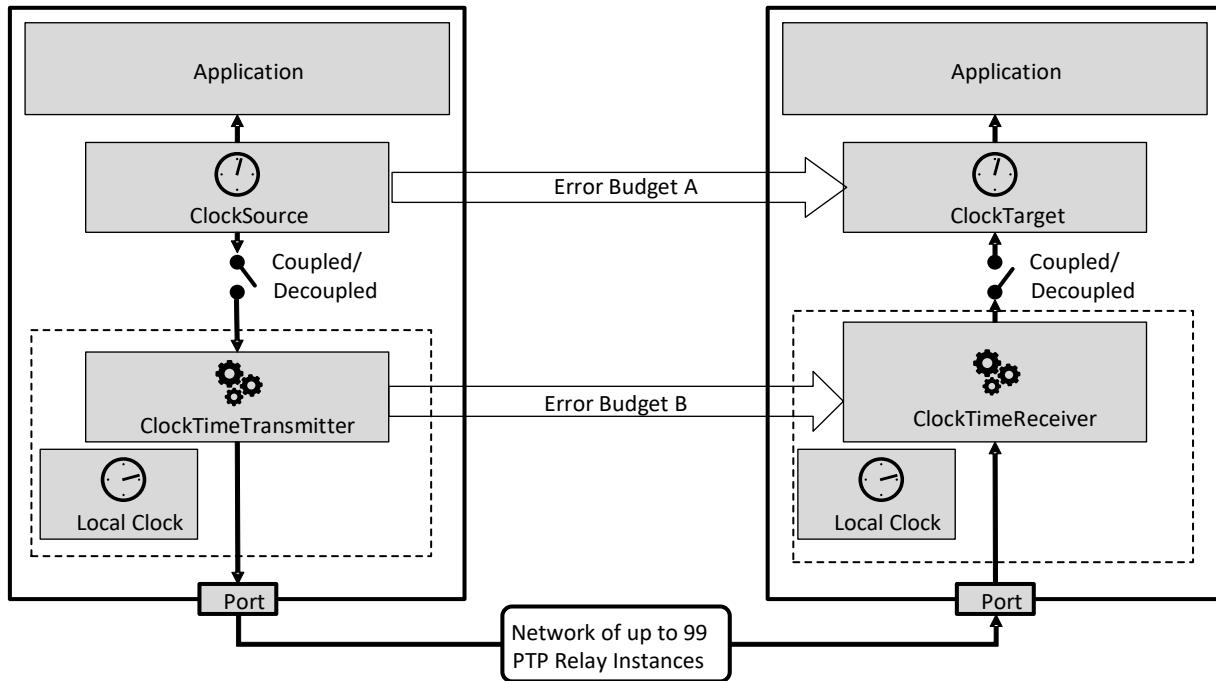
**Figure 15 – Error budget scheme**

Table 15 shows example values for the splitting of the available error budgets (see Figure 15).

Table 15 – 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.

6.2.13 gPTP domains and PTP Instances

Any valid gPTP domain number as specified in IEEE Std 802.1AS-2020 can be used. The IEEE Std 1588-2019 attribute descriptionDS.userDescription shall be used according to Table 16 to support the translation of PTP Instances and middleware as described in 4.6.2. One gPTP domain can be used for both Working Clock and Global Time. If only one gPTP domain is used, then the requirements for the Working Clock apply (see 6.2.8).

Table 16 – descriptionDS.userDescription of gPTP Domains

gPTP Domain	descriptionDS.userDescription
Working Clock (no hot standby configured)	“60802-WorkingClock”
Primary Working Clock (with configured hot standby)	“60802-Primary-WorkingClock”
Secondary Working Clock (with configured hot standby)	“60802-Secondary-WorkingClock”
Global Time (no hot standby configured)	“60802-GlobalTime”
Primary Global Time (with configured hot standby)	“60802-Primary-GlobalTime”
Secondary Global Time (with configured hot standby)	“60802-Secondary-GlobalTime”

gPTP Domain	descriptionDS.userDescription
GlobalTime and WorkingClock (no hot standby configured)	“60802-GlobalTime-WorkingClock”
Primary GlobalTime and WorkingClock (with configured hot standby)	“60802-Primary-GlobalTime-WorkingClock”
Secondary GlobalTime and WorkingClock (with hot standby configured)	“60802-Secondary-GlobalTime-WorkingClock”

1975

1976 The descriptionDS.userDescription attribute is represented in the ieee1588-ptp YANG module
 1977 by the user-description leaf in the description-ds container of a PTP Instance.

1978 The linking between a gPTP domain and the IETF interfaces is provided by the underlying-
 1979 interface.

1980 **6.3 Security model**

1981 **6.3.1 General**

1982 Subclause 6.3 specifies the security model starting with NETCONF/YANG. It describes the
 1983 security functionality, the security objects in factory default state, the imprinting of Configuration
 1984 Domain-specific security objects and the secure configuration based on Configuration Domain-
 1985 specific security objects.

1986 **6.3.2 Security functionality**

1987 **6.3.2.1 Message exchange protection**

1988 **6.3.2.1.1 General**

1989 Network configuration with NETCONF/YANG is protected by NETCONF-over-TLS according to
 1990 IETF RFC 7589 and IETF draft-ietf-netconf-over-tls13. NETCONF-over-SSH according to IETF
 1991 RFC 6242 is not used in this document. The to-be-configured IA-stations act in the NETCONF
 1992 server role.

1993 NOTE This document selects TLS as a secure transport for NETCONF since TLS is the better match for the case
 1994 of configuration clients that rely upon unattended or automated operation. This case is dominant in industrial
 1995 automation.

1996 **6.3.2.1.2 TLS profile**

1997 TLS protocol version 1.2 according to IETF RFC 5246, 6.2.3.3, 7.4.7.2 and 8.1.2 shall be
 1998 supported with mutual authentication according to the following list of requirements and options.

1999 a) Mutual authentication in conjunction with the IDevID and LDevID credentials according to
 2000 6.3.4 and 6.3.5. shall be supported.

2001 b) The cipher suite TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 according to IETF
 2002 RFC 5289, 3.2 and Clause 5, shall be supported.

2003 NOTE IETF RFC 7589 implicitly mandates the cipher suite TLS_RSA_WITH_AES_128_CBC_SHA by referring to
 2004 IETF RFC 5246. This cipher suite is not used in this document because it requires excessive asymmetric key lengths,
 2005 it is not an Authenticated Encryption with Associated Data (AEAD) scheme, and it does not provide perfect forward
 2006 secrecy.

2007 c) The cipher suites TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 according to
 2008 according to IETF RFC 5289, 3.2 and Clause 5, and
 2009 TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 according to IETF RFC
 2010 7905, Clause 2, may be supported.

2011 d) Signature algorithm ECDSA with SHA-256 and Curve P-256 according to NIST FIPS 186-5
 2012 Digital Signature Standard (DSS) shall be supported.

2013 e) Signature algorithms ECDSA with SHA-512 and Curve P-521 according to NIST FIPS 186-
 2014 5, Ed25519 according to IETF RFC 8032, 5.1, and Ed448 according to IETF RFC 8032, 5.2,
 2015 may be supported.

2016 TLS protocol version 1.3 according to IETF RFC 8446 may be used with mutual authentication
 2017 for NETCONF/YANG as follows:

2018 f) The cipher suites TLS_AES_128_GCM_SHA256, TLS_AES_256_GCM_SHA384 and
 2019 TLS_CHACHA20_POLY1305_SHA256 may be supported, and

2020 g) The signature schemes ecdsa_secp256r1_sha256, ecdsa_secp521r1_sha512, ed25519
 2021 and ed448 may be supported.

2022 Independent from the TLS version, the TLS Certificate message from the TLS client and server
 2023 contains the self-signed root certificate. This approach allows to simplify/flatten the PKI
 2024 hierarchy on base of the current TLS client certificate to NETCONF username mapping
 2025 algorithm in IETF RFC 7589. Implementations shall support TLS Certificate message with at
 2026 least 2 certificate objects.

2027 **6.3.2.1.3 Certificate-to-name mapping**

2028 The IETF RFC 7589 based certificate-to-name mapping procedure is as follows.

2029 NOTE IETF RFC 7589, Clause 7, specifies that NETCONF servers map client certificates to "NETCONF usernames"
 2030 and specifies a concrete mapping procedure for this purpose. This mapping is represented by the YANG module ietf-
 2031 x509-cert-to-name.

2032 The list of mapping entries has a single element containing:

- 2033 • fingerprint: the fingerprint of the trust anchor for the Configuration Domain, and
- 2034 • map_type: ext-60802-roles.

2035 The map-type ext-60802-roles maps the roles provided in the id-60802-pe-roles extension
 2036 (defined in 6.3.2.1.4) of the end entity certificate presented by the NETCONF client to a
 2037 NETCONF username. The UTF-8 string representation of each role is added to the NETCONF
 2038 username in chronological order of the enumeration values, whereas multiple roles are
 2039 separated by ':' character.

2040

2041 **6.3.2.1.4 Role extension**

2042 The id-60802-pe-roles extension in LDevID-NETCONF end entity certificates shall be
 2043 constructed as follows:

2044 **a) Extension field extnID**

2045 The extnID shall provide the following OBJECT IDENTIFIER to identify the id-60802-pe-roles
 2046 extension:

```
2047 id-60802 OBJECT IDENTIFIER ::= { <60802-specific OID> }
2048
2049 id-60802-pe OBJECT IDENTIFIER ::= { id-60802 1 }
2050
2051 id-60802-pe-roles OBJECT IDENTIFIER ::= { id-60802-pe 1 }
2052
```

2053 **Editor's note: A 60802-specific OID cannot be provided until SA Ballot.**

2054

2055 **b) Extension field critical**

2056 The id-60802-pe-roles extension is marked as non-critical (critical:= FALSE).

2057

2058 **c) Extension field extnValue**

```
2059 60802RoleNamesSyntax ::= SEQUENCE OF 60802RoleName
2060
2061 60802RoleName ::= ENUMERATED {
2062   SecurityAdminRole (0),
2063   ConfiguratorRole (1),
2064   StreamConfiguratorRole (2),
2065   SubscriberRole (3)}
```

2066

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 role-based access control.

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

This role-based model for security resources should be applied according to the following list of requirements.

- The global switch enable-nacm is set to true.
- The set of NETCONF/YANG resources of an IA-station is partitioned according to the YANG modules specified in 6.4.9 with a permission-to-role assignment as listed below. An access operation is allowed through the keyword “permitted” and not allowed through the keyword “denied”.

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.

- All authenticated entities (default rules): All YANG modules: read access permitted, write access denied, exec-access denied.

NOTE 3 The default rules apply for YANG modules that are listed in 6.4.9 but are not listed in the rules of the individual roles.

- Rules for StreamConfiguratorRole: YANG module ieee802-dot1q-tsn-config: write and execute operations permitted.
- Rules for SubscriberRole:
 - YANG module ietf-subscribed-notifications: write and execute operations permitted, and
 - YANG module ietf-yang-push: write and execute operations permitted.
- Rules for ConfiguratorRole: All YANG modules except those listed below, write and execute operations permitted:
 - YANG modules for security configuration, i.e., ietf-truststore, ietf-keystore, path to cert-to-name nodes of ietf-netconf-server, path to tls-server-parameters nodes of ietf-netconf-server,
 - YANG modules for stream configuration, i.e., ieee802-dot1q-tsn-config, and
 - YANG modules for subscription configuration, i.e., ietf-subscribed-notifications, ietf-yang-push.
- Rules for SecurityAdminRole:
 - YANG module ietf-truststore, path to certificate node of IDevID trust anchor: write and execute operations denied, and
 - YANG module ietf-truststore (besides path to certificate node of IDevID trust anchor): write and execute operations permitted.
 - YANG module ietf-keystore, path to asymmetric-key node of IDevID credential: write and execute operations denied, and
 - YANG module ietf-keystore (besides path to asymmetric-key node of IDevID credential): write and execute operations permitted.
 - YANG module ietf-netconf-server (besides path to cert-to-name nodes and path to tls-server-parameters nodes): write and execute operations denied, and
 - YANG module ietf-netconf-server, path to cert-to-name nodes: write and execute operations permitted.
 - YANG module ietf-netconf-server, path to tls-server-parameters nodes: write and execute operations permitted.

2117 In addition, the following access control should be applied for NETCONF protocol operations:

- 2118 • <lock>, <unlock>: permitted for any role specified in this document,
- 2119 • <partial-lock>, <partial-unlock>: denied (not used in this document),
- 2120 • <get> and <get-config>: mapped to a "read" access operation to the target datastore,
- 2121 • <edit-config>: permitted for any role specified in this document,
- 2122 • <copy-config>: permitted for ConfiguratorRole,
- 2123 • <delete-config>: denied (not used in this document),
- 2124 • <commit>: permitted for any role specified in this document,
- 2125 • <discard-changes>: permitted for any role specified in this document,
- 2126 • <close-session>: permitted for any role specified in this document, and
- 2127 • <kill-session>: denied (not used in this document).

2128

2129 This document does not specify the assignment of role names to actual system entities. This is
2130 a duty of system owners or operators.

2131

2132 **6.3.3 IDevID Profile**

2133 **6.3.3.1 General**

2134 IA-stations shall possess IDevID credentials according to 6.3.3. CNCs shall contain trust
2135 anchors for validating IDevID credentials.

2136 **6.3.3.2 Object Contents**

2137 **6.3.3.2.1 General**

2138 The IDevID credential contents shall comply to 6.3.3.2.2, 6.3.3.2.3, and IEEE Std 802.1AR-
2139 2018, Clause 6.

2140 **6.3.3.2.2 IA-station Identity**

2141 Any IDevID EE certificate of an IA-station shall take one of the following forms:

- 2142 • raw form: the IDevID EE certificate complies to IEEE Std 802.1AR-2018, Clause 8, and
- 2143 • extended form: the IDevID EE certificate complies to requirements provided IEEE Std
2144 802.1AR-2018, Clause 8. The extended form of an IDevID EE certificate shall be constructed
2145 as follows:
- 2146 • the verifiable device identity shall appear as a URN in a GeneralName of type
2147 uniformResourceIdentifier in the subjectAltName extension,
- 2148 • the URN value shall be constructed according to IETF RFC 8141 and as follows:
- 2149 • namespace identifier: ieee (see IETF RFC 8069), and
- 2150 • namespace-specific string: iec-ieee-60802#verifiable-device-identity,
- 2151 • q-component (see IETF RFC 8141, 2.3.2) to parameterize the named resource: an
2152 ampersand-separated list of keyword=value tuples with following keywords and
2153 values. These tuples can appear in any order inside the q-component.
- 2154 • The keywords: hardware-rev, serial-num, mfg-name, model-name.
- 2155 • Their corresponding values from the single "chassis" component list entry in the
2156 ietf-hardware YANG module (see 6.4.9.2.5.8) that represents the management
2157 entity of the IA-station respectively from its pre-material form in percent-encoding
2158 (see IETF RFC 3986).

2159 NOTE 1 These are the items with the YANG property config=false from the 'component' list entry that represents
2160 the management entity of the IA-station. The config=false items firmware-rev and software-rev are excluded to avoid
2161 IDevID credential updates in case of FW or SW updates.

2162 NOTE 2 An object looks like urn:ieee:iec-ieee-60802#verifiable-device-identity?=mfg-name=<mfg-name>&model-
2163 name=<model-name>&hardware-rev=<hardware-rev>&serial-num=<serial-num>.

2164 NOTE 3 One IDevID EE certificate can have one subjectAltName extension which can have one or more
2165 GeneralName entries. In particular, there can be one or more GeneralName entries of type
2166 uniformResourceIdentifier. This allows other organizations e.g., middleware and application consortia or individual
2167 manufacturers to also represent their perception of verifiable device identity in addition to the perception of this
2168 document.

2169 **6.3.3.2.3 Signature Suites**

2170 An IDevID shall utilize the signature suite: ECDSA P-256/SHA-256 according to NIST FIPS 186-
2171 5/180-4 and NIST SP 800-186 using the algorithm identifiers according to IETF RFC 5480.

2172 An IDevID may utilize the following signature suites:

- 2173 • ECDSA P-521/SHA-512 according to NIST FIPS 186-5/180-4 and NIST SP 800-186 using
2174 the algorithm identifiers according to IETF RFC 5480,
- 2175 • EdDSA instance Ed25519 according to IETF RFC 8032 using Curve25519 according to IETF
2176 RFC 7748 and using the algorithm identifiers according to IETF RFC 8410, and
- 2177 • EdDSA instance Ed448 according to IETF RFC 8032 using Curve448 according to IETF
2178 RFC 7748 and using the algorithm identifiers according to IETF RFC 8410.

2179 **6.3.3.3 Information Model**

2180 **6.3.3.3.1 General**

2181 The information model for IDevID credentials and trust anchors shall comply to YANG and
2182 NMRA, in particular the YANG modules ietf-keystore and ietf-truststore, as well as subsequent
2183 subclauses of 6.3.3.3.

2184 **6.3.3.3.2 Entries**

2185 IDevID credentials shall be provided in form of built-in keys of an IA-station by its manufacturer.
2186 In YANG, they are modeled as config-false nodes and are represented in the ‘keystore’
2187 container that is instantiated by the YANG module ietf-keystore. The private key shall use the
2188 private-key-type choice hidden-private-key i.e., the IDevID private key is not presented in
2189 NETCONF/YANG. The details of storing and protecting IDevID private keys as well as using
2190 them for signing purposes are implementation specific.

2191 Trust anchors for IDevID credentials are CNC user-configured data objects; these objects shall
2192 be available as applied configuration (IETF RFC 8342) upon CNCs. In YANG, they are modeled
2193 as config-true nodes and are represented in the ‘truststore’ container that is instantiated by the
2194 YANG module ietf-truststore.

2195 NOTE IA-station built-in trust anchors for use cases such as firmware/software update are not addressed in this
2196 document.

2197 **6.3.3.3.3 Entry Manifolds**

2198 An IA-station shall possess one IDevID credential with a certification path plus trust anchor
2199 information issued under the required signature suite according to 6.3.3.2.3 as part of its factory
2200 default state.

2201 If an IA-station supports an optional signature suite according to 6.3.3.2.3, it shall possess in
2202 addition one IDevID credential with a certification path plus trust anchor information issued
2203 under the optional signature suite as part of its factory default state.

2204 An IA-station can have additional IDevID credential(s) with a certification path plus trust anchor
2205 information issued under a combination of any required or any supported optional DevID
2206 signature suites.

2207 If an IA-station possesses multiple IDevID credentials, then they shall be issued by the same
2208 organization (the IA-station manufacturer). Their EE certificates shall contain the same device
2209 identity information.

2210 A CNC shall support at least one trust anchor for IDevID credentials per supported IA-station
2211 manufacturer.

2212 6.3.3.3.4 Entry Naming

2213 IDevID credentials shall be present in an ‘asymmetric-key’ entry that is identified as: /ietf-
2214 keystore:keystore/asymmetric-keys/asymmetric-key/name=
2215 IDevID-<SignatureSuiteName>-<CertificateSerialNumberOfEECertificate>.

2216 IDevID trust anchors shall be present in ‘certificate’ entries that are identified as: /ietf-
2217 truststore:truststore/certificate-bags/certificate-bag/certificate/name=
2218 IDevID-<SignatureSuiteName>-<CertificateSerialNumberOfCACertificate>.

2219 Such entries shall be present underneath a ‘certificate-bag’ entry that is identified as: /ietf-
2220 truststore:truststore/certificate-bags/certificate-bag/name=IDevID.

2221 6.3.3.4 Processing Model**2222 6.3.3.4.1 General**

2223 The processing model for IDevID credentials and trust anchors shall comply to IEEE Std
2224 802.1AR-2018 and 6.3.3.4.

2225 6.3.3.4.2 Credentials**2226 6.3.3.4.2.1 General**

2227 IDevID credentials are used in following use cases:

- 2228 • NETCONF/YANG security setup from factory default; the number of such events scales with
2229 the number of factory resets i.e., this use case is performed sporadically. It is conducted by
2230 CNCs and encompasses a device identity verification, and
- 2231 • device identity verification happens as a subtask during NETCONF/YANG security setup
2232 from factory default. It can also happen at the discretion of the CNC user. The details of
2233 device identity verification are also subject to given policy.

2234 In these use cases, IA-stations act in claimant role and CNCs act in verifier role:

- 2235 • IA-stations shall present the certification path of and prove private key possession for an
2236 IDevID credential, and
- 2237 • CNCs shall validate the certification path, check the proof-of-possession for the private key,
2238 and verify the obtained device identity information.

2239 6.3.3.4.2.2 Creation

2240 IA-station manufacturers select the form factor for representing verifiable device identity in
2241 IDevID credentials: raw or extended form. The details of the IDevID credential issuance process
2242 are manufacturer-specific and not addressed in this document.

2243 IA-station manufacturers are not required to offer an update feature for IDevID credentials.

2244 6.3.3.4.2.3 Distribution

2245 IA-stations shall supply IDevID credentials in form of built-in keys, see 6.3.3.3.

2246 6.3.3.4.2.4 Use

2247 Verifiers (CNCs) shall perform the following checks when they challenge claimants (IA-stations)
2248 to authenticate themselves by means of an IDevID credential.

- 2249 • IDevID certification path validation according to IETF RFC 5280, Clause 6. Whether this
2250 validation happens with or without revocation checks is at the discretion of the CNC user.
 - 2251 • It is the responsibility of the CNC user to supply a trust anchor configuration (set of
2252 trusted certificates or trusted public keys), a revocation check instruction (Boolean) and
2253 optionally, X.509 CRL objects according to IETF RFC 5280, Clause 5, to CNCs. The
2254 certification path validation is passed if and only if the IDevID EE certificate is the leaf
2255 of a valid certification path that ends with a CA certificate which is signed by a configured
2256 trust anchor and which is not revoked (if revocation check is enabled).

- 2257 • Proof-of-possession checking for the private key. The proof-of-possession check is passed
2258 if and only if the IA-station possesses the private key which matches the public key in the
2259 IDevID EE certificate.
- 2260 • It is the responsibility of the CNC user to establish and supply to CNCs: a device identity
2261 verification policy which determines the verifiable device identity subset that shall be
2262 checked by the CNC for the IA-stations in a Configuration Domain. This is a subset of
2263 {hardware-rev, serial-num, mfg-name, model-name}. The empty subset (“no-identity-check”)
2264 as well as the whole set are allowed. The device identity verification for an IA-station
2265 instance shall behave according to the following list of requirements.
 - 2266 • If this subset is empty, then the device identity check is passed. If the user chooses not
2267 to verify identity, information about the devices is considered unreliable. Tracking the
2268 unverified status of such devices is the responsibility of the user. It is the responsibility
2269 of the user to establish policies for the use of such devices.
 - 2270 • If this subset is non-empty, then the CNC performs the following expected vs. actual
2271 check for each verifiable device identity item in this subset:
 - 2272 • The check for any item in this subset is passed if the expected value (from ietf-
2273 hardware YANG module) matches the actual value (from the verifiable device identity
2274 URN value for this document in the subjectAltName extension of the IDevID EE
2275 certificate). This check fails if the IDevID has raw form.
 - 2276 • The device identity check is passed if it is passed for all items in the subset.

2277 IDeVIDs in raw form (without verifiable device identity URN) can be used if the device identity
2278 verification setting option “no-identity-check” is employed. This allows to perform the
2279 NETCONF/YANG security setup from factory default for IA-stations with IDeVID credentials in
2280 raw form. From CNC perspective these IA-stations remain anonymous.

2281 NOTE This document does not specify a mechanism for device identity verification for IDeVIDs in raw form. Whether
2282 and how device identity checks for such IA-stations are done in an offline mode is at the discretion of CNC users.

2283 **6.3.3.4.2.5 Storage**

2284 Credentials shall be stored persistently upon an IA-station. The details for implementing this
2285 persistent storage are IA-station manufacturer-specific and not addressed in this document.

2286 IA-stations shall support storage of at least one IDeVID credential.

2287 **6.3.3.4.2.6 Revocation**

2288 It is the responsibility of IA-station manufacturers to report revocation for the IDeVID credentials
2289 issued by them in form of X.509 CRL objects according to IETF RFC 5280, Clause 5. These
2290 objects are made available in a form that allows relying parties i.e., CNC users to retrieve them
2291 at their own discretion.

2292 CNC users decide whether they support IDeVID certification path validation with or without
2293 revocation:

- 2294 • if revocation checks are disabled, then certificate path validation shall be performed
2295 according to IETF RFC 5280, 6.1, and
- 2296 • if revocation checks are enabled, then certificate path validation shall be performed
2297 according to IETF RFC 5280, 6.1 and 6.3.

2298 NOTE It is the responsibility of CNC users to obtain up-to-date X.509 CRL objects from manufacturers and make
2299 them locally available for verifiers.

2300 **6.3.3.4.3 Trust Anchors**

2301 **6.3.3.4.3.1 General**

2302 Trust anchors are input arguments for certification path validation according to IETF RFC 5280,
2303 6.1.1 input argument (d). Relying parties decide about these input arguments in a discretionary
2304 fashion i.e., these objects are not created and distributed as literal trust anchor objects but in
2305 a pre-material form of, for example, self-signed certificate objects.

2306 NOTE The digital signature in self-signed certificates do not vouch for authenticity of this object: Actor X can issue
2307 self-signed certificates featuring the name of actor A that cannot be distinguished from self-signed certificates issued
2308 by A. The mechanisms to verify the authenticity of self-signed certificates are not addressed in this document.

2309 The trust anchors for use cases where IA-stations act in claimant role are determined by CNC
2310 users.

2311 **6.3.3.4.3.2 Creation**

2312 The details of the issuance and update processes for trust anchors for validation of IDevID
2313 credentials are not addressed by this document.

2314 **6.3.3.4.3.3 Distribution**

2315 With respect to use cases where IA-stations act in claimant role e.g., NETCONF/YANG security
2316 setup and device identity verification the following model applies:

- 2317 • issuers (IA-station manufacturers) create and distribute trust anchors. Issuers also provide
2318 out-of-band means that allow relying parties to check the authenticity of these objects, and
- 2319 • relying parties (CNC users) check the authenticity of trust anchors and decide about their
2320 acceptance as trust anchors for certification path validation in a discretionary manner and
2321 configure their verifiers (CNCs) accordingly.

2322 The details of distribution and validation of trust anchors are not addressed by this document.

2323 **6.3.3.4.3.4 Use**

2324 Trust anchors for IDevID credentials are used for certification path validation according to IETF
2325 RFC 5280, 6.1.1 d). This concerns CNCs with respect to the use cases NETCONF/YANG
2326 security setup from factory default, device identity verification.

2327 **6.3.3.4.3.5 Storage**

2328 Trust anchors for IDevID credentials shall be stored persistently upon CNCs. The details for
2329 implementing this persistent storage are not addressed in this document.

2330 **6.3.3.4.3.6 Revocation**

2331 IA-station manufacturers are not required to support an authority revocation feature for IDevID
2332 credential certification authorities.

2333 **6.3.4 Security setup based on IDevID**

2334 **6.3.4.1 General**

2335 IA-stations in factory default state shall conduct a security setup sequence for the Configuration
2336 Domain. This sequence consists of the following steps, each step is described in 6.3.4.

- 2337 • imprintTrustAnchor: imprint of a Configuration Domain specific trust anchor to an IA-station
2338 that allows to validate LDevID-NETCONF certificates presented by communication partners.
- 2339 • imprintCredential: imprint of a Configuration Domain specific credential to an IA-station, i.e.,
2340 a private key and the corresponding X.509 v3 end entity certificate according to ISO/IEC
2341 9594-8 as profiled in IETF RFC 5280, Clause 4, (plus intermediate CA certificates, if
2342 applicable) plus self-signed root CA certificate that serves as own LDevID credential.
- 2343 • imprintCertToNameMapping: imprint a Configuration Domain specific certificate-to-name
2344 mapping to an IA-station.

2345 Credentials shall be stored persistently upon an IA-station. The details for implementing this
2346 persistent storage are IA-station manufacturer-specific and not addressed in this document.

2347 IA-stations shall support storage of at least one LDevID-NETCONF credential.

2348 **6.3.4.2 imprintTrustAnchor**

2349 IA-stations in factory default state shall support the imprinting of a single Configuration Domain
2350 specific trust anchor via NETCONF-over-TLS according to a procedure called “provisional
2351 accept of client certificate”, which uses an IDevID credential on NETCONF and TLS server side

2352 (IA-station) and a LDevID credential on NETCONF and TLS client side (for example, a CNC)
2353 and operates as follows at the NETCONF and TLS server.

- 2354 a) Challenge the client for TLS client authentication according to IETF RFC 7589 by sending
2355 a CertificateRequest message with an empty certificateAuthorities entry.
- 2356 b) Perform certification path validation according to IETF RFC 5280, Clause 6, for the contents
2357 of the client's Certificate message. This certification path validation fails due to a missing
2358 trust anchor for the LDevID credential.
- 2359 c) Provisionally accept the failing certification path validation when the reason is "no matching
2360 trust anchor" (and only this reason) and proceed with the TLS exchange.
- 2361 d) Expect the client to send a trust anchor for LDevID over the provisionally accepted TLS
2362 session (no other object type).
- 2363 e) If the trust anchor in the NETCONF application payload was accepted, then redo the priorly
2364 failing certification path validation using this trust anchor, see step b).
- 2365 f) If this certification path revalidation is successful, then keep the TLS session alive and send
2366 an <rpc-reply> with success. The client then is expected to perform the NETCONF
2367 exchanges for imprintCredential (described in 6.3.4.3) and for imprintCertToNameMapping
2368 (described in 6.3.4.4) via the already established TLS session.
- 2369 g) If this certification path revalidation is not successful, then terminate the TLS session. The
2370 usual NETCONF/YANG hygiene applies. This is expected to remove the entry in the ietf-
2371 truststore that was created in step d).

2372 NOTE This "provisional accept of client certificate" is a mirrored version of the "provisional accept of server cert" in
2373 IETF RFC 8995.

2374 The "provisional accept of client cert" in factory default state shall skip the certificate-to-name
2375 mapping and shall use the NACM recovery session, i.e., skip permission checking. In this model
2376 all authenticated clients are accepted as authorized for doing the first imprinting of the LDevID
2377 credential and the corresponding trust anchor. Only contextual checks such as "once only when
2378 being in factory default state" are feasible. This model is also known as "trust on first use"
2379 (TOFU) and, e.g., also allows to read contents of the ietf-hardware module by the client for an
2380 extended identity check.

2381 The imprinting NETCONF client checks the actual server identity that is stated by the IA-station
2382 on TLS level.

2383 The NETCONF client checks the IDevID end entity certificate presented by the NETCONF
2384 server on TLS level for existence of subjectAltName extension with GeneralName entries of
2385 type uniformResourceIdentifier. If an entry contains the namespace identifier and the
2386 namespace-specific string as defined in 6.3.3.2.2, the presented server certificate is in
2387 extended form, otherwise it is in raw form.

2388 In case that the server certificate is in raw form, the following matching can be done:

- 2389 • Match a list of accepted (or blocked) manufacturers against the issuer or subject field entries
2390 of the certificate.
- 2391 • Match a list of accepted (or blocked) product instances against the product serial number
2392 from the subject field per accepted manufacturer.
- 2393 • Match the end entity certificate object as a whole against a list of pinned certificates.

2394 In case that the server certificate is in extended form, the following additional matching can be
2395 done: Match the q-components included in the verifiable device identity according to 6.3.3.2.2
2396 against those that can be read out from the corresponding leaves of the YANG module ietf-
2397 hardware or against reference values obtained by a method not addressed in this document.

2398 Details of how the matching happens depend on the implementation of the client that performs
2399 this imprinting.

2400 The LDevID-NETCONF trust anchor certificate shall be imprinted using the truststore container
2401 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 draft-ietf-netconf-crypto-types, i.e., enveloped in Base64-encoded CMS SignedData in degenerated form “certs-only” (no signature value), and
 - The imprintTrustAnchor step shall use the NETCONF operation <edit-config> according to IETF RFC 6241 for the truststore container. The NETCONF operation <commit> is not yet applied, but rather after successful completion of all security setup sequence steps.

2413 **6.3.4.3 imprintCredential**

2414 **6.3.4.3.1 General**

2415 The LDevID-NETCONF end entity certificate shall be provided as X.509 v3 public key certificate
2416 according to ISO/IEC 9594-8 as profiled in IETF RFC 5280, Clause 4, with the following criteria.

- Contains the FQDN of the NETCONF server in its subjectAltName extension according to IETF RFC 7589, Clause 6, and IETF RFC 6125, 2.2 and B.7.
- Contains a public key and is signed by a signature suite according to 5.5.4.2 or 5.6.3.
- Contains a digitalSignature in its keyUsage extension.
- Has a finite validity period.

2422 NOTE The actual length of the validity period is at the discretion of the user of the Configuration Domain.

2423 Depending on the key generation capabilities, different steps are applied to this keystore
2424 container.

2425 **6.3.4.3.2 Internal key generation**

2426 For IA-station with internal key generation capabilities, two NETCONF exchanges are
2427 performed. Processing steps for the first NETCONF exchange shall be applied as follows at the
2428 NETCONF server.

- a) Receive and process the NETCONF request message with action <generate-csr> and input values as follows:
 - /ks:keystore/ks:asymmetric-keys/ks:asymmetric-key/[ks:name=LDevID_NETCONF]/ks:generate-csr/ks:input/ks:csr-format containing identity according to draft-ietf-netconf-crypto-types, and
 - /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, Clause 4.
- 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.

2450 In the second NETCONF exchange, the LDevID-NETCONF end entity certificate (plus
2451 intermediate CA certificates) shall be imprinted using the keystore container of the ietf-keystore
2452 module with:

- 2453 • /ks:keystore/ks:asymmetric-keys/ks:asymmetric-key/ks:name = LDevID-NETCONF,
- 2454 • /ks:keystore/ks:asymmetric-keys/ks:asymmetric-key/[ks:name=LDevID-NETCONF]/,
 - 2455 • ks:certificates/ks:certificate/ks:name = LDevID-NETCONF, and
 - 2456 • ks:certificates/ks:certificate/ks:cert-data containing the certificate chain LDevID-
2457 NETCONF end entity certificate (plus intermediate CA certificates, if applicable) plus
2458 self-signed root CA certificate as data object of type end-entity-cert-cms according to
2459 draft-ietf-netconf-crypto-types

2460 The imprintCredential step shall use the NETCONF operation <edit-config> according to IETF
2461 RFC 6241 for the keystore container. The NETCONF operation <commit> is not yet applied,
2462 but rather after successful completion of all security setup sequence steps.

2463 **6.3.4.3.3 External key generation**

2464 External key generation can be used for IA-stations without internal key generation capability.
2465 For external key generation, one NETCONF exchange is performed.

2466 The LDevID-NETCONF private key and end entity certificate (plus intermediate CA certificates)
2467 shall be imprinted using the keystore container of the ietf-keystore module with:

- 2468 • /ks:keystore/ks:asymmetric-keys/ks:asymmetric-key/ks:name = LDevID-NETCONF,
- 2469 • /ks:keystore/ks:asymmetric-keys/ks:asymmetric-key/[ks:name=LDevID-NETCONF]/,
 - 2470 • ks:certificates/ks:certificate/ks:name = LDevID-NETCONF,
 - 2471 • ks:certificates/ks:certificate/ks:public-key-format describing the encoding of the public
2472 key of the selected cryptographic algorithm according to draft-ietf-netconf-crypto-types,
 - 2473 • ks:certificates/ks:certificate/ks:public-key containing the public key value in the selected
2474 public-key-format,
 - 2475 • ks:certificates/ks:certificate/ks:private-key-format describing the encoding of the private
2476 key of the selected cryptographic algorithm according to draft-ietf-netconf-crypto-types,
 - 2477 • ks:certificates/ks:certificate/ks:cleartext-private-key containing the private key value in
2478 the selected private-key-format,

2479 NOTE The private key is confidentially protected by NETCONF-over-TLS even if the option <cleartext-private-key>
2480 is used.

- 2481 • ks:certificates/ks:certificate/ks:name = LDevID-NETCONF, and
- 2482 • ks:certificates/ks:certificate/ks:cert-data containing the certificate chain LDevID-
2483 NETCONF end entity certificate (plus intermediate CA certificates, if applicable) plus
2484 self-signed root CA certificate as data object of type end-entity-cert-cms according to
2485 draft-ietf-netconf-crypto-types.

2486 The imprintCredential step shall use the NETCONF operation <edit-config> according to IETF
2487 RFC 6241 for the keystore container. The NETCONF operation <commit> is not yet applied,
2488 but rather after successful completion of all security setup sequence steps.

2489 External key generation can introduce security vulnerabilities during the generation and loading
2490 process. Ensuring those processes are secure is the responsibility of the user and not
2491 addressed in this document.

2492

2493 **6.3.4.4 imprintCertToNameMapping**

2494 The Configuration Domain specific certificate-to-name mapping is imprinted in the ietf-netconf-
2495 server YANG module under the following node.

- /ncs:netconf-server/ncs:listen/ncs:endpoint/ncs:tls/ncs:netconf-server-parameters/ncs:client-identity-mappings/ncs:cert-to-name, with the following leaves:
 - id = 1,
 - fingerprint = Configuration Domain specific fingerprint of the LDevID-NETCONF trust anchor using the hash algorithm sha256 according to IETF RFC 7589, Clause 7, and
 - map-type = ext-60802-roles.

The application of this map-type is described in 6.3.5, steps e) and f).

The imprintCertToNameMapping step uses the NETCONF operation <edit-config> according to IETF RFC 6241 for the certificate-to-name mapping. Afterwards the NETCONF operation <commit> is 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 credentials for authentication.

The procedure called “provisional accept of client certificate” as described in 6.3.4.2 is not 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 and IETF draft-ietf-netconf-over-tls13, 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 specified 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 certificate of the NETCONF server.

6.4 Management

6.4.1 General

Subclause 6.4 describes a model for configuration, deployment, and management of an industrial automation network.

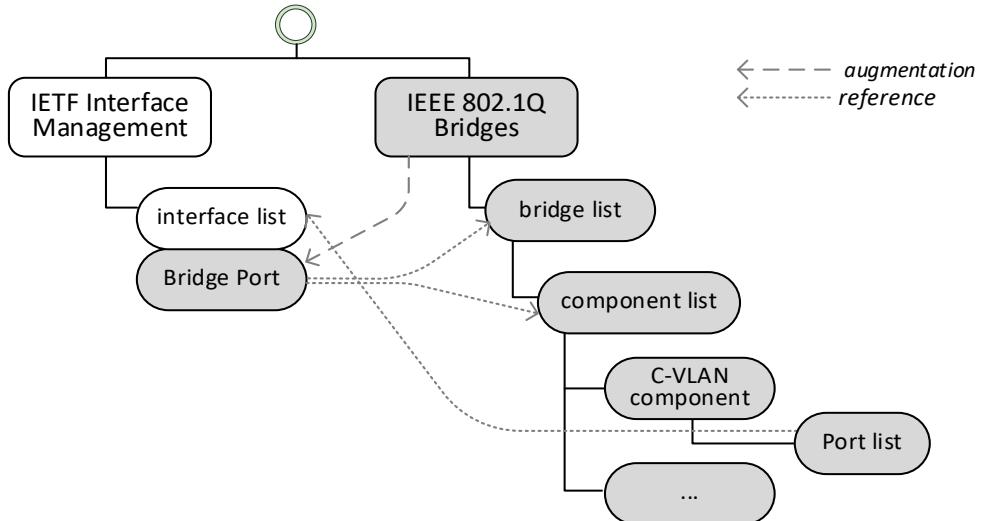
6.4.2 IA-station management model

6.4.2.1 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.

2544 **6.4.2.2 IEEE 802.1Q management model**

2545 In industrial automation both Bridge and end station components make use of IEEE 802.1Q
 2546 specified functionality (for example, traffic classes, gate control). Thus, the IEEE 802.1Q
 2547 management model is the basic management model to be applied to all IA-stations. Figure 16
 2548 shows the implementation of the IEEE Std 802.1Q Bridge model in YANG as specified in IEEE
 2549 Std 802.1Q-2022, Clause 48. The IETF Interface Management YANG data model is specified
 2550 in IETF RFC 8343.



2551

Figure 16 – Generic IEEE 802.1Q YANG Bridge management model

2553 The IEEE 802.1Q Bridge model is organized as a bridge list where each bridge includes an
 2554 underlying component list (for example, C-VLAN components). Each component has a Port list
 2555 attached with references to the representation of the ports in the IETF interface list. The
 2556 managed data of the ports is defined as Bridge Port augmentation to the IETF interface model.
 2557 Each Bridge Port includes a reference to its bridge and component instances in the IEEE
 2558 802.1Q Bridge model.

2559 The YANG data model for an IEEE 802.1Q Bridge is applied to IA-stations as follows.

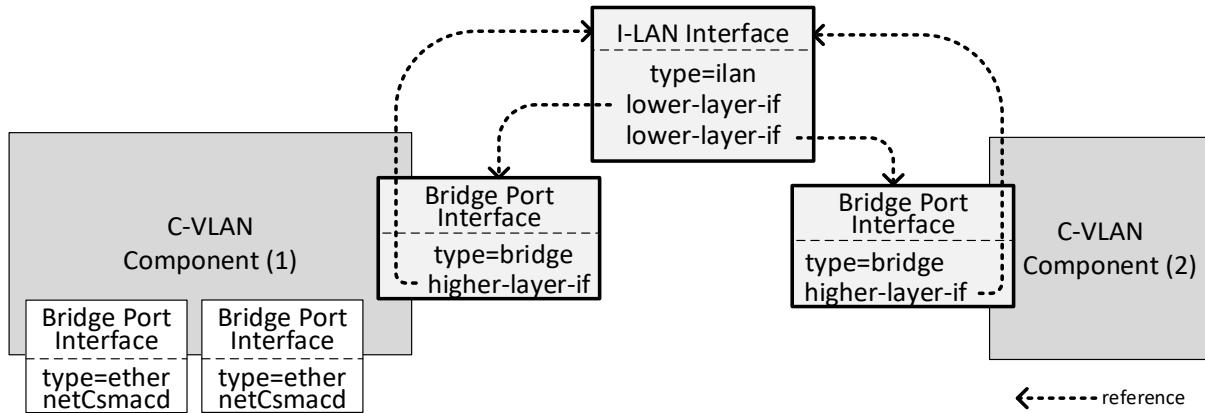
- 2560 • Each functional unit of an IA-station is modeled as bridge entry in the bridge list.
- 2561 • Each Bridge and end station component of an IA-station is modeled as C-VLAN component.
- 2562 • IA-station components belonging to the same functional unit are added to the component
 2563 list of this functional unit's bridge entry.
- 2564 • Each IA-station external or internal port is modeled as Bridge Port.

2565 IA-station ports belonging to the same component are added to the Port list of the related
 2566 component list entry.

2567 Further YANG data models which are relevant for IA-stations are described in 6.4.9.

2568 **6.4.2.3 Internal LAN connection model**

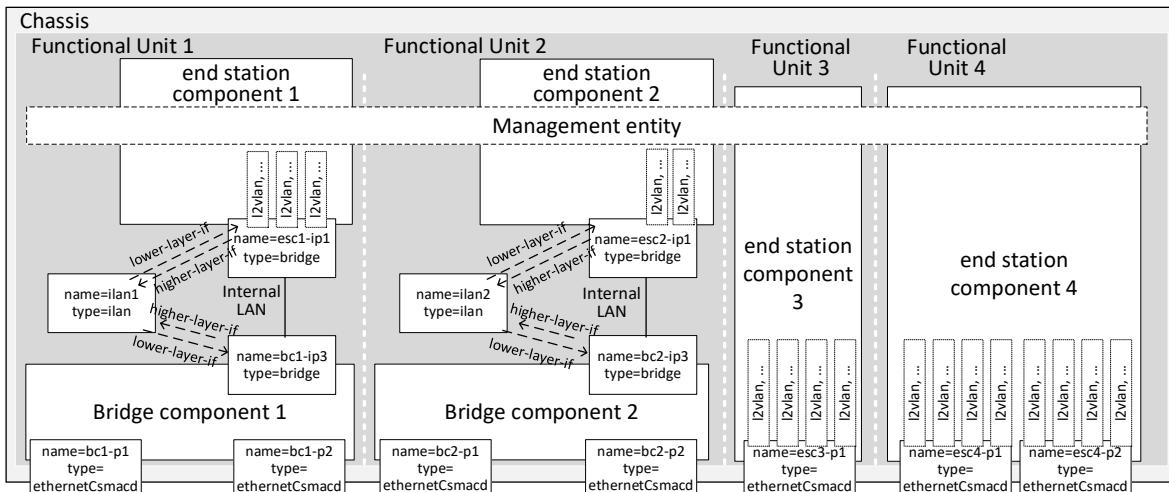
2569 The modeling of internal connections between C-VLAN components within an IA-station is
 2570 aligned to IEEE Std 802.1Q-2022, 17.3.2.2, which includes an I-LAN interface. As shown in
 2571 Figure 17, the I-LAN interface is modeled as an ilan IETF interface object (see IETF RFC 7224)
 2572 together with appropriate higher-layer-if and lower-layer-if reference objects to
 2573 describe the internal connection.

**Figure 17 – 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 interface of type ilan as described in IETF RFC 7224 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 18 shows the application of this model to the example IA-station of Figure 17.

**Figure 18 – IA-station example with IETF interfaces**

NOTE Figure 18 represents an abstract model and is not intended to imply a particular implementation or partitioning.

Figure 18 also shows the IETF Interfaces of type I2vlan which allow late binding of IA-station applications to the configured VLANs and priorities. The I2vlan interfaces of end station components are described in 6.4.2.5.

2591

2592 **6.4.2.4 Spanning Tree, VLAN and TE-MSTID configuration**

2593 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.

2598 The MSTP configuration is either default or accomplished by IA-station specific means.

2599 CNCs configure VLANs in the `vlan` list in the `bridge-vlan` container of the `ieee802-dot1q-bridge`
2600 YANG module. Ports are assigned to a `vlan` as `static-filtering-entries` in a `filtering-database`.

2601 NOTE `vlan`, in lowercase, refers to a YANG element.

2602 VLANs are assigned to filtering databases in the `vid-to-fid` list of the `bridge-vlan` container. The
2603 filtering databases, and in consequence the VLANs, are by default assigned to the MSTP
2604 calculated Internal Spanning Tree and can be assigned to the TE-MSTID by management. IA-
2605 time-aware streams and IA-streams are assigned to the TE-MSTID.

2606 TE-MSTID assignment is accomplished via the `bridge-mst` container of the `ieee802-dot1q-`
2607 `bridge` YANG module.

2608 It is the responsibility of the user to ensure that VLAN names are configured to conform to the
2609 scheme specified in 6.4.2.4 to support the required translations for VLAN-ID and PCP values
2610 as described in 4.3 and 6.4.2.5. The length of a VLAN name is restricted to a maximum of 32
2611 characters so that a compact name scheme is selected.

2612 • VLAN name in the form of: `60802-[<TrafficTypeCode><PCP>]{1,6}-<VID>[R]`, where:
2613 – `<TrafficTypeCode>` values are described in the Traffic type code column of Table 7,
2614 – `<PCP>` values are in the range of [0..7],
2615 – `<VID>` values are in the range of [1..4094],
2616 – There can be 1 to 6 `[<TrafficTypeCode><PCP>]` tuples in a VLAN name, and
2617 – VLANs with the optional `[R]` suffix represent VLANs which are used for redundant stream
2618 transmission. The VLAN which is associated to a redundant VLAN is identified by the
2619 VLAN name without the `[R]` suffix, with identical `<TrafficTypeCode><PCP>` tuple values.

2620 VLAN name examples:

Table 17 – VLAN name examples

VLAN Name	Description
60802-H6-101	VID 101 is used for isochronous traffic, which is mapped to PCP 6.
60802-H6-102R	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.

2622

2623 The following example shows the VID/FID/MSTID configuration of an IA-station's C-VLAN
2624 Bridge component, which supports three VLANs in three Forwarding Databases (VID 100 in FID
2625 1, VID 101 in FID 2 and VID 102 in FID 3). FID 2 and FID 3 – and in consequence VID 101 and
2626 VID 102 - are assigned to the TE-MSTID. FID 1 – and in consequence VID 100 - is not assigned
2627 to a MSTID and thus, is implicitly assigned to the Internal Spanning Tree (IST).

2628 Figure 19 shows the representation of this example configuration in the MST configuration
2629 table.

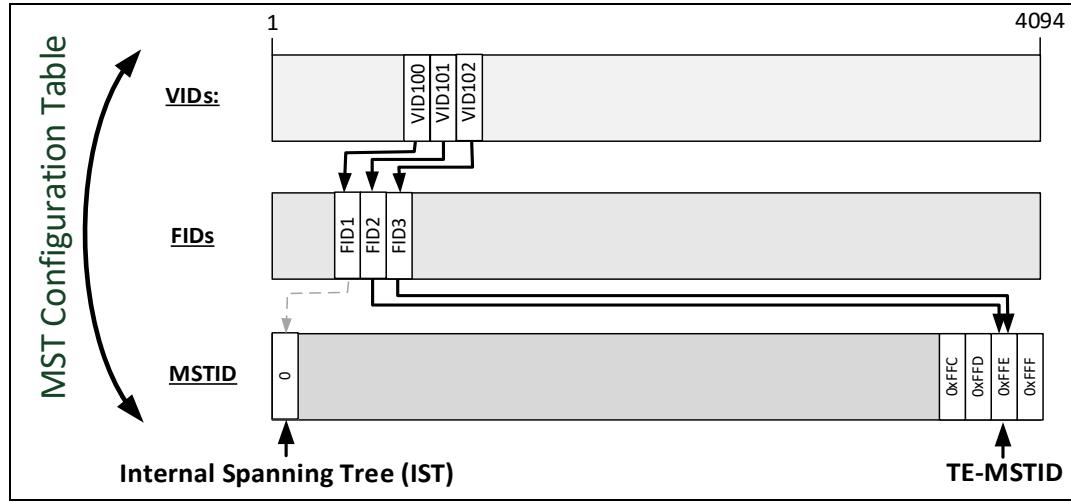


Figure 19 – VID/FID/MSTID example

2632 The YANG-based configuration of this example is shown as YANG instance data snippet of the
 2633 ieee802-dot1q-bridge YANG module. Herein the MST configuration table is included in
 2634 component “bridge-component-x”, which is part of bridge “functional-unit-x”.

```

2635 <ieee802-dot1q-bridge xmlns="urn:ietf:params:xml:ns:yang:ieee802-dot1q-bridge">
2636   <bridges>
2637     <bridge> <!-- list -->
2638       <name>functional-unit-x</name>
2639       ...
2640       <component> <!-- list -->
2641         <name>bridge-component-x</name>
2642         ...
2643         <bridge-vlan>
2644           <version>2</version> <!-- MST supported -->
2645           ...
2646           <vlan>
2647             <vid>100</vid>
2648             <name>60802-A0B1-100</name> <!-- best effort high and low -->
2649             </vlan>
2650             <vlan>
2651               <vid>101</vid>
2652               <name>60802-H6-101</name> <!-- isochronous -->
2653               </vlan>
2654               <vlan>
2655                 <vid>102</vid>
2656                 <name>60802-H6-102R</name> <!-- isochronous -->
2657               </vlan>
2658               ...
2659               <vid-to-fid>
2660                 <vid>100</vid>
2661                 <fid>1</fid>
2662               </vid-to-fid>
2663               <vid-to-fid>
2664                 <vid>101</vid>
2665                 <fid>2</fid>
2666               </vid-to-fid>
2667               <vid-to-fid>
2668                 <vid>102</vid>
2669                 <fid>3</fid>
2670               </vid-to-fid>
2671             </bridge-vlan>
2672             ...
2673             <bridge-mst>
2674               ...
2675               <fid-to-mstid> <!-- list -->
2676                 <!-- fid 1 is implicitly assigned to mstid 0 -->
2677                 <fid>2</fid>
2678               <mstid>4094</mstid> <!-- TE-MSTID -->
```

```
2679             </fid-to-mstid>
2680             <fid-to-mstid> <!-- list -->
2681                 <fid>3</fid>
2682                 <mstid>4094</mstid> <!-- TE-MSTID -->
2683             </fid-to-mstid>
2684         </bridge-mst>
2685         ...
2686     </component>
2687   </bridge>
2688 </bridges>
2689 </ieee802-dot1q-bridge>
```

2691 6.4.2.5 I2vlan type interfaces

Figure 18 shows the IETF Interfaces of type l2vlan (see IETF RFC 7224) in the end station components, which allow late binding of IA-station middleware components and applications to the configured VLANs and priorities.

2695 The CNC/NPE configures the VLANs using the Bridge Component YANG module (ieee802-
2696 dot1q-bridge) as shown in 6.4.2.4 with VLAN names describing the usage of PCP/VID values
2697 for various traffic types.

2698 Additionally, the CNC/NPE configures the I2Vlan interfaces with names composed of the VLAN
2699 names appended with the port interface name for every member port of the VLAN. The lower-
2700 layer-if reference can be set by the IA-stations internally to the end station component port
2701 interface if required by the end station component.

2702 NOTE The CNC cannot configure the lower-layer-if reference because it is defined read-only in the ietf-interfaces
2703 YANG module.

2704 The I2vlan interface names shall conform to the scheme specified in 6.4.2.5 to allow the
2705 required translations for VLAN-ID and PCP values as described in 4.6.

- VLAN name as specified in 6.4.2.4
 - l2vlan interface name: <VLAN name>-<PortIfName>

2708 <PortIfName> is the name of the end station component Port interface in the interface table.

2709 I2vlan name examples:

Table 18 – I2vlan name examples

I2vlan name	Description
60802-H6-101-ESC1-IP1	Isochronous traffic on interface ESC1-IP1 is mapped to PCP 6 and VID 101.
60802-H6-102R-ESC1-IP1	Redundant isochronous traffic on interface ESC1-IP1 is mapped to PCP 6 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.

2711

2712

2713 Table 19 provides a mapping of traffic type code to traffic type.

2714 **Table 19 – Map of traffic type code to traffic type**

Traffic type name	Traffic type code
Isochronous	H
Cyclic-synchronous	G
Cyclic-asynchronous	F
Alarms & Events	E
Configuration & Diagnostics	D
Network Control	C
Best Effort High	B
Best Effort Low	A

2715

2716 **6.4.3 Discovery of IA-station internal structure**

2717 LLDP provides information about the external connectivity of IA-stations. To identify the internal
 2718 structure of complex IA-stations (see 4.3) the IEEE 802.1Q management model (see 6.4.2.2)
 2719 and the IETF Interface management model are applied.

- 2720 • The functional units of an IA-station are represented as bridge entries in the bridge-list.
 2721 • The components of a functional unit are represented as component entries in the associated
 2722 bridge entry's component-list.
 2723 • Internal LAN connections between components of a functional unit are identified by I-LAN
 2724 entries in the IETF interface list (6.4.2.3).

2725

2726 **6.4.4 Network engineering model**

2727 To understand the requirements for network configuration, deployment and management, an
 2728 engineering model covering industrial use cases is required. The “fully centralized model”
 2729 described in IEEE Std 802.1Q-2022, 46.1.3.3 includes two functional entities: the CUC and the
 2730 CNC. The relationship between user and network configuration is described in IEEE Std
 2731 802.1Q-2022, Clause 46. This document further elaborates this relationship to address use
 2732 cases for industrial automation. A conceptual block diagram of a CNC is shown in Figure 20,
 2733 which adds further details to the CNC specified in IEEE Std 802.1Q-2022 to serve the industrial
 2734 automation use case. The following functional entities are introduced.

2735 a) **The Topology Discovery Entity (TDE)**

2736 The topology discovery entity is responsible for the topology discovery (i.e., Bridge
 2737 component and end station component discovery). The TDE also performs a topology
 2738 verification in cases where an expected topology is provided by the engineering tool. The
 2739 resulting topology information is used by the CNC. The TDE detects added or removed IA-
 2740 stations, including internal structure and connectivity. Thus, the CNC becomes aware of
 2741 them. Overall, the TDE discovers and maintains an inventory of the devices, including their
 2742 capabilities and the topology they form.

2743 b) The Path Entity (PE)

2744 The PE computes, establishes and maintains the forwarding paths for the IA time-aware
2745 stream and IA stream traffic type categories according to 4.7.3.

2746 c) The Sync Tree Entity (STE)

2747 The STE computes, establishes and maintains the sync trees. For example, for Working
2748 Clock and Global Time.

2749 d) The Resource Allocation Entity (RAE)

2750 The RAE is responsible for the allocation of the resources that are necessary for all traffic
2751 type categories, according to 4.7.3, to meet their requirements via their forwarding paths.
2752 For example, frame buffers at egress ports and FDB entries.

2753 e) The Network Provisioning Entity (NPE)

2754 The NPE applies a network policy provided by the Engineering Tool to the IA-stations within
2755 the Configuration Domain. It uses the information discovered by the TDE to create a network
2756 configuration based upon this policy which is then applied to all IA-stations. The CNC uses
2757 the chosen network configuration together with the discovered IA-stations and their
2758 capabilities as input for its stream calculation and deployment.

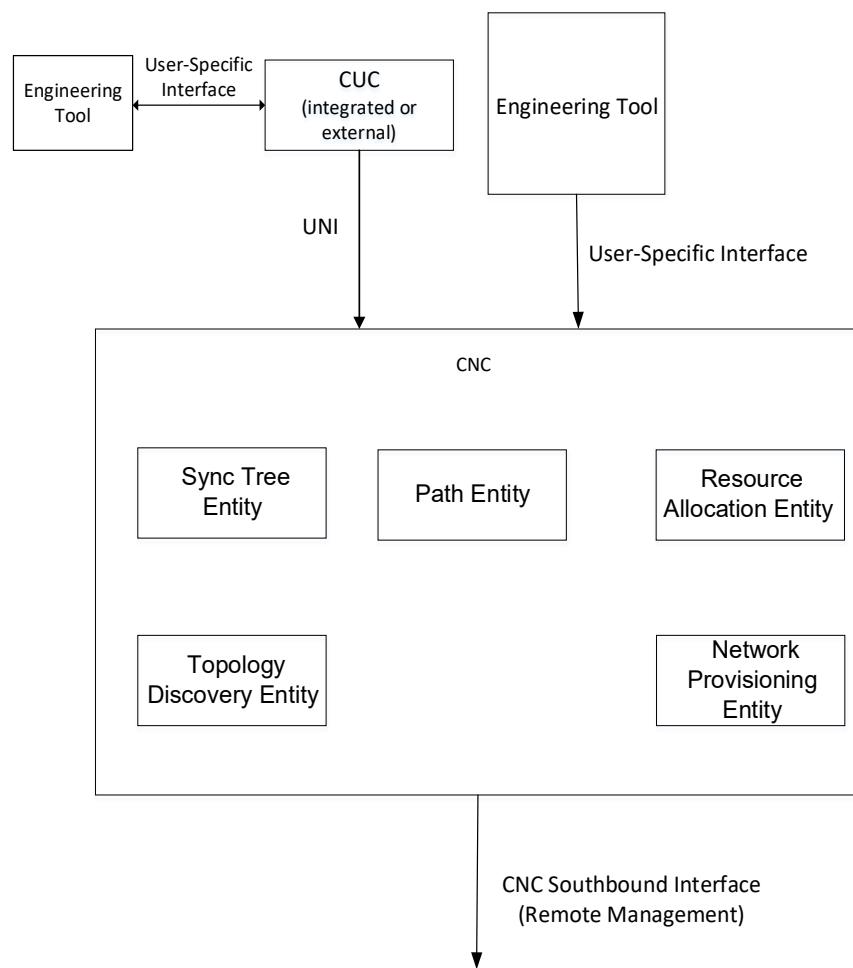
2759 A CNC includes these functional entities. The implementation of these functional entities and
2760 the CNC can vary. The means of communication among these functional entities is
2761 implementation dependent.

2762 If there are multiple CNCs in one Configuration Domain, then, by some means not addressed
2763 by this document, only a single CNC is in charge at any time in the given Configuration Domain.

2764 The CNC can be in a dedicated station or integrated into any IA-controller or IA-device.
2765 Generally, its engineering tool interface is user-specific and can only work with the compatible
2766 engineering tools. The definition of this interface is not addressed in this document.

2767 The CUC can be in a dedicated station or integrated into any IA-controller or IA-device.
2768 Generally, the CUC is user-specific. In industrial automation use cases, an IA-controller
2769 integrated CUC is very likely.

2770 For stream establishment, the UNI of the CNC component is exposed.



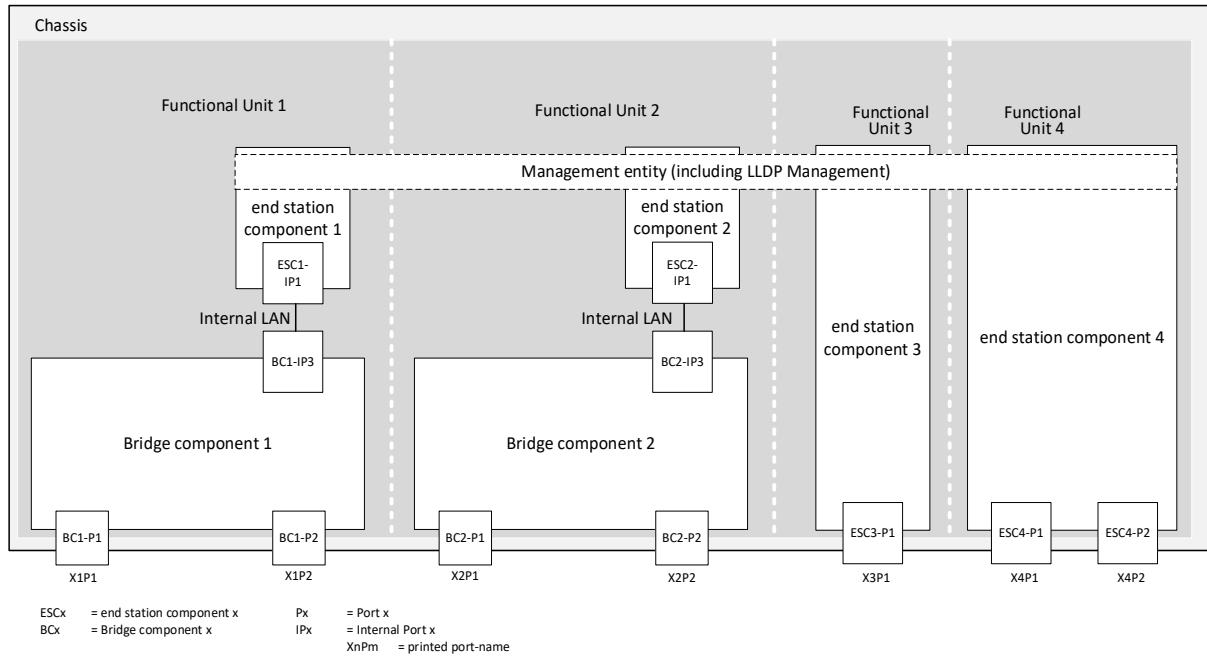
2771

2772

Figure 20 – Structure and interfaces of a CNC

2773

2774 Figure 21 shows an example of the structure of an IA-station which the CNC might discover and
2775 manage.



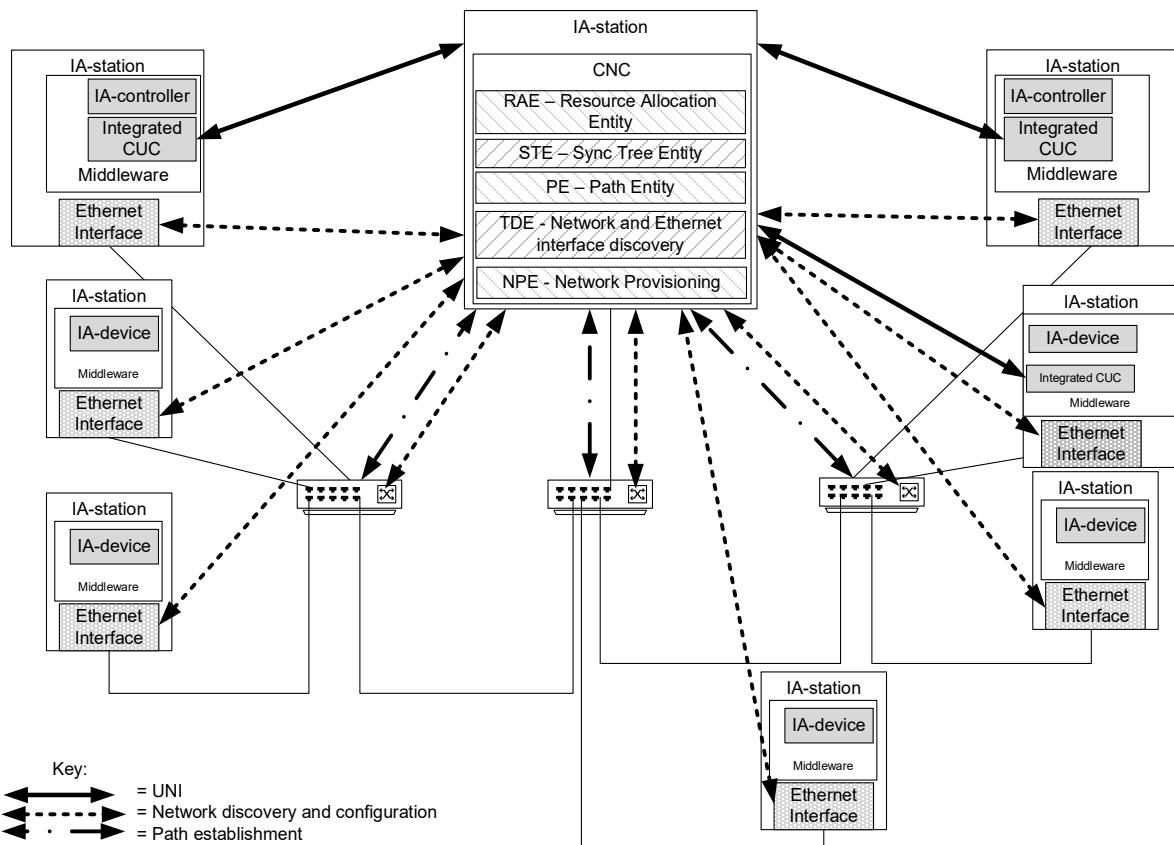
2776

2777

Figure 21 – IA-station structure example

2778

Figure 22 shows the interaction of IA-stations with the CNC.



2779

2780

Figure 22 – CNC interaction

2781

6.4.5 Operation

6.4.5.1 General

A representative model for network configuration is shown in Figure 23. This diagram maintains the traditional role of the IA-controller and the IA-device in an industrial automation network. IA-devices and IA-controllers require configuration from engineering tools (refer to engineering tools A, B, D, and E). These tools and associated interfaces are not addressed by this document. 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 an 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 goes 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 23, reflects the model used in industrial automation. Figure 23 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.

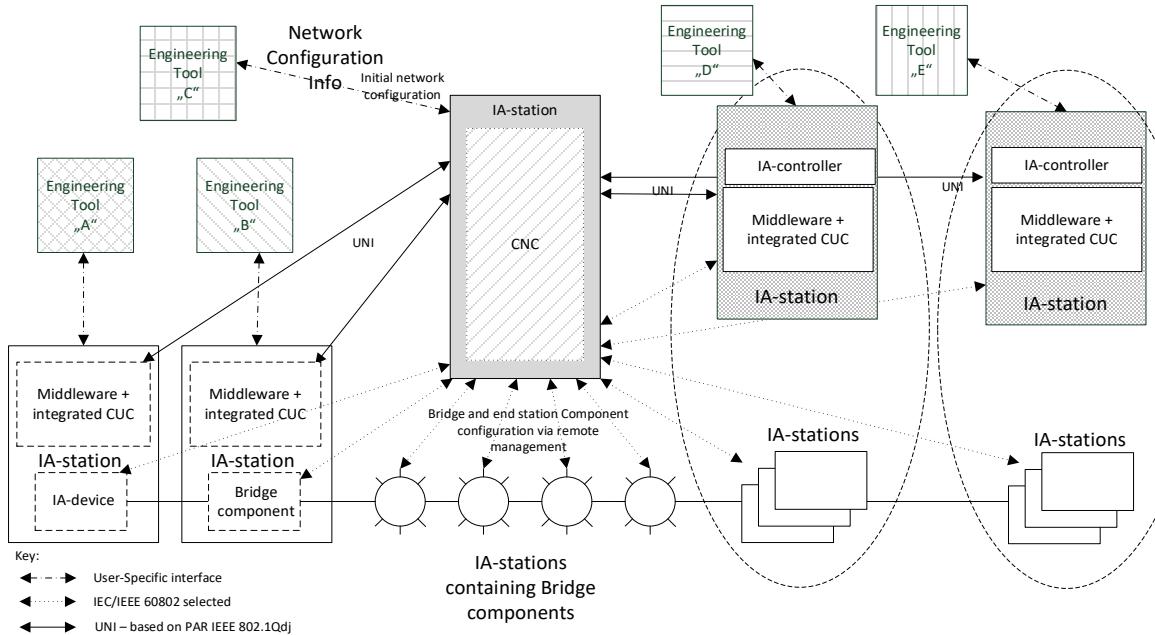
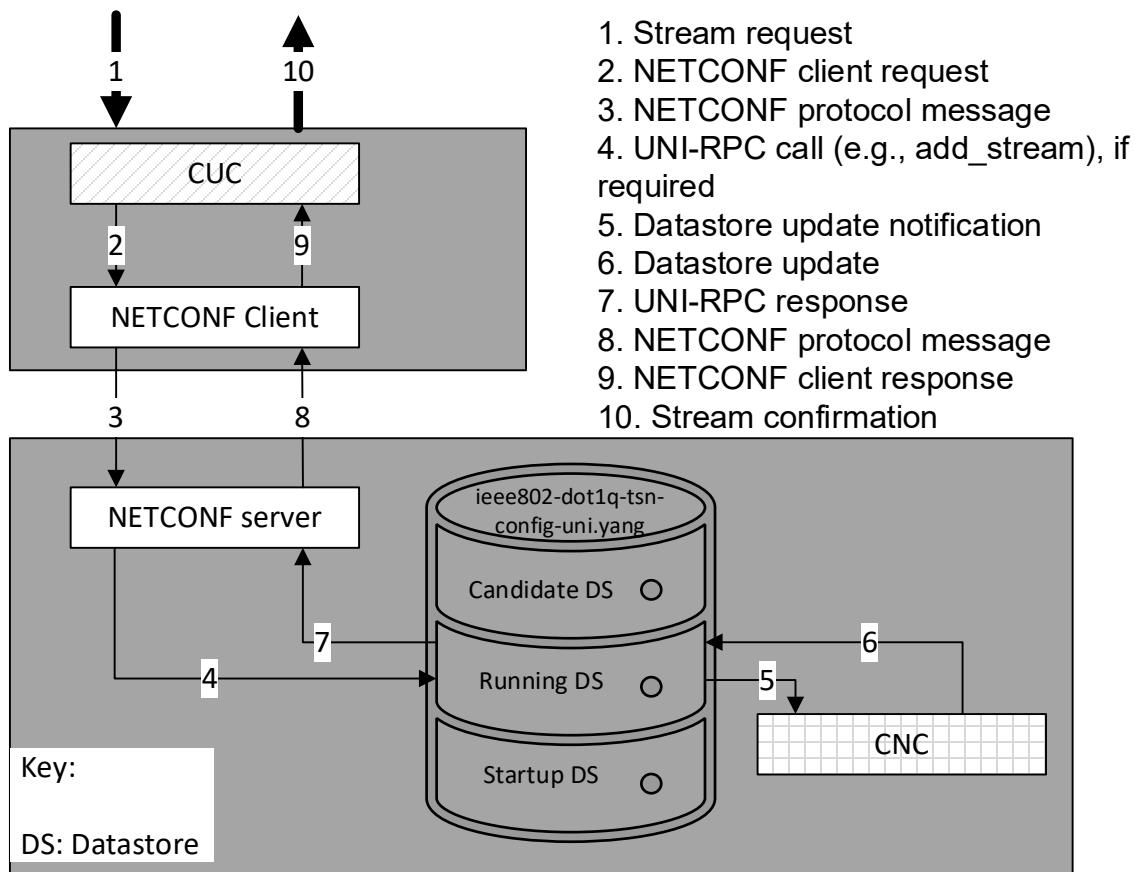


Figure 23 – Operational management model

Figure 24 shows the steps that are typically performed in the scope of the CUC-CNC interaction.

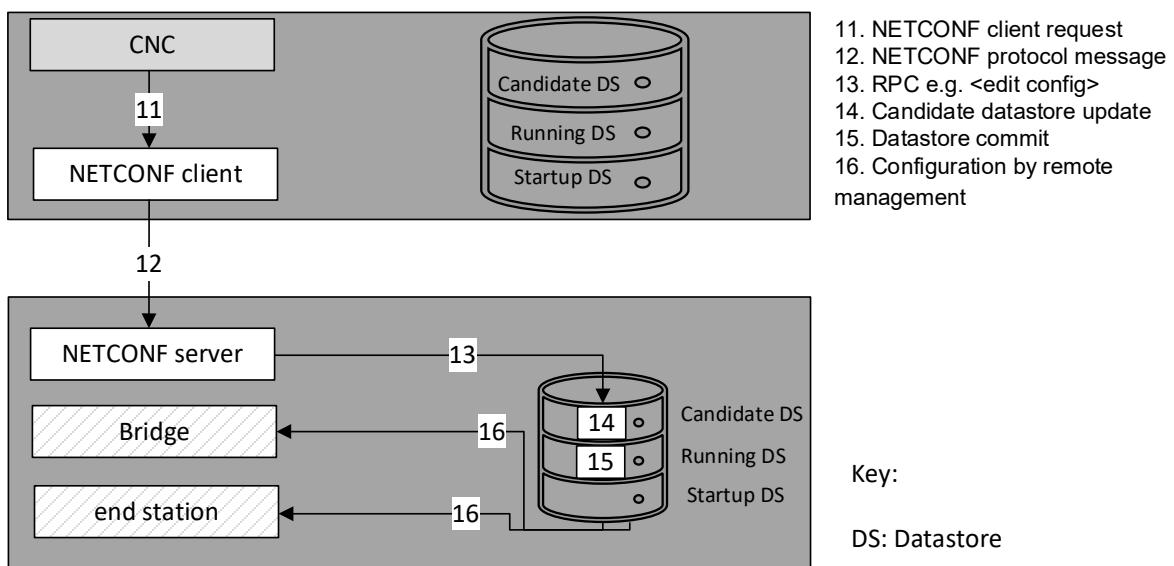
**Figure 24 – UNI service model**

2813

2814

2815

2816 After the computation of the paths and the scheduling and/or shaping configuration have been
 2817 done, the CNC configures the IA-stations via NETCONF client. The typical steps that are
 2818 performed in this process are shown in Figure 25 below.

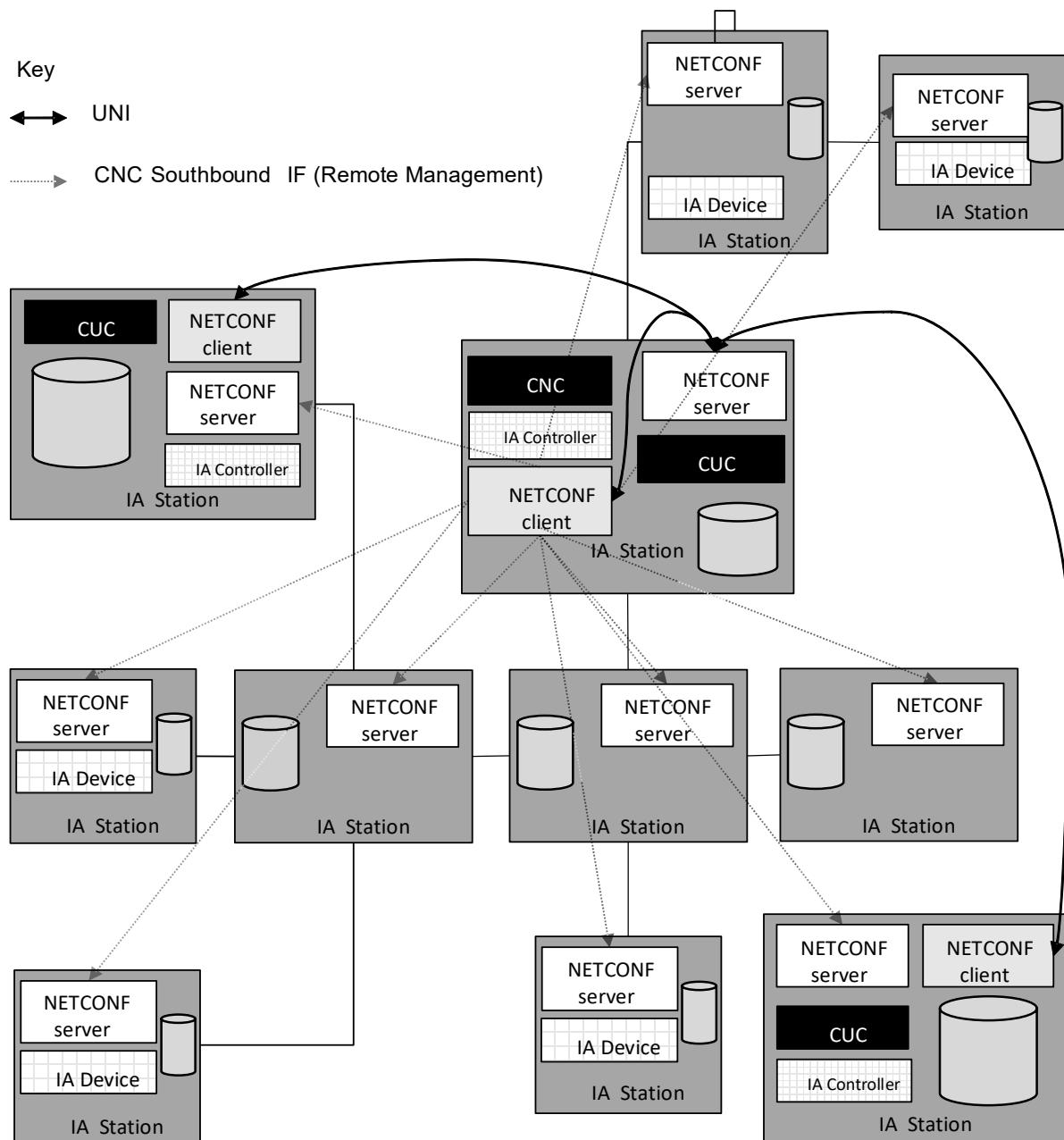
**Figure 25 – CNC southbound**

2819

2820

2821 Instances of NETCONF servers and clients within a Configuration Domain are shown in
 2822 Figure 26. IA-stations that contain a CNC and/or CUC entity contain both a NETCONF server
 2823 and a NETCONF client. A NETCONF client at the CUC side is needed for the UNI. A NETCONF
 2824 server at the CNC side is needed to accommodate the UNI as well as remote network
 2825 management of the end stations and bridges that are contained in the same chassis as the
 2826 CNC entity. The NETCONF client on the CNC side is needed for the southbound interface of
 2827 the CNC i.e., for the remote management of the bridges and end stations in the scope of stream
 2828 configuration. All IA-stations have a NETCONF server to make remote management possible.
 2829 The NETCONF server used by the CNC serves multiple NETCONF Clients (CUCs) within a
 2830 single Configuration Domain whose requests clients can occur simultaneously.

2831



2832

2833

Figure 26 – NETCONF usage in a Configuration Domain

2834

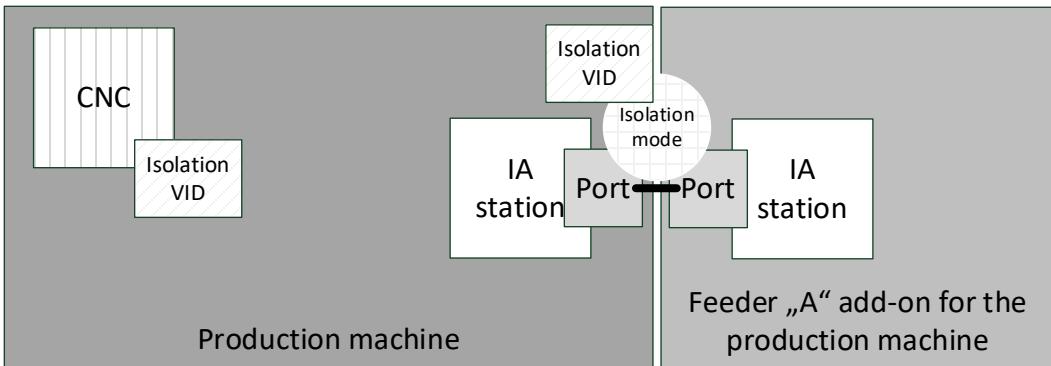
2835 **6.4.5.2 Domain port states**

2836 A CNC manages available network resources and assigns them to the IA-stations. Management
 2837 of the network resources is only possible if the CNC owns these resources. Thus, no connected

2838 station is allowed to make use of network resources that are not granted by the CNC. The
 2839 security configuration of a connected station allows remote access for the CNC.

2840 Protection of the network resources is done by managing the ports (see Figure 27) at the
 2841 boundary of the Configuration Domain. The state of any newly connected station is unknown.
 2842 The CNC is responsible for determining if the newly connected station is added to the
 2843 Configuration Domain and configuring the IA-station appropriately.

2844 This port state model avoids any assumptions about configuration of added stations or network
 2845 portions.



2846

2847 **Figure 27 – Boundary port model**

2848 Ports of an IA-station that is a member of a Configuration Domain have different states:

- 2849 • Isolated – a station connected via this port can only exchange information with a CNC. The
 2850 CNC is responsible for establishing an isolation VID and for on boarding the station. In the
 2851 isolated state:
 - 2852 – 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;
 - 2853 – the port gets to or remains in isolated state in case of a link up event;
 - 2854 – the port stays in isolated state as long as the neighbor is unknown, not able to enter
 Boundary state.
- 2855 • Boundary – a station connected via this port is not part of the Configuration Domain, but is
 2856 allowed to access devices inside the Configuration Domain and to pass traffic through the
 2857 Configuration Domain
- 2858 • Inside – a station connected via this port is part of the Configuration Domain

2859 The determination of whether a given port of an IA-station remains in the Isolated state or
 2860 transitions to the Boundary or Inside state is performed by the CNC using remote management.
 2861 A port acts as a domain boundary if it is in the Isolated or Boundary state.

2862 For example, a port could be configured as follows:

- 2863 • Isolated state
 - 2864 – Port is IST boundary
 - 2865 – Port is not part of a sync tree
 - 2866 – Port uses VLAN stripping for egress
 - 2867 – Port uses VLAN assignment and priority regeneration to assign all traffic to an isolated
 VLAN
 - 2868 – Port uses an ingress rate limiter to control the amount of traffic for the Configuration
 Domain

- 2873 • Boundary state
 - 2874 – Port is part of IST
 - 2875 – Port is part of a sync tree
 - 2876 – Port uses VLAN stripping for egress
 - 2877 – Port uses VLAN assignment and priority regeneration to assign all traffic to a default
2878 VLAN
 - 2879 – Port uses an ingress rate limiter to control the amount of traffic for the Configuration
2880 Domain
- 2881 • Inside state
 - 2882 – Port is part of IST
 - 2883 – Port is part of a sync tree
 - 2884 – Port is part of the active topology for stream and non-stream traffic

2885
2886 An example workflow includes the following steps executed by the CNC:

- 2887 a) Topology discovery
 - 2888 1) Case A: Link down / Port not connected
 - 2889 i) Set port to isolated state
 - 2890 ii) Configure a NETCONF subscription “on data change” to the port state leaf
 - 2891 2) Case B: Neighbor is not a Configuration Domain member
 - 2892 i) Set port to boundary state
 - 2893 ii) Configure a NETCONF subscription “on data change” to the port state leaf
 - 2894 3) Case C: Neighbor is not a Configuration Domain member – but part of expected topology
 - 2895 i) Set port to boundary state
 - 2896 ii) Configure the neighbor station as Configuration Domain member
 - 2897 iii) Set port to inside state
- 2898 b) NETCONF subscription trigger
 - 2899 Issued to the CNC upon change of subscribed YANG data.

2900 **6.4.5.3 Engineered network**

2901 For an offline engineered (based on the available digital data sheets of the used IA-stations)
2902 centralized approach with fixed topology, fixed stations and fixed paths, the user provides traffic
2903 requirements, path information, topology information and expected network configuration to the
2904 CNC. The CNC then uses the TDE, RAE and the NPE to perform the calculation of paths,
2905 resources, and stream schedules necessary to meet the specified traffic requirements and
2906 deploys the result of these calculations via remote management. The CNC also provides the
2907 relevant results to the CUC via the UNI. The CUC then configures the end stations using the
2908 User-to-User interface (see Figure 3).

2909 The workflow for this example consists of the following steps:

- 2910 a) The user determines:
 - 2911 1) the expected network topology
 - 2912 2) the expected stations and its capabilities, value ranges and quantities
 - 2913 3) the expected paths and resources
 - 2914 4) the required streams
 - 2915 5) the requirements for IA non-stream traffic.

2917 This step focuses on network capabilities including the Ethernet interface of the end stations.
2918 For example, if the end station is a sensor, the user needs to consider the Ethernet interface
2919 capabilities of the sensor as they apply to the physical world.

2920 b) Engineering Tool provides this information to the CNC via a user-specific interface.

2921

2922 Although the communication between the CNC and any Engineering Tool is user-specific, the
2923 CNC needs to obtain all information needed by the integrated TDE and NPE.

2924 c) The CNC uses the TDE to discover the topology and checks it against the expected
2925 topology. The NPE is used to configure the IA-stations of the Configuration Domain.

2926 d) The CNC uses STE and NPE to setup, validate, and monitor synchronization configuration
2927 in the Configuration Domain.

2928 e) The CNC uses the information from engineering item a), steps 1 to 5, above to respond to
2929 requests from Middleware (with integrated CUC) using UNI. These requests are handled
2930 using the already established communication paths received from the user.

2931 If the CNC is not required after commissioning, then the CNC can be removed after setting up
2932 the IA-stations. That requires that all IA-stations have a persistent storage for the data provided
2933 by the CNC.

2934 **6.4.5.4 Dynamic topology**

2935 **6.4.5.4.1 General**

2936 For a centralized approach with a dynamic topology and dynamic paths, the user provides the
2937 network policy to the CNC. The TDE performs topology discovery including IA-station
2938 capabilities (YANG representation of the digital data sheet) and the NPE performs network
2939 configuration for the CNC. IA-stations then provide traffic requirements via the Middleware to
2940 the CNC via the UNI. The CNC then uses the TDE, RAE, and NPE to perform the calculation of
2941 paths, resources, and stream schedules necessary to meet the specified traffic requirements
2942 and deploys the result of these calculations via remote management. The CNC also provides
2943 the relevant results to the CUC via the UNI. The CUC then configures the end stations using
2944 the User-to-User interface (see Figure 3).

2945 The workflow for this example consists of the following steps:

- 2946 a) The user determines the network policy and provides it to the CNC.
- 2947 b) The TDE continuously discovers the physical network topology and station capabilities of
each station using remote management.
- 2949 c) The NPE uses the information gathered in steps a) to b) to configure the IA-stations in the
2950 Configuration Domain.
- 2951 d) The CNC uses STE and NPE to setup, validate and monitor time synchronization
2952 configuration in the Configuration Domain.

2953 The CNC uses the information from steps a) to d) to respond to requests from Middleware using
2954 UNI. The CNC establishes streams in the bridges via a remote management protocol.

2955 **6.4.5.4.2 Adding an IA-station**

2956 Each IA-station added to the Configuration Domain is discovered by the TDE and receive the
2957 network configuration from the NPE. After this, the Middleware can request stream
2958 establishment.

2959 When an IA-station is added to the network, it is isolated until the CNC determines that its traffic
2960 requirements can be accommodated without disrupting other traffic (see 6.4.5.2).

2961 **6.4.5.4.3 Removing an IA-station**

2962 Each IA-station removed from the Configuration Domain is discovered by the TDE. A
2963 neighboring station can receive an updated network configuration by the NPE. After this, the
2964 removed IA-station is no longer part of the Configuration Domain.

6.4.5.4.4 Replacing an IA-station

In the simplest case, replacing an IA-station is simply the sequence of removing an IA-station (6.4.5.4.3) and adding an IA-station (6.4.5.4.2). In more complex cases, other precautions or user actions can be needed following deployment.

6.4.5.5 Engineered network extended by dynamic topology

The engineered and dynamic topology workflows can be used together. For instance, modular machines, robot tool changers or more general plug & produce can add or remove modules. The basic machine is handled as an engineered network. Additional modules or removed modules are handled dynamically.

6.4.6 Engineered time-synchronization spanning tree

6.4.6.1 General

Engineered time-synchronization spanning tree (sync tree) for a given gPTP domain refers to the usage of external port configuration instead of BTCA 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). The Grandmaster PTP Instance can reside in a dedicated grandmaster-capable IA-station.

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. Hot standby (see IEEE Draft Std P802.1ASdm) is a use case of an engineered sync tree.

6.4.6.2 Sync tree requirements

If an engineered synchronization spanning tree is used, the sync tree requirements for all participating PTP Instances in a gPTP domain are specified in 5.5.3 h).

6.4.6.3 STE phases

6.4.6.3.1 General

The STE should follow the logical sequence described in 6.4.6.3 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.

6.4.6.3.2 Discovery phase

In discovery phase, STE utilizes the topology discovered by the TDE to verify the capabilities and status of participating IA-stations via a diagnostics entity (see 6.4.7.1) 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 timeReceiver PTP End Instance is within the limit prescribed by for example, CNC.

3013

3014 **6.4.6.3.3 Provisioning phase**

3015 In provisioning phase, STE should apply the desired configuration to all participating PTP
3016 Instances, for example:

- 3017 • the desiredState of all PTP ports of the Grandmaster PTP Instance is set to
3018 TimeTransmitterPort,
- 3019 • the desiredState of exactly one PTP port of all the other PTP Instances is set to
3020 TimeReceiverPort,
- 3021 • the desiredState of remaining PTP ports that are part of sync tree in non-Grandmaster PTP
3022 Relay Instances is set to TimeTransmitterPort, and
- 3023 • The desiredState of all other PTP ports is set to PassivePort.

3024 Then STE should validate, for example, the syncLocked (see IEEE Std 802.1AS-2020, 14.8.52)
3025 parameter is TRUE for all PTP ports of PTP Relay Instances that are in TimeTransmitterPort
3026 state.

3027

3028 **6.4.6.4 Adding an IA-station**

3029 Each IA-station added to the gPTP domain is discovered by STE via TDE. It is the responsibility
3030 of the CNC to on-board this newly added station. IA-stations can receive an updated gPTP
3031 configuration via STE.

3032 A newly installed IA-station can disrupt the operation of a gPTP domain. The extent of disruption
3033 is dependent on the location of the IA-station in the gPTP domain and the type of PTP Instance
3034 running on that IA-station. For example, if PTP Instances are arranged in a daisy-chain
3035 formation and if a IA-station with a non-Grandmaster Relay Instance is installed in the middle
3036 of a daisy-chain then this change will disrupt for example, the operation of downstream PTP
3037 Instances.

3038

3039 **6.4.6.5 Removing an IA-station**

3040 The removal of a station from the gPTP domain is detected by STE via TDE. IA-stations can
3041 receive an updated gPTP configuration via STE.

3042 **6.4.6.6 Replacing an IA-station**

3043 An IA-station replacement follows the sequence of removing a IA-station according to 6.4.6.5
3044 and adding a IA-station according to 6.4.6.4.

3045 **6.4.7 Diagnostics**3046 **6.4.7.1 General**

3047 Diagnosis for an IA-station is done by monitoring YANG representation of the IA-station's local
3048 database.

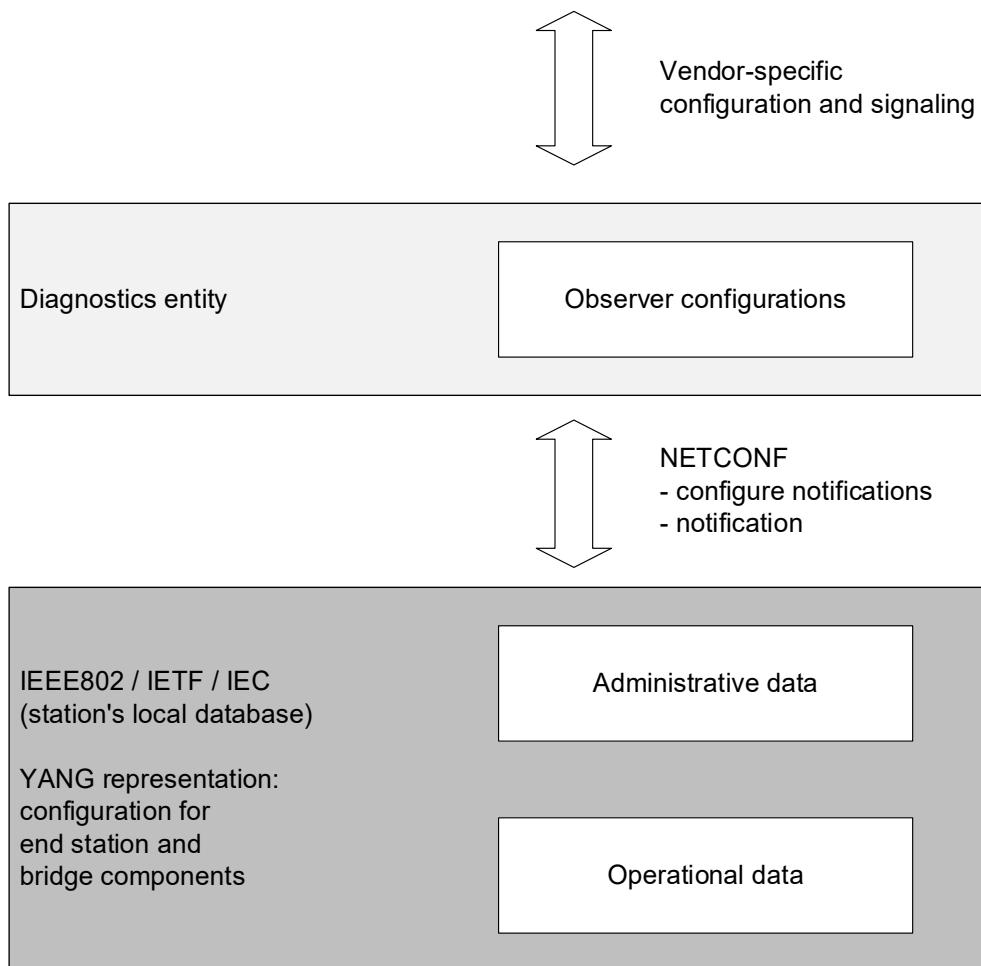
3049 A vendor can implement an observer in a diagnostics entity, which could reside in the CNC.
3050 This diagnostics entity uses the information provided by remote management to define the
3051 monitored objects and set up fitting notifications.

3052 **6.4.7.2 Observer model**

3053 A diagnostic entity can select any objects described via YANG and observe them via NETCONF.
3054 The NETCONF binding is specified in IETF RFC 8640, and the subscription model in IETF RFC
3055 8641. NETCONF messages can be pipelined, i.e., a client can invoke multiple RPCs without
3056 having to wait for RPC result messages first. RPC messages are specified in IETF RFC 6241,
3057 and notification messages are specified in IETF RFC 5277. To reduce the load on the diagnostic
3058 entity when many stations are providing notifications, the diagnostic objects can be monitored
3059 and notifications can be retrieved from individual IA-stations.

3060 Figure 28 shows the model of a diagnostic observer.

3061



3062

Figure 28 – Observer model

3064

3065

3066 **6.4.7.3 Usage of YANG Push**

3067 For diagnostics, an IA-station shall support YANG-Push subscriptions according to IETF RFC
 3068 8641 (YANG Push) and IETF RFC 8639 (Subscribed Notifications).

3069 IA-stations shall support the “subtree” selection filter as specified in IETF RFC 8041, 3.6

3070 **6.4.7.4 Mandatory RPCs**

3071 An IA-station shall support following RPCs as specified in IETF RFC 8641:

- 3072 a) establish-subscription,
- 3073 b) modify-subscription,
- 3074 c) delete-subscription, and
- 3075 d) kill-subscription.

3076

3077 6.4.7.5 Mandatory notifications

3078 An IA-station shall support following notifications as specified in IETF RFC 8641:

- 3079 a) subscription-resumed,
- 3080 b) subscription-modified,
- 3081 c) subscription-terminated,
- 3082 d) subscription-suspended,
- 3083 e) push-update, and
- 3084 f) push-change-update.

3085

3086 6.4.7.6 Mandatory diagnostics data nodes

3087 An IA-station shall provide following data nodes for diagnostic purpose.

- 3088 a) Change of link-status per Ethernet port:

/ietf-interfaces/interfaces-state/interface/oper-status

- 3090 b) Change of MAU-type per Ethernet port:

/ieee802-ethernet-lldp/lldp/port/ operational-mau-type

- 3092 c) Change of sync-status

- 3093 1) per PTP Instance

- 3094 – /dot1as-hs/ptp/instances/instance/ptp-instance-sync-ds/ptp-
 - 3095 instance-state

- 3096 – if Grandmaster PTP Instance: /iecieee60802-
 - 3097 ptp/instances/instance/default-ds/clock-source/clock-state

- 3098 – for every application-clock: /iecieee60802-
 - 3099 bridge/bridges/bridge/component/clock/is-synced

- 3100 2) per hot standby Instance

- 3101 /dot1as-hs/ptp/common-services/hss/hot-standby-system-list/hot-
 - 3102 standby-system-ds/hot-standby-system-state

- 3103 d) Data to be provided as periodic time-aligned subscriptions:

- 3104 1) Dropped frames statistic counters per Ethernet interface

- 3105 – /ietf-interfaces/interface/statistics/in-octets

- 3106 – /ietf-interfaces/interface/statistics/in-discards

- 3107 – /ietf-interfaces/interface/statistics/in-errors

- 3108 – /ietf-interfaces/interface/statistics/out-octets

- 3109 – /ietf-interfaces/interface/statistics/out-discards

- 3110 – /ietf-interfaces/interface/statistics/out-errors

- 3111 2) VLAN specific counters per Ethernet Interface and VLAN ID

- 3112 – /ieee802-dot1q-bridge/interfaces/interface/bridge-
 - 3113 port/statistics/octets-rx

- 3114 – /ieee802-dot1q-bridge/interfaces/interface/bridge-
 - 3115 port/statistics/octets-tx

- 3116 – /ieee802-dot1q-bridge/interfaces/interface/bridge-
 - 3117 port/statistics/forward-outbound

- 3118 – /ieee802-dot1q-bridge/interfaces/interface/bridge-
 - 3119 port/statistics/discard-inbound

3120

6.4.7.7 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 specified in IETF RFC 8640 Clauses 5, 6 and 7. The number of dynamic subscriptions shall be reported.

6.4.8 Data sheet**6.4.8.1 General**

Data sheets containing the capabilities, value ranges and quantities of IA-stations will allow a user to select appropriate IA-stations and enable users to configure a system using online and offline engineering. See Annex B for quantities in a representative Configuration Domain.

Online data sheets are modeled using YANG. YANG modeling is used for the offline data sheet to keep the offline (6.4.5.3) and online (6.4.5.4) format the same.

6.4.8.2 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, or supported features. An example depicting the creation of a digital data sheet is provided in Figure 29.

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 a digital data sheet file.

The digital data sheet of an IA-station provides a collection of all instantiated data nodes of all YANG modules that are required by this document (see 6.4.9). A manufacturer may reduce the instance data set by removing statistical config-false YANG nodes.

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 specified in IETF RFC 9195. The format of the YANG instance data set is specified 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 all YANG modules included in the digital data sheet.

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 6.4.9.2.5.11.

Any IA-station can include a CNC entity in which case the collection of YANG modules of such IA-station includes all CNC specific YANG modules for example, the ieee802-dot1q-tsn-config-uni YANG module. Since all IA-stations meet the requirements from 5.5.4, 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 6.4.9.2.

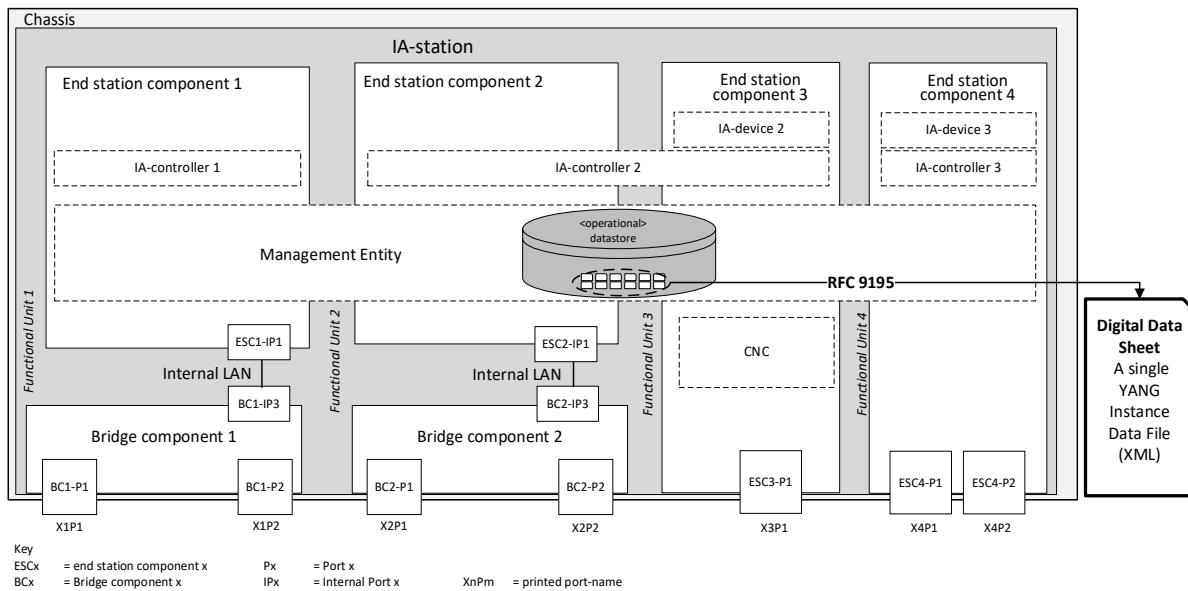


Figure 29 – Creation of the digital data sheet of an IA-station

6.4.9 YANG representation of managed objects and nodes^{5, 6}

6.4.9.1 General

All managed objects shall be represented in the YANG 1.1 format as described in IETF RFC 7950. The markings (i.e., [m], [o], [c]) indicate whether the node is included in the digital data sheet (see 3.5.4). These markings are independent of the conformance criteria for an IA-station (see 5.2).

6.4.9.2 Common YANG modules, features, and nodes

6.4.9.2.1 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 nodes:

- 3179 [o] /ieee802-ethernet-interface/interfaces/interface/ethernet/duplex
- 3180 [o] /ieee802-ethernet-interface/interfaces/interface/ethernet/speed
- 3181 [o] /ieee802-ethernet-interface/interfaces/interface/ethernet/flow-control/pause/direction (if the feature "ethernet-pause" is supported)

6.4.9.2.2 Station and media access control connectivity discovery

IA-stations shall support the following nodes from the ieee802-dot1ab-lldp YANG module according to IEEE Std 802.1ABcu-2021 with values and value ranges according to 6.5.

- 3186 [o] /ieee802-dot1ab-lldp/lldp/message-fast-tx
- 3187 [o] /ieee802-dot1ab-lldp/lldp/message-tx-hold-multiplier
- 3188 [o] /ieee802-dot1ab-lldp/lldp/message-tx-interval

⁵ Copyright release for YANG: Users of this document may freely reproduce the YANG modules contained in this document so that they can be used for their intended purpose.

⁶ An ASCII version of each YANG module defined in this document is attached to the PDF of this document and can also be obtained from the IEEE 802 Website at <https://1.ieee802.org/yang-modules/>.

3189 [o] /ieee802-dot1ab-lldp/lldp/reinit-delay
3190 [o] /ieee802-dot1ab-lldp/lldp/tx-credit-max
3191 [o] /ieee802-dot1ab-lldp/lldp/tx-fast-init
3192 [o] /ieee802-dot1ab-lldp/lldp/notification-interval
3193 [o] /ieee802-dot1ab-lldp/lldp/remote-statistics
3194 [o] /ieee802-dot1ab-lldp/lldp/remote-statistics/last-change-time
3195 [o] /ieee802-dot1ab-lldp/lldp/remote-statistics/remote-inserts
3196 [o] /ieee802-dot1ab-lldp/lldp/remote-statistics/remote-deletes
3197 [o] /ieee802-dot1ab-lldp/lldp/remote-statistics/remote-drops
3198 [o] /ieee802-dot1ab-lldp/lldp/remote-statistics/remote-ageouts
3199 [m] /ieee802-dot1ab-lldp/lldp/local-system-data
3200 [o] /ieee802-dot1ab-lldp/lldp/local-system-data/chassis-id-subtype
3201 [o] /ieee802-dot1ab-lldp/lldp/local-system-data/chassis-id
3202 [o] /ieee802-dot1ab-lldp/lldp/local-system-data/system-name
3203 [o] /ieee802-dot1ab-lldp/lldp/local-system-data/system-description
3204 [m] /ieee802-dot1ab-lldp/lldp/local-system-data/system-capabilities-supported
3205 [o] /ieee802-dot1ab-lldp/lldp/local-system-data/system-capabilities-enabled
3206 [o] /ieee802-dot1ab-lldp/lldp/port
3207 [o] /ieee802-dot1ab-lldp/lldp/port/name
3208 [o] /ieee802-dot1ab-lldp/lldp/port/dest-mac-address
3209 [o] /ieee802-dot1ab-lldp/lldp/port/admin-status
3210 [o] /ieee802-dot1ab-lldp/lldp/port/notification-enable
3211 [o] /ieee802-dot1ab-lldp/lldp/port/tlvs-tx-enable
3212 [o] /ieee802-dot1ab-lldp/lldp/port/message-fast-tx
3213 [o] /ieee802-dot1ab-lldp/lldp/port/message-tx-hold-multiplier
3214 [o] /ieee802-dot1ab-lldp/lldp/port/message-tx-interval
3215 [o] /ieee802-dot1ab-lldp/lldp/port/reinit-delay
3216 [o] /ieee802-dot1ab-lldp/lldp/port/tx-credit-max
3217 [o] /ieee802-dot1ab-lldp/lldp/port/tx-fast-init
3218 [o] /ieee802-dot1ab-lldp/lldp/port/notification-interval
3219 [o] /ieee802-dot1ab-lldp/lldp/port/management-address-tx-port
3220 [o] /ieee802-dot1ab-lldp/lldp/port/port-id-subtype

3223 [o] /ieee802-dot1ab-lldp/lldp/port/port-id
3224 [o] /ieee802-dot1ab-lldp/lldp/port/port-desc
3225 [o] /ieee802-dot1ab-lldp/lldp/port/remote-systems-data

3226 **6.4.9.2.3 Synchronization**

3227 **6.4.9.2.3.1 Timesync**

3228 IA-stations shall support the ieee1588-ptp YANG module according to IEEE Draft Std P1588e
3229 with the following features:

3230 • cmlds (Common Mean Link Delay Service), and
3231 • external-port-config.

3232 IA-stations shall support the ieee1588-ptp YANG module according to IEEE Draft Std P1588e
3233 with the following nodes:

3234 [o] /ieee1588-ptp/ptp/instances/instance/instance-index
3235 [o] /ieee1588-ptp/ptp/instances/instance/default-ds/clock-identity
3236 [o] /ieee1588-ptp/ptp/instances/instance/default-ds/number-ports
3237 [o] /ieee1588-ptp/ptp/instances/instance/default-ds/priority1
3238 [o] /ieee1588-ptp/ptp/instances/instance/default-ds/domain-number
3239 [o] /ieee1588-ptp/ptp/instances/instance/default-ds/time-receiver-only
3240 [o] /ieee1588-ptp/ptp/instances/instance/default-ds/sdo-id
3241 [o] /ieee1588-ptp/ptp/instances/instance/default-ds/instance-enable
3242 [o] /ieee1588-ptp/ptp/instances/instance/default-ds/external-port-
3243 config-enable
3244 [o] /ieee1588-ptp/ptp/instances/instance/default-ds/instance-type
3245 [o] /ieee1588-ptp/ptp/instances/instance/description-ds/user-
3246 description
3247 [o] /ieee1588-ptp/ptp/instances/ports/port/port-index
3248 [o] /ieee1588-ptp/ptp/instances/ports/port/underlying-interface
3249 [o] /ieee1588-ptp/ptp/instances/ports/port/port-ds/port-state
3250 [o] /ieee1588-ptp/ptp/instances/ports/port/port-ds/delay-mechanism
3251 [o] /ieee1588-ptp/ptp/instances/ports/port/port-ds/port-enable
3252 [o] /ieee1588-ptp/ptp/instances/ports/port/external-port-config-port-
3253 ds/desired-state
3254 [o] /ieee1588-ptp/ptp/common-services/cmlds/default-ds/clock-identity
3255 [o] /ieee1588-ptp/ptp/common-services/cmlds/default-ds/number-link-
3256 ports
3257 [o] /ieee1588-ptp/ptp/common-services/cmlds/ports/port/port-index
3258 [o] /ieee1588-ptp/ptp/common-services/cmlds/ports/port/underlying-
3259 interface

```

3260 [o] /ieee1588-ptp/ptp/common-services/cmlds/ports/port/link-port-
3261 ds/port-identity/clock-identity
3262 [o] /ieee1588-ptp/ptp/common-services/cmlds/ports/port/link-port-
3263 ds/port-identity/port-number
3264 [o] /ieee1588-ptp/ptp/common-services/cmlds/ports/port/link-port-
3265 ds/domain-number
3266 [o] /ieee1588-ptp/ptp/common-services/cmlds/ports/port/link-port-
3267 ds/service-measurement-valid
3268 [o] /ieee1588-ptp/ptp/common-services/cmlds/ports/port/link-port-
3269 ds/mean-link-delay
3270 [o] /ieee1588-ptp/ptp/common-services/cmlds/ports/port/link-port-
3271 ds/scaled-neighbor-rate-ratio
3272 [o] /ieee1588-ptp/ptp/common-services/cmlds/ports/port/link-port-
3273 ds/log-min-pdelay-req-interval
3274 [m] /ieee1588-ptp/ptp/common-services/cmlds/ports/port/link-port-
3275 ds/version-number
3276 [m] /ieee1588-ptp/ptp/common-services/cmlds/ports/port/link-port-
3277 ds/minor-version-number
3278 [o] /ieee1588-ptp/ptp/common-services/cmlds/ports/port/link-port-
3279 ds/delay-asymmetry
3280
3281 6.4.9.2.3.2 Timesync (draft ieee802-dot1as-ptp)
3282 IA-stations shall support the ieee802-dot1as-ptp YANG module according to IEEE Draft Std
3283 P802.1ASdn with the following nodes:
3284 [o] /ieee802-dot1as-ptp/ptp/instances/instance/default-ds/gm-capable
3285 [o] /ieee802-dot1as-ptp/ptp/instances/instance/default-ds/current-utc-
3286 offset-valid
3287 [o] /ieee802-dot1as-ptp/ptp/instances/instance/default-ds/ptp-
3288 timescale
3289 [o] /ieee802-dot1as-ptp/ptp/instances/ports/port/port-ds/sync-receipt-
3290 timeout
3291 [o] /ieee802-dot1as-ptp/ptp/instances/ports/port/port-ds/current-one-
3292 step-tx-oper
3293 [o] /ieee802-dot1as-ptp/ptp/instances/ports/port/port-ds/use-mgt-one-
3294 step-tx-oper
3295 [o] /ieee802-dot1as-ptp/ptp/instances/ports/port/port-ds/mgt-one-step-
3296 tx-oper
3297 [o] /ieee802-dot1as-ptp/ptp/instances/ports/port/port-ds/sync-locked
3298 [o] /ieee802-dot1as-ptp/ptp/common-services/cmlds/ports/port/link-
3299 port-ds/cmlds-link-port-enabled
3300 [o] /ieee802-dot1as-ptp/ptp/common-services/cmlds/ports/port/link-
3301 port-ds/is-measuring-delay

```

3302 [o] /ieee802-dot1as-ptp/ptp/common-services/cmlds/ports/port/link-
3303 port-ds/as-capable-across-domains

3304 [o] /ieee802-dot1as-ptp/ptp/common-services/cmlds/ports/port/link-
3305 port-ds/mean-link-delay-thresh

3306 [o] /ieee802-dot1as-ptp/ptp/common-services/cmlds/ports/port/link-
3307 port-ds/current-log-pdelay-req-interval

3308 [o] /ieee802-dot1as-ptp/ptp/common-services/cmlds/ports/port/link-
3309 port-ds/use-mgt-log-pdelay-req-interval

3310 [o] /ieee802-dot1as-ptp/ptp/common-services/cmlds/ports/port/link-
3311 port-ds/mgt-log-pdelay-req-interval

3312 [o] /ieee802-dot1as-ptp/ptp/common-services/cmlds/ports/port/link-
3313 port-ds/current-compute-rate-ratio

3314 [o] /ieee802-dot1as-ptp/ptp/common-services/cmlds/ports/port/link-
3315 port-ds/use-mgt-compute-rate-ratio

3316 [o] /ieee802-dot1as-ptp/ptp/common-services/cmlds/ports/port/link-
3317 port-ds/mgt-compute-rate-ratio

3318 [o] /ieee802-dot1as-ptp/ptp/common-services/cmlds/ports/port/link-
3319 port-ds/current-compute-mean-link-delay

3320 [o] /ieee802-dot1as-ptp/ptp/common-services/cmlds/ports/port/link-
3321 port-ds/use-mgt-compute-mean-link-delay

3322 [o] /ieee802-dot1as-ptp/ptp/common-services/cmlds/ports/port/link-
3323 port-ds/mgt-compute-mean-link-delay

3324 [o] /ieee802-dot1as-ptp/ptp/common-services/cmlds/ports/port/link-
3325 port-ds/allowed-lost-responses

3326 [o] /ieee802-dot1as-ptp/ptp/common-services/cmlds/ports/port/link-
3327 port-ds/allowed-faults

3328

3329 **6.4.9.2.3.3 Timesync (ieee802-dot1as-hs)**

3330 IA-stations shall support the ieee802-dot1as-hs YANG module according to IEEE Draft Std
3331 P802.1ASdm with the following nodes:

3332 [o] /ieee802-dot1as-hs/ptp/instances/instance/ptp-instance-ds-/is-
3333 synced

3334

3335 **6.4.9.2.4 Security configuration modules**

3336 **6.4.9.2.4.1 YANG module for a keystore**

3337 IA-stations shall support the ietf-keystore YANG module according to draft-ietf-netconf-keystore
3338 with the following features:

- 3339 • central-truststore-supported, and
3340 • asymmetric-keys.

3341

3342 IA-stations shall support the ietf-keystore YANG module according to draft-ietf-netconf-keystore
3343 with the following nodes:

3344 [o] /ietf-keystore/keystore/asymmetric-keys/asymmetric-key/name

3345 [o] /ietf-keystore/keystore/asymmetric-keys/asymmetric-key/public-key-
3346 format
3347 [o] /ietf-keystore/keystore/asymmetric-keys/asymmetric-key/public-key
3348 [o] /ietf-keystore/keystore/asymmetric-keys/asymmetric-key/private-
3349 key-format
3350 [o] /ietf-keystore/keystore/asymmetric-keys/asymmetric-key/hidden-
3351 private-key
3352 [o] /ietf-keystore/certificates/certificate/name
3353 [o] /ietf-keystore/certificates/certificate/cert-data
3354 [o] /ietf-keystore/certificates/certificate/expiration-date
3355 [o] /ietf-keystore/certificates/certificate/csr-info
3356 [o] /ietf-keystore/certificates/certificate/certificate-signing-
3357 request
3358

3359 **6.4.9.2.4.2 Network configuration access control**

3360 IA-stations shall support the ietf-netconf-acm YANG module according to IETF RFC 8341 with
3361 the following nodes:

3362 [o] /ietf-netconf-acm/nacm/enable-nacm
3363 [o] /ietf-netconf-acm/nacm/read-default
3364 [o] /ietf-netconf-acm/nacm/write-default
3365 [o] /ietf-netconf-acm/nacm/exec-default
3366 [o] /ietf-netconf-acm/nacm/enable-external-groups
3367 [o] /ietf-netconf-acm/nacm/groups
3368 [o] /ietf-netconf-acm/nacm/rule-list
3369

3370 **6.4.9.2.4.3 A YANG data module for a truststore**

3371 IA-stations shall support the ietf-truststore YANG module according to draft-ietf-netconf-trust-
3372 anchors with the following features:

- 3373 • central-keystore-supported, and
3374 • certificates.

3375 IA-stations shall support the ietf-truststore YANG module according to draft-ietf-netconf-trust-
3376 anchors with the following nodes:

3377 [o] /ietf-truststore/truststore/certificate-bags/certificate-bag/name
3378 [o] /ietf-truststore/truststore/certificate-bags/certificate-
3379 bag/certificate/name
3380 [o] /ietf-truststore/truststore/certificate-bags/certificate-
3381 bag/certificate/cert-data
3382 [o] /ietf-truststore/truststore/certificate-bags/certificate-
3383 bag/certificate/expiration-date

3384

3385 **6.4.9.2.5 IA-station management**3386 **6.4.9.2.5.1 System capabilities**

3387 IA-stations shall support the ietf-system-capabilities and the ietf-notification-capabilities YANG
3388 modules according to IETF RFC 9196 with the following nodes:

3389 [m] /ietf-system-capabilities/system-capabilities/datastore-
3390 capabilities/datastore

3391 [m] /ietf-system-capabilities/system-capabilities/datastore-
3392 capabilities/per-node-capabilities

3393 [m] /ietf-system-capabilities/system-capabilities/datastore-
3394 capabilities/on-change-supported

3395

3396 **6.4.9.2.5.2 YANG library**

3397 IA-stations shall support the ietf-yang-library YANG module according to IETF RFC 8525 with
3398 the following nodes:

3399 [m] /ietf-yang-library/yang-library/module-set

3400 [m] /ietf-yang-library/yang-library/schema

3401 [m] /ietf-yang-library/yang-library/datastore

3402 [m] /ietf-yang-library/yang-library/content-id

3403

3404 **6.4.9.2.5.3 YANG push**

3405 IA-stations shall support the ietf-yang-push YANG module according to IETF RFC 8641, 4.1,
3406 with the on-change feature.

3407 IA-stations shall support the ietf-yang-push YANG module according to IETF RFC 8641, 4.1,
3408 with the following nodes:

3409 [o] /ietf-subscribed-notifications/filters/selection-filter

3410 [o] /ietf-subscribed-
3411 notifications/subscriptions/subscription/target/datastore

3412 [o] /ietf-subscribed-notifications/subscriptions/subscription/update-
3413 trigger

3414

3415 **6.4.9.2.5.4 YANG notification capabilities**

3416 IA-stations shall support the ietf-notification-capabilities YANG module according to IETF RFC
3417 9196 with the following nodes:

3418 [m] /ietf-notification-capabilities/system-capabilities/subscription-
3419 capabilities

3420 [m] /ietf-notification-capabilities/system-capabilities/datastore-
3421 capabilities/per-node-capabilities/subscription-capabilities

3422

3423

3424 6.4.9.2.5.5 YANG notifications

3425 IA-stations shall support the ietf-subscribed-notifications YANG module according to IETF RFC
3426 8639 with the following features:

- 3427 • Configured,
3428 • encode-xml, and
3429 • subtree.

3430 IA-stations shall support the ietf-subscribed-notifications YANG module according to IETF RFC
3431 8639 with the following nodes:

3432 [o] /ietf-subscribed-notifications/streams/stream/name
3433 [o] /ietf-subscribed-notifications/streams/stream/description
3434 [o] /ietf-subscribed-notifications/streams/stream/replay-support
3435 [o] /ietf-subscribed-notifications/streams/stream/replay-log-creation-
3436 time
3437 [o] /ietf-subscribed-notifications/streams/stream/replay-log-aged-time
3438 [o] /ietf-subscribed-notifications/filters/stream-filter/name
3439 [o] /ietf-subscribed-notifications/filters/stream-filter/filter-spec
3440 [o] /ietf-subscribed-notifications/subscriptions/subscription/id
3441 [o] /ietf-subscribed-notifications/subscriptions/subscription/target
3442 [o] /ietf-subscribed-notifications/subscriptions/subscription/stop-
3443 time
3444 [o] /ietf-subscribed-notifications/subscriptions/subscription/dscp
3445 [o] /ietf-subscribed-
3446 notifications/subscriptions/subscription/weighting
3447 [o] /ietf-subscribed-
3448 notifications/subscriptions/subscription/dependency
3449 [o] /ietf-subscribed-
3450 notifications/subscriptions/subscription/transport
3451 [o] /ietf-subscribed-notifications/subscriptions/subscription/encoding
3452 [o] /ietf-subscribed-notifications/subscriptions/subscription/purpose
3453 [o] /ietf-subscribed-
3454 notifications/subscriptions/subscription/notification-message-origin
3455 [o] /ietf-subscribed-
3456 notifications/subscriptions/subscription/configured-subscription-state
3457 [o] /ietf-subscribed-
3458 notifications/subscriptions/subscription/receivers

3459

3460 6.4.9.2.5.6 NETCONF monitoring

3461 IA-stations shall support the ietf-netconf-monitoring YANG module according to IETF RFC 6022
3462 with the following nodes:

3463 [m] /ietf-netconf-monitoring/netconf-state/capabilities

3464 [m] /ietf-netconf-monitoring/netconf-state/datastores

3465 [m] /ietf-netconf-monitoring/netconf-state/schemas

3466

3467

3468 **6.4.9.2.5.7 System management**

3469 IA-stations shall support the ietf-system YANG module according to IETF RFC 7317 with the
3470 following nodes:

3471 [o] /ietf-system/system/contact

3472 [o] /ietf-system/system/hostname

3473 [o] /ietf-system/system/location

3474

3475 **6.4.9.2.5.8 Hardware management**

3476 IA-stations shall support the ietf-hardware YANG module according to IETF RFC 8348 with the
3477 following nodes:

3478 [m] /ietf-hardware/hardware/component/name

3479 [m] /ietf-hardware/hardware/component/class

3480 [m] /ietf-hardware/hardware/component/description

3481 [m] /ietf-hardware/hardware/component/hardware-rev

3482 [m] /ietf-hardware/hardware/component/software-rev

3483 [o] /ietf-hardware/hardware/component/serial-num

3484 [m] /ietf-hardware/hardware/component/mfg-name

3485 [m] /ietf-hardware/hardware/component/model-name

3486 An IA-station shall provide exactly one /ietf-hardware/component with class “chassis” and may
3487 provide further components with other classes.

3488 **6.4.9.2.5.9 Interface management**

3489 IA-stations shall support the ietf-interfaces YANG module according to IETF RFC 8343 with the
3490 following nodes:

3491 [m] /ietf-interfaces/interfaces/interface/name

3492 [m] /ietf-interfaces/interfaces/interface/description

3493 [m] /ietf-interfaces/interfaces/interface/type

3494 [o] /ietf-interfaces/interfaces/interface/enabled

3495 [o] /ietf-interfaces/interfaces/interface/oper-status

3496 [o] /ietf-interfaces/interfaces/interface/phys-address

3497 [o] /ietf-interfaces/interfaces/interface/higher-layer-if

3498 [o] /ietf-interfaces/interfaces/interface/lower-layer-if

3499 [o] /ietf-interfaces/interfaces/interface/speed

3500 [o] /ietf-interfaces/interfaces/interface/statistics/discontinuity-
3501 time
3502 [o] /ietf-interfaces/interfaces/interface/statistics/in-octets
3503 [o] /ietf-interfaces/interfaces/interface/statistics/in-discards
3504 [o] /ietf-interfaces/interfaces/interface/statistics/in-errors
3505 [o] /ietf-interfaces/interfaces/interface/statistics/out-octets
3506 [o] /ietf-interfaces/interfaces/interface/statistics/out-discards
3507 [o] /ietf-interfaces/interfaces/interface/statistics/out-errors
3508
3509 **6.4.9.2.5.10 Bridge and end station component management**
3510 **6.4.9.2.5.10.1 General**

3511 IA-stations shall support the ieee802-dot1q-bridge YANG module according to
3512 IEEE Std 802.1Q-2022, Clause 48, as amended by IEEE Std 802.1Qcw-2023 with the following
3513 feature: ingress-filtering.

3514 IA-stations shall support the ieee802-dot1q-bridge YANG module according to
3515 IEEE Std 802.1Q-2022, Clause 48, as amended by IEEE Std 802.1Qcw-2023 with the following
3516 nodes. A distinction is made between nodes that shall be supported by bridge and end station
3517 components, or by bridge components only.

3518 **6.4.9.2.5.10.2 Bridge nodes to be supported by bridge and end station components**

3519 [m] /ieee802-dot1q-bridge/bridges/bridge/name
3520 [o] /ieee802-dot1q-bridge/bridges/bridge/address
3521 [m] /ieee802-dot1q-bridge/bridges/bridge/bridge-type
3522 [m] /ieee802-dot1q-bridge/bridges/bridge/ports
3523 [m] /ieee802-dot1q-bridge/bridges/bridge/components
3524 [m] /ieee802-dot1q-bridge/bridges/bridge/component/name
3525 [o] /ieee802-dot1q-bridge/bridges/bridge/component/id
3526 [m] /ieee802-dot1q-bridge/bridges/bridge/component/type
3527 [o] /ieee802-dot1q-bridge/bridges/bridge/component/traffic-class-
3528 enabled
3529 [m] /ieee802-dot1q-bridge/bridges/bridge/component/ports
3530 [o] /ieee802-dot1q-bridge/bridges/bridge/component/bridge-port
3531 [m] /ieee802-dot1q-bridge/bridges/bridge/component/capabilities
3532 [m] /ieee802-dot1q-bridge/bridges/bridge/component/filtering-
3533 database/size
3534 [o] /ieee802-dot1q-bridge/bridges/bridge/component/filtering-
3535 database/static-vlan-registration-entries
3536 [o] /ieee802-dot1q-bridge/bridges/bridge/component/filtering-
3537 database/vlan-registration-entry

3538 **6.4.9.2.5.10.3 Filtering-database nodes to be supported by bridge components**

3539 [o] /ieee802-dot1q-bridge/bridges/bridge/component/filtering-

3540 database/aging-time

3541 [o] /ieee802-dot1q-bridge/bridges/bridge/component/filtering-

3542 database/static-entries

3543 [o] /ieee802-dot1q-bridge/bridges/bridge/component/filtering-

3544 database/dynamic-entries

3545 [o] /ieee802-dot1q-bridge/bridges/bridge/component/filtering-

3546 database/dynamic-vlan-registration-entries

3547 [o] /ieee802-dot1q-bridge/bridges/bridge/component/filtering-

3548 database/mac-address-registration-entries

3549 [o] /ieee802-dot1q-bridge/bridges/bridge/component/filtering-

3550 database/filtering-entry

3551 **6.4.9.2.5.10.4 Permanent-database nodes to be supported by bridge components**

3552 [m] /ieee802-dot1q-bridge/bridges/bridge/component/permanent-

3553 database/size

3554 [o] /ieee802-dot1q-bridge/bridges/bridge/component/permanent-

3555 database/static-entries

3556 [o] /ieee802-dot1q-bridge/bridges/bridge/component/permanent-

3557 database/static-vlan-registration-entries

3558 [o] /ieee802-dot1q-bridge/bridges/bridge/component/permanent-

3559 database/filtering-entry

3560 **6.4.9.2.5.10.5 Bridge-vlan nodes to be supported by bridge and end station components**

3561 [m] /ieee802-dot1q-bridge/bridges/bridge/component/bridge-vlan/version

3562 [m] /ieee802-dot1q-bridge/bridges/bridge/component/bridge-vlan/max-

3563 vids

3564 [o] /ieee802-dot1q-bridge/bridges/bridge/component/bridge-

3565 vlan/override-default-pvid

3566 [o] /ieee802-dot1q-bridge/bridges/bridge/component/bridge-vlan/vlan

3567 **6.4.9.2.5.10.6 Bridge-vlan nodes to be supported by bridge components**

3568 [m] /ieee802-dot1q-bridge/bridges/bridge/component/bridge-vlan/max-

3569 msti

3570 [o] /ieee802-dot1q-bridge/bridges/bridge/component/bridge-vlan/vid-to-

3571 fid-allocation

3572 [o] /ieee802-dot1q-bridge/bridges/bridge/component/bridge-vlan/fid-to-

3573 vid-allocation

3574 [o] /ieee802-dot1q-bridge/bridges/bridge/component/bridge-vlan/vid-to-

3575 fid

3576 **6.4.9.2.5.10.7 Bridge-mst nodes to be supported by bridge components**

3577 [o] /ieee802-dot1q-bridge/bridges/bridge/component/bridge-mst

3578 **6.4.9.2.5.10.8 Bridge-port nodes to be supported by bridge and end station components**

3579 [m] /ietf-interfaces/interfaces/interface/bridge-port/bridge-name

3580 [m] /ietf-interfaces/interfaces/interface/bridge-port/component-name
3581 [m] /ietf-interfaces/interfaces/interface/bridge-port/port-type
3582 [o] /ietf-interfaces/interfaces/interface/bridge-port/pvid
3583 [o] /ietf-interfaces/interfaces/interface/bridge-port/default-priority
3584 [m] /ietf-interfaces/interfaces/interface/bridge-port/traffic-class
3585 [o] /ietf-interfaces/interfaces/interface/bridge-port/statistics
3586 [m] /ietf-interfaces/interfaces/interface/bridge-port/capabilities
3587 [m] /ietf-interfaces/interfaces/interface/bridge-port/type-capabilities
3588 [o] /ietf-interfaces/interfaces/interface/bridge-port/transmission-
3589 selection-algorithm-table

6.4.9.2.5.10.9 Bridge-port nodes to be supported by bridge component ports

3590 [o] /ietf-interfaces/interfaces/interface/bridge-port/priority-
3592 regeneration
3593 [o] /ietf-interfaces/interfaces/interface/bridge-port/acceptable-frame
3594 [o] /ietf-interfaces/interfaces/interface/bridge-port/enable-ingress-
3595 filtering
3596 [o] /ietf-interfaces/interfaces/interface/bridge-port/enable-vid-
3597 translation-table
3598 [o] /ietf-interfaces/interfaces/interface/bridge-port/vid-translations
3599 [o] /ietf-interfaces/interfaces/interface/bridge-port/enable-egress-
3600 vid-translation-table
3601 [o] /ietf-interfaces/interfaces/interface/bridge-port/egress-vid-
3602 translations
3603

6.4.9.2.5.11 IEC/IEEE 60802 YANG modules

3605 IA-stations shall support the iecieee60802-ethernet-interface YANG module according to this
3606 document with the following nodes:

3607 [m] /iecieee60802-ethernet-
3608 interface/interfaces/interface/ethernet/supported-mau-types/mau-type
3609 [m] /iecieee60802-ethernet-
3610 interface/interfaces/interface/ethernet/supported-mau-
3611 types/preemption-supported

3612

3613 IA-stations shall support the iecieee60802-bridge YANG module according to this document
3614 with the following nodes:

3615 [m] /iecieee60802-bridge/interfaces/interface/bridge-port/max-burst-
3616 params
3617 [m] /iecieee60802-bridge/interfaces/interface/bridge-port/committed-
3618 data-rates
3619 [m] /iecieee60802-bridge/interfaces/interface/bridge-
3620 port/transmission-selection-algorithm

3621 [m] /iecieee60802/interfaces/interface/bridge-port/supported-resource-
3622 pools

3623 [m] /iecieee60802-bridge/bridges/bridge/component/frer-supported

3624 [m] /iecieee60802-bridge/bridges/bridge/component/max-redundant-
3625 streams

3626 [m] /iecieee60802-bridge/bridges/bridge/component/max-fids

3627 [m] /iecieee60802-bridge/bridges/bridge/component/max-fdb-entries

3628 [m] /iecieee60802-bridge/bridges/bridge/component/delay-variance

3629 [m] /iecieee60802-bridge/bridges/bridge/component/max-ptp-instances

3630 [m] /iecieee60802-bridge/bridges/bridge/component/max-hot-standby-
3631 systems

3632 [m] /iecieee60802-bridge/bridges/bridge/component/clock

3633 IA-stations shall support the iecieee60802-ia-station YANG module according to this document
3634 with the following nodes:

3635 [m] /iecieee60802-ia-station/ia-station-capabilities/capability-lldp

3636 [m] /iecieee60802-ia-station/ia-station-capabilities/capability-timesync

3637 [m] /iecieee60802-ia-station/ia-station-capabilities/capability-keystore

3638 [m] /iecieee60802-ia-station/ia-station-capabilities/capability-truststore

3639 [m] /iecieee60802-ia-station/ia-station-capabilities/capability-nacm

3640 [m] /iecieee60802-ia-station/ia-station-capabilities/capability-yang-library

3641 [m] /iecieee60802-ia-station/ia-station-capabilities/capability-yang-push

3642 [m] /iecieee60802-ia-station/ia-station-capabilities/capability-yang-
3643 notifications

3644 [m] /iecieee60802-ia-station/ia-station-capabilities/capability-netconf-
3645 monitoring

3646 [m] /iecieee60802-ia-station/ia-station-capabilities/capability-netconf-
3647 client

3648 [m] /iecieee60802-ia-station/ia-station-capabilities/capability-tsn-uni

3649 [m] /iecieee60802-ia-station/ia-station-capabilities/capability-sched-
3650 traffic

3651 [m] /iecieee60802-ia-station/ia-station-capabilities/capability-frame-
3652 preemption

3653

3654 **6.4.9.2.5.12 NETCONF server**

3655 IA-stations shall support the ietf-netconf-server YANG module according to draft-ietf-netconf-
3656 netconf-client-server, 3.1.1, with the following features:

3657 • tls-call-home, and

3658 • central-netconf-server-supported.

3659 IA-stations shall support the ietf-netconf-server YANG module according to draft-ietf-netconf-
3660 netconf-client-server, 3.3, with the following nodes:

3661 [o] /ietf-netconf-server/netconf-server/listen/idle-timeout
3662 [o] /ietf-netconf-server/netconf-server/listen/endpoint/name
3663 [o] /ietf-netconf-server/netconf-
3664 server/listen/endpoint/transport/tls/netconf-server-parameters
3665 [o] /ietf-netconf-server/netconf-
3666 server/listen/endpoint/transport/tls/tls-server-parameters
3667 [o] /ietf-netconf-server/netconf-server/call-home/netconf-client/name
3668 [o] /ietf-netconf-server/netconf-server/call-home/netconf-
3669 client/endpoints/endpoint/name
3670 [o] /ietf-netconf-server/netconf-server/call-home/netconf-
3671 client/endpoints/endpoint/transport/tls/netconf-server-parameters
3672 [o] /ietf-netconf-server/netconf-server/call-home/netconf-
3673 client/endpoints/endpoint/transport/tls/tls-server-parameters

3674

3675

3676 **6.4.9.2.5.13 Subscribed Notifications**

3677 IA-stations shall support the ietf-subscribed-notifications YANG module according to RFC 8639
3678 with the following nodes:

3679 [o] /ietf-subscribed-notifications/streams/stream/name
3680 [o] /ietf-subscribed-notifications/streams/stream/description
3681 [o] /ietf-subscribed-notifications/filters/stream-filter/name
3682 [o] /ietf-subscribed-notifications/filters/stream-filter/filter-spec
3683 [o] /ietf-subscribed-notifications/subscriptions/subscription/id
3684 [o] /ietf-subscribed-notifications/subscriptions/subscription/target
3685 [o] /ietf-subscribed-
3686 notifications/subscriptions/subscription/receivers

3687

3688 IA-stations shall support the iecieee60802-subscribed-notifications YANG module according to
3689 this document with the following nodes:

3690 [m] /iecieee60802-subscribed-notifications/subscriptions/max-
3691 subscriptions
3692 [m] /iecieee60802-subscribed-notifications/subscriptions/max-on-
3693 change-subscription-leaves
3694 [m] /iecieee60802-subscribed-notifications/subscriptions/max-periodic-
3695 subscription-leaves
3696 [m] /iecieee60802-subscribed-notifications/subscriptions/max-periodic-
3697 subscription-interval

3698

3699 6.4.9.2.5.14 Flow Meter Management

3700 IA-stations which incorporate a bridge component shall support the ieee802-dot1q-stream-
3701 filters-gates YANG module according to IEEE Std 802.1Qcz-2023 as amended by IEEE Std
3702 802.1Qcw-2023 with the following nodes:

3703 [o] /ieee802-dot1q-bridge/bridges/bridge/component/stream-
3704 filters/stream-filter-instance-table/stream-filter-instance-id

3705 [o] /ieee802-dot1q-bridge/bridges/bridge/component/stream-
3706 filters/stream-filter-instance-table/stream-handle

3707 [o] /ieee802-dot1q-bridge/bridges/bridge/component/stream-
3708 filters/stream-filter-instance-table/flow-meter-ref

3709 [o] /ieee802-dot1q-bridge/bridges/bridge/component/stream-
3710 filters/stream-filter-instance-table/flow-meter-enable

3711 [m] /ieee802-dot1q-bridge/bridges/bridge/component/stream-filters/max-
3712 stream-filter-instances

3713 IA-stations which incorporate a bridge component shall support the ieee802-dot1cb-stream-
3714 identification YANG module according to IEEE Std 802.1CBcv-2021 as amended by IEEE Std
3715 802.1CBdb-2021 with the following nodes:

3716 [o] /ieee802-dot1cb-stream-identification/stream-identity/index
3717 [o] /ieee802-dot1cb-stream-identification/stream-identity/handle
3718 [o] /ieee802-dot1cb-stream-identification/stream-identity/out-
3719 facing/input-port

3720 [o] /ieee802-dot1cb-stream-identification/stream-
3721 identity/parameters/mask-and-match-stream-identification/destination-
3722 mac-mask

3723 [o] /ieee802-dot1cb-stream-identification/stream-
3724 identity/parameters/mask-and-match-stream-identification/destination-
3725 mac-match

3726 NOTE For example, an implementation could contain per out-facing/input-port one mask and match stream
3727 identification for broadcast traffic, one mask and match stream identification for multicast traffic and one mask and
3728 match stream identification for unicast traffic.

3729 IA-stations which incorporate a bridge component shall support the ieee802-dot1q-psfp-bridge
3730 YANG module according to IEEE Std 802.1Qcw-2023 with the following nodes:

3731 [o] /ieee802-dot1q-psfp-bridge/bridges/bridge/component/flow-
3732 meters/flow-meter-instance-table/flow-meter-instance-id

3733 [o] /ieee802-dot1q-psfp-bridge/bridges/bridge/component/flow-
3734 meters/flow-meter-instance-table/committed-information-rate

3735 [o] /ieee802-dot1q-psfp-bridge/bridges/bridge/component/flow-
3736 meters/flow-meter-instance-table/committed-burst-size

3737 [o] /ieee802-dot1q-psfp-bridge/bridges/bridge/component/flow-
3738 meters/flow-meter-instance-table/excess-information-rate

3739 [o] /ieee802-dot1q-psfp-bridge/bridges/bridge/component/flow-
3740 meters/flow-meter-instance-table/excess-burst-size

3741 [o] /ieee802-dot1q-psfp-bridge/bridges/bridge/component/flow-
3742 meters/flow-meter-instance-table/coupling-flag

3743 [o] /ieee802-dot1q-psfp-bridge/bridges/bridge/component/flow-
3744 meters/flow-meter-instance-table/color-mode

3745 [o] /ieee802-dot1q-psfp-bridge/bridges/bridge/component/flow-
3746 meters/flow-meter-instance-table/drop-on-yellow

3747 [m] /ieee802-dot1q-psfp-bridge/bridges/bridge/component/flow-
3748 meters/max-flow-meter-instances

3749

3750 **6.4.9.3 Optional YANG data models, features, and nodes**

3751 **6.4.9.3.1 General**

3752 The following YANG modules, features and nodes shall be supported by IA-stations if the
3753 functionality they describe is included.

3754 **6.4.9.3.2 Scheduled traffic**

3755 IA-stations supporting the enhancements for scheduled traffic shall support the ieee802-dot1q-
3756 sched-bridge YANG module according to IEEE Std 802.1Qcw-2023 with the following feature:
3757 scheduled-traffic.

3758 IA-stations supporting the enhancements for scheduled traffic shall support the ieee802-dot1q-
3759 sched-bridge YANG module according to IEEE Std 802.1Qcw-2023 with the following nodes:

3760 [o] ieee802-dot1q-sched-bridge/interfaces/interface/bridge-port/gate-
3761 parameter-table/queue-max-sdu-table

3762 [o] ieee802-dot1q-sched-bridge/interfaces/interface/bridge-port/gate-
3763 parameter-table/gate-enabled

3764 [o] ieee802-dot1q-sched-bridge/interfaces/interface/bridge-port/gate-
3765 parameter-table/admin-gate-states

3766 [o] ieee802-dot1q-sched-bridge/interfaces/interface/bridge-port/gate-
3767 parameter-table/oper-gate-states

3768 [o] ieee802-dot1q-sched-bridge/interfaces/interface/bridge-port/gate-
3769 parameter-table/admin-control-list

3770 [o] ieee802-dot1q-sched-bridge/interfaces/interface/bridge-port/gate-
3771 parameter-table/oper-control-list

3772 [o] ieee802-dot1q-sched-bridge/interfaces/interface/bridge-port/gate-
3773 parameter-table/admin-cycle-time

3774 [o] ieee802-dot1q-sched-bridge/interfaces/interface/bridge-port/gate-
3775 parameter-table/oper-cycle-time

3776 [o] ieee802-dot1q-sched-bridge/interfaces/interface/bridge-port/gate-
3777 parameter-table/admin-cycle-time-extension

3778 [o] ieee802-dot1q-sched-bridge/interfaces/interface/bridge-port/gate-
3779 parameter-table/oper-cycle-time-extension

3780 [o] ieee802-dot1q-sched-bridge/interfaces/interface/bridge-port/gate-
3781 parameter-table/admin-base-time

3782 [o] ieee802-dot1q-sched-bridge/interfaces/interface/bridge-port/gate-
3783 parameter-table/oper-base-time

3784 [o] ieee802-dot1q-sched-bridge/interfaces/interface/bridge-port/gate-
3785 parameter-table/config-change

3786 [o] ieee802-dot1q-sched-bridge/interfaces/interface/bridge-port/gate-
3787 parameter-table/config-change-time

3788 [o] ieee802-dot1q-sched-bridge/interfaces/interface/bridge-port/gate-
3789 parameter-table/tick-granularity

3790 [o] ieee802-dot1q-sched-bridge/interfaces/interface/bridge-port/gate-
3791 parameter-table/current-time

3792 [o] ieee802-dot1q-sched-bridge/interfaces/interface/bridge-port/gate-
3793 parameter-table/config-pending

3794 [o] ieee802-dot1q-sched-bridge/interfaces/interface/bridge-port/gate-
3795 parameter-table/config-change-error

3796 [c] ieee802-dot1q-sched-bridge/interfaces/interface/bridge-port/gate-
3797 parameter-table/supported-list-max

3798 [c] ieee802-dot1q-sched-bridge/interfaces/interface/bridge-port/gate-
3799 parameter-table/supported-cycle-max

3800 [c] ieee802-dot1q-sched-bridge/interfaces/interface/bridge-port/gate-
3801 parameter-table/supported-interval-max

3802

3803 **6.4.9.3.3 IEC/IEEE 60802 YANG modules**

3804 IA-stations that support enhancements for scheduled traffic shall support the iecieee60802-
3805 sched-bridge YANG module according to this document with the following nodes:

3806 [c] /iecieee60802-sched-bridge/interfaces/interface/bridge-port/gate-
3807 parameter-table/min-gating-times

3808

3809 **6.4.9.3.4 Frame preemption**

3810 IA-stations supporting frame preemption according to IEEE Std 802.1Q-2022, 5.4.1 ae), shall
3811 support the ieee802-dot1q-preemption-bridge YANG module according to IEEE Std 802.1Qcw-
3812 2023 with the following feature: frame-preemption.

3813

3814 IA-stations supporting frame preemption according to IEEE Std 802.1Q-2022, 5.4.1 ae), shall
3815 support the ieee802-dot1q-preemption-bridge YANG module according to IEEE Std 802.1Qcw-
3816 2023 with the following nodes:

3817 [o] ieee802-dot1q-preemption-bridge/interfaces/interface/bridge-
3818 port/frame-preemption-parameters/frame-preemption-status-table

3819 [o] ieee802-dot1q-preemption-bridge/interfaces/interface/bridge-
3820 port/frame-preemption-parameters/preemption-active

3821

3822 **6.4.9.3.5 Credit-based shaper**

3823 IA-stations supporting the credit-based shaper according to IEEE Std 8021.Q-2022, 8.6.8.2,
3824 shall support the <ieee-cbs> YANG module according to IEEE Draft Std P802.1Qdx.

3825

3826 **6.4.9.3.6 FRER**

3827 IA-stations supporting FRER according to 5.10.1 item b) or item c), shall support the ieee802-
 3828 dot1cb-stream-identification and ieee802-dot1cb-frer YANG modules according to IEEE Std
 3829 802.1CBcv-2021 with the following nodes:

```

 3830 [o] /ieee802-dot1cb-stream-identification/stream-identity/index
 3831 [o] /ieee802-dot1cb-stream-identification/stream-identity/handle
 3832 [o] /ieee802-dot1cb-stream-identification /stream-identity/out-
 3833 facing/input-port
 3834 [o] /ieee802-dot1cb-stream-identification /stream-identity/out-
 3835 facing/output-port
 3836 [o] /ieee802-dot1cb-stream-identification /stream-
 3837 identity/parameters/null-stream-identification
 3838 [o] /ieee802-dot1cb-frer/frer/sequence-generation/index
 3839 [o] /ieee802-dot1cb-frer/frer/sequence-generation/stream
 3840 [o] /ieee802-dot1cb-frer/frer/sequence-generation/direction-out-facing
 3841 [o] /ieee802-dot1cb-frer/frer/sequence-recovery/index
 3842 [o] /ieee802-dot1cb-frer/frer/sequence-recovery/stream
 3843 [o] /ieee802-dot1cb-frer/frer/sequence-recovery/port
 3844 [o] /ieee802-dot1cb-frer/frer/sequence-recovery/direction-out-facing
 3845 [o] /ieee802-dot1cb-frer/frer/sequence-recovery/algorithm/vector
 3846 [o] /ieee802-dot1cb-frer/frer/sequence-identification/port
 3847 [o] /ieee802-dot1cb-frer/frer/sequence-identification/direction-out-
 3848 facing
 3849 [o] /ieee802-dot1cb-frer/frer/sequence-identification/stream
 3850 [o] /ieee802-dot1cb-frer/frer/sequence-identification/encapsulation/r-
 3851 tag
 3852 [o] /ieee802-dot1cb-frer/frer/stream-split

```

3853 **6.4.9.4 CUC/CNC YANG**3854 **6.4.9.4.1 NETCONF Client**

3855 IA-stations with CNC and/or CUC functionality shall support the ietf-netconf-client YANG
 3856 module according to draft-ietf-netconf-netconf-client-server, 2.1.1, with the following features:

- 3857 • tls-initiate,
- 3858 • tls-listen, and
- 3859 • central-netconf-client-supported.

3860

3861 **6.4.9.4.2 YANG Module for TSN UNI**

3862 IA-stations with CNC and/or CUC functionality shall support the ieee802-dot1q-tsn-config-uni
 3863 YANG module according to IEEE Draft Std P802.1Qdj with the node: [o] /ieee802-dot1q-
 3864 tsn-config/tsn-uni.

3865

3866 **6.4.10 YANG Data Model**3867 **6.4.10.1 General**

3868 Subclause 6.4.10 specifies the YANG data model for IA-stations. YANG (IETF RFC 7950) is a
3869 data modeling language used to model configuration data and state data for remote network
3870 management protocols. The selected YANG-based remote network management protocol is
3871 NETCONF (IETF RFC 6241). A YANG module specifies the organization and rules for the
3872 management data, and a mapping from YANG to the specific encoding enables the data to be
3873 understood correctly by both client (e.g., network manager) and server (e.g., IA-stations).

3874 **6.4.10.2 YANG framework**

3875 The core of the YANG module for IEC/IEEE 60802 IA-stations consists of YANG “augment”
3876 statements, used to add members to the tree of existing YANG modules plus one new module
3877 for IEC/IEEE 60802 specific objects.

3878 **6.4.10.3 IEC/IEEE 60802 Specific Managed Objects**3879 **6.4.10.3.1 General**

3880 Subclause 6.4.10.3 defines the set of managed objects, and their functionality, that provides
3881 additional information about an IA-station that is required by a CNC to calculate network
3882 configurations.

3883 IEC/IEEE 60802 specific managed objects are specified:

- 3884 • per Ethernet interface, i.e., external port, in 6.4.10.3.2,
- 3885 • per end station component internal or external port in 6.4.10.3.3 and 6.4.10.3.4,
- 3886 • per bridge component internal or external port in 6.4.10.3.4,
- 3887 • per end station component in 6.4.10.3.5 and 6.4.10.3.7,
- 3888 • per bridge component in 6.4.10.3.6 and 6.4.10.3.7, and
- 3889 • per IA-station in 6.4.10.3.8.

3890 IEC/IEEE 60802 specific managed objects for CNC entities are specified in 6.4.10.3.9.

3891

3892 **6.4.10.3.2 IEC/IEEE 60802 managed objects per Ethernet interface**3893 **6.4.10.3.2.1 supportedMauTypes**

3894 The list of supported MAU Types including the data:

3895 a) mauType

3896 The value is the supported MAU Type derived from the list position of the corresponding
3897 dot3MauType as listed in IETF RFC 4836, Clause 5.

3898 b) preemptionSupported

3899 The Boolean value indicates if preemption is supported by the MAU Type.

3900 NOTE The operational MAU Type of an Ethernet interface is provided as leaf operational-mau-type of the ieee802-
3901 ethernet-lldp YANG module. The operational MAU Type is included in the supportedMauTypes list.

3902

3903 **6.4.10.3.3 IEC/IEEE 60802 managed objects per end station component port**3904 **6.4.10.3.3.1 worstCasePacketGap**

3905 The value is the worst case maximum inter-packet gap between consecutive frames in a traffic
3906 burst expressed in bit-times.

3907 NOTE Minimum interPacketGap is defined in IEEE Std 802.3-2022, 1.4.362. The worst-case-packet-gap will never
3908 be less than the minimum interPacketGap.

6.4.10.3.3.2 maxBurstFrames

The value is the maximum number of frames that can be sent with minimal inter packet gap.

6.4.10.3.3.3 maxBurstBytes

The value is the maximum number of octets that can be sent with minimal inter packet gap.

6.4.10.3.3.4 committedDataRates

The list of committed data rates per traffic class and supported line speed including the data:

a) committedInformationRate

The value is the bandwidth limit in kbit/s.

b) committedBurstSize

The value is the burst size limit in octets.

6.4.10.3.4 IEC/IEEE 60802 managed objects per bridge or end station component port**6.4.10.3.4.1 transmissionSelectionAlgorithm**

The list of supported transmission selection algorithms according to IEEE Std 802.1Q-2022 8.6.8 per traffic class.

6.4.10.3.4.2 supportedResourcePools

The list of supported buffer resource pools including the data:

a) resourcePoolName

The value is the name of a resource pool.

b) coveredTimeInterval

The value specifies the covered buffering time given as rational number of seconds for the highest supported link speed.

c) resourcePoolTrafficClasses

The list of the traffic classes to be served by the resource pool.

6.4.10.3.4.3 minGatingTimes

The list of minimum gating times per supported line speed including the data:

a) minCycleTime

The value is the minimum value supported by this port of the AdminCycleTime and OperCycleTime parameters given as rational number of seconds.

b) minIntervalTime

The value is the minimum value supported by this port of the TimeIntervalValue parameter in nanoseconds.

6.4.10.3.5 IEC/IEEE 60802 managed objects per end station component.**6.4.10.3.5.1 frerSupported**

The value indicates if FRER is supported.

6.4.10.3.5.2 maxRedundantStreams

The value is the maximum number of supported redundant streams.

6.4.10.3.6 IEC/IEEE 60802 managed objects per bridge component.**6.4.10.3.6.1 delayVariance**

The value indicates variance in delay depending upon the use of a singleValue or multipleValues (see 6.4.10.3.6.2).

3949 **6.4.10.3.6.2 delayTimes**

3950 The list of minimum and maximum frame length independent and frame length dependent delay
3951 time values of frames as they pass through a bridge component. These values are given:

- 3952 • per supported MAU Type pair and traffic class, if delayVariance is singleValue, or
3953 • per port pair with supported MAU Types and traffic class, if delayVariance is multipleValues.

3954 The list includes the data:

- 3955 a) independentDelayMin

3956 The value is the minimum delay portion that is independent of frame length according to IEEE
3957 Std 802.1Q-2022, 12.32.1.1.

- 3958 b) independentDelayMax

3959 The value is the maximum delay portion that is independent of frame length according to IEEE
3960 Std 802.1Q-2022, 12.32.1.1.

- 3961 c) dependentDelayMin

3962 The value is the minimum delay portion that is dependent on frame length according to IEEE
3963 Std 802.1Q-2022, 12.32.1.2.

- 3964 d) dependentDelayMax

3965 The value is the maximum delay portion that is dependent on frame length according to IEEE
3966 Std 802.1Q-2022, 12.32.1.2.

3967 **6.4.10.3.7 IEC/IEEE 60802 managed objects per bridge or end station component**

3968 **6.4.10.3.7.1 maxFids**

3969 The value is the maximum number of supported FIDs.

3970 **6.4.10.3.7.2 maxFdbEntries**

3971 The list of the maximum number of static (6.4.10.3.7.3) and dynamic (6.4.10.3.7.4) FDB entries
3972 per FDB.

3973 **6.4.10.3.7.3 maxStaticFdbEntries**

3974 The value is the maximum number of static FDB entries.

3975 **6.4.10.3.7.4 maxDynamicFdbEntries**

3976 The value is the maximum number of dynamic FDB entries.

3977 **6.4.10.3.7.5 maxPtpInstances**

3978 The value is the maximum number of supported PTP Instances.

3979 **6.4.10.3.7.6 maxHotStandbySystems**

3980 The value is the maximum number of supported HotStandbySystem entities (see IEEE Draft
3981 Std P802.1ASdm).

3982 **6.4.10.3.7.7 clockList**

3983 The list of supported application clock entities including the data:

- 3984 a) clockIdentity

3985 The clock identity of the application clock.

- 3986 b) clockTarget

3987 The Boolean value indicates if the application clock is a clock target (TRUE) or clock source
3988 (FALSE).

- 3989 c) arbSupported

- 3990 The Boolean value indicates if the application clock supports the ARB timescale.
- 3991 d) **ptpSupported**
- 3992 The Boolean value indicates if the application clock supports the PTP timescale.
- 3993 e) **hotStandbySupported**
- 3994 The Boolean value indicates if the application clock supports hot standby.
- 3995 f) **attachedPtInstance**
- 3996 The value is a reference to the PTP or hot standby Instance, that is attached to the application
3997 clock.
- 3998 g) **isSynced**
- 3999 The Boolean value indicates if the application clock is either synchronized to the attached PTP
4000 Instance (TRUE) or to an internal/external ClockSource (FALSE).
- 4001 **6.4.10.3.8 IEC/IEEE 60802 managed objects per IA-station**
- 4002 **6.4.10.3.8.1 maxSubscriptions**
- 4003 The value is the maximum number of supported NETCONF Server subscriptions.
- 4004 **6.4.10.3.8.2 maxOnChangeSubscriptionLeaves**
- 4005 The value is the maximum number of supported leaves for NETCONF Server on-change
4006 subscriptions according to IETF RFC 8641.
- 4007 **6.4.10.3.8.3 maxPeriodicSubscriptionLeaves**
- 4008 The value is the maximum number of supported leaves for NETCONF Server periodic
4009 subscriptions according to IETF RFC 8641.
- 4010 **6.4.10.3.8.4 minPeriodicSubscriptionInterval**
- 4011 The value is the minimum periodic subscription interval in centiseconds (0.01 seconds) for
4012 NETCONF Server periodic subscriptions according to IETF RFC 8641.
- 4013 **6.4.10.3.8.5 capabilityLLDP**
- 4014 This Boolean value indicates if LLDP is supported.
- 4015 **6.4.10.3.8.6 capabilityTimesync**
- 4016 This Boolean value indicates if Timesync is supported.
- 4017 **6.4.10.3.8.7 capabilityKeystore**
- 4018 This Boolean value indicates if Keystore is supported.
- 4019 **6.4.10.3.8.8 capabilityNACM**
- 4020 This Boolean value indicates if NACM is supported.
- 4021 **6.4.10.3.8.9 capabilityTruststore**
- 4022 This Boolean value indicates if Truststore is supported.
- 4023 **6.4.10.3.8.10 capabilityYangLibrary**
- 4024 This Boolean value indicates if YANG library is supported.
- 4025 **6.4.10.3.8.11 capabilityYangPush**
- 4026 This Boolean value indicates if Yang Push is supported.
- 4027 **6.4.10.3.8.12 capabilityYangNotifications**
- 4028 This Boolean value indicates if YANG notifications is supported.

4029 **6.4.10.3.8.13 capabilityNetconfMonitoring**

4030 This Boolean value indicates if NETCONF Monitoring is supported.

4031 **6.4.10.3.8.14 capabilityNetconfClient**

4032 This Boolean value indicates if NETCONF client is supported.

4033 **6.4.10.3.8.15 capabilityTsnUni**

4034 This Boolean value indicates if TSN UNI is supported.

4035 **6.4.10.3.8.16 capabilitySchedTraffic**

4036 This Boolean value indicates if scheduled traffic is supported.

4037 **6.4.10.3.8.17 capabilityFramePreemption**

4038 This Boolean value indicates if frame preemption is supported.

4039 **6.4.10.3.9 IEC/IEEE 60802 managed objects for CNC entities**

4040 **6.4.10.3.9.1 maxConfigurationDomains**

4041 The value is the maximum number of supported Configuration Domains.

4042 **6.4.10.3.9.2 maxCUCs**

4043 The value is the maximum number of supported CUC entities.

4044 **6.4.10.3.9.3 maxIAstations**

4045 The value is the maximum number of supported IA-stations.

4046 **6.4.10.3.9.4 maxNetworkDiameter**

4047 The value is the maximum supported network diameter.

4048 **6.4.10.3.9.5 maxStreams**

4049 The value is the maximum number of supported streams.

4050 **6.4.10.3.9.6 maxNumSeamlessTrees**

4051 The value is the maximum number of trees supported for seamless redundancy of a stream.

4052 **6.4.10.3.9.7 hotStandbySupported**

4053 The Boolean value indicates if hot standby is supported.

4054

4055 **6.4.10.4 RPCs and actions specific to this document**

4056 **6.4.10.4.1 RPC ia-factory-reset**

4057 **6.4.10.4.1.1 General**

4058 In contrast to the original factory-reset RPC in IETF RFC 8808, this RPC puts the device into a state where a subsequent configuration by a CNC component results in a functioning IA-station according to this document. Depending on the factory default configuration, after being reset, the device may become unreachable on the network.

4062 **6.4.10.4.1.2 Input**

4063 None.

4064 **6.4.10.4.1.3 Output**

4065 None.

4066 **6.4.10.4.2 Action add-streams**4067 **6.4.10.4.2.1 General**

4068 This Action requests a CNC to add a list of streams.

4069 **6.4.10.4.2.2 Input**

- 4070 a) CuId - The ID of the CUC for which the streams are to be added.
- 4071 b) StreamId - The Stream ID is a unique identifier of a Stream request and corresponding
4072 configuration.
- 4073 c) Container Talker - The Talker container contains:
 - 4074 – Talker's behavior for Stream (how/when transmitted),
 - 4075 – Talker's requirements from the network, and
 - 4076 – TSN capabilities of the Talker's interface(s).
- 4077 d) List Listener - Each Listener list entry contains:
 - 4078 – Listener's requirements from the network, and
 - 4079 – TSN capabilities of the Listener's interface(s).

4080 **6.4.10.4.2.3 Output**

4081 Result - Status information indicating if Stream addition has been successful.

4082 **6.4.10.4.3 Action remove-listener**4083 **6.4.10.4.3.1 General**

4084 This Action removes listeners from a stream.

4085 **6.4.10.4.3.2 Input**

4086 List Listener - A list of indices of listeners to be removed from a stream.

4087 **6.4.10.4.3.3 Output**

4088 Result - Status information indicating if Stream addition has been successful.

4089 **6.4.10.5 IEC/IEEE 60802 YANG data models**

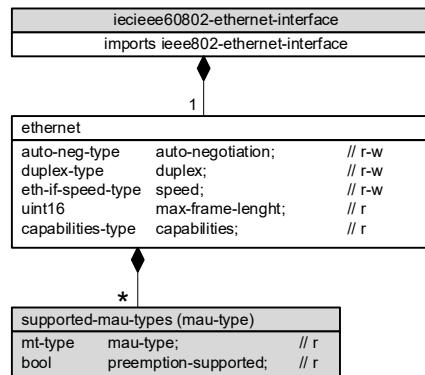
4090 A UML® representation is used to provide an overview of the hierarchy of the IEC/IEEE 60802
4091 YANG data model.

4092 A UML-like representation of the management model is provided in Figure 30 through Figure 34.
4093 The purpose of a UML-like diagram is to express the model design in a concise manner. The
4094 structure of the UML-like representation shows the name of the object followed by a list of
4095 properties for the object. The properties indicate their type and accessibility. It should be noted
4096 that UML-like representation is meant to express simplified semantics for the properties. It is
4097 not meant to provide the specific datatype used to encode the object in either MIB or YANG.

4098 NOTE OMG® UML® 2.5 conventions together with C++ language constructs are used as a representation to convey
4099 model structure and relationships.

4100 For all UML® figures, data that is imported from original modules is shown in white, and data
4101 in augment of IEC/IEEE 60802 is shown in grey.

4102 Figure 30 through Figure 35 provide an overview of the IEC/IEEE 60802 augmentations.

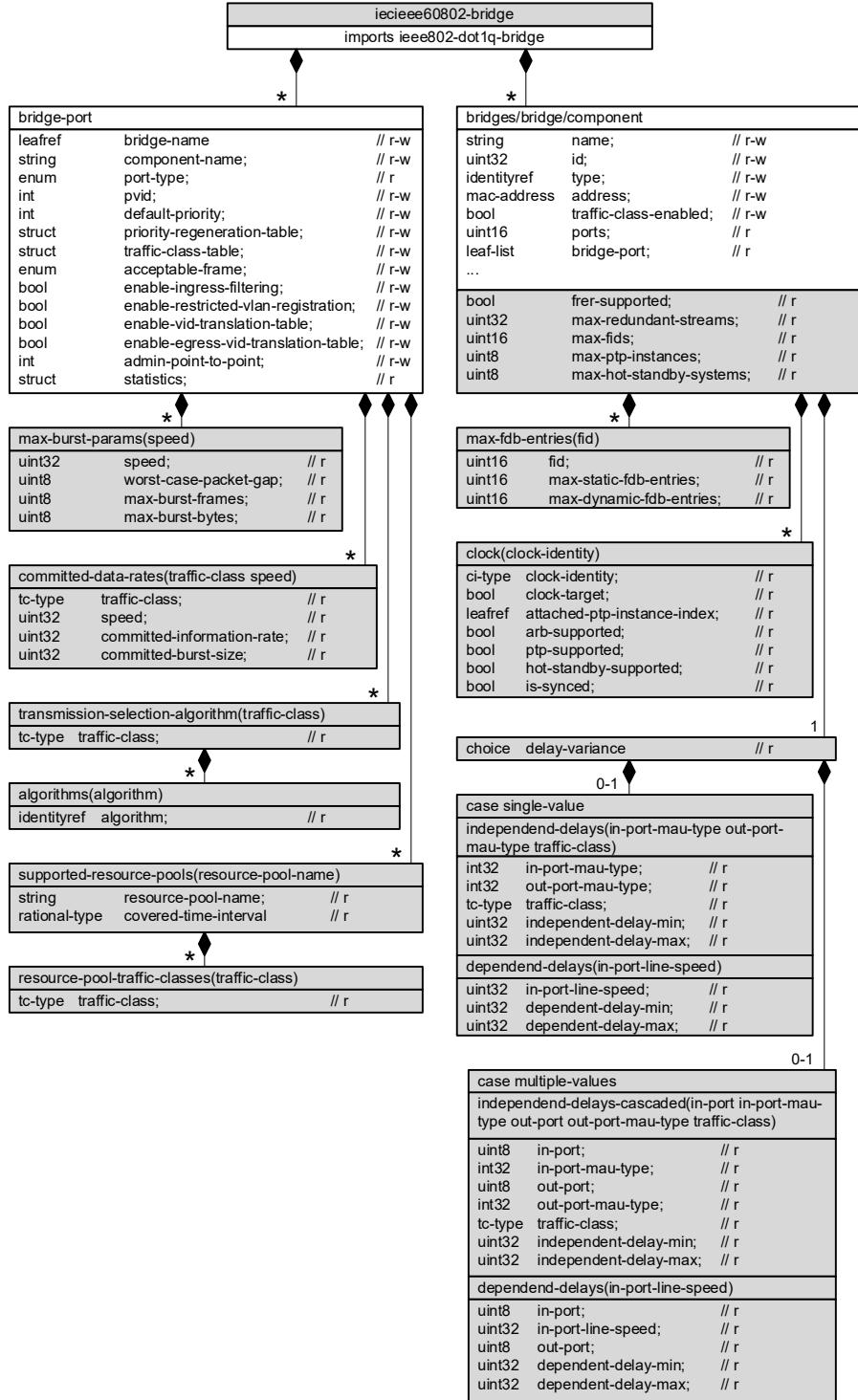


4103

4104

4105

Figure 30 – Module iecieee60802-ethernet-interface

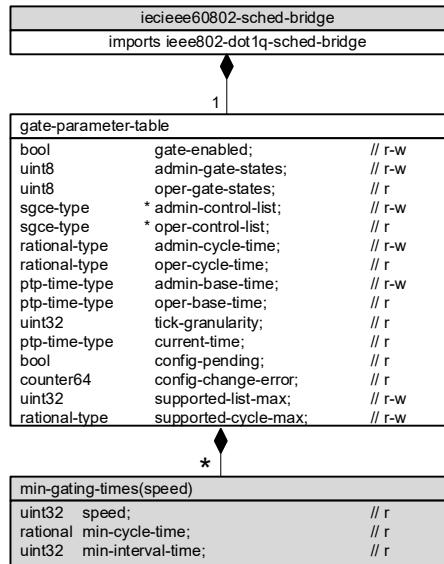


4106

4107

4108

Figure 31 – Module `iecieee60802-bridge`



4109

4110

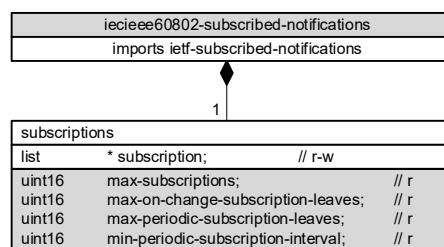
Figure 32 – Module iecieee60802-dot1-sched-bridge

4111

4112

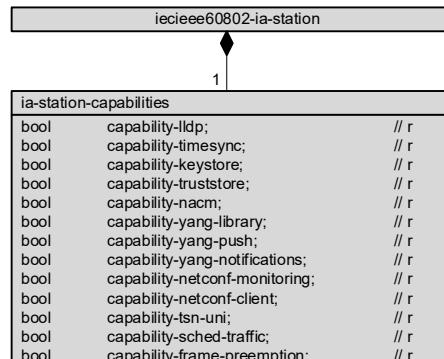
4113

4114



4115

4116

Figure 33 – Module iecieee60802-subscribed-notifications**Figure 34 – Module iecieee60802-ia-station**

iecieee60802-tsn-config-uni		
imports ieee802-dot1q-tsn-config-uni		
1		
tsn-uni		
list	domain;	// r-w
uint8	max-config-domains;	// r
uint8	max-cucs;	// r
uint16	max-ia-stations;	// r
uint8	max-network-diameter;	// r
uint16	max-streams;	// r
uint8	max-num-seamless-trees;	// r
uint8	hot-standby-supported;	// r

4117

4118

Figure 35 – Module iecieee60802-tsn-config-uni

4119

4120 **6.4.10.6 Structure of IEC/IEEE 60802 YANG data models**

4121 The YANG data models specified by this standard use the YANG modules summarized in
4122 Table 20.

4123 In the YANG module definitions, if any discrepancy between the “description” text and the
4124 corresponding definition in any other part of this standard occurs, the definitions outside Clause
4125 6 take precedence.

4126

4127

Table 20 – Summary of the YANG modules

Module	Description
ieee802-ethernet-interface	This module contains YANG definitions for configuring IEEE Std 802.3 Ethernet Interfaces.
ietf-interfaces	This module contains a collection of YANG definitions for managing network interfaces.
iecieee60802-ethernet-interface	This module augments ieee802-ethernet-interface.
ieee802-types	This module contains a collection of generally useful derived data types for IEEE YANG data models.
ieee802-dot1q-bridge	This module describes the bridge configuration model for IEEE 802.1Q Bridges.
ieee802-dot1q-types	This module contains common types used within dot1Q-bridge modules.
iecieee60802-bridge	This module augments ieee802-dot1q-bridge.
ieee802-dot1q-sched-bridge	This module provides for management of IEEE Std 802.1Q Bridges that support Scheduled Traffic Enhancements.
iecieee60802-dot1q-sched-bridge	This module augments ieee802-dot1q-sched-bridge.
ieee802-dot1cb-frer	This module provides management objects that control the frame replication and elimination from IEEE Std 802.1CB-2017.
ieee1588-ptp	This module defines a data model for the configuration and state of IEEE Std 1588 clocks.
ietf-netconf-acm	This module provides management for the Network Configuration Access Control Model.
ieee802-dot1q-tsn-config-uni	This module provides the Time-Sensitive Networking (TSN) User/Network Interface (UNI) for the exchange of information between CUC and CNC that are required to configure TSN Streams in a TSN network.
iecieee60802-tsn-config-uni	This module augments ieee802-dot1q-tsn-config-uni.
iecieee60802-ia-station	This module provides read-only information about the capabilities and RPCs for IEC/IEEE 60802 IA-stations.
ietf-subscribed-notifications	This module defines a YANG data model for subscribing to event records and receiving matching content in notification messages.
iecieee60802-subscribed-notifications	This module augments ietf-subscribed-notifications.

4128

4129 **6.4.10.7 YANG schema tree definitions**

4130 **6.4.10.7.1 General**

4131 The schema tree is provided as an overview of the YANG modules. The symbols and their
 4132 meaning are specified in YANG Tree Diagrams (IETF RFC 8340).

4133 **6.4.10.7.2 Module ieieee60802-ethernet-interface**

4134 module: ieieee60802-ethernet-interface

4135
 4136 augment /if:interfaces/if:interface/eth-if:ether:
 4137 +-ro supported-mau-types* [mau-type]
 4138 +-ro mau-type int32
 4139 +-ro preemption-supported? boolean
 4140

4141 **6.4.10.7.3 Module ieieee60802-bridge**

4142 module: ieieee60802-bridge

4143
 4144 augment /if:interfaces/if:interface/bridge:bridge-port:
 4145 +-ro max-burst-params* [speed]

```

4146     | +-ro speed                      uint32
4147     | +-ro worst-case-packet-gap?    uint8
4148     | +-ro max-burst-frames?        uint8
4149     | +-ro max-burst-bytes?         uint8
4150     +-ro committed-data-rates* [traffic-class speed]
4151     | +-ro traffic-class           dot1q-types:traffic-class-type
4152     | +-ro speed                  uint32
4153     | +-ro committed-information-rate? uint32
4154     | +-ro committed-burst-size?   uint32
4155     +-ro transmission-selection-algorithm* [traffic-class]
4156     | +-ro traffic-class          dot1q-types:traffic-class-type
4157     | +-ro algorithms* [algorithm]
4158     |   +-ro algorithm      identityref
4159     +-ro supported-resource-pools* [resource-pool-name]
4160       +-ro resource-pool-name    string
4161       +-ro covered-time-interval
4162       | +-u ieee802:rational-grouping
4163       +-ro resource-pool-traffic-classes* [traffic-class]
4164         +-ro traffic-class      dot1q-types:traffic-class-type
4165 augment /bridge:bridges/bridge:bridge/bridge:component:
4166   +-ro frer-supported?          boolean
4167   +-ro max-redundant-streams?  uint32
4168   +-ro max-fids?              uint16
4169   +-ro max-fdb-entries* [fid]
4170     | +-ro fid                  uint16
4171     | +-ro max-static-fdb-entries? uint16
4172     | +-ro max-dynamic-fdb-entries? uint16
4173   +-ro (delay-variance)?
4174     | +-:(single-value)
4175       | | +-ro independent-delays* [in-port-mau-type out-port-mau-type
4176 traffic-class]
4177       | | | +-ro in-port-mau-type      int32
4178       | | | +-ro out-port-mau-type    int32
4179       | | | +-ro traffic-class       dot1q-types:traffic-class-type
4180       | | | +-ro independent-delay-min? uint32
4181       | | | +-ro independent-delay-max? uint32
4182       | | | +-ro dependent-delays* [in-port-line-speed]
4183         +-ro in-port-line-speed  uint32
4184         +-ro dependent-delay-min? uint32
4185         +-ro dependent-delay-max? uint32
4186       | +-:(multiple-values)
4187         +-ro independent-delays-cascaded* [in-port in-port-mau-type out-
4188 port out-port-mau-type traffic-class]
4189       | | | +-ro in-port            uint8
4190       | | | +-ro in-port-mau-type  int32
4191       | | | +-ro out-port          uint8
4192       | | | +-ro out-port-mau-type int32
4193       | | | +-ro traffic-class     dot1q-types:traffic-class-type
4194       | | | +-ro independent-delay-min? uint32
4195       | | | +-ro independent-delay-max? uint32
4196       | | | +-ro dependent-delays-cascaded* [in-port in-port-line-speed out-
4197 port]
4198       | | | +-ro in-port          uint8
4199       | | | +-ro in-port-line-speed int32
4200       | | | +-ro out-port          uint8
4201       | | | +-ro dependent-delay-min? uint32
4202       | | | +-ro dependent-delay-max? uint32
4203     +-ro max-ptp-instances?      uint8
4204     +-ro max-hot-standby-systems? uint8
4205     +-ro clock* [clock-identity]
4206       +-ro clock-identity      ptp:clock-identity
4207       +-ro clock-target?       boolean

```

```

4208      +-ro attached-ptp-instance-index?    ->
4209 /ptp:ptp/instances/instance/instance-index
4210      +-ro arb-supported?                boolean
4211      +-ro ptp-supported?                boolean
4212      +-ro hot-standby-supported?       boolean
4213      +-ro is-synced?                  boolean
4214

```

4215 **6.4.10.7.4 Module iecieee60802-sched-bridge**

```

4216 module: iecieee60802-sched-bridge
4217
4218     augment /if:interfaces/if:interface/bridge:bridge-port/sched-bridge:gate-
4219 parameter-table:
4220     +-ro min-gating-times* [speed]
4221         +-ro speed          uint32
4222         +-ro min-cycle-time
4223         | +-u ieee802:rational-grouping
4224         +-ro min-interval-time?   uint32
4225

```

4226 **6.4.10.7.5 Module iecieee60802-tsn-config-uni**

```

4227 module: iecieee60802-tsn-config-uni
4228
4229     augment /tsn:tsn-uni:
4230         +-ro max-config-domains?      uint8
4231         +-ro max-cucs?            uint8
4232         +-ro max-ia-stations?      uint16
4233         +-ro max-network-diameter? uint8
4234         +-ro max-streams?        uint16
4235         +-ro max-num-seamless-trees? uint8
4236         +-ro hot-standby-supported? uint8
4237         +---x add_streams
4238             +---w input
4239             | +---w cuc-id?           string
4240             | +---w stream-list* [stream-id]
4241             |     +---w stream-id    tsn-types:stream-id-type
4242             |     +---w talker
4243             |     | +---w tsn-types:group-talker
4244             |     +---w listener* [index]
4245             |         +---w index          uint32
4246             |         +---w tsn-types:group-listener
4247             +---rw output
4248                 +---rw result?   boolean
4249     augment /tsn:tsn-uni/tsn:domain/tsn:cuc/tsn:stream:
4250         +---x remove_listener
4251             +---w input
4252             | +---w listener* [index]
4253             |     +---w index      uint32
4254             +---rw output
4255                 +---rw result?   Boolean
4256

```

4257 **6.4.10.7.6 Module iecieee60802-ia-station**

```

4258 module: iecieee60802-ia-station
4259     +-ro ia-station-capabilities
4260         +-ro capability-lldp?        boolean
4261         +-ro capability-timesync?   boolean
4262         +-ro capability-keystore?   boolean
4263         +-ro capability-truststore? boolean
4264         +-ro capability-nacm?       boolean
4265         +-ro capability-yang-library? boolean
4266         +-ro capability-yang-push?   boolean
4267         +-ro capability-yang-notifications? boolean

```

```

4268     +-ro capability-netconf-monitoring?    boolean
4269     +-ro capability-netconf-client?      boolean
4270     +-ro capability-tsn-uni?           boolean
4271     +-ro capability-sched-traffic?     boolean
4272     +-ro capability-frame-preemption?   boolean
4273
4274     rpcs:
4275         +--x ia-factory-reset
4276

```

6.4.10.7.7 Module iecieee60802-subscribed-notifications

```

4277 module: iecieee60802-subscribed-notifications
4278
4279     augment /sn:subscriptions:
4280         +-ro max-subscriptions?          uint16
4281         +-ro max-on-change-subscription-leaves?  uint16
4282         +-ro max-periodic-subscription-leaves?  uint16
4283         +-ro min-periodic-subscription-interval? uint16
4284
4285

```

6.4.10.8 YANG modules

6.4.10.8.1 Module iecieee60802-ethernet-interface

```

4286 module iecieee60802-ethernet-interface {
4287     yang-version 1.1;
4288     namespace
4289         "urn:ieee:std:60802:yang:iecieee60802-ethernet-interface";
4290     prefix ia-eth-if;
4291
4292     import ieee802-ethernet-interface {
4293         prefix eth-if;
4294     }
4295     import ietf-interfaces {
4296         prefix if;
4297     }
4298
4299
4300     organization
4301         "IEEE 802.1 Working Group and IEC subcommittee 65C:
4302             Industrial networks, of IEC technical committee 65:
4303                 Industrial-process measurement, control and automation";
4304     contact
4305         "WG-URL: http://ieee802.org/1/
4306         WG-EMail: stds-802-1-l@ieee.org
4307
4308         Contact: IEEE 802.1 Working Group Chair
4309             Postal: C/O IEEE 802.1 Working Group
4310                 IEEE Standards Association
4311                     445 Hoes Lane
4312                         Piscataway, NJ 08854
4313                         USA
4314
4315
4316         E-mail: stds-802-1-chairs@ieee.org";
4317     description
4318         "Management objects that provide information about IEC/IEEE 60802
4319             IA-Stations as specified in IEC/IEEE 60802.
4320
4321         Copyright (C) IEC/IEEE (2025).
4322         This version of this YANG module is part of IEC/IEEE 60802;
4323             see the standard itself for full legal notices.";
4324
4325     revision 2024-02-19 {
4326         description "Published as part of IEC/IEEE 60802-2025.
4327             The following reference statement identifies each referenced
4328             IEEE Standard as updated by applicable amendments.";
```

```

4329     reference
4330         "IEC/IEEE 60802 TSN profile for industrial automation:
4331         IEC/IEEE 60802-2025.
4332         IEEE Std 802.1Q Bridges and Bridged Networks:
4333         IEEE Std 802.1Q-2022, IEEE Std 802.1Qcz-2023,
4334         IEEE Std 802.1Qcw-2023, IEEE Std 802.1Qdj-2024,
4335         IEEE Std 802.1Qdx-2024, IEEE Std 802.1Qdy-2024.";
4336     }
4337
4338     augment "/if:interfaces/if:interface/eth-if:ethernet" {
4339         description
4340             "Augment IEEE Std 802.3 ethernet.";
4341         list supported-mau-types {
4342             description
4343                 "Contains a list of supported MAU parameters.";
4344             key "mau-type";
4345             config false;
4346             leaf mau-type {
4347                 type int32;
4348                 config false;
4349                 description
4350                     "The value is the supported MAU Type derived from the list
4351                     position of the corresponding dot3MauType as listed in
4352                     Clause 5 of IETF RFC 4836.";
4353                 reference
4354                     "Item a) in 6.4.10.3.2.1 of IEC/IEEE 60802";
4355             }
4356             leaf preemption-supported {
4357                 type boolean;
4358                 config false;
4359                 description
4360                     "The Boolean value indicates if preemption is supported by
4361                     the MAU Type.";
4362                 reference
4363                     "Item b) in 6.4.10.3.2.1 of IEC/IEEE 60802";
4364             }
4365         }
4366     }
4367 }
4368

```

4369 6.4.10.8.2 Module iecieee6802-bridge

```

4370 module iecieee6802-bridge {
4371     yang-version 1.1;
4372     namespace "urn:ieee:std:60802:yang:iecieee6802-bridge";
4373     prefix ia-bridge;
4374
4375     import ieee802-types {
4376         prefix ieee802;
4377     }
4378     import ieee802-dot1q-bridge {
4379         prefix bridge;
4380     }
4381     import ietf-interfaces {
4382         prefix if;
4383     }
4384     import ieee802-dot1q-types {
4385         prefix dot1q-types;
4386     }
4387     import ieee1588-ptp {
4388         prefix ptp;
4389     }

```

```
4390
4391     organization
4392         "IEEE 802.1 Working Group and IEC subcommittee 65C:
4393             Industrial networks, of IEC technical committee 65:
4394                 Industrial-process measurement, control and automation";
4395     contact
4396         "WG-URL: http://ieee802.org/1/
4397             WG-EMail: stds-802-1-l@ieee.org
4398
4399             Contact: IEEE 802.1 Working Group Chair
4400                 Postal: C/O IEEE 802.1 Working Group
4401                     IEEE Standards Association
4402                         445 Hoes Lane
4403                         Piscataway, NJ 08854
4404                         USA
4405
4406             E-mail: stds-802-1-chairs@ieee.org";
4407     description
4408         "Management objects that provide information about
4409             IEC/IEEE 60802 IA-Stations as specified in IEC/IEEE 60802.
4410
4411         Copyright (C) IEC/IEEE (2025).
4412         This version of this YANG module is part of IEC/IEEE 60802;
4413         see the standard itself for full legal notices.";
4414
4415     revision 2024-02-19 {
4416         description "Published as part of IEC/IEEE 60802-2025.
4417             The following reference statement identifies each referenced
4418                 IEEE Standard as updated by applicable amendments.";
4419     reference
4420         "IEC/IEEE 60802 TSN profile for industrial automation:
4421             IEC/IEEE 60802-2025.
4422             IEEE Std 802.1Q Bridges and Bridged Networks:
4423                 IEEE Std 802.1Q-2022, IEEE Std 802.1Qcz-2023,
4424                 IEEE Std 802.1Qcw-2023, IEEE Std 802.1Qdj-2024,
4425                 IEEE Std 802.1Qdx-2024, IEEE Std 802.1Qdy-2024.";
4426     }
4427
4428     augment "/if:interfaces/if:interface/bridge:bridge-port" {
4429         description
4430             "Augment IEEE Std 802.1 bridge.";
4431         list max-burst-params {
4432             description
4433                 "The list of maximum burst parameters per supported line
4434                     speed.";
4435                 key "speed";
4436                 config false;
4437                 leaf speed {
4438                     type uint32;
4439                     description
4440                         "This value is the line speed in Mbps.";
4441                 }
4442                 leaf worst-case-packet-gap {
4443                     type uint8;
4444                     config false;
4445                     description
4446                         "The value is the worst case maximum inter-packet gap
4447                             between consecutive frames in a traffic burst expressed
4448                             in bit-times.";
4449                     reference
4450                         "Item a) in 6.4.10.3.3.1 of IEC/IEEE 60802";
4451                 }
4452                 leaf max-burst-frames {
```

```
4453     type uint8;
4454     config false;
4455     description
4456         " The value is the maximum number of frames that can be sent with
4457             minimal inter packet gap.";
4458     reference
4459         "Item b) in 6.4.10.3.3.1 of IEC/IEEE 60802";
4460 }
4461 leaf max-burst-bytes {
4462     type uint8;
4463     config false;
4464     description
4465         " The value is the maximum number of octets that can be sent with
4466             minimal inter packet gap.";
4467     reference
4468         "Item c) in 6.4.10.3.3.1 of IEC/IEEE 60802";
4469 }
4470 }
4471 list committed-data-rates {
4472     description
4473         "The list of committed data rates per traffic class and
4474             supported line speed.";
4475     key "traffic-class speed";
4476     config false;
4477     leaf traffic-class {
4478         type dot1q-types:traffic-class-type;
4479         description
4480             "The traffic class of the entry (0..7).";
4481         reference
4482             "8.6.6 of IEEE Std 802.1Q";
4483     }
4484     leaf speed {
4485         type uint32;
4486         description
4487             "This value is the line speed in Mbps.";
4488     }
4489     leaf committed-information-rate {
4490         type uint32;
4491         config false;
4492         description
4493             "The value is the bandwidth limit in kbit/s.";
4494         reference
4495             "Item a) in 6.4.10.3.3.2 of IEC/IEEE 60802";
4496     }
4497     leaf committed-burst-size {
4498         type uint32;
4499         config false;
4500         description
4501             "The value is the burst size limit in bytes.";
4502         reference
4503             "Item b) in 6.4.10.3.3.2 of IEC/IEEE 60802";
4504     }
4505 }
4506 list transmission-selection-algorithm {
4507     description
4508         "The list of supported transmission selection algorithms
4509             according to 8.6.8 of IEEE Std 802.1Q per traffic class.";
4510     key "traffic-class";
4511     config false;
4512     leaf traffic-class {
4513         type dot1q-types:traffic-class-type;
4514         config false;
4515         description
```

```
4516         "Traffic class. (0..7)";
4517         reference
4518             "8.6.6 of IEEE Std 802.1Q";
4519     }
4520     list algorithms {
4521         description
4522             "The list of supported transmission selection algorithms
4523                 according to 8.6.8 of IEEE Std 802.1Q for this traffic
4524                 class.";
4525         key "algorithm";
4526         config false;
4527         leaf algorithm {
4528             type identityref {
4529                 base dot1q-types:transmission-selection-algorithm;
4530             }
4531             config false;
4532             description
4533                 "Transmission selection algorithm";
4534             reference
4535                 "8.6.8 of IEEE Std 802.1Q";
4536         }
4537     }
4538 }
4539 list supported-resource-pools {
4540     description
4541         "The list of supported buffer resource pools.";
4542     key "resource-pool-name";
4543     config false;
4544     leaf resource-pool-name {
4545         type string;
4546         config false;
4547         description
4548             "The value is the name of a resource pool.";
4549         reference
4550             "Item a) in 6.4.10.3.4.2 of IEC/IEEE 60802";
4551     }
4552     container covered-time-interval {
4553         config false;
4554         uses ieee802:rational-grouping;
4555         description
4556             "The value is the covered buffering time given as rational
4557                 number of seconds for the highest supported link speed.";
4558         reference
4559             "Item b) in 6.4.10.3.4.2 of IEC/IEEE 60802";
4560     }
4561     list resource-pool-traffic-classes {
4562         description
4563             "The list of the traffic classes to be served by the
4564                 resource pool.";
4565         reference
4566             "Item c) in 6.4.10.3.4.2 of IEC/IEEE 60802";
4567         key "traffic-class";
4568         config false;
4569         leaf traffic-class {
4570             type dot1q-types:traffic-class-type;
4571             description
4572                 "The traffic class of the entry.";
4573             reference
4574                 "8.6.6 of IEEE Std 802.1Q";
4575         }
4576     }
4577 }
```

```
4579
4580     augment "/bridge:bridges/bridge:bridge/bridge:component" {
4581         description
4582             "Augment IEEE Std 802.1 bridge component.";
4583         leaf frer-supported {
4584             type boolean;
4585             config false;
4586             description
4587                 "The Boolean value indicates if FRER is supported.";
4588             reference
4589                 "6.4.10.3.5.1 of IEC/IEEE 60802";
4590         }
4591         leaf max-redundant-streams {
4592             type uint32;
4593             config false;
4594             description
4595                 "The value is the maximum number of supported redundant
4596                     streams.";
4597             reference
4598                 "6.4.10.3.5.2 of IEC/IEEE 60802";
4599         }
4600         leaf max-fids {
4601             type uint16;
4602             config false;
4603             description
4604                 "The value is the maximum number of supported FIDs.";
4605             reference
4606                 "6.4.10.3.7.1 of IEC/IEEE 60802";
4607         }
4608         list max-fdb-entries {
4609             config false;
4610             description
4611                 "The list of the maximum number of static and dynamic
4612                     FDB entries per FID.";
4613             reference
4614                 "6.4.10.3.7.2 of IEC/IEEE 60802";
4615             key "fid";
4616             leaf fid {
4617                 type uint16;
4618                 config false;
4619                 description
4620                     "The FID number";
4621             }
4622             leaf max-static-fdb-entries {
4623                 type uint16;
4624                 config false;
4625                 description
4626                     "The value is the maximum number of static FDB
4627                         entries.";
4628                 reference
4629                     "6.4.10.3.7.3 of IEC/IEEE 60802";
4630             }
4631             leaf max-dynamic-fdb-entries {
4632                 type uint16;
4633                 config false;
4634                 description
4635                     "The value is the maximum number of dynamic FDB entries.";
4636                 reference
4637                     "6.4.10.3.7.4 of IEC/IEEE 60802";
4638             }
4639         }
4640         choice delay-variance {
4641             config false;
```

```
4642     description
4643         "The value indicates variance in delay depending upon the use of a
4644             singleValue or multipleValues.";
4645     reference
4646         "6.4.10.3.6.1 of IEC/IEEE 60802";
4647     case single-value {
4648         list independent-delays {
4649             description
4650                 "The list of minimum and maximum frame length
4651                     independent delay time values of frames as they pass
4652                         through a bridge component.";
4653             reference
4654                 "6.4.10.3.6.2 of IEC/IEEE 60802";
4655             key "in-port-mau-type out-port-mau-type traffic-class";
4656             config false;
4657             leaf in-port-mau-type {
4658                 type int32;
4659                 config false;
4660                 description
4661                     "The MAU type of the input port";
4662             }
4663             leaf out-port-mau-type {
4664                 type int32;
4665                 config false;
4666                 description
4667                     "The MAU type of the input port";
4668             }
4669             leaf traffic-class {
4670                 type dot1q-types:traffic-class-type;
4671                 config false;
4672                 description
4673                     "The traffic class of the entry.";
4674                 reference
4675                     "8.6.6 of IEEE Std 802.1Q";
4676             }
4677             leaf independent-delay-min {
4678                 type uint32;
4679                 config false;
4680                 description
4681                     "The value is the minimum delay portion that is
4682                         independent of frame length according to 12.32.1.1.
4683                         of IEEE 802.1Q";
4684                 reference
4685                     "Item a) in 6.4.10.3.6.2 of IEC/IEEE 60802";
4686             }
4687             leaf independent-delay-max {
4688                 type uint32;
4689                 config false;
4690                 description
4691                     "The value is the maximum delay portion that is
4692                         independent of frame length according to 12.32.1.1.
4693                         of IEEE 802.1Q";
4694                 reference
4695                     "Item b) in 6.4.10.3.6.2 of IEC/IEEE 60802";
4696             }
4697         }
4698         list dependent-delays {
4699             description
4700                 "The list of minimum and maximum frame length dependent
4701                     delay time values of frames as they pass through a
4702                         bridge component";
4703             reference
4704                 "6.4.10.3.6.2 of IEC/IEEE 60802";
```

```
4705 key "in-port-line-speed";
4706 config false;
4707 leaf in-port-line-speed {
4708     type uint32;
4709     config false;
4710     description
4711         "This value is the line speed in Mbps.";
4712 }
4713 leaf dependent-delay-min {
4714     type uint32;
4715     config false;
4716     description
4717         "The value is the minimum delay portion that is
4718             dependent on frame length according to 12.32.1.2.
4719             of IEEE 802.1Q";
4720     reference
4721         "Item c) in 6.4.10.3.6.2 of IEC/IEEE 60802";
4722 }
4723 leaf dependent-delay-max {
4724     type uint32;
4725     config false;
4726     description
4727         "The value is the maximum delay portion that is
4728             dependent on frame length according to 12.32.1.2.
4729             of IEEE 802.1Q";
4730     reference
4731         "Item d) in 6.4.10.3.6.2 of IEC/IEEE 60802";
4732 }
4733 }
4734 }
4735 case multiple-values {
4736     list independent-delays-cascaded {
4737         description
4738             "The list of minimum and maximum frame length
4739                 independent delay time values of frames as they pass
4740                     through a bridge component.";
4741         reference
4742             "6.4.10.3.6.2 of IEC/IEEE 60802";
4743     key "in-port in-port-mau-type out-port out-port-mau-type
4744         traffic-class";
4745     config false;
4746     leaf in-port {
4747         type uint8;
4748         config false;
4749         description
4750             "The port number of the input port";
4751     }
4752     leaf in-port-mau-type {
4753         type int32;
4754         config false;
4755         description
4756             "The MAU type of the input port";
4757     }
4758     leaf out-port {
4759         type uint8;
4760         config false;
4761         description
4762             "The port number of the output port";
4763     }
4764     leaf out-port-mau-type {
4765         type int32;
4766         config false;
4767         description
```

```
4768      "The MAU type of the input port";
4769 }
4770 leaf traffic-class {
4771   type dot1q-types:traffic-class-type;
4772   config false;
4773   description
4774     "The traffic class of the entry.";
4775   reference
4776     "8.6.6 of IEEE Std 802.1Q";
4777 }
4778 leaf independent-delay-min {
4779   type uint32;
4780   config false;
4781   description
4782     "The value is the minimum delay portion that is
4783       independent of frame length according to 12.32.1.1.
4784       of IEEE 802.1Q";
4785   reference
4786     "Item a) in 6.4.10.3.6.2 of IEC/IEEE 60802";
4787 }
4788 leaf independent-delay-max {
4789   type uint32;
4790   config false;
4791   description
4792     "The value is the maximum delay portion that is
4793       independent of frame length according to 12.32.1.1.
4794       of IEEE 802.1Q";
4795   reference
4796     "Item b) in 6.4.10.3.6.2 of IEC/IEEE 60802";
4797 }
4798 }
4799 list dependent-delays-cascaded {
4800   description
4801     "The list of minimum and maximum frame length dependent
4802       delay time values of frames as they pass through a
4803       bridge component";
4804   reference
4805     "6.4.10.3.6.2 of IEC/IEEE 60802";
4806   key "in-port in-port-line-speed out-port";
4807   config false;
4808   leaf in-port {
4809     type uint8;
4810     config false;
4811     description
4812       "The port number of the input port";
4813   }
4814   leaf in-port-line-speed {
4815     type uint32;
4816     config false;
4817     description
4818       "This value is the line speed in Mbps.";
4819   }
4820   leaf out-port {
4821     type uint8;
4822     config false;
4823     description
4824       "The port number of the output port";
4825   }
4826   leaf dependent-delay-min {
4827     type uint32;
4828     config false;
4829     description
4830       "The value is the minimum delay portion that is
```

```
4831      dependent on frame length according to 12.32.1.2.  
4832      of IEEE 802.1Q";  
4833      reference  
4834      "Item c) in 6.4.10.3.6.2 of IEC/IEEE 60802";  
4835    }  
4836    leaf dependent-delay-max {  
4837      type uint32;  
4838      config false;  
4839      description  
4840      "The value is the maximum delay portion that is  
4841      dependent on frame length according to 12.32.1.2.  
4842      of IEEE 802.1Q";  
4843      reference  
4844      "Item d) in 6.4.10.3.6.2 of IEC/IEEE 60802";  
4845    }  
4846  }  
4847 }  
4848 }  
4849 leaf max-ptp-instances {  
4850   type uint8;  
4851   config false;  
4852   description  
4853   "The value is the maximum number of supported PTP  
4854   Instances.";  
4855   reference  
4856   "6.4.10.3.7.5 of IEC/IEEE 60802";  
4857 }  
4858 leaf max-hot-standby-systems {  
4859   type uint8;  
4860   config false;  
4861   description  
4862   "The value is the maximum number of supported HotStandbySystem  
4863   entities.";  
4864   reference  
4865   "6.4.10.3.7.6 of IEC/IEEE 60802";  
4866 }  
4867 list clock {  
4868   description  
4869   "The list of supported application clock entities.";  
4870   reference  
4871   "6.4.10.3.7.7 of IEC/IEEE 60802";  
4872   key "clock-identity";  
4873   config false;  
4874   leaf clock-identity {  
4875     type ptp:clock-identity;  
4876     config false;  
4877     description  
4878     "The clock identity of the application clock.";  
4879     reference  
4880     "Item a) in 6.4.10.3.7.7 of IEC/IEEE 60802";  
4881   }  
4882   leaf clock-target {  
4883     type boolean;  
4884     config false;  
4885     description  
4886     "The Boolean value indicates if the application clock is a  
4887     clock target (TRUE) or clock source (FALSE).";  
4888     reference  
4889     "Item b) in 6.4.10.3.7.7 of IEC/IEEE 60802";  
4890   }  
4891   leaf attached-ptp-instance-index {  
4892     type leafref {  
4893       path "/ptp:ptp/ptp:instances/ptp:instance/ptp:instance-index";
```

```

4894     }
4895     config false;
4896     description
4897         "The value is a reference to the index of the PTP or hot
4898             standby Instance, that is attached to the application
4899             clock.";
4900     reference
4901         "Item f) in 6.4.10.3.7.7 of IEC/IEEE 60802";
4902 }
4903 leaf arb-supported {
4904     type boolean;
4905     config false;
4906     description
4907         "The Boolean value indicates if the application clock
4908             supports the ARB timescale.";
4909     reference
4910         "Item c) in 6.4.10.3.7.7 of IEC/IEEE 60802";
4911 }
4912 leaf ptp-supported {
4913     type boolean;
4914     config false;
4915     description
4916         "The Boolean value indicates if the application clock
4917             supports the PTP timescale.";
4918     reference
4919         "Item d) in 6.4.10.3.7.7 of IEC/IEEE 60802";
4920 }
4921 leaf hot-standby-supported {
4922     type boolean;
4923     config false;
4924     description
4925         "The Boolean value indicates if the application clock
4926             supports the hot standby.";
4927     reference
4928         "Item e) in 6.4.10.3.7.7 of IEC/IEEE 60802";
4929 }
4930 leaf is-synced {
4931     type boolean;
4932     config false;
4933     description
4934         "The Boolean value indicates if the application clock is
4935             either synchronized to the attached PTP Instance (TRUE)
4936             or to an internal/external ClockSource (FALSE).";
4937     reference
4938         "Item g) in 6.4.10.3.7.7 of IEC/IEEE 60802";
4939     }
4940 }
4941 }
4942 }
4943

```

4944 6.4.10.8.3 Module iecieee60802-sched-bridge

```

4945 module iecieee60802-sched-bridge {
4946     yang-version 1.1;
4947     namespace "urn:ieee:std:60802:yang:iecieee60802-sched-bridge";
4948     prefix ia-sched-bridge;
4949
4950     import ieee802-types {
4951         prefix ieee802;
4952     }
4953     import ieee802-dot1q-bridge {
4954         prefix bridge;

```

```
4955 }
4956 import ieee802-dot1q-sched-bridge {
4957     prefix sched-bridge;
4958 }
4959 import ietf-interfaces {
4960     prefix if;
4961 }
4962
4963 organization
4964     "IEEE 802.1 Working Group and IEC subcommittee 65C:
4965         Industrial networks, of IEC technical committee 65:
4966             Industrial-process measurement, control and automation";
4967 contact
4968     "WG-URL: http://ieee802.org/1/
4969     WG-EMail: stds-802-1-l@ieee.org
4970
4971     Contact: IEEE 802.1 Working Group Chair
4972         Postal: C/O IEEE 802.1 Working Group
4973             IEEE Standards Association
4974                 445 Hoes Lane
4975                 Piscataway, NJ 08854
4976                 USA
4977
4978     E-mail: stds-802-1-chairs@ieee.org";
4979 description
4980     "Management objects that provide information about IEC/IEEE 60802
4981     IA-Stations as specified in IEC/IEEE 60802.
4982
4983     Copyright (C) IEC/IEEE (2025).
4984     This version of this YANG module is part of IEC/IEEE 60802;
4985     see the standard itself for full legal notices.";
4986
4987 revision 2024-02-19 {
4988     description "Published as part of IEC/IEEE 60802-2025.
4989         The following reference statement identifies each referenced
4990             IEEE Standard as updated by applicable amendments.";
4991 reference
4992     "IEC/IEEE 60802 TSN profile for industrial automation:
4993         IEC/IEEE 60802-2025.
4994         IEEE Std 802.1Q Bridges and Bridged Networks:
4995             IEEE Std 802.1Q-2022, IEEE Std 802.1Qcz-2023,
4996             IEEE Std 802.1Qcw-2023, IEEE Std 802.1Qdj-2024,
4997             IEEE Std 802.1Qdx-2024, IEEE Std 802.1Qdy-2024.";
4998 }
4999
5000 augment "/if:interfaces/if:interface/bridge:bridge-port/sched-bridge:gate-
5001 parameter-table" {
5002     description
5003         "Augment IEEE Std 802.1 bridge/gate-parameter-table.";
5004     list min-gating-times {
5005         description
5006             "The list of minimum gating times per supported line speed.";
5007         reference
5008             "6.4.10.3.4.3 of IEC/IEEE 60802";
5009         key "speed";
5010         config false;
5011         leaf speed {
5012             type uint32;
5013             config false;
5014             description
5015                 "This value is the line speed in Mbps.";
5016         }
5017         container min-cycle-time {
```

```

5018     uses ieee802:rational-grouping;
5019     description
5020         "The value is the minimum value supported by this port of
5021             the AdminCycleTime and OperCycleTime parameters given as
5022                 rational number of seconds.";
5023     reference
5024         "Item a) in 6.4.10.3.4.3 of IEC/IEEE 60802";
5025     }
5026     leaf min-interval-time {
5027         type uint32;
5028         description
5029             "The value is the minimum value supported by this port of
5030                 the TimeIntervalValue parameter in nanoseconds.";
5031         reference
5032             "Item b) in 6.4.10.3.4.3 of IEC/IEEE 60802";
5033     }
5034 }
5035 }
5036 }
5037

```

5038 **6.4.10.8.4 Module iecieee60802-tsn-config-uni**

```

5039 module iecieee60802-tsn-config-uni {
5040     yang-version 1.1;
5041     namespace "urn:ieee:std:60802:yang:iecieee60802-tsn-config-uni";
5042     prefix ia-tsn;
5043
5044     import ieee802-dot1q-tsn-config-uni {
5045         prefix tsn;
5046     }
5047     import ieee802-dot1q-tsn-types {
5048         prefix tsn-types;
5049     }
5050
5051     organization
5052         "IEEE 802.1 Working Group and IEC subcommittee 65C:
5053             Industrial networks, of IEC technical committee 65:
5054                 Industrial-process measurement, control and automation";
5055     contact
5056         "WG-URL: http://ieee802.org/1/
5057             WG-EMail: stds-802-1-l@ieee.org
5058
5059             Contact: IEEE 802.1 Working Group Chair
5060                 Postal: C/O IEEE 802.1 Working Group
5061                     IEEE Standards Association
5062                         445 Hoes Lane
5063                             Piscataway, NJ 08854
5064                             USA
5065
5066             E-mail: stds-802-1-chairs@ieee.org";
5067     description
5068         "Management objects that provide information about IEC/IEEE 60802
5069             IA-Stations as specified in IEC/IEEE 60802.
5070
5071         Copyright (C) IEC/IEEE (2025).
5072         This version of this YANG module is part of IEC/IEEE 60802;
5073             see the standard itself for full legal notices.";
5074
5075     revision 2024-02-19 {
5076         description "Published as part of IEC/IEEE 60802-2025.
5077             The following reference statement identifies each referenced
5078                 IEEE Standard as updated by applicable amendments.";
```

```
5079 reference
5080     "IEC/IEEE 60802 TSN profile for industrial automation:
5081     IEC/IEEE 60802-2025.
5082     IEEE Std 802.1Q Bridges and Bridged Networks:
5083     IEEE Std 802.1Q-2022, IEEE Std 802.1Qcz-2023,
5084     IEEE Std 802.1Qcw-2023, IEEE Std 802.1Qdj-2024,
5085     IEEE Std 802.1Qdx-2024, IEEE Std 802.1Qdy-2024.";
5086 }
5087
5088 augment "/tsn:tsn-uni" {
5089     description
5090         "Augment main container in tsc-config-uni.";
5091     leaf max-config-domains {
5092         type uint8;
5093         config false;
5094         description
5095             "The value is the maximum number of supported configuration
5096             domains.";
5097         reference
5098             "6.4.10.3.9.1 of IEC/IEEE 60802";
5099     }
5100     leaf max-cucs {
5101         type uint8;
5102         config false;
5103         description
5104             "The value is the maximum number of supported CUC entities.";
5105         reference
5106             "6.4.10.3.9.2 of IEC/IEEE 60802";
5107     }
5108     leaf max-ia-stations {
5109         type uint16;
5110         config false;
5111         description
5112             "The value is the maximum number of supported IA-stations.";
5113         reference
5114             "6.4.10.3.9.3 of IEC/IEEE 60802";
5115     }
5116     leaf max-network-diameter {
5117         type uint8;
5118         config false;
5119         description
5120             "The value is the maximum supported network diameter.";
5121         reference
5122             "6.4.10.3.9.4 of IEC/IEEE 60802";
5123     }
5124     leaf max-streams {
5125         type uint16;
5126         config false;
5127         description
5128             "The value is the maximum number of supported streams.";
5129         reference
5130             "6.4.10.3.9.5 of IEC/IEEE 60802";
5131     }
5132     leaf max-num-seamless-trees {
5133         type uint8;
5134         config false;
5135         description
5136             "The value is the maximum number of trees supported for
5137                 seamless redundancy of a stream.";
5138         reference
5139             "6.4.10.3.9.6 of IEC/IEEE 60802";
5140     }
5141     leaf hot-standby-supported {
```

```
5142     type uint8;
5143     config false;
5144     description
5145         "The Boolean value indicates if PTP hot standby is
5146         supported.";
5147     reference
5148         "6.4.10.3.9.7 of IEC/IEEE 60802";
5149 }
5150 action add_streams {
5151     description
5152         "This Action requests a CNC to add a list of streams.";
5153     input {
5154         leaf cuc-id {
5155             type string;
5156             description
5157                 "The CUC ID where the streams are to be added";
5158         }
5159         list stream-list {
5160             key "stream-id";
5161             description
5162                 "List of Streams that should be added.";
5163             leaf stream-id {
5164                 type tsn-types:stream-id-type;
5165                 description
5166                     "The Stream ID is a unique identifier of a Stream
5167                     request and corresponding configuration. It is used to
5168                     associate a CUC's Stream request with a CNC's
5169                     corresponding response.";
5170         }
5171         container talker {
5172             description
5173                 "The Talker container contains: - Talker's behavior for
5174                     Stream (how/when transmitted) - Talker's requirements
5175                     from the network - TSN capabilities of the Talker's
5176                     interface(s).";
5177             uses tsn-types:group-talker;
5178         }
5179         list listener {
5180             key "index";
5181             description
5182                 "Each Listener list entry contains: - Listener's
5183                     requirements from the network - TSN capabilities of
5184                     the Listener's interface(s).";
5185             leaf index {
5186                 type uint32;
5187                 description
5188                     "This index is provided in order to provide a unique
5189                     key per list entry.";
5190             }
5191             uses tsn-types:group-listener;
5192         }
5193     }
5194 }
5195 output {
5196     leaf result {
5197         type boolean;
5198         description
5199             "Returns status information indicating if Stream addition
5200             has been successful.";
5201     }
5202 }
5203 }
5204 }
```

```
5205
5206     augment "/tsn:tsn-uni/tsn:domain/tsn:cuc/tsn:stream" {
5207         description
5208             "Augment stream list in tsc-config-uni.";
5209         action remove_listener {
5210             description
5211                 "This Action removes listeners from a stream.";
5212             input {
5213                 list listener {
5214                     key "index";
5215                     description
5216                         "Each Listener list entry contains: - Listener's
5217                             requirements from the network - TSN capabilities of the
5218                             Listener's interface(s).";
5219                     leaf index {
5220                         type uint32;
5221                         description
5222                             "This index is provided in order to provide a unique
5223                             key per list entry.";
5224                     }
5225                 }
5226             }
5227             output {
5228                 leaf result {
5229                     type boolean;
5230                     description
5231                         "Returns status information indicating if listene removal
5232                             has been successful.";
5233                 }
5234             }
5235         }
5236     }
5237 }
```

6.4.10.8.5 Module iecieee60802-ia-station

```
5240 module iecieee60802-ia-station {  
5241     yang-version 1.1;  
5242     namespace "urn:ieee:std:60802:yang:iecieee60802-ia-station";  
5243     prefix ias;  
5244  
5245     import ietf-datastores {  
5246         prefix ds;  
5247         reference  
5248             "IETF RFC 8342: Network Management Datastore Architecture  
5249             (NMDA)";  
5250     }  
5251     import ietf-netconf-acm {  
5252         prefix nacm;  
5253         reference  
5254             "IETF RFC 8341: Network Configuration Access Control Model";  
5255     }  
5256  
5257     organization  
5258         "IEEE 802.1 Working Group and IEC subcommittee 65C:  
5259             Industrial networks, of IEC technical committee 65:  
5260                 Industrial-process measurement, control and automation";  
5261     contact  
5262         "WG-URL: http://ieee802.org/1/  
5263             WG-EMail: stds-802-1-1@ieee.org  
5264  
5265             Contact: IEEE 802.1 Working Group Chair  
5266                 Postal: C/O IEEE 802.1 Working Group
```

```
5267             IEEE Standards Association
5268                 445 Hoes Lane
5269                 Piscataway, NJ 08854
5270                 USA
5271
5272     E-mail: stds-802-1-chairs@ieee.org";
5273     description
5274         "Capability information and reset to factory defaults
5275             functionality for IEC/IEEE 60802 IA-Stations as specified in
5276             IEC/IEEE 60802.
5277
5278     Copyright (C) IEC/IEEE (2025).
5279     This version of this YANG module is part of IEC/IEEE 60802;
5280     see the standard itself for full legal notices.";
5281
5282     revision 2024-02-19 {
5283         description "Published as part of IEC/IEEE 60802-2025.
5284             The following reference statement identifies each referenced
5285                 IEEE Standard as updated by applicable amendments.";
5286         reference
5287             "IEC/IEEE 60802 TSN profile for industrial automation:
5288                 IEC/IEEE 60802-2025.
5289                 IEEE Std 802.1Q Bridges and Bridged Networks:
5290                     IEEE Std 802.1Q-2022, IEEE Std 802.1Qcz-2023,
5291                     IEEE Std 802.1Qcw-2023, IEEE Std 802.1Qdj-2024,
5292                     IEEE Std 802.1Qdx-2024, IEEE Std 802.1Qdy-2024.";
5293     }
5294
5295     feature ia-factory-default-datastore {
5296         description
5297             "Indicates that the factory default configuration is
5298                 available as a datastore.";
5299     }
5300
5301     identity ia-factory-default {
5302         if-feature "ia-factory-default-datastore";
5303         base ds:datastore;
5304         description
5305             "This read-only datastore contains the factory default
5306                 configuration for the device that will be used to replace
5307                 the contents of the read-write conventional configuration
5308                 datastores during a 'ia-factory-reset' RPC operation.";
5309     }
5310
5311     container ia-station-capabilities {
5312         description
5313             "This container provides read only information about an
5314                 ia-station's capabilities.";
5315         reference
5316             "IEC/IEEE 60802 - YANG Data Model";
5317         config false;
5318         leaf capability-lldp {
5319             type boolean;
5320             config false;
5321             description
5322                 "The value is true if the device supports LLDP.";
5323             reference
5324                 "6.4.10.3.8.5 of IEC/IEEE 60802";
5325         }
5326         leaf capability-timesync {
5327             type boolean;
5328             config false;
5329             description
```

```
5330      "The value is true if the device supports Timesync.";  
5331      reference  
5332          "6.4.10.3.8.6 of IEC/IEEE 60802";  
5333    }  
5334  leaf capability-keystore {  
5335      type boolean;  
5336      config false;  
5337      description  
5338          "The value is true if the device supports Keystore.";  
5339      reference  
5340          "6.4.10.3.8.7 of IEC/IEEE 60802";  
5341    }  
5342  leaf capability-truststore {  
5343      type boolean;  
5344      config false;  
5345      description  
5346          "The value is true if the device supports Truststore.";  
5347      reference  
5348          "6.4.10.3.8.9 of IEC/IEEE 60802";  
5349    }  
5350  leaf capability-nacm {  
5351      type boolean;  
5352      config false;  
5353      description  
5354          "The value is true if the device supports NACM.";  
5355      reference  
5356          "6.4.10.3.8.8 of IEC/IEEE 60802";  
5357    }  
5358  leaf capability-yang-library {  
5359      type boolean;  
5360      config false;  
5361      description  
5362          "The value is true if the device supports YANG library.";  
5363      reference  
5364          "6.4.10.3.8.10 of IEC/IEEE 60802";  
5365    }  
5366  leaf capability-yang-push {  
5367      type boolean;  
5368      config false;  
5369      description  
5370          "The value is true if the device supports YANG push.";  
5371      reference  
5372          "6.4.10.3.8.11 of IEC/IEEE 60802";  
5373    }  
5374  leaf capability-yang-notifications {  
5375      type boolean;  
5376      config false;  
5377      description  
5378          "The value is true if the device supports YANG  
5379              notifications.";  
5380      reference  
5381          "6.4.10.3.8.12 of IEC/IEEE 60802";  
5382    }  
5383  leaf capability-netconf-monitoring {  
5384      type boolean;  
5385      config false;  
5386      description  
5387          "The value is true if the device supports NETCONF  
5388              monitoring.";  
5389      reference  
5390          "6.4.10.3.8.13 of IEC/IEEE 60802";  
5391    }  
5392  leaf capability-netconf-client {
```

```

5393     type boolean;
5394     config false;
5395     description
5396       "The value is true if the device supports NETCONF client.";
5397     reference
5398       "6.4.10.3.8.14 of IEC/IEEE 60802";
5399   }
5400   leaf capability-tsn-uni {
5401     type boolean;
5402     config false;
5403     description
5404       "The value is true if the device supports TSN uni.";
5405     reference
5406       "6.4.10.3.8.15 of IEC/IEEE 60802";
5407   }
5408   leaf capability-sched-traffic {
5409     type boolean;
5410     config false;
5411     description
5412       "The value is true if the device supports scheduled
5413         traffic.";
5414     reference
5415       "6.4.10.3.8.16 of IEC/IEEE 60802";
5416   }
5417   leaf capability-frame-preemption {
5418     type boolean;
5419     config false;
5420     description
5421       "The value is true if the device supports frame preemption.";
5422     reference
5423       "6.4.10.3.8.17 of IEC/IEEE 60802";
5424   }
5425 }
5426
5427 rpc ia-factory-reset {
5428   nacm:default-deny-all;
5429   description
5430     "The server resets all datastores to their factory
5431       default contents and any nonvolatile storage back to
5432         factory condition, deleting all dynamically
5433           generated files, including those containing keys,
5434             certificates, logs, and other temporary files.
5435
5436     Depending on the factory default configuration, after
5437       being reset, the device may become unreachable on the
5438         network.
5439
5440     In contrast to the original factory-reset RPC in IETF RFC
5441       8808, this RPC puts the device into a state where a
5442         subsequent configuration by a CNC component results in a
5443           functioning 60802 IA-station";
5444   }
5445 }
5446

```

5447 **6.4.10.8.6 Module iecieee60802-subscribed-notifications**

```

5448 module iecieee60802-subscribed-notifications {
5449   yang-version 1.1;
5450   namespace
5451     "urn:ieee:std:60802:yang:iecieee60802-subscribed-notifications";
5452   prefix ia-sn;
5453
5454   import ietf-subscribed-notifications {

```

```
5455     prefix sn;
5456 }
5457
5458 organization
5459   "IEEE 802.1 Working Group and IEC subcommittee 65C:
5460     Industrial networks, of IEC technical committee 65:
5461     Industrial-process measurement, control and automation";
5462 contact
5463   "WG-URL: http://ieee802.org/1/
5464     WG-EMail: stds-802-1-l@ieee.org
5465
5466   Contact: IEEE 802.1 Working Group Chair
5467     Postal: C/O IEEE 802.1 Working Group
5468     IEEE Standards Association
5469     445 Hoes Lane
5470     Piscataway, NJ 08854
5471     USA
5472
5473   E-mail: stds-802-1-chairs@ieee.org";
5474 description
5475   "Management objects that provide information about IEC/IEEE 60802
5476   IA-Stations as specified in IEC/IEEE 60802.
5477
5478 Copyright (C) IEC/IEEE (2025).
5479 This version of this YANG module is part of IEC/IEEE 60802;
5480 see the standard itself for full legal notices.";
5481
5482 revision 2024-02-19 {
5483   description "Published as part of IEC/IEEE 60802-2025.
5484     The following reference statement identifies each referenced
5485     IEEE Standard as updated by applicable amendments.";
5486   reference
5487     "IEC/IEEE 60802 TSN profile for industrial automation:
5488       IEC/IEEE 60802-2025.
5489       IEEE Std 802.1Q Bridges and Bridged Networks:
5490       IEEE Std 802.1Q-2022, IEEE Std 802.1Qcz-2023,
5491       IEEE Std 802.1Qcw-2023, IEEE Std 802.1Qdj-2024,
5492       IEEE Std 802.1Qdx-2024, IEEE Std 802.1Qdy-2024.";
5493 }
5494
5495 augment "/sn:subscriptions" {
5496   description
5497     "Augment subscriptions in ietf-subscribed-notifications.";
5498   leaf max-subscriptions {
5499     type uint16;
5500     config false;
5501     description
5502       "The value is the maximum number of supported NETCONF Server
5503         subscriptions.";
5504     reference
5505       "6.4.10.3.8.1 of IEC/IEEE 60802";
5506   }
5507   leaf max-on-change-subscription-leaves {
5508     type uint16;
5509     config false;
5510     description
5511       "The value is the maximum number of supported leaves for
5512         NETCONF Server on-change subscriptions according to IETF
5513         RFC 8641.";
5514     reference
5515       "6.4.10.3.8.2 of IEC/IEEE 60802";
5516   }
5517   leaf max-periodic-subscription-leaves {
```

```
5518     type uint16;
5519     config false;
5520     description
5521       "The value is the maximum number of supported leaves for
5522         NETCONF Server periodic subscriptions according to IETF
5523           RFC 8641.";
5524     reference
5525       "6.4.10.3.8.3 of IEC/IEEE 60802";
5526   }
5527   leaf min-periodic-subscription-interval {
5528     type uint16;
5529     config false;
5530     description
5531       "The value is the minimum periodic subscription interval in
5532         centiseconds (0.01 seconds) for NETCONF Server periodic
5533           subscriptions according to IETF RFC 8641.";
5534     reference
5535       "6.4.10.3.8.4 of IEC/IEEE 60802";
5536   }
5537 }
5538 }
```

5539

5540 **6.5 Topology discovery and verification**5541 **6.5.1 Topology discovery and verification requirements**

5542 Electrical engineering of machines with multiple IA-stations includes the definition of the
5543 machine internal network topology (i.e., the engineered topology).

5544 The machine internal network topology includes type specific data of IA-stations (for example
5545 model name or manufacturer name) as well as instance specific data (for example IP addresses
5546 or DNS names).

5547 The electrical engineering data of the network topology is used:

- 5548 • During commissioning so that machine planning and installation are identical.
- 5549 • By the TDE during operation to verify that the actual topology of the Configuration Domain
5550 matches the engineered topology.
- 5551 • By maintenance staff during repair to easily identify failed IA-stations, ports, or links to be
5552 replaced.

5553 Repair and replacement of an IA-station do not require verification of the updated engineered
5554 topology so that the TDE does not produce a verification error.

5555 IA-stations do not need to be pre-configured when they are repaired or replaced. IA-stations
5556 report type and instance data as described in 6.5.3.

5557

5558 **6.5.2 Topology discovery overview**5559 **6.5.2.1 General**

5560 LLDP enables the discovery of IA-stations, their external ports, and their external connectivity.
5561 A Topology Discovery Entity can query LLDP data by remote management to derive the physical
5562 network topology.

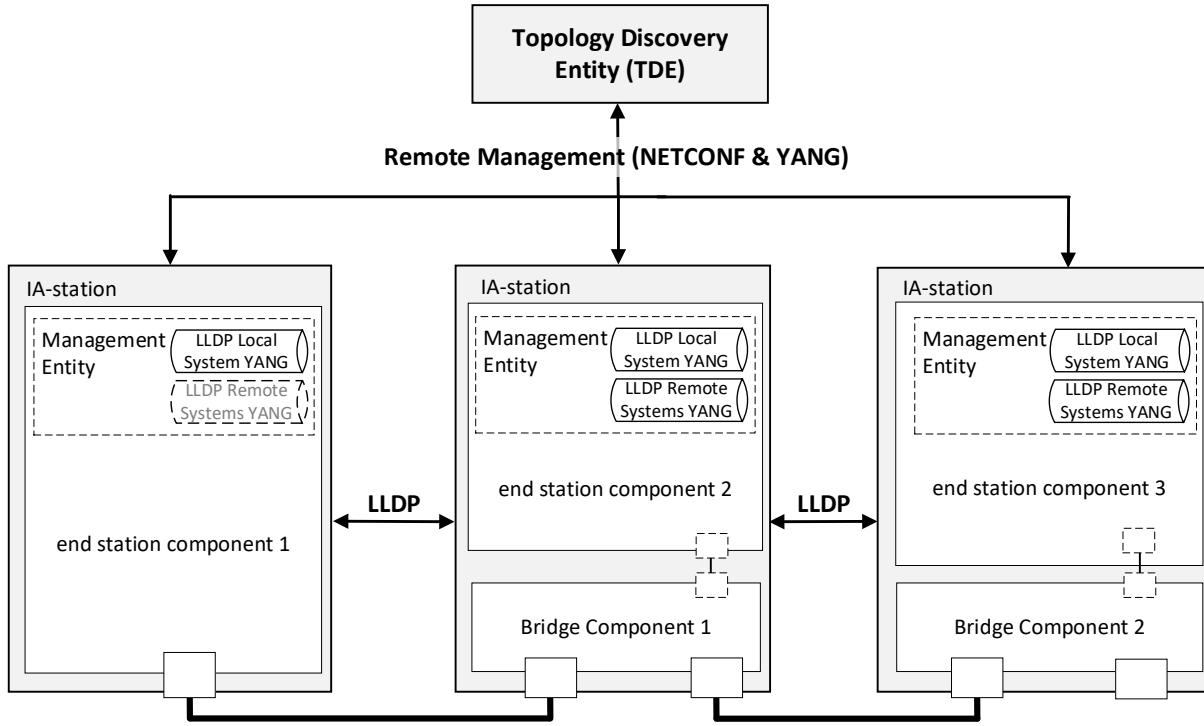


Figure 36 – Usage example of LLDP

5563

5564

5565

5566 Figure 36 illustrates a network showing the LLDP agent implementations in an IA-station
 5567 consisting of a single end station component and two IA-stations with end station and Bridge
 5568 components (see 4.3). The LLDP protocol is used to convey neighborhood information among
 5569 peers, and NETCONF is used between the TDE and the IA-stations to query this neighborhood
 5570 information from the IA-stations. This information allows the TDE to discover IA-stations and
 5571 the physical network topology.

5572 NOTE A Topology Discovery Entity (TDE) can be run from anywhere in the network with reachability to the to-be-
 5573 discovered devices.

5574 IA-stations announce themselves via LLDP to support discovery by the TDE. Announcements
 5575 contain the management address (see 6.5.2.4.6) and system capabilities (see 6.5.2.4.5) for the
 5576 discovery operation. The announced system capabilities information enables the TDE to identify
 5577 IA-stations with multiple end station and Bridge components. The TDE can use the definitions
 5578 in 6.4.3 for the discovery of the internal structure of such IA-stations.

5579 To allow for operational behavior and exchanged information, IA-stations support the local
 5580 system YANG (see 6.4.9.2.2). IA-stations that include a Bridge component additionally support
 5581 the processing of received LLDP messages and support the remote systems YANG (see
 5582 6.4.9.2.2).

5583 **6.5.2.2 LLDP operational control parameters**

5584 LLDP defines several operational parameters that control the protocol behavior (see IEEE Std
 5585 802.1AB-2016, 10.5.1). These parameter definitions apply to all external ports of an IA-station.

5586 NOTE According to IEEE Std 802.1AB-2016, 9.1.1 c), changes to the local system that impact information
 5587 exchanged via LLDP immediately trigger the transmission of an LLDPDU to communicate the local changes as quickly
 5588 as possible to any neighboring systems.

5589 An IA-station shall support LLDP transmit mode (adminStatus enabledTxOnly) on an external
 5590 end station component port and may support transmit and receive mode (adminStatus
 5591 enabledRxTx) on that port (see IEEE Std 802.1AB-2016, 10.5.1).

5592 An IA-station shall support LLDP transmit and receive mode (adminStatus enabledRxTx) on an
 5593 external Bridge component port (see IEEE Std 802.1AB-2016, 10.5.1).

5594 6.5.2.3 LLDPDU transmission, reception, and addressing

5595 The destination address to be used for LLDPDU transmission (dest-mac-address) shall be the
5596 nearest bridge group MAC address, i.e., 01-80-C2-00-00-0E, on all ports to limit the scope of
5597 LLDPDU propagation to a single physical link (see IEEE Std 802.1AB-2016, 7.1 item a).

5598 NOTE IEEE Std 802.1AB-2016 defines LLDPDUs to be transmitted untagged, i.e., frames do not carry priority
5599 information for traffic class selection. At the same time, IEEE Std 802.1AB-2016 neither specifies a well-defined
5600 device-internal priority nor management capabilities for the configuration of the traffic class to be used for the
5601 transmission of LLDPDUs. It is the user's responsibility to prevent LLDPDUs from interfering with the transmission
5602 of time-critical control data.

5603 6.5.2.4 LLDP TLV selection**5604 6.5.2.4.1 General**

5605 An IA-station transmitting LLDPDUs shall include the LLDP TLVs selected in 6.5.2.4 and may
5606 include additional TLVs (tlvs-tx-enable). An IA-station receiving LLDPDUs shall process
5607 LLDPDUs.

5608 Each LLDPDU shall contain the following LLDP TLVs specified in IEEE Std 802.1AB-2016, 8.5:

- 5609 • Exactly one Chassis ID TLV according to 6.5.2.4.2,
- 5610 • Exactly one Port ID TLV according to 6.5.2.4.3,
- 5611 • Exactly one Time To Live TLV according to 6.5.2.4.4,
- 5612 • Exactly one System Capabilities TLV according to 6.5.2.4.5, and
- 5613 • One or more Management Address TLVs according to 6.5.2.4.6.

5614 NOTE The concatenation of the Chassis ID and Port ID fields enables the recipient of an LLDPDU to identify the
5615 sending LLDP agent/port.

5616 6.5.2.4.2 Chassis ID TLV

5617 The Chassis ID field shall contain the same value for all transmitted LLDPDUs independent
5618 from the transmitting port of the IA-station, i.e., be a non-volatile identifier which is unique within
5619 the context of the administrative domain.

5620 The Chassis ID subtype field (chassis-id-subtype) should contain subtype 4, indicating that the
5621 Chassis ID field (chassis-id) contains a MAC address to achieve the Chassis ID's desired
5622 uniqueness. For IA-stations with multiple unique MAC addresses, any one of the IA-station's
5623 MAC addresses may be used and shall be the same for all external ports of that IA-station.

5624 6.5.2.4.3 Port ID TLV

5625 The Port ID field shall contain the same value for all transmitted LLDPDUs for a given external
5626 port, i.e., be a non-volatile, IA-station-unique identifier of the LLDPDU-transmitting port.

5627 The Port ID subtype field (port-id-subtype) should contain subtype 5, indicating that the Port ID
5628 field contains the port interface name (name) according to IETF RFC 8343.

5629 IA-stations should restrict the system-defined port ID to read-only access and a maximum name
5630 length of 255 characters. The names should match the port names printed on the chassis.

5631 6.5.2.4.4 Time To Live TLV

5632 The Time To Live value shall be set according to IEEE Std 802.1AB-2016, 8.5.4.

5633 6.5.2.4.5 System capabilities TLV

5634 An IA-station consisting of a single end station component shall set the system capabilities and
5635 enabled capabilities fields (system-capabilities-supported, system-capabilities-enabled) to
5636 Station Only (i.e., bit 8 set to 1) for all transmitted LLDPDUs.

5637 An IA-station consisting of at least one end station component and at least one Bridge
5638 component shall set the system capabilities and enabled capabilities fields to Station Only (i.e.,
5639 bit 8 set to 1) and C-VLAN component (i.e., bit 9 set to 1) for all transmitted LLDPDUs.

5640 NOTE The combination of the Station Only and C-VLAN component flags is used as a marker indicating to the TDE
5641 that the internal structure of the IA-station consists of multiple components. This is a deliberate deviation from IEEE
5642 Std 802.1AB-2016, Table 8-4, which states in a footnote: "The Station Only capability is intended for devices that
5643 implement only an end station capability, and for which none of the other capabilities in the table apply. Bit 8 should
5644 therefore not be set in conjunction with any other bits."

5645 **6.5.2.4.6 Management address TLV**

5646 An IA-station shall announce at least one IPv4 address by which its Management entity (see
5647 4.3) can be reached (management-address-tx-port).

5648 **6.5.2.5 LLDP remote systems data**

5649 An IA-station supporting the remote systems YANG shall be able to store information from at
5650 least one neighbor per external port.

5651 Receiving LLDPDUs from more neighbors than supported on a given port shall result in the last
5652 one received being saved to the remote systems YANG as described in IEEE Std 802.1AB-
5653 2016, 9.2.7.7.5.

5654 **6.5.3 Topology verification overview**

5655 Topology verification checks discovered topologies against engineered topologies. Topology
5656 verification data includes for every IA-station:

- 5657 • model name,
- 5658 • manufacturer name,
- 5659 • management address.

5660

5661 Topology verification data includes for every external port of an IA-station:

- 5662 • port name,
- 5663 • remote connection (i.e., management address and port name of connected IA-station).

5664

5665 To support topology verification IA-stations shall support LLDP YANG data as specified in
5666 6.4.9.2.2 and Hardware Management YANG data as specified in 6.4.9.2.5.8.

5667 IA-station hardware instance specific data like MAC addresses or serial numbers are not
5668 considered for topology verification. This kind of data changes after a repair and replacement
5669 operation and thus, induces a topology verification error.

5670 **6.6 CNC**

5671 **6.6.1 General**

5672 Subclause 6.6 describes stream destination MAC address handling at the CNC.

5673 **6.6.2 Stream destination MAC address range**

5674 A CNC manages the destination MAC address for requested streams. This destination MAC
5675 address together with the VID identifies the path used for these streams. Thus, a stream
5676 destination MAC address is unique together with the VID in a Configuration Domain.

5677 Figure 37 shows the possible selections of a CNC for a contiguous address range. The CNC
5678 selects an OUI and an offset of the address range for the stream destination MAC addresses.

5679 An address range of 2048 stream destination MAC addresses allows together with a VID the
5680 usage of 2048 streams. Each additional VID used for streams allows an additional 2048
5681 streams.

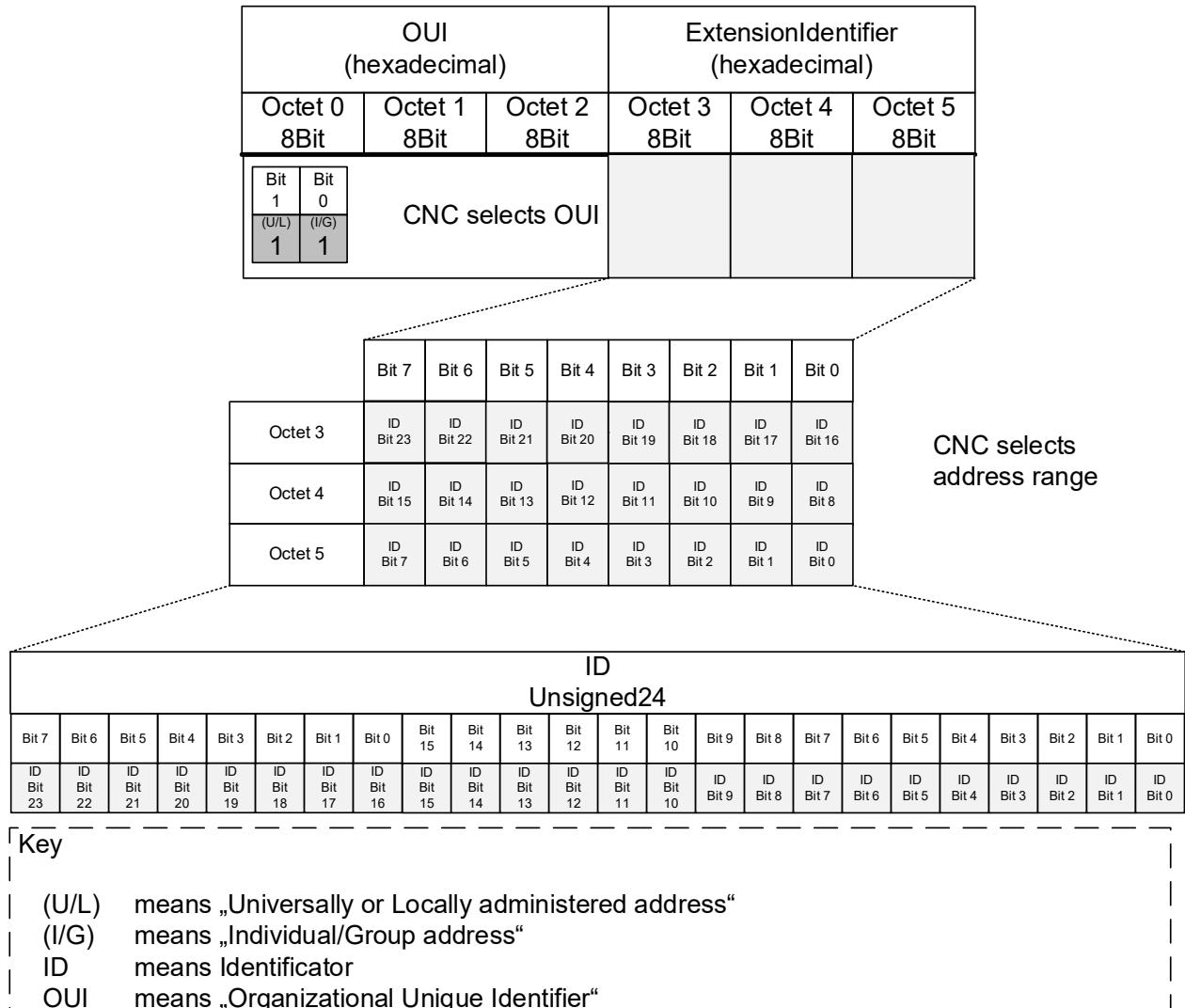
5682 **EXAMPLE**

5683 CNC selected OUI := 00-80-C2

5684 CNC selected address range := 0..2047

5685 CNC selected VID := 101

5686



5687

5688

Figure 37 – Stream Destination MAC Address

5689

5690
5691
5692
5693 **Annex A**
5694 (normative)

5695
5696 **PCS proforma – Time-sensitive networking profile for industrial
5697 automation**

5698 **A.1 General⁷**

5699 The supplier of an implementation that is claimed to conform to the profile specified in this
5700 document shall complete the corresponding Profile Conformance Statement (PCS) proforma,
5701 which is presented in a tabular format based on the format used for Protocol Implementation
5702 Conformance Statement (PICS) proformas.

5703 The tables do not contain an exhaustive list of all requirements that are stated in the referenced
5704 standards; for example, if a row in a table asks whether the implementation is conformant to
5705 Standard X, and the answer “Yes” is chosen, then it is assumed that it is possible, for that
5706 implementation, to fill out the PCS proforma specified in Standard X to show that the
5707 implementation is conformant; however, the tables in this document will only further refine those
5708 elements of conformance to Standard X where particular answers are required for the profiles
5709 specified here.

5710 A completed PCS proforma is the PCS for the implementation in question. The PCS is a
5711 statement of which capabilities and options of the protocol have been implemented. The PCS
5712 can have several uses, including use by the following.

- 5713 a) Protocol implementer, as a checklist to reduce the risk of failure to conform to the document
5714 through oversight.
5715 b) Supplier and acquirer, or potential acquirer, of the implementation, as a detailed indication
5716 of the capabilities of the implementation, stated relative to the common basis for
5717 understanding provided by the standard PCS proforma.
5718 c) User, or potential user, of the implementation, as a basis for initially checking the possibility
5719 of interworking with another implementation.
5720 d) Protocol tester, as the basis for selecting appropriate tests against which to assess the
5721 claim for conformance of the implementation.
5722 e) The user, to verify whether the IA-station, as described by the PCS, fulfills use-case
5723 requirements.

5724 **A.2 Abbreviations and special symbols**

5725 **A.2.1 Status symbols**

5726 M: mandatory

5727 O: optional

5728 O.n: optional, but support of at least one of the group of options labeled by the same
5729 numeral n is required

5730 X: prohibited

5731 pred: conditional-item symbol, including predicate identification: see A.3.4

5732 \neg : logical negation, applied to a conditional item’s predicate

7 Copyright release for the PCS: Users of this document may freely reproduce the PCS contained in this document so that they can be used for their intended purpose.

A.2.2 General abbreviations

5734 N/A: not applicable

5735 PCS: Profile Conformance Statement

A.3 Instructions for completing the PCS proforma**A.3.1 General structure of the PCS proforma**

5738 The first part of the PCS proforma, implementation identification and protocol summary, is to
5739 be completed as indicated with the information necessary to identify fully both the supplier and
5740 the implementation.

5741 The main part of the PCS proforma is a fixed-format questionnaire, divided into several
5742 subclauses, each containing a number of individual items. Answers to the questionnaire items
5743 are to be provided in the rightmost column, either by simply marking an answer to indicate a
5744 restricted choice (usually Yes or No) or by entering a value or a set or range of values. There
5745 are some items where two or more choices from a set of possible answers can apply; all relevant
5746 choices are to be marked. Each item is identified by an item reference in the first column. The
5747 second column contains the question to be answered; the third column records the status of
5748 the item—whether support is mandatory, optional, or conditional; see also A.3.4. The fourth
5749 column contains the reference or references to the material that specifies the item in the main
5750 body of this document, and the fifth column provides the space for the answers.

5751 The PCS indicates support of one of the conformance classes, ccA or ccB, per bridge and end-
5752 station component, specified in this profile.

5753 A single IA-station can incorporate the functionality of one or more of the functions listed in this
5754 PCS. For example, an IA-station could have both an end station component and a Bridge
5755 component.

5756 A supplier can also provide (or be required to provide) further information, categorized as either
5757 additional information (see A.3.2) or exception information (see A.3.3). When present, each
5758 kind of further information is to be provided in a further subclause of items labeled Ai or Xi,
5759 respectively, for cross-referencing purposes, where (i) is any unambiguous identification for the
5760 item (for example, simply a numeral). There are no other restrictions on its format and
5761 presentation.

5762 A completed PCS proforma, including any Additional Information and Exception Information, is
5763 the Protocol Implementation Conformation Statement for the implementation in question.

5764 NOTE Where an implementation is capable of being configured in more than one way, a single PCS can be used
5765 to describe all such configurations. However, the supplier has the choice of providing more than one PCS, each
5766 covering some subset of the implementation's configuration capabilities, in case that makes for easier and clearer
5767 presentation of the information.

A.3.2 Additional information

5769 Items of Additional Information allow a supplier to provide further information intended to assist
5770 the interpretation of the PCS. It is not intended or expected that a large quantity will be supplied,
5771 and a PCS can be considered complete without any such information. Examples might be an
5772 outline of the ways in which a (single) implementation can be set up to operate in a variety of
5773 environments and configurations, or information about aspects of the implementation that are
5774 outside the scope of this document but that have a bearing on the answers to some items.

5775 References to items of Additional Information can be entered next to any answer in the
5776 questionnaire and can be included in items of Exception Information.

A.3.3 Exception information

5778 It can occasionally happen that a supplier will wish to answer an item with mandatory status
5779 (after any conditions have been applied) in a way that conflicts with the indicated requirement.
5780 No preprinted answer will be found in the Support column for this item. Instead, the supplier
5781 shall write the missing answer into the Support column, together with an Xi reference to an item
5782 of Exception Information and shall provide the appropriate rationale in the Exception item itself.

5783 An implementation for which an Exception item is required in this way does not conform to this
 5784 document.

5785 NOTE A possible reason for the situation described previously is that a defect in this document has been reported,
 5786 a correction for which is expected to change the requirement not met by the implementation.

5787 **A.3.4 Conditional status**

5788 **A.3.4.1 Conditional items**

5789 The PCS proforma contains a number of conditional items. These are items for which both the
 5790 applicability of the item itself, and its status if it does apply (mandatory or optional) are
 5791 dependent on whether certain other items are supported.

5792 Where a group of items is subject to the same condition for applicability, a separate preliminary
 5793 question about the condition appears at the head of the group, with an instruction to skip to a
 5794 later point in the questionnaire if the “Not Applicable” (N/A) answer is selected. Otherwise,
 5795 individual conditional items are indicated by a conditional symbol in the Status column.

5796 A conditional symbol is of the form “pred: S” where pred is a predicate as described in A.3.4.2,
 5797 and S is a status symbol, M or O.

5798 If the value of the predicate is true (see A.3.4.2), the conditional item is applicable, and its
 5799 status is indicated by the status symbol following the predicate: The answer column is to be
 5800 marked in the usual way. If the value of the predicate is false, the “Not Applicable” (N/A) answer
 5801 is to be marked.

5802 **A.3.4.2 Predicates**

5803 A predicate is one of the following:

5804 a) An item-reference for an item in the PCS proforma: The value of the predicate is true if the
 5805 item is marked as supported and is false otherwise.

5806 1) A predicate-name, for a predicate defined as a Boolean expression constructed by
 5807 combining item-references using the Boolean operator OR: The value of the predicate
 5808 is true if one or more of the items is marked as supported.

5809 2) The logical negation symbol “¬” prefixed to an item-reference or predicate-name: The
 5810 value of the predicate is true if the value of the predicate formed by omitting the “¬”
 5811 symbol is false, and vice versa.

5812 Each item whose reference is used in a predicate or predicate definition, or in a preliminary
 5813 question for grouped conditional items, is indicated by an asterisk in the Item column.

5814 **A.4 Common requirements**

5815 **A.4.1 Instructions**

5816 One instance of Clause A.4 shall be filled out per IA-station.

5817 **A.4.2 Implementation identification**

5818 The entire PCS pro forma is a form that shall be filled out by a supplier according to Table A.1.

5819 **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	

5820

5821 Only the first three items are required for all implementations; other information can be
 5822 completed as appropriate in meeting the requirement for full identification. The terms “Name”

5823 and “Version” should be interpreted appropriately to correspond with a supplier’s terminology
 5824 (for example, Type, Series, Model).

5825 **A.4.3 Profile summary, IEC/IEEE 60802**

5826 Table A.2 shows the profile summary template.

5827 **Table A.2 – Profile summary template**

Identification of profile specification	IEC/IEEE 60802 - Time-Sensitive Networking profile for industrial automation			
Identification of amendments (Amd) and corrigenda (Corr) to the PCS proforma that have been completed as part of the PCS	Amd. : Corr. :			
	Amd. : 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				

5828

5829 **A.4.4 Implementation summary**

5830 The form in Table A.3 is used to indicate the type of system that the PCS describes.

5831 **Table A.3 – Implementation type**

Item	Feature	Status	References	Support
BC-CCA-N	State the number of Conformance Class A bridge components implemented by the IA-station.	O	5.7.2, 5.8.2	Number _____
BC-CCB-N	State the number of Conformance Class B bridge components implemented by the IA-station.	O	5.7.3, 5.8.3	Number _____
ESC-CCA-N	State the number of Conformance Class A end station components implemented by the IA-station.	O.1	5.9.2, 5.10.2	Number _____
ESC-CCB-N	State the number of Conformance Class B end station components implemented by the IA-station.	O.1	5.9.3, 5.10.3	Number _____
CNC	Does the IA-station include a CNC?	O	5.11	Yes [] No []
CUC	Does the IA-station include a CUC?	O	5.13	Yes [] No []

5832

5833 **A.5 IA-station Requirements and Options**

5834 **A.5.1 Instructions**

5835 One instance of Clause A.5 shall be filled out for an IA-station.

5836 **A.5.2 IA-station requirements**

5837 The form in Table A.4 is used to indicate the IA-station requirements.

5838 **Table A.4 – IA-station requirements**

Item	Feature	Status	References	Support
IASTA-1	Does the IA-station support PHY and MAC requirements for external ports?	M	5.5.1	Yes []
IASTA-2	Does the IA-station support topology discovery requirements?	M	5.5.2	Yes []
IASTA-3	Does the IA-station support requirements for time synchronization?	M	5.5.3	Yes []

IASTA-4	Does the IA-station support requirements for Secure management exchanges?	M	5.5.4.2	Yes []
IASTA-5	Number of of Dynamic Subscriptions to YANG Events and Datastores over NETCONF	M	5.5.4.2 h)	Number _____
IASTA-6	Does the IA-station support management YANG modules?	M	5.5.4.3	Yes []
IASTA-7	Does the IA-station provide a digital data sheet?	M	5.5.4.4	Yes []

5839
5840**A.5.3 IA-station PHY and MAC options for external ports**5841 The form in Table A.5 is used to indicate PHY and MAC options for external ports.
58425843 **Table A.5 – IA-station PHY and MAC options**

Item	Feature	Status	References	Support
DOT3-1	Does the IA-station support PoE over 2 pairs?	O	5.6.1:a)	Yes [] No [] N/A []
DOT3-2	Does the IA-station support Power Interfaces?	O	5.6.1:b)	Yes [] No [] N/A []
DOT3-3	Does the IA-station support PoE?	O	5.6.1:c)	Yes [] No [] N/A []

5844
5845**A.5.4 IA-station options for time synchronization**5846 The form in Table A.6 is used to indicate options for time synchronization.
58475848 **Table A.6 – IA-station time synchronization options**

Item	Feature	Status	References	Support
PTP-1	Does the IA-station support media-independent timeTransmitter capability according to IEEE Std 802.1AS-2020, 5.4.2 item b) as amended by IEEE Std 802.1ASdr-2024?	O	5.6.2:a)	Yes [] No []
PTP-2	Does the IA-station support Grandmaster PTP Instance capability according to IEEE Std 802.1AS-2020, 5.4.2 item c)?	O	5.6.2:b)	Yes [] No []
PTP-3	Does the IA-station support more than one PTP port as a PTP Relay Instance according to IEEE Std 802.1AS-2020, 5.4.2 item d)?	O	5.6.2:c)	Yes [] No []
PTP-4	Does the IA-station support transmit of the Signaling message according to IEEE Std 802.1AS-2020, 5.4.2 item e)?	O	5.6.2:d)	Yes [] No []
PTP-5	Does the IA-station support more than 1 PTP Instance according to IEEE Std 802.1AS-2020, 5.4.2 item f)?	O	5.6.2:e)	Yes [] No []
PTP-6	Does the IA-station support the SyncIntervalSetting state machine according to IEEE Std 802.1AS-2020, 5.4.2 item h)?	O	5.6.2:f)	Yes [] No []
PTP-7	Does the IA-station support one or more application interfaces according to IEEE Std 802.1AS-2020, 5.4.2 item i)?	O	5.6.2:g)	Yes [] No []
PTP-8	Does the IA-station support hot standby redundancy requirements?	O	5.6.2:h)	Yes [] No []

5849

A.5.5 IA-station secure management exchange options5850 The form in Table A.7 is used to indicate options for secure management exchange.
5851

5852

Table A.7 – IA-station secure management exchange options

Item	Feature	Status	References	Support
SECMGMT-5	Does the IA-station support Writable-Running capability?	O	5.6.3:a)	Yes [] No []
SECMGMT-6	Does the IA-station support Confirmed Commit capability?	O	5.6.3:b)	Yes [] No []
SECMGMT-7	Does the IA-station support Distinct Startup capability?	O	5.6.3:c)	Yes [] No []
SECMGMT-8	Does the IA-station support URL capability?	O	5.6.3:d)	Yes [] No []
SECMGMT-9	Does the IA-station support XPath capability?	O	5.6.3:e)	Yes [] No []
SECMGMT-10	Does the IA-station support NETCONF-over-TLS server with the TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA3 84 cypher suite?	O	5.6.3:f)	Yes [] No []
SECMGMT-11	Does the IA-station support NETCONF-over-TLS server with the TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY130 5_SHA256 cypher suite?	O	5.6.3:f)	Yes [] No []
SECMGMT-12	Does the IA-station support TLS with the Curve P-521 elliptic curve?	O	5.6.3:g)	Yes [] No []
SECMGMT-13	Does the IA-station support TLS with the Curve25519 elliptic curve?	O	5.6.3:g)	Yes [] No []
SECMGMT-14	Does the IA-station support TLS with the Curve448 elliptic curve?	O	5.6.3:g)	Yes [] No []
SECMGMT-15	Does the IA-station support PKIX?	O	5.6.3:h)	Yes [] No []

5853

A.5.6 CNC Requirements

5854

The form in Table A.8 is used to indicate requirements for CNCs.

5855

Table A.8 – CNC Requirements

Item	Feature	Status	References	Support
CNC-1	Does the IA-station support CNC requirements?	CNC:M	5.11	Yes [] N/A []

5856

A.5.7 CUC Requirements

5857

The form in Table A.9 is used to indicate requirements for CUCs.

5859

Table A.9 – CUC Requirements

Item	Feature	Status	References	Support
CUC-1	Does the IA-station support CUC requirements?	CUC:M	5.13	Yes [] N/A []

5860

5861 **A.6 Bridge Component**

5862 **A.6.1 Instructions**

5863 One instance of Clause A.6 shall be filled out per bridge component implemented by an IA-
5864 station.

5865 **A.6.2 Bridge Component Requirements**

5866 The form in Table A.10 is used to indicate bridge component requirements.

5867 **Table A.10 –Bridge Component Requirements**

Item	Feature	Status	References	Support
BC-1	Does the bridge component support the common bridge component requirements?	M	5.7.1	Yes []
BC-2	Does the bridge component support ccA bridge component requirements?	O.2	5.7.2	Yes [] No []
BC-3	Does the bridge component support ccB bridge component requirements?	O.2	5.7.3	Yes [] No []

5868

5869 **A.6.3 Common Bridge Component Options**

5870 The form in Table A.11 is used to indicate bridge component options.

5871 **Table A.11 – Common Bridge Component Options**

Item	Feature	Status	References	Support
BC-4	Does the bridge component support the operation of the credit-based shaper algorithm?	O	5.8.1	Yes [] No []

5872

5873 **A.6.4 ccA Bridge Component Options**

5874 The form in Table A.12 is used to indicate options for bridge components conforming to
5875 conformance class A.

5876 **Table A.12 – ccA Bridge Component Options**

Item	Feature	Status	References	Support
CCA-BC-1	Does the bridge component support any of the common bridge component options?	O	5.8.2:a)	Yes [] No [] N/A []
CCA-BC-2	Does the bridge component support more than 2 PTP instances?	O	5.8.2:b)	Yes [] No [] N/A []
CCA-BC-3	State the number of PTP instances supported by the bridge component.	CCA-BC-2:M	5.8.2:b)	Number _____
CCA-BC-4	Does the bridge component support enhancements for scheduled traffic for the 10 Mb/s, 2,5 Gb/s, 5 Gb/s, or 10 Gb/s data rates?	O	5.8.2:c)	Yes [] No [] N/A []
CCA-BC-5	Does the bridge component support frame preemption for the 10 Mb/s, 2,5 Gb/s, 5 Gb/s, or 10 Gb/s data rates?	O	5.8.2:d)	Yes [] No [] N/A []

5877

5878 **A.6.5 ccB Bridge Component Options**

5879 The form in Table A.13 is used to indicate options for bridge components conforming to
5880 conformance class B.

5881

Table A.13 – cCB Bridge Component Options

Item	Feature	Status	References	Support
CCB-BC-1	Does the bridge component support any of the common bridge component options?	O	5.8.3:a)	Yes [] No [] N/A []
CCB-BC-2	Does the bridge component support more than 4 but not more than 8 egress queues?	O	5.8.3:b)	Yes [] No [] N/A []
CCB-BC-3	State the number of egress queues supported by the bridge component.	CCB-BC-2:M	5.8.3:b)	Number ____
CCB-BC-4	Does the bridge component support more than 1 PTP instance?	O	5.8.3:c)	Yes [] No [] N/A []
CCB-BC-5	State the number of PTP instances supported by the bridge component.	CCB-BC-4:M	5.8.3:c)	Number ____
CCB-BC-6	Does the bridge component support enhancements for scheduled traffic?	O	5.8.3:d)	Yes [] No [] N/A []
CCB-BC-7	Does the bridge component support frame preemption?	O	5.8.3:e)	Yes [] No [] N/A []

5882

5883

5884 **A.7 End Station Component**

5885 **A.7.1 Instructions**

5886 One instance of Clause A.7 shall be filled out per end station component implemented by an
5887 IA-station.

5888 **A.7.2 Common End Station Component Requirements**

5889 The form in Table A.14 is used to indicate common requirements for end station components.

5890 **Table A.14 – Common End Station Component Requirements**

Item	Feature	Status	References	Support
ESC-1	Does the end station component support the common end station component requirements?	M	5.9.1	Yes []
ESC-2	Does the end station component support the ccA end station component requirements?	O.3	5.9.2	Yes [] No []
ESC-3	Does the end station component support the ccB end station component requirements?	O.3	5.9.3	Yes [] No []

5891

5892 **A.7.3 Common End Station Component Options**

5893 The form in Table A.15 is used to indicate options for end station components.

5894 **Table A.15 – Common End Station Component Options**

Item	Feature	Status	References	Support
ESC-4	Does the end station component support the operation of the credit-based shaper?	O	5.10.1:a)	Yes [] No []
ESC-5	Does the end station component support talker end system behaviors?	O	5.10.1:b)	Yes [] No []
ESC-6	Does the end station component support listener end system behaviors?	O	5.10.1:c)	Yes [] No []

5895

5896 **A.7.4 ccA End Station Component Options**

5897 The form in Table A.16 is used to indicate options for end station components conforming to
5898 conformance class A.

5899 **Table A.16 – ccA End Station Component Options**

Item	Feature	Status	References	Support
CCA-ESC-1	Does the end station component support any of the common end station component options?	O	5.10.2:a)	Yes [] No [] N/A []
CCA-ESC-2	Does the end station component support more than 2 PTP instances?	O	5.10.2:b)	Yes [] No [] N/A []
CCA-ESC-3	State the number of PTP instances supported by the end-station component.	CCA-ESC-2:M	5.10.2:b)	Number _____
CCA-ESC-4	Does the end station component support enhancements for scheduled traffic for data rates 10 Mb/s, 2,5 Gb/s, 5 Gb/s, or 10 Gb/s?	O	5.10.2:c)	Yes [] No [] N/A []
CCA-ESC-5	Does the end station component support requirements for frame pre-emption for data rates 10 Mb/s, 2,5 Gb/s, 5 Gb/s, or 10 Gb/s?	O	5.10.2:d)	Yes [] No [] N/A []

5900

5901 **A.7.5 ccB End Station Component Options**

5902 The form in Table A.17 is used to indicate options for end station components conforming to
5903 conformance class B.

5904

Table A.17 – cCB End Station Component Options

Item	Feature	Status	References	Support
CCB-ESC-1	Does the end station component support any of the common end station component options?	O	5.10.3:a)	Yes [] No [] N/A []
CCB-ESC-2	Does the end station component support one or more PTP instances?	O	5.10.3:b)	Yes [] No [] N/A []
CCB-ESC-3	State the number of PTP instances supported by the end-station component.	CCB-ESC-2:M	5.10.3:b)	Number ____
CCB-ESC-4	Does the end station component support enhancements for scheduled traffic?	O	5.10.3:c)	Yes [] No [] N/A []
CCB-ESC-5	Does the end station component support requirements for frame preemption?	O	5.10.3:d)	Yes [] No [] N/A []

5905

5906
5907
5908
5909

Annex B
(informative)

Representative Configuration Domain

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, and
 - 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, and
 - 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, and
 - 4 Talker and 4 Listener streams in case of seamless redundancy.
- Example calculation of data flow quantities for eight PLCs – without seamless redundancy:
 - $8 \times 512 \times 2$ = 8 192 streams for C2D communication,
 - $8 \times 64 \times 2$ = 1 024 streams for C2C communication, and
 - $(8 \times 192 + 1 \times 1024) \times 2 \times 000$ = 18 432 000 octets data for all streams.

5927

5928
5929
5930
5931

Annex C (informative)

Description of Clock Control System

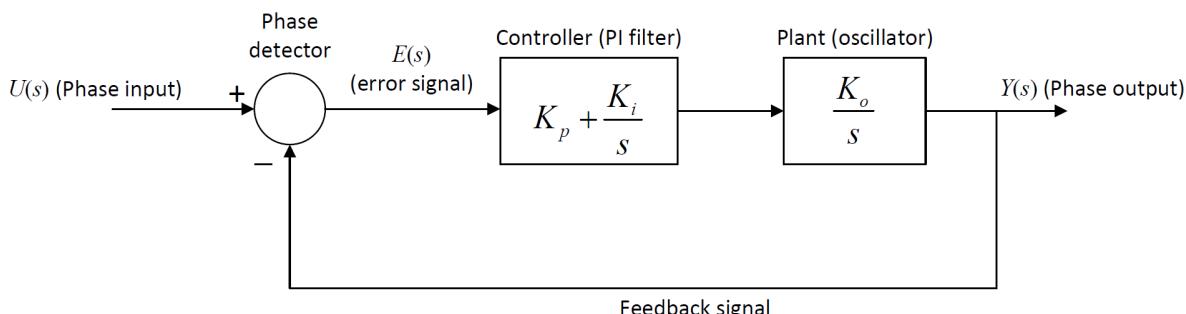
5932

C.1 Clock control system introduction

5933 Annex C provides an introductory discussion of a basic clock control system. For more detailed
5934 information, see the Bibliography References for Annex C.

5935

5936 Figure C.1 shows a basic control system model that uses a proportional plus integral (PI)
5937 controller. This is meant to be reference model, i.e., it is not meant to specify an implementation.
5938 Requirements for the clock control system can be expressed using parameters (e.g., 3dB
5939 bandwidth, gain peaking, frequency response) that are based on this reference model. Any
5940 implementation whose parameters are within the requirements is considered to be acceptable.
5941 For example, the model of Figure C.1 is expressed in the analog domain (i.e., s-domain), and
5942 will be shown shortly to be second order. An actual implementation can be digital, and can be
5943 higher order, as long as it meets the respective requirements.



5944

5945

5946 **Figure C.1 – Reference model for clock control system**

5947 In Figure C.1, the plant, i.e., the entity being controlled, represents the clock oscillator. It is
5948 desired that the phase output, $y(t)$ of the oscillator follows the phase input, $u(t)$, as closely as
5949 possible (the signals are shown in the frequency domain (i.e., as Laplace Transforms) in
5950 Figure C.1; however, they can equivalently be expressed in the time domain, with t representing
5951 time). The parameter K_o is the oscillator gain; the oscillator frequency is equal to the oscillator
5952 input multiplied by K_o . In some implementations the input signal to the oscillator is a voltage,
5953 and the oscillator is referred to as a voltage-controlled oscillator (VCO). However, other
5954 implementations are possible, e.g., digital implementations, where the oscillator is a digital
5955 controlled oscillator (DCO). Since the input to the oscillator depends on the implementation, it
5956 is not labeled in Figure C.1.

5957

5958 The control system of Figure C.1 uses negative feedback to enable the phase output to follow
5959 the phase input. The phase detector computes the difference between the input and output
5960 signals to produce the error signal $e(t)$. The error signal is then filtered by the PI filter to produce
5961 the input to the oscillator. The filter is referred to as a PI filter because its output is the sum of
5962 the proportional gain, K_p , multiplied by the error signal and the integral gain, K_i , multiplied by
5963 the integral of the error signal. The gains K_o , K_p , and K_i must be chosen such that the
5964 performance of the control system is acceptable, i.e., the time-domain behavior of the output
5965 with respect to the input is acceptable. However, an alternative set of parameters, which are
5966 more convenient, can be defined in terms of K_o , K_p , and K_i ; this is done in Clause C.2.

5967

5968 **C.2 Transfer function for control system**

5969 From the block diagram of Figure C.1, the input and output are related by:

5970

$$Y(s) = \left(K_p + \frac{K_i}{s} \right) \left(\frac{K_o}{s} \right) (U(s) - Y(s)) \quad (\text{C.1})$$

5971

5972 where

5973 $Y(s)$ is the phase output, expressed in the s-domain;5974 $U(s)$ is the phase input, in the s-domain;5975 K_p is the proportional gain;5976 K_i is the integral gain;5977 K_o is the oscillator gain.

5978

5979 or

$$Y(s) = \frac{\left(K_p + \frac{K_i}{s} \right) \left(\frac{K_o}{s} \right)}{1 + \left(K_p + \frac{K_i}{s} \right) \left(\frac{K_o}{s} \right)} U(s) \quad (\text{C.2})$$

5980

5981

5982 This can be simplified by multiplying the numerator and denominator by s^2 to produce:

5983

$$Y(s) = H(s)U(s) \quad (\text{C.3})$$

5984

5985 where the transfer function $H(s)$ is given by:

5986

$$H(s) = \frac{K_p K_o s + K_i K_o}{s^2 + K_p K_o s + K_i K_o} \quad (\text{C.4})$$

5987

5988 In Formula (C.4), the parameter K_o does not appear independently of K_p and K_i ; rather, only
 5989 the products $K_p K_o$ and $K_i K_o$ appear. The plant and PI filter could have been combined in the
 5990 model of Figure C.1; this is consistent with the fact that the exact nature of the signal between
 5991 the PI filter and plant is unimportant in this reference model. The units of $K_p K_o$ are (time)⁻¹ and
 5992 the units of $K_i K_o$ are (time)⁻². The frequency units need to be the same as the units of s , e.g., if
 5993 s has units rad/s, then $K_p K_o$ has units rad/s and $K_i K_o$ has units (rad/s)². The integration operation

5994 in the plant results in the transfer function being dimensionless, which is consistent with the
 5995 fact that the input and output of the control system both have units of phase.

5996

5997 The transfer function can be expressed in an equivalent form by defining the undamped natural
 5998 frequency, ω_n , and damping ratio, ζ :

$$H(s) = \frac{2\zeta\omega_n s + \omega_n^2}{s^2 + 2\zeta\omega_n s + \omega_n^2} \quad (\text{C.5})$$

5999

6000 where

6001 ζ is the damping ratio;

6002 ω_n is the undamped natural frequency expressed in rad/s.

6003

6004

6005 And, ζ and ω_n are given by:

$$\omega_n = \sqrt{K_i K_o} \quad (\text{C.6})$$

$$\zeta = \frac{K_p K_o}{2\sqrt{K_i K_o}} = \frac{K_p}{2} \sqrt{\frac{K_o}{K_i}} \quad (\text{C.7})$$

6006

6007 In the Formula (C.7), the first form shows explicitly that ζ depends only on the products $K_p K_o$
 6008 and $K_i K_o$.

6009 C.3 Frequency response for control system

6010 The frequency response is obtained by setting $s = j\omega$ in Formula (C.5) and taking the absolute
 6011 value (here j rather than i is used for $\sqrt{-1}$ to avoid confusion with other uses of i), where ω is
 6012 the frequency in rad/s. The result is:

$$|H(j\omega)| = \left| \frac{2\zeta\omega_n \omega j + \omega_n^2}{-\omega^2 + \omega_n^2 + 2\zeta\omega_n \omega j} \right| = \left(\frac{4\zeta^2 \omega_n^2 \omega^2 + \omega_n^4}{(\omega_n^2 - \omega^2)^2 + 4\zeta^2 \omega_n^2 \omega^2} \right)^{1/2} \quad (\text{C.8})$$

6013

6014 Dividing the numerator and denominator of Formula (C.7) by ω_n^4 and defining the dimensionless
 6015 frequency $x = \omega/\omega_n$ produces:

6016

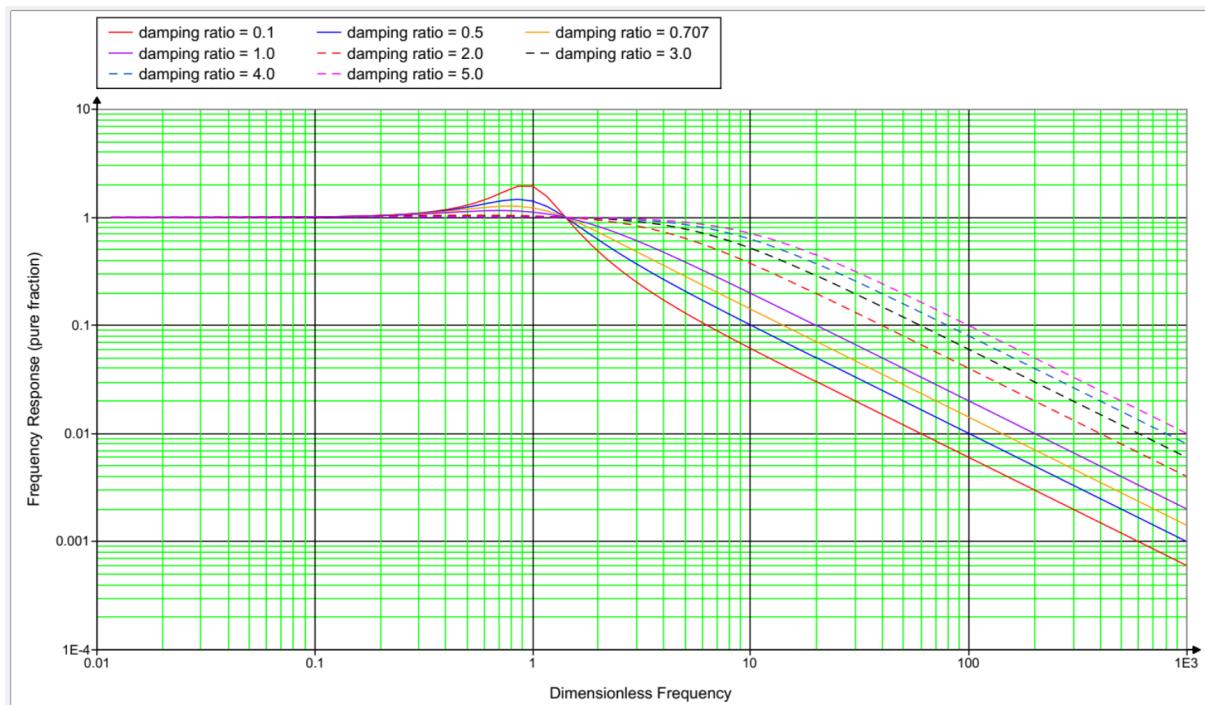
$$|H(j\omega)| = \left(\frac{4\zeta^2 x^2 + 1}{(1 - x^2)^2 + 4\zeta^2 x^2} \right)^{1/2} \quad (\text{C.9})$$

6017

6018 where

6019 ζ is the damping ratio;6020 ω is the frequency expressed in rad/s;6021 $x = \omega/\omega_n$.

6022 Figure C.2 contains plots of frequency response (Formula (C.9)) versus dimensionless
 6023 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,
 6024 and 5.0. It is seen that the frequency response is very close to 1 for values of dimensionless
 6025 frequency much less than 1 (i.e., for $\omega \ll \omega_n$). The frequency response increases as the
 6026 frequency approaches the undamped natural frequency (i.e., as dimensionless frequency
 6027 approaches 1) and reaches a peak for dimensionless frequency slightly less than 1. The
 6028 frequency response then decreases, eventually having a slope (i.e., roll-off) of 20 dB/decade
 6029 (i.e., frequency response decreases by a factor of 10 for every factor of 10 increase in x for
 6030 $x > 1$). Figure C.3 shows the detail of frequency response for x in the range 0.1 to 10.



6031

6032 **Figure C.2 – Frequency response for the control system of Figure C.1**

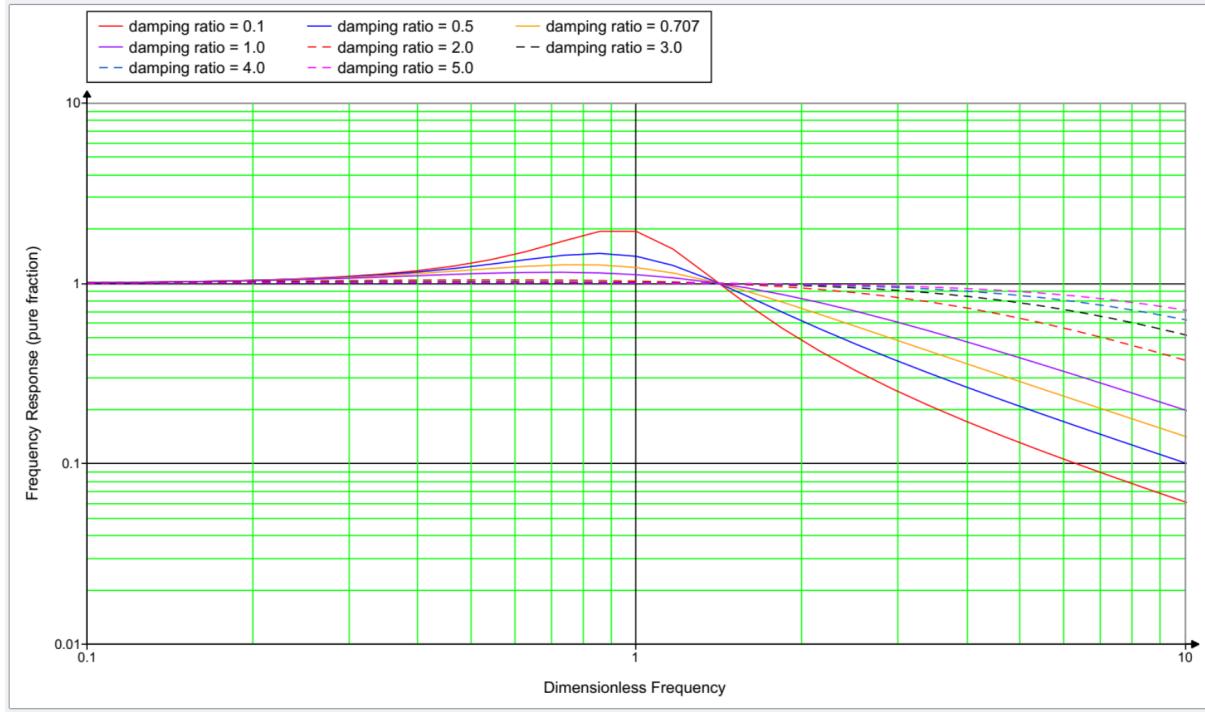


Figure C.3 – Detail of frequency response for the control system of Figure C.1 for dimensionless frequency in the range 0,1 to 10

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 Formula (C.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 Formula (C.8) equal to $10^{-3/10}$ and solving for x . Now, $10^{-3/10}$ is approximately equal to 0,501 2, i.e., it is very close to $\frac{1}{2}$. Then the 3dB bandwidth can be obtained by solving the following formula for x in terms of ζ :

$$\frac{4\zeta^2x^2 + 1}{(1 - x^2)^2 + 4\zeta^2x^2} = \frac{1}{2} \quad (\text{C.10})$$

or

$$x^4 - 2(2\zeta^2 + 1)x^2 - 1 = 0 \quad (\text{C.11})$$

The result is:

$$x = \left[2\zeta^2 + 1 + \sqrt{(2\zeta^2 + 1)^2 + 1} \right]^{1/2} \quad (\text{C.12})$$

or

$$\omega_{3\text{dB}} = \omega_n \left[2\zeta^2 + 1 + \sqrt{(2\zeta^2 + 1)^2 + 1} \right]^{1/2} \quad (\text{C.13})$$

6051

6052 The gain peaking is the maximum value of the frequency response, in dB. It is computed by
 6053 differentiating Formula (C.8) with respect to x , setting the result to zero, solving for x , and then
 6054 substituting this value of x into Formula (C.8) to obtain the maximum. The result is:

$$H_p = [1 - 2\alpha - 2\alpha^2 + 2\alpha(2\alpha + \alpha^2)^{1/2}]^{-1/2} \quad (\text{C.14})$$

6055

6056

6057 where α is related to damping ratio by:

$$\alpha = \frac{1}{4\zeta^2} \quad (\text{C.15})$$

6058

6059

6060 and H_p is the gain peaking expressed as a pure fraction. The gain peaking in dB is equal to
 6061 $20 \cdot \log_{10} H_p$. In some cases, it is necessary to compute damping ratio from gain peaking. The
 6062 result for this is:

$$\alpha = \frac{(1 - q)(1 + \sqrt{1 - q})}{2q} \quad (\text{C.16})$$

6063

6064 where

$$q = \frac{1}{H_p^2} \quad (\text{C.17})$$

6065

6066

6067 Damping ratio is obtained from α using Formula (C.15).

6068

6069 If 3dB bandwidth and gain peaking are given, damping ratio can be obtained using Formulas
 6070 (C.15) through (C.17). Undamped natural frequency can then be obtained using Formula (C.13).

6071

6072 Figure C.4 shows gain peaking, expressed as a pure fraction, as a function of damping ratio.
 6073 Figure C.5 shows gain peaking in dB as a function of damping ratio.

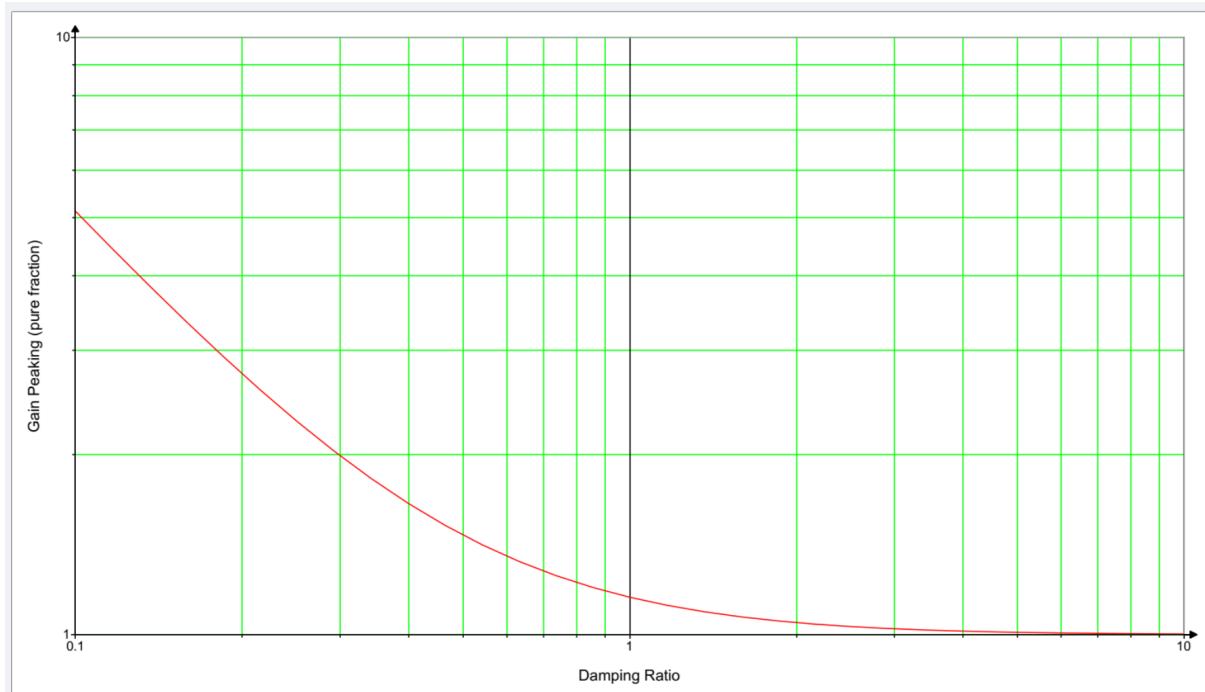


Figure C.4 – Gain peaking (pure fraction) as a function of damping ratio

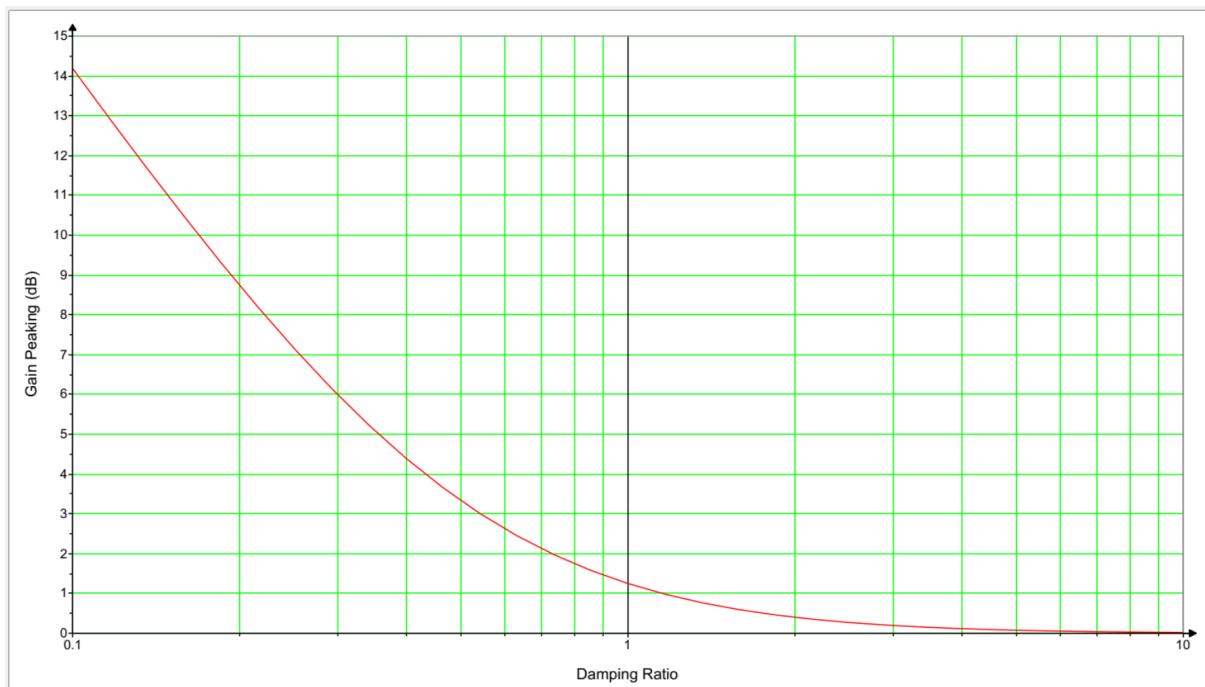


Figure C.5 – Gain peaking in dB as a function of damping ratio

The performance of the clock control system can be described using the frequency response as follows:

- 6081 a) Maximum 3dB bandwidth in Hz,
- 6082 b) Maximum gain peaking in dB, and
- 6083 c) Frequency response plot (mask) corresponding to (a) and (b) that is not to be exceeded.

6084 **C.4 Example**

6085 Consider a clock control system with $K_p K_o = 4,23 \text{ rad/s}$ and $K_i K_o = 9,62 (\text{rad/s})^2$. The undamped
6086 natural frequency and damping ratio are:

$$\omega_n = \sqrt{K_i K_o} = \sqrt{9,62 (\text{rad/s})^2} = 3,10 \text{ rad/s} \quad (\text{C.18})$$

$$\zeta = \frac{K_p K_o}{2\sqrt{K_i K_o}} = \frac{4,23 \text{ rad/s}}{2\sqrt{9,62 (\text{rad/s})^2}} = 0,682 \quad (\text{C.19})$$

6087

6088 The gain peaking is obtained from:

$$\alpha = \frac{1}{4(0,682)^2} = 0,537 \quad (\text{C.20})$$

$$H_p (\text{purefraction}) = [1 - 2(0,537) - 2(0,537)^2 + 2(0,537)\sqrt{2(0,537) + (0,537)^2}]^{-\frac{1}{2}} = 1,288\ 03 \quad (\text{C.21})$$

$$H_p (\text{dB}) = 20 \log_{10}(1,288\ 03) \text{ dB} = 2,2 \text{ dB} \quad (\text{C.22})$$

6089

6090 The 3dB bandwidth is:

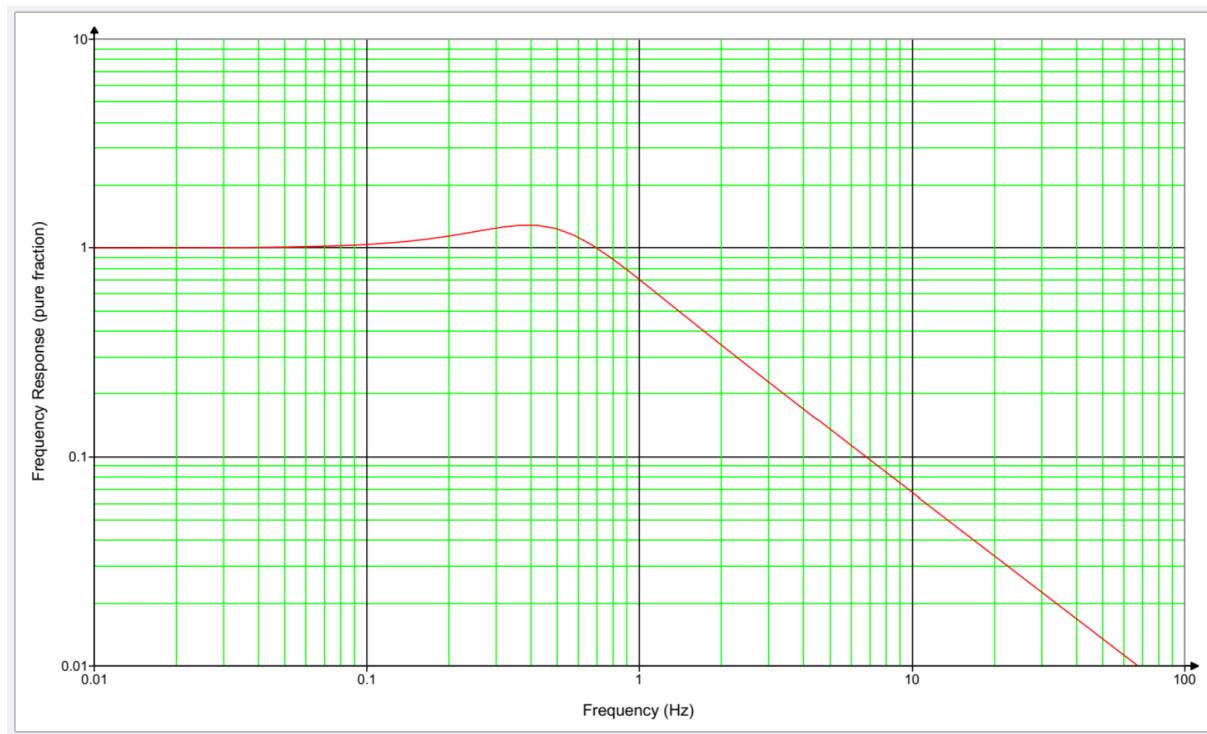
$$f_{3\text{dB}} (\text{Hz}) = \frac{\omega_n}{2\pi} [1 + 2\zeta^2 + \sqrt{(1 + 2\zeta^2)^2 + 1}]^{1/2} \quad (\text{C.23})$$

$$\begin{aligned} 6091 &= \frac{3,10}{2\pi} [1 + 2(0,682)^2 + \sqrt{(1 + 2(0,682)^2)^2 + 1}]^{1/2} \\ 6092 &= 1,0 \text{ Hz} \end{aligned}$$

6093

6094

6095 The frequency response is shown in Figure C.6.



6096

6097

Figure C.6 – Example Frequency response

6098
6099
6100
6101
6102
6103

Annex D (informative)

Time Synchronization Annex

D.1 Overview

Annex D describes how a network of compliant devices can achieve a time synchronization accuracy, at the application level, of $\pm 1 \mu\text{s}$, relative to the Clock Source at the Grandmaster, over 100 network hops. To achieve this, it allocates the overall error budget of 1 000 ns as described in Table D.1.

Table D.1 – Time Synchronisation Error Budget

Network Aspect	Error Type	Network-Level Error Budget (ns)
All PTP Instances	Constant Time Error	200
	Dynamic Time Error	600
All PTP Links	Constant Time Error	200
	Dynamic Time Error	

A chain of 1 Grandmaster PTP Instance, 99 PTP Relay Instances and 1 PTP End Instance (100 network hops) that all comply with the normative requirements of 6.2.2, 6.2.3, 6.2.4, and 6.2.5 will generate a network-level Time Error at or below the Error Budget for All PTP Instances.

Clause D.2 describes the principles of operation this document assumes.

Clause D.3 provides additional information on specific normative requirements.

The principles of operation include the use of crystal oscillators (XOs) as opposed to more accurate, stable, and costly options such as temperature-compensated crystal oscillators (TCXOs).

Clause D.4 describes a potential approach to testing the normative requirements. It is not a test specification, but rather a high-level overview of one potential approach that might be adopted by a full test specification.

The use of XOs means that some of the normative requirements are difficult or impossible to meet without employing algorithms that track Neighbor Rate Ratio drift and Rate Ratio drift and compensate for consequent errors in calculating Rate Ratio and Correction Field.

Clause D.5 provides examples of algorithms that can be used for this purpose, and which have been shown to enable compliance with the normative requirements.

Implementations that employ TCXOs or other more accurate, stable oscillators can still find some of the normative requirements difficult or impossible to meet without employing algorithms to track and compensate for errors due to clock drift. This is because other PTP Instances that use XOs can still cause the implementation to experience Neighbor Rate Ratio drift, Rate Ratio drift or both.

There is no normative requirement to use the algorithms described in Clause D.5; an implementation can employ alternative algorithms provided the normative requirements are met. Clause D.5 describes the potential risks of deploying a network whose instances employ a mix of different algorithms. It is the responsibility of implementers to mitigate the risks and ensure alternative algorithms deliver the desired network-level performance.

6136 This document does not include normative requirements for PTP Links. Annex D.2.4 describes
 6137 PTP Link characteristics that influence achieving 1 μ s time synchronization accuracy. It
 6138 includes some examples using common PTP Link characteristics.

6139 This document's normative requirements regarding instance-level error generation are
 6140 necessitated by the need to ensure not just an overall level of dTE generation at each node,
 6141 but also the performance of drift tracking and error compensation algorithms and the amount of
 6142 dTE generation due to timestamp error versus clock drift. The algorithms are employed to
 6143 mitigate errors due to clock drift but cannot mitigate timestamp errors.

6144 **D.2 Principles of Operation**

6145 **D.2.1 General**

6146 Achieving $\pm 1 \mu$ s time synchronisation accuracy across 100 network hops involves managing
 6147 the accumulation of errors in the preciseOriginTimestamp plus correctionField and the Rate
 6148 Ratio as they are passed, via Sync or Follow_Ups messages, down the chain of PTP instances
 6149 and are then used by the PTP End Instance to keep its ClockTarget in line with the ClockSource
 6150 at the Grandmaster PTP Instance. The majority of significant errors can ultimately be traced
 6151 back to one of three sources: timestamp error, clock drift, or path delay asymmetry. The
 6152 selection of PTP protocol parameters often involves trading off one source of error against the
 6153 other. This document requires specific PTP protocol configurations, and assumes the use of
 6154 mechanisms (algorithms), that reduce dTE due to timestamp error but would also – without
 6155 additional measures – increase dTE due to clock drift to the point where the latter exceeds the
 6156 allocated error budget. However, this document also assumes additional measures to minimise
 6157 some sources of dTE due to clock drift, and mechanisms and to track and compensate for errors
 6158 from other sources to a sufficient degree that the error budget is not exceeded.

6159 The specific protocol configurations and other measures, along with their intended effects, are
 6160 described in Table D.2.

6161 **Table D.2 – Protocol configurations & other measures to achieve dTE budget**

Configuration or Measure	Description and Intended Effect(s)
Sync Interval 125 ms	<p>Effects:</p> <ol style="list-style-type: none"> 1. Calibrate the balance between dTE from timestamp error vs error due to clock drift. Larger intervals lead to less timestamp error and more error due to clock drift. 2. Keep below acceptable limits the impact of errors in Rate Ratio and Rate Ratio Drift estimation when keeping ClockTarget in line with ClockSource between arrival of Sync messages. Larger intervals increase the impact of any errors.
Drift_Tracking TLV - syncEgressTimestamp	<p>Effect:</p> <p>Enables calculation of NRR using Sync message timestamps, which eliminates error due to NRR clock drift that would otherwise occur between calculation of NRR using Pdelay_Resp messages and use during Sync message processing (i.e. calculation of Rate Ratio and output Correction Field values)</p>
NRR Smoothing	<p>Description:</p> <p>Algorithm to use timestamps from multiple past Sync messages to estimate NRR drift rate and then apply compensation to correct for consequent errors in NRR Smoothing calculation.</p> <p>Effect:</p> <p>Reduce the amount of error in the estimate of NRR due to timestamp error while increasing the amount of error due to clock drift.</p>
NRR Drift Tracking & Compensation	<p>Description:</p> <p>Algorithm to use timestamps from multiple past Sync messages to estimate NRR drift rate and then apply compensation to correct for consequent errors in NRR Smoothing calculation.</p> <p>Effect:</p> <p>Mitigate the effect of errors due to clock drift when calculating and using the estimated NRR.</p>

Drift_Tracking TLV – rateRatioDrift	<p>Description:</p> <p>Carries estimate of Rate Ratio drift rate from one node to the next.</p> <p>Effect:</p> <p>Allows each node to estimate its own Rate Ratio drift rate by combining the incoming Rate Ratio drift rate with the local estimate of NRR drift rate.</p>
RR Drift Compensation	<p>Description:</p> <p>Algorithm that uses the estimate of RR drift rate to compensate for that drift, adjusting the estimated RR over time according to the drift rate.</p> <p>Effect:</p> <p>For PTP Relay Instances, minimises errors in the Correction Field caused by Rate Ratio drift.</p> <p>For PTP End Instances, a similar approach can reduce errors in keeping ClockTarget in line with ClockSource between arrival of Sync messages, but is outside the scope of this document.</p>
Pdelay Interval Consistency	<p>Description:</p> <p>This document requires tighter control of the interval between Pdelay messages generated at the Grandmaster PTP Instance than the defaults in IEEE Std 802.1AS-2020.</p> <p>Effect:</p> <p>This document requires the use of Sync messages to calculate NRR (see above). However, when a sufficient number of Sync messages are not available, for example on startup or after a reconfiguration, Pdelay_Resp messages can be used instead. In such cases, errors due to clock drift at Relay Instances have a tendency to cancel out. A clock drift that generates a positive error in NRR measurement on receipt of a Pdelay_Resp message generates a negative error in NRR measurement at the next node. The degree of cancellation depends on the consistency of the intervals over which NRR is measured at neighboring nodes. Tighter control of the Pdelay Interval increases the consistency of the measurement interval and thus decreases the amount of error.</p>
Mean Residence Time	<p>Description:</p> <p>This document defines a mean Residence Time requirement, which is significantly lower than the default maximum Residence Time in IEEE Std 802.1AS-2020.</p> <p>Effect:</p> <p>The amount of error in the Correction Field at the PTP End Instance due to clock drift is proportional to the cumulative meanLinkDelay and residenceTime experienced by a Sync message during transit from the Grandmaster PTP Instance to the PTP End Instance. Specifying a lower mean residenceTime reduces this source of error.</p>

6162

6163 **D.2.2 Grandmaster PTP Instance Implementation**

6164 Depending on implementation, a Grandmaster PTP Instance can:

- 6165 a) Contain a single oscillator used for both Local Clock and Clock Source,
- 6166 b) Contain separate oscillators for Local Clock and Clock Source, or
- 6167 c) Contain only an oscillator for Local Clock and accept an external input for Clock Source.

6168 In some cases, a Grandmaster PTP instance can support more than one mode of operation and
 6169 transition between them depending on changes in network configuration (see Splitting, Joining
 6170 and Aligning Time Domains).

6171 In the first case the rateRatio and rateRatioDrift fields transmitted by the Grandmaster PTP
 6172 Instance will be zero, reflecting the fact there is no difference between the Local Clock and
 6173 Clock Source frequencies.

6174 In the second and third cases there can be differences between the Local Clock and Clock
 6175 Source frequencies. Any differences will be reflected in the rateRatio and rateRatioDrift fields
 6176 transmitted by the Grandmaster PTP Instance. This means that the Grandmaster PTP instance

6177 will track rateRatio over time in order to calculate rateRatioDrift, similarly to PTP Relay
6178 Instances and PTP End Instances. The exact implementation can vary.

6179 **D.2.3 Splitting, Joining and Aligning Time Domains**

6180 Modular machines or production cells can allow the splitting and combining of machines if this
6181 is required by the production process. When separate, the ClockSources of two machines run
6182 separately, each with its own time domain. If both ClockSources are traceable to the same PTP
6183 timescale, the difference between the ClockSources can be relatively small. If traceable to
6184 different timescales, especially if one or both are ARB timescales, there can be a very large
6185 difference between the ClockSources.

6186 When two machines are joined, the first machine's time domain remains unaffected, and it can
6187 continue operation without disruption. There are two typical approaches to how the second
6188 machine behaves. In the first case, at a time of the end user's choosing, the second machine's
6189 time domain ceases to exist, with its PTP Instances becoming part of the first machine's time
6190 domain. In the second case, the second machine's time domain is gradually aligned with the
6191 first machine's time domain such that control loop cycles are coordinated. In the first case the
6192 second machine's time domain is unaffected, and it can continue production even if the
6193 machines are accidentally connected, until the end user chooses to join the time domains. In
6194 the second case the second machine can continue production while its time domain is being
6195 aligned.

6196 **D.2.3.1 Joining Machines with Single Time Domain**

6197 In the first case, where the second machine's time domain ceases to exist, a discontinuity in
6198 timing for the second machine's PTP Instances can occur, as they switch to use the first
6199 machine's Grandmaster. Some implementations implement measures to limit such timing
6200 discontinuities, but these measures are outside the scope of this document. Typically, in this
6201 case, the second machine is not operational while it is joined to the first. It resumes operation
6202 once its PTP Instances have synchronized with the first machine's Grandmaster.

6203 **D.2.3.2 Joining Machines with Multiple Coordinated Time Domains**

6204 In the second case, where the second machine's time domain is gradually aligned with the first
6205 machine's time domain, this typically requires both machines to be implementing the same
6206 control loop cycle time. The goal is that, once coordinated, each control loop cycle of the first
6207 machine will be aligned with the start of a control loop cycle of the second machine, even though
6208 the two machines maintain separate time domains and there can be a large time difference
6209 between their Clock Sources.

6210 In this case, after being joined together, the first machine effectively drives the second
6211 machine's Clock Source faster or slower, during an alignment period, until coordination is
6212 achieved. During the alignment period, this drive from the first machine can result in the second
6213 machine's Clock Source temporarily exceeding the usual normative requirement on range of
6214 fractional frequency offset relative to the nominal frequency of ± 50 ppm. The usual normative
6215 requirement on range of rate of change of fractional frequency offset of ± 1 ppm/s, applicable
6216 when split (i.e. independent) or coordinated (i.e. joined and stable, after the alignment period),
6217 may also be temporarily exceeded. However, if the value stays within the range ± 3 ppm/s, the
6218 network-level performance of 1 μ s time synchronisation accuracy can be maintained. For this
6219 reason, this document specifies a separate normative requirement for temporary, externally
6220 driven, rate of rate of change of fractional frequency offset.

6221 Since the second machine experiences no time discontinuities and the network-level
6222 performance is maintained the second machine can, if desired, continue operation during the
6223 alignment period.

6224 Once coordinated, the first machine continues to drive the Clock Source of the second machine
6225 to maintain coordination. In this stable, coordinated mode of operation the normal range of ± 1
6226 ppm/s is not exceeded.

6227 The mechanism by which the first machine drives the Clock Source of the second machine is
6228 not addressed in this document.

6229 **D.2.3.3 Splitting Machines**

6230 In the first case, where the second machine's time domain ceased to exist while joined to the
6231 first, splitting machines means that the second machine must create its own time domain again.
6232 The second machine's Clock Source typically starts at the PTP Grandmaster Instance's last,
6233 best estimate of the first machine's Clock Source. The goal is for no discontinuities in time
6234 sync to occur; however, depending on implementation, it can take some time to before the time
6235 synchronization accuracy of all the second machine's PTP Instances relative to its Grandmaster
6236 can be relied upon. For this reason, it is possible the second machine is not operational during
6237 the split. Hot Standby can be employed to mitigate this transition time, but the details of how
6238 to do so are out of scope for this document.

6239 In the second case, where the second machine maintains its time domain while joined to the
6240 first, splitting machines means that the first machine ceases driving the second machine's Clock
6241 Source to maintain coordination of control loop cycle times. Without this drive, the two time
6242 domains can drift relative to each other resulting in loss of coordination. Time synchronization
6243 performance within the second machine is maintained during the split and the second machine
6244 can, if desired, continue operation throughout the process.

6245 **D.2.4 PTP Link Characteristics**

6246 A vast majority of time synchronization error due to PTP link characteristics is caused by
6247 asymmetrical path delay in one direction versus the other. The mechanism to measure path
6248 delay assumes the link is symmetrical and cannot detect asymmetry, thus asymmetry causes
6249 an error. The potential maximum asymmetry and thus error typically scales linearly with
6250 physical path length.

6251 The error budget due to PTP link characteristics for an entire network is 200 ns. In any specific
6252 network this budget can be allocated as required with some links allocated a higher budget
6253 (typically longer length) than others.

6254 A typical specified maximum delay skew for Category 6 Ethernet cables is 50 ns per 100 m. If
6255 such cables are used, a maximum total cable length between Clock Source and Clock Target
6256 with 99 PTP Relay Instances between them (i.e. 100 network hops) is 400m. Extending the
6257 cable length beyond 400 m without jeopardizing network-level performance would require the
6258 use of cables with less delay skew or asymmetry compensation for delay skew.

6259 It is possible for the delay skew in one section of cable to cancel all or part of a delay skew in
6260 the opposite direction from prior section but, depending on how cables are manufactured and
6261 deployed, it is feasible for the delay skews of every cable segment between a Grandmaster
6262 PTP Instance and a PTP End Instance to be additive.

6263 **D.3 Notes on Normative Requirements**

6264 **D.3.1 Oscillator Requirements**

6265 Clock drift at the Grandmaster PTP Instance causes greater dTE than the same amount of clock
6266 drift at a PTP Relay Instance or the PTP End Instance. This document therefore requires tighter
6267 limits on maximum fractional frequency offset for an oscillator at the Grandmaster PTP Instance
6268 than at other instances.

6269 This document does not place requirements on operational temperature range or other
6270 environmental factors. The required oscillator behavior is delivered for the operational
6271 conditions across which a device claims it is compliant. These conditions typically include
6272 temperature range but can also include rate of change of ambient temperature, supply voltage
6273 stability, amount of vibration and others.

6274 **D.3.2 Timestamp Granularity Error**

6275 Timestamp Granularity Error (TSGE) is the error in timestamping each incoming and outgoing
6276 message due to the maximum timestamp resolution of which an implementation is capable. It
6277 is typically directly related to an implementation's clock rate.

6278 For example: a clock rate of 125 MHz typically results in a maximum resolution of 8 ns.
6279 Depending on implementation the consequent TSGE range can be -8 ns to 0 ns, 0 ns to 8 ns,

6280 or anything in between. In some implementations, offsets are applied to ensure the average
 6281 TSGE is 0 ns with, assuming uniform error distribution, a range of -4 ns to +4 ns

6282 Similarly, a clock rate of 500 MHz results in a maximum resolution of 2 ns; a consequent TSGE
 6283 range between -2 ns to 0 ns and 0 ns to 2 ns; and, if a suitable offset is applied to ensure a
 6284 TSGE average of 0 ns, a range of -1 ns to +1 ns.

6285 A minimum resolution of 8 ns, i.e. minimum clock rate of 125 MHz is assumed. It is further
 6286 assumed that TSGE for the sum of the preciseOriginTimestamp and followUpCorrectionField at
 6287 the Grandmaster PTP Instance (see IEEE Std 802.1AS-2020, 10.2.9.2.1) has an average of 0
 6288 ns and that the TSGE averages for other timestamps are stable and consistent across all a PTP
 6289 Instance's ports. No assumption needs to be made regarding the value of the TSGE average
 6290 for these other timestamps as they are always used to measure intervals such that any stable,
 6291 consistent offset will cancel out.

6292 **D.3.3 Dynamic Timestamp Error**

6293 Dynamic Timestamp Error (DTSE) is the, effectively random, error in timestamping each
 6294 incoming and outgoing event message due to an implementation's inherent inaccuracies,
 6295 excluding TSGE. It is assumed to vary between a minimum of -6 ns and a maximum of + 6 ns
 6296 with an average of 0 ns. Lower levels of DTSE are better.

6297 If an implementation timestamps an incoming or outgoing message at a point other than the
 6298 PHY, any variability in delay between that point and the PHY (PHY delay) will translate to DTSE.
 6299 Some common implementations were not designed to limit this variability. If care is not taken
 6300 to avoid implementations with high variability, the assumed DTSE range is easily exceeded.
 6301 Such implementations will find some of the normative requirements difficult or impossible to
 6302 meet.

6303 **D.3.4 Grandmaster PTP Instance Error Generation**

6304 Table 12 sets normative requirements for error generation at a Grandmaster PTP Instance that
 6305 ensure the relevant fields in the Sync and Follow_Up messages it transmits are sufficiently
 6306 accurate to deliver the network-level performance. Table D.3 describes how the normative
 6307 requirements align with major sources of error.

6308 **Table D.3 – Protocol configurations & other measures to achieve dTE budget**

Item	Normative Requirement	Main Sources of Error
1	preciseOriginTimestamp + correctionField vs Direct measurement of Working Clock at Grandmaster (acting as a Clock Source)	Timestamp Error relative to Clock Source plus accuracy measuring any internal delay between generation of the preciseOriginTimestamp and Sync message transmission.
2	rateRatio vs Direct measurement of Rate Ratio of Clock Source vs Local Clock	Accuracy of internal mechanism to measure Rate Ratio of Clock Source vs. Local Clock, potentially including algorithms that track RateRatioDrift and modify Rate Ratio accordingly ^a
3	syncEgressTimestamp vs Direct measurement of Local Clock	Timestamp Error relative to Local Clock

^aOnly applicable if Clock Source and Local Clock are not locked to the same frequency by the implementation. If they are locked, then rateRatio will be 0 ppm and rateRatioDrift will be 0 ppm/s.

6309

6310 **D.3.5 PTP Relay Instance Error Generation**

6311 Table 13 sets normative requirements for error generation at a PTP Relay Instance that ensure
 6312 the relevant fields in the Sync and Follow_Up messages it transmits as part of Sync processing
 6313 are sufficiently accurate to deliver the network-level time sync performance. The requirements
 6314 include the ability to mitigate errors in rateRatio and rateRatio drift that would otherwise occur
 6315 due to clock drift at the current PTP Relay Instance, an adjacent PTP Relay Instance, or the

6316 Grandmaster PTP Instance. Table D.4 describes how the normative requirements align with
 6317 major sources of error.

6318 **Table D.4 – Protocol configurations & other measures to achieve dTE budget**

Item	Normative Requirement	Clock Drifts	Main Sources of Error
1	preciseOriginTimestamp + correctionField vs Direct measurement of Clock Source at Grandmaster PTP Instance	None	Timestamp Errors relative to Local Clock when measuring Residence Time, i.e. Sync message ingress and egress. Accuracy of meanLinkDelay measurement. Errors in Rate Ratio used when translating Residence Time measured in terms of Local Clock to Residence time in terms of Clock Source, although these are typically orders of magnitude smaller than those from Timestamp Errors.
2		None	Timestamp Error affecting measurement of NRR when there is no NRR Drift. The effect should be low. This normative requirement is a baseline for the next two requirements.
3		Clock Source (RR Drift)	Accuracy of measurement of NRR when there is no NRR Drift (as above). Accuracy of calculation of rateRatio, including algorithms for RR Drift tracking & error compensation.
4	rateRatio vs Direct measurement of Rate Ratio of Clock Source vs Local Clock	Clock Source and Local Clock at previous PTP Instance (RR Drift & NRR drift)	Accuracy of measurement of NRR when there is NRR Drift, including algorithms for NRR Drift tracking & error compensation Accuracy of calculation of rateRatio, including algorithms for RR Drift tracking & error compensation. Combined with test 3 this effectively requires a level of performance regarding NRR Drift tracking & error compensation, whether the source of the NRR drift is the Local Clock of the current PTP Instance or the previous PTP Instance.
5		None	Timestamp Error affecting measurement of NRR Drift when there is no NRR Drift. The effect should be low. This normative requirement is a baseline for the next two requirements.
6	rateRatioDrift vs Direct measurement of Rate Ratio Drift of Clock Source vs Local Clock	Clock Source (RR Drift)	Accuracy of measurement of NRR Drift when there is no NRR Drift (as above). Accuracy of calculation of rateRatioDrift, including algorithms for RR Drift tracking & error compensation.
7		Clock Source and Local Clock at	Accuracy of measurement of NRR Drift when there is NRR Drift, including

Item	Normative Requirement	Clock Drifts	Main Sources of Error
		previous PTP Instance (RR Drift & NRR drift)	algorithms for NRR Drift tracking & error compensation. Accuracy of calculation of rateRatioDrift, including algorithms for RR Drift tracking & error compensation. Combined with test 6 this effectively requires a level of performance regarding NRR Drift tracking & error compensation, whether the source of the NRR drift is the Local Clock of the current PTP Instance or the previous PTP Instance.
8	syncEgressTimestamp vs Direct measurement of Local Clock	None	Timestamp Error relative to Local Clock

6319

6320 D.3.6 PTP End Instance Error Generation

6321 Table 14 sets normative requirements for error generation at a PTP End Instance that ensure
 6322 the ClockTarget it generates from incoming Sync and Follow_Ups messages is sufficiently
 6323 accurate to deliver the network-level time sync performance. Table D.5 describes how the
 6324 normative requirements align with major sources of error.

6325 **Table D.5 – Protocol configurations & other measures to achieve dTE budget**

Item	Normative Requirement	Clock Drifts	Main Sources of Error
1	ClockTarget vs ClockSource	None	Timestamp Error affecting measurement of NRR Drift when there is no NRR Drift. The effect should be low. This normative requirement is a baseline for the next two tests.
2		Clock Source (RR Drift)	Accuracy of measurement of NRR Drift when there is no NRR Drift (as above). Accuracy of calculation of rateRatioDrift, including algorithms for RR Drift tracking & error compensation.
3		Clock Source and Local Clock at previous PTP Instance (RR Drift & NRR drift)	Accuracy of measurement of NRR Drift when there is NRR Drift, including algorithms for NRR Drift tracking & error compensation. Accuracy of calculation of rateRatioDrift, including algorithms for RR Drift tracking & error compensation. Combined with test 2 this effectively requires a level of performance regarding NRR Drift tracking & error compensation, whether the source of the NRR drift is the Local Clock of the current PTP Instance or the previous PTP Instance.

6326

6327 D.4 Approach to Testing Normative Requirements

6328 D.4.1 General

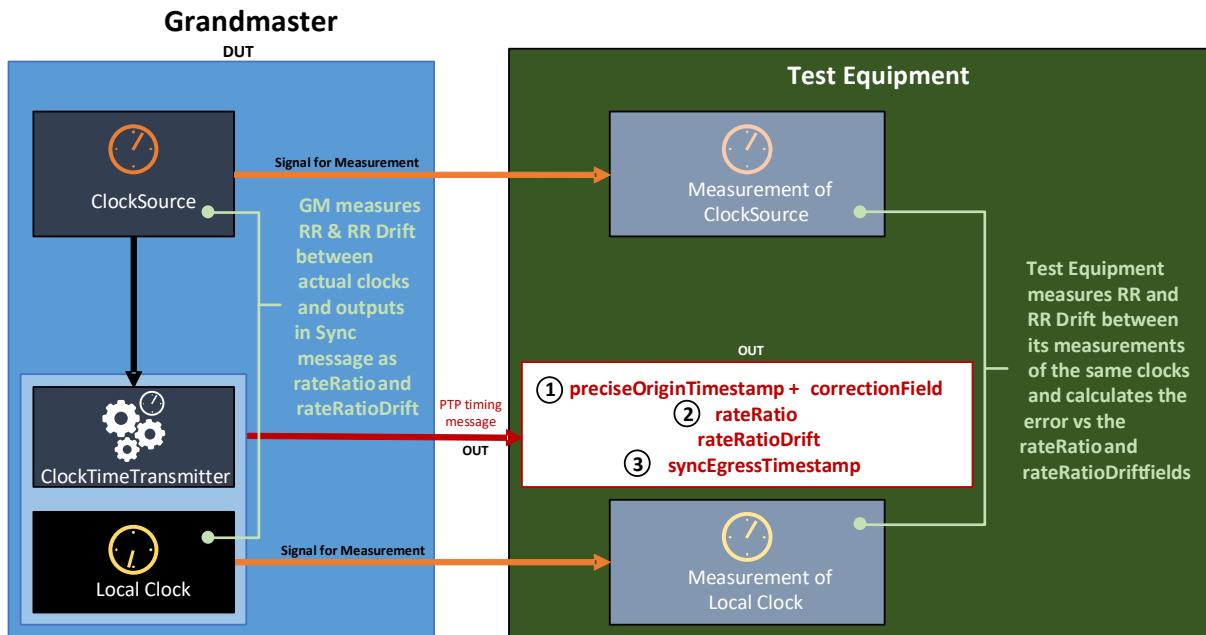
6329 This document does not specify tests to ensure conformance with the normative requirements.
 6330 However, it is important that the normative requirements are, in principle, testable. Clause D.4
 6331 describes, at a high level, approaches a test specification might take to testing conformance
 6332 with some of the normative requirements related to time synchronization.

6333 It is assumed that test equipment can precisely measure the output of the ClockSource (at a
 6334 Grandmaster PTP Instance), ClockTarget (at a PTP End Instance) and Local Clock (at any PTP
 6335 Instance) to ensure conformance with frequency offset and frequency offset drift requirements.
 6336 This might be via a Pulse per Second (PPS) plus Time-of-Day information or another
 6337 mechanism.

6338 It is also assumed that test equipment can generate sequences of PTP messages with precise
 6339 timing and content (for testing PTP Relay Instances and PTP End Instances) and receive, log,
 6340 and process sequences of PTP messages with precise timing measurement, e.g. of message
 6341 arrival.

6342 D.4.2 Testing Grandmaster PTP Instance

6343 Figure D.1 illustrates an approach to testing the three normative requirements discussed in
 6344 D.3.4.



6346 **Figure D.1 – Approach to Testing Normative Requirements for Grandmaster PTP**
 6347 **Instance**

6348 The test equipment can calculate the time the Sync message is output at the DUT by subtracting
 6349 the link delay from the measured arrival time at the test equipment.

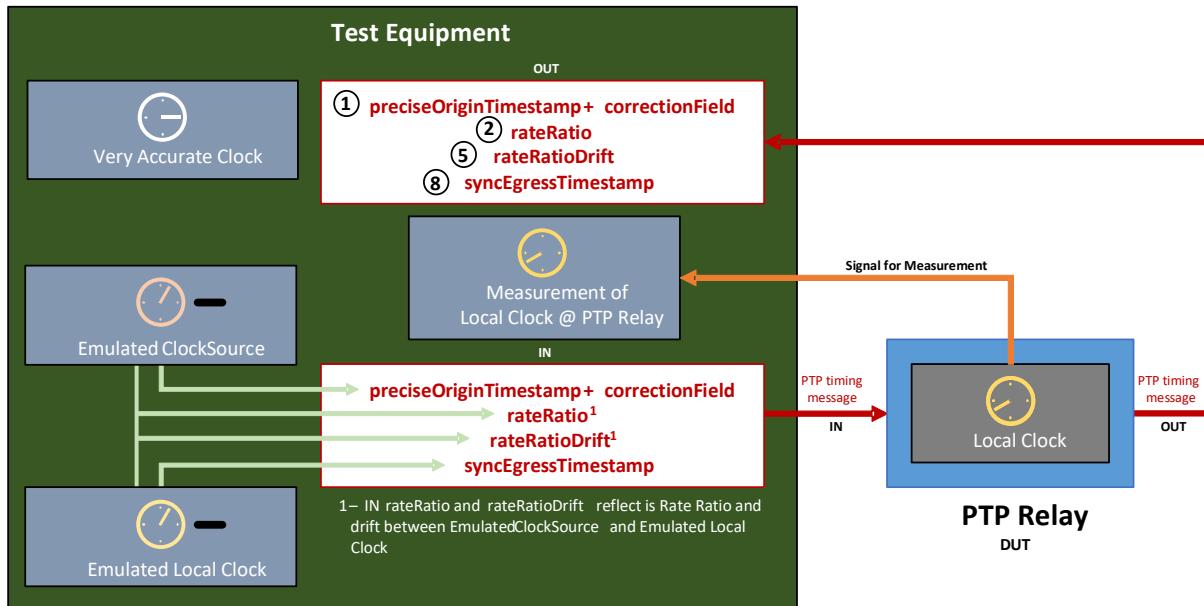
6350 For test 1, the test equipment compares the value of the preciseOriginTimestamp +
 6351 correctionField against its measurement of the ClockSource.

6352 For tests 2, the test equipment compares the value in the rateRatio field with its calculation of
 6353 the equivalent value based on its measurement of the ClockSource.

6354 For test 3, the test equipment compares the value of the syncEgressTimestamp against its
 6355 measurement of the Local Clock.

6356 **D.4.3 Testing PTP Relay Instance**

6357 Figure D.2 illustrates an approach to testing normative requirements 1, 2, 5 and 8 discussed in
6358 D.3.5.



6359 **Figure D.2 – Approach to Testing Normative Requirements for PTP Relay Instance - 1**

6360 The test equipment can compare the DUT's output Sync message to the expected result given
6361 the measurement of the Local Clock and the timing of the input PTP timing message
6362 transmission and output PTP timing message reception.

6363 For these four tests, the Emulated ClockSource and Emulated Local Clock are stable and in
6364 sync. In practice, both can be equal to the test equipment's Very Accurate Clock. In the input
6365 Follow_Upt information TLV, rateRatio will be 0 ppm, and in the input Drift_Tracking TLV
6366 rateRatioDrift will be 0 ppm/s. If the Local Clock of the PTP Relay Instance is also stable, it
6367 will measure NRR of 0 ppm and NRR Drift of 0 ppm/s.

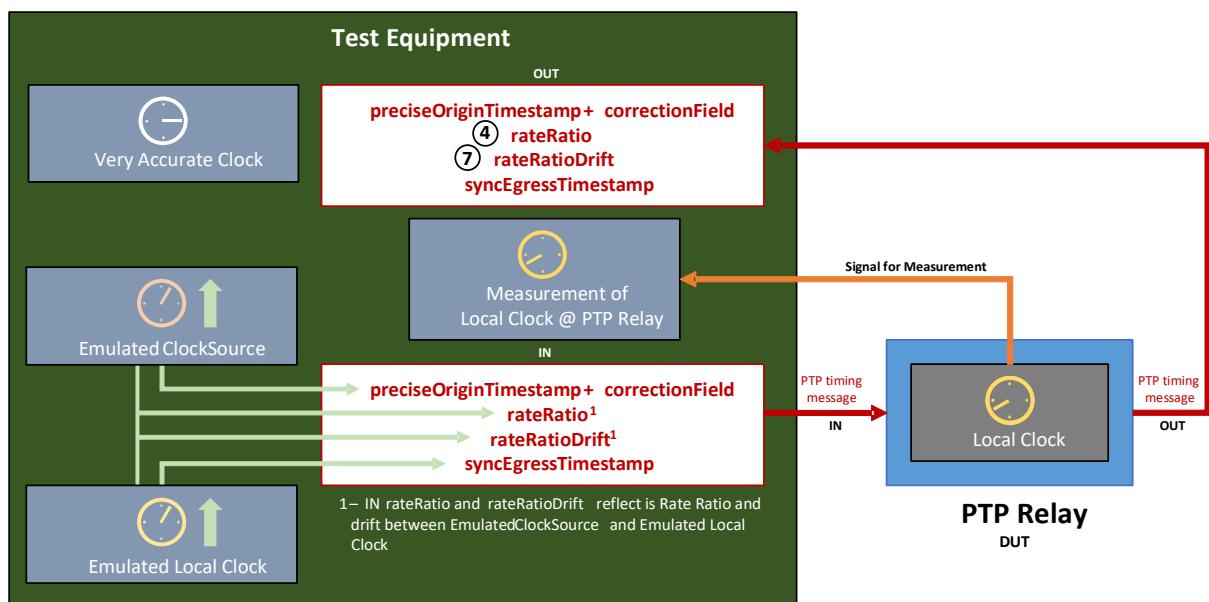
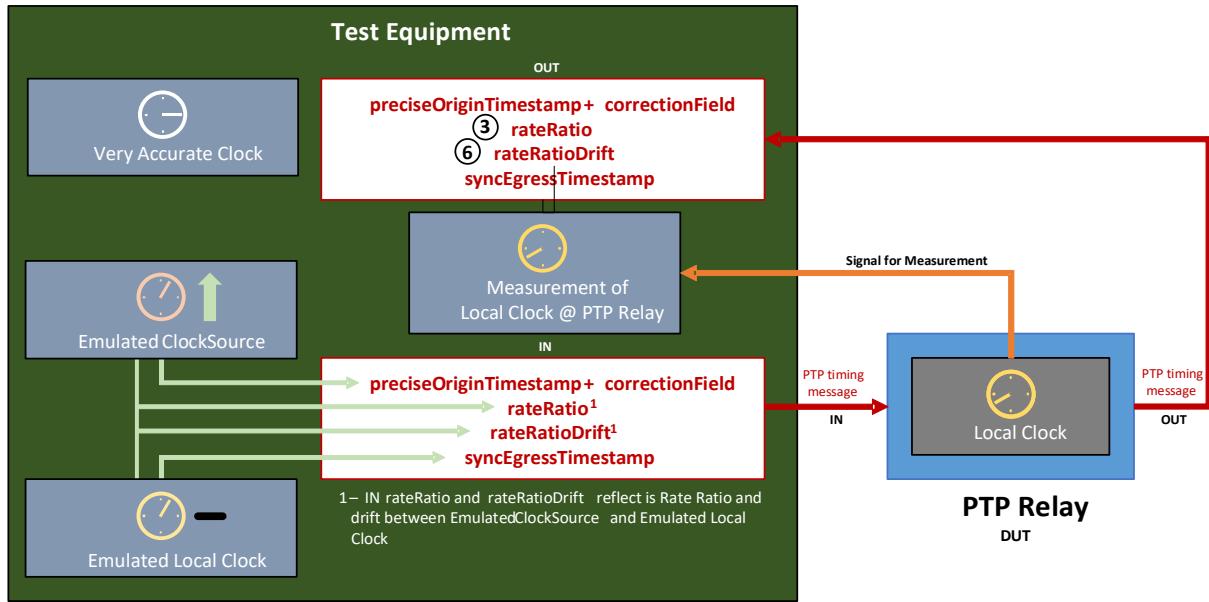
6368 The test equipment can calculate the time the output Sync message is output at the DUT by
6369 subtracting the link delay from the measured arrival time at the test equipment.

6370 For test 1, the test equipment can compare the increase in the value of the correctionField to
6371 the measured meanLinkDelay (from the test equipment to the DUT) plus residenceTime. The
6372 test equipment will need to account for the additional delay between the PTP Relay Instance's
6373 transmission of the input PTP timing message and its reception by the test equipment.

6374 For tests 2 and 5, the test equipment can compare the rateRatio and rateRatioDrift fields in the
6375 output PTP timing message with the equivalent calculated values between the measured Local
6376 Clock and the Emulated ClockSource.

6377 For test 8, the test equipment can compare syncEgressTimestamp value in the output PTP
6378 timing message with its measurement of the Local Clock.

6379 Figure D.3 illustrates an approach to testing normative requirements 3 and 6 discussed in D.3.5.

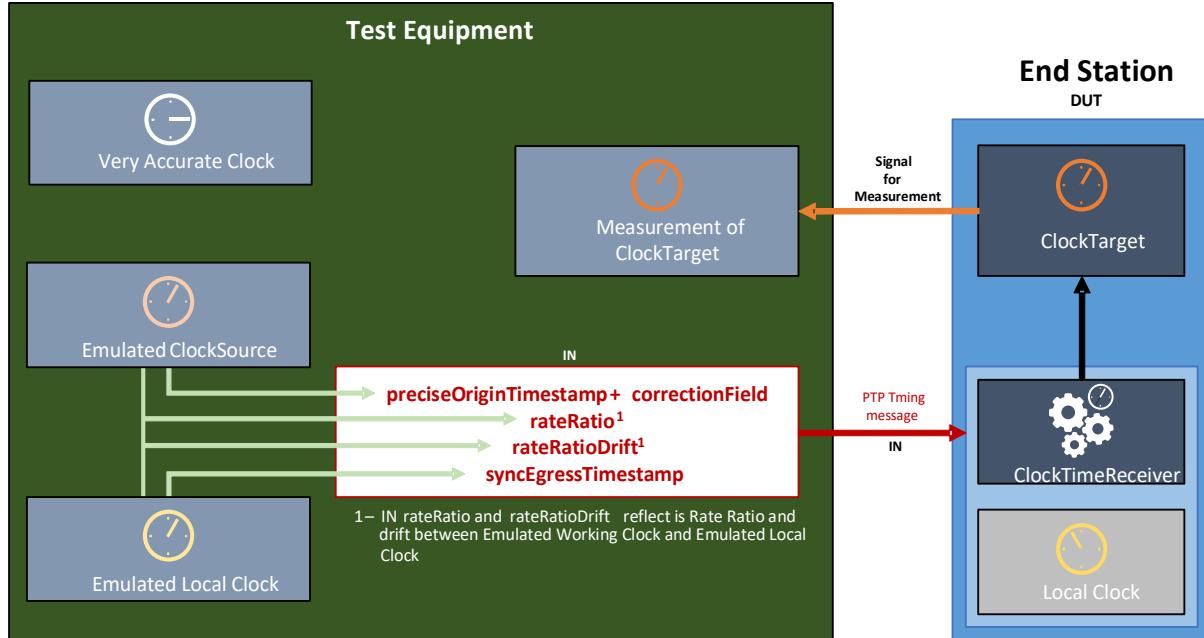


6399 PTP Relay Instance is stable, the NRR it measures will increase over time and the NRR Drift it
 6400 measures will maintain a matching positive value.

6401 For tests 4 and 7, the test equipment can compare the rateRatio and rateRatioDrift fields in the
 6402 output Follow_Up information TLV and Drift_Tracking TLV respectively with the equivalent
 6403 calculated values between the measured Local Clock and the Emulated ClockSource.

6404 D.4.4 Testing PTP End Instance

6405 Figure D.5 illustrates an approach to testing the three normative requirements discussed in
 6406 D.3.6.



6407 **Figure D.5 – Approach to Testing Normative Requirements for PTP End Instance**

6409 The test equipment can compare its measurement of the DUT's ClockTarget to the Emulated
 6410 ClockSource. It will need to account for the additional delay between its transmission of the
 6411 input Sync message and the reception of the message by the DUT.

6412 For test 1, the Emulated ClockSource and Emulated Local Clock are stable and in sync. In
 6413 practice, both can be equal to the test equipment's Very Accurate Clock. In the input Follow_Up
 6414 information TLV, rateRatio will be 0 ppm, and in the input Drift_Tracking TLV, rateRatioDrift will
 6415 be 0 ppm/s. If the Local Clock of the PTP End Instance is also stable, it will measure NRR of
 6416 0 ppm and NRR Drift of 0 ppm/s.

6417 For test 2, the fractional frequency offset of the Emulated ClockSource is increasing at a defined
 6418 ppm/s rate relative to the Very Accurate Clock. The Emulated Local Clock is stable; in practice,
 6419 it can be equal to the test equipment's Very Accurate Clock. In the output Follow_Up
 6420 information TLV, the rateRatio field will increase over time, and the output Drift_Tracking TLV,
 6421 the rateRatioDrift field will maintain a matching positive value. If the Local Clock of the PTP
 6422 Relay Instance is also stable, it will measure NRR of 0 ppm and NRR Drift of 0 ppm/s.

6423 For test 3, the fractional frequency offsets of the Emulated ClockSource and the Emulated Local
 6424 Clock are equal and increasing at a defined ppm/s rate relative to the Very Accurate Clock. In
 6425 the output Follow_Up information TLV, the rateRatio field will be 0 ppm, and in the output output
 6426 Drift_Tracking TLV, the rateRatioDrift field will be 0 ppm/s. If the Local Clock of the PTP Relay
 6427 Instance is stable, the NRR it measures will increase over time and the NRR Drift it measures
 6428 will maintain a matching positive value.

6429 **D.5 Example Algorithms**

6430 **D.5.1 General**

6431 This document does not place normative requirements on the use of specific algorithms.
 6432 However, the normative requirements assume the use of algorithms to reduce the effect of
 6433 errors in meanLinkDelay and to track clock drift and compensate for consequent errors. PTP
 6434 instances that do not implement algorithms will find it difficult or impossible to meet the
 6435 normative requirements.

6436 D.5 provides examples of algorithms that can be used for:

- 6437 • Tracking NRR drift.
- 6438 • Correcting for errors in measured NRR (mNRR) due to NRR drift.
- 6439 • Calculating RR drift.
- 6440 • Correcting for errors in measured RR (mRR) due to RR drift.
- 6441 • Reducing the effect of errors in meanLinkDelay

6442 **D.5.2 Algorithm for Tracking NRR Drift**

6443 For measured NRR, measured RR, and meanLinkDelay, an example for how startup behavior
 6444 can be handled is provided.

6445 NRR Drift Tracking and Error Correction is carried out for each network hop, i.e. at every node
 6446 other than the Grandmaster. It is based on pairs of timestamps with each pair associated with
 6447 a Sync message transmitted from the previous node (n-1) to the current node (n).

- 6448 • t_{s1outP} – Timestamp of the Sync message egress from the **previous** node (n-1), timestamped
 by that node's Local Clock. Unit: **ns**.
- 6450 • t_{s2in} – Timestamp of the Sync message ingress to the current node (n), timestamped by that
 node's Local Clock. Unit: **ns**.

6452 All timestamps are affected by Timestamp Errors.

6453 The algorithm uses information from the 32 most recent Sync messages. However, a node
 6454 need only keep track of the 9 most recent pairs of timestamps from the most recent (x) to the
 6455 9th most recent ($x-8$) Sync message. The algorithm generates one measurement of NRR using
 6456 the prior 2 s of Sync message data (on average, based on a nominal Sync Interval of 125 ms),
 6457 and a second measure based on the 2 s of Sync message data prior to that. It then uses the
 6458 difference in the two measurements over the interval between the effective measurement points
 6459 to calculate the NRR drift rate.

6460 On arrival of a new Sync message (x), or Follow_Up in the case of two-step time transport, a node
 6461 executes a NRR calculation:

$$NRR_{calc}(x) = \left(\frac{t_{s1outP}(x) - t_{s1outP}(x-8)}{t_{s2in}(x) - t_{s2in}(x-8)} - 1 \right) \times 10^6 \quad (D.1)$$

6462

6463 where

6464 NRR_{calc} is the calculated Neighbor Rate Ratio, expressed in ppm;

6465 x is the most recent Sync message;

6466 t_{s1outP} is the timestamp of the Sync message egress from the previous node (n-1), timestamped
 6467 by that node's Local Clock, expressed in ns;

6468 t_{s2in} is the Timestamp of the Sync message ingress to the current node (n), timestamped by that
 6469 node's Local Clock, expressed in ns.

6470

6471 with an associated effective measurement point:

$$NRRcalcT(x) = \frac{t_{s2in}(x) + t_{s2in}(x-8)}{2} \quad (\text{D.2})$$

6472

6473 where

6474 $NRRcalcT$ is the effective measurement point, expressed in ns;

6475 t_{s1outP} is the timestamp of the Sync message egress from the previous node (n-1), timestamped
6476 by that node's Local Clock, expressed in ns;

6477 t_{s2in} is the Timestamp of the Sync message ingress to the current node (n), timestamped by that
6478 node's Local Clock, expressed in ns.

6479

6480 A node keeps track of the 24 most recent NRR calculations and effective measurement points,
6481 from the most recent (x) to the 24th most recent ($x-23$).

6482 After of a new most-recent NNR calculation, a node calculates an NRR drift rate:

$$NRRaverageA = \sum_{i=x-7}^x \frac{mNRRcalc(i)}{8} \quad (\text{D.3})$$

6483

6484 where

6485 $NRRaverageA$ is the average of the 8 most recent Neighbor Rate Ratio calculations, expressed
6486 in ppm.

$$NRRaverageB = \sum_{i=x-23}^{x-16} \frac{mNRRcalc(i)}{8} \quad (\text{D.4})$$

6487

6488 where

6489 $NRRaverageB$ is the average of the 8 least recent Neighbor Rate Ratio calculations, expressed
6490 in ppm;

$$NRRdriftInterval = \sum_{i=x-7}^x \frac{mNRRcalcT(i)}{8} - \sum_{i=x-23}^{x-16} \frac{mNRRcalcT(i)}{8} \quad (\text{D.5})$$

6491

6492 where

6493 $NRRdriftInterval$ is the period across which Neighbor Rate Ratio drift is measured,
6494 expressed in ns.

$$NRRdriftRate(n) = \left(\frac{NRRaverageA - NRRaverageB}{NRRdriftInterval} \right) \times 10^9 \quad (\text{D.6})$$

6495

6496 where

6497 $NRRdriftRate(n)$ is the the NRR drift rate for the current Node n, expressed in ppm/s.

6498

6499 **D.5.3 Algorithm to Compensate for Errors in measured NRR due to Clock Drift**

6500 **D.5.3.1 General**

6501 The algorithm to measure NRR uses data from the previous 1 s of Sync message data,
 6502 combined with the NRR drift estimate from the previous step. This smaller amount of data (vs.
 6503 that used for either of the NRR measurements in the previous step) is employed as it improves
 6504 responsiveness to sudden changes in NRR drift with minimal loss of accuracy.

6505 On arrival of a Sync message (x), or Follow_Up in the case of two-step time transport, a node
 6506 executes a NRR calculation:

$$mNRR_{calc}(x) = \left(\frac{t_{s1outP}(x) - t_{s1outP}(x-4)}{t_{s2in}(x) - t_{s2in}(x-4)} - 1 \right) \times 10^6 \quad (\text{D.7})$$

6507
 6508 with an associated effective measurement point:

$$mNRR_{calcT}(x) = \frac{t_{s2in}(x) + t_{s2in}(x-4)}{2} \quad (\text{D.8})$$

6509
 6510 A node keeps track of the 4 most recent mNRR calculations and effective measurement points,
 6511 from the most recent (x) to the 4th most recent ($x-3$). (The mNRR calculations use information
 6512 from the 5 most recent Sync messages, but the node is already keeping track of information
 6513 from the 9 most recent Sync messages for the NRR drift tracking algorithm.)

6514 The node then calculates an error corrected measured NRR value.

6515 For $i = x$ to $(x-3)$

$$mNRR_{corrected}(i) = mNRR_{calc}(i) + \left(NRRdriftRate(n) \times \frac{(t_{s2in}(x) - mNRR_{calcT}(i))}{10^9} \right) \quad (\text{D.9})$$

6516
 6517 where
 6518 $mNRR_{corrected}(i)$ is the error-corrected measured NRR value at message i , expressed in ppm.

$$mNRR(n) = \sum_{i=x-3}^x \frac{mNRR_{corrected}(i)}{4} \quad (\text{D.10})$$

6519
 6520 where
 6521 $mNRR$ is the error-corrected measured NRR value, expressed in ppm.

6522
 6523 The result is a measured NRR value, error-corrected to the time when the most recent Sync
 6524 message was received.

6525 **D.5.3.2 Measured NRR Algorithm – Startup Behaviour**

6526 NRR is used when calculating meanLinkDelay and output Sync/Follow_Up message fields. The
 6527 first NRR drift calculation will only be available after receipt of 32 Sync/Follow_Up messages,
 6528 i.e. after approximately 4 seconds of operation given the 125 ms Sync Interval. During this time
 6529 meanLinkDelay and output Sync/Follow_Up messages fields must still be calculated, so an

6530 alternative must be used, even if it cannot deliver the same assurances regarding network-level
 6531 performance.

6532 If measured NRR from Sync/Follow_Up message information is unavailable but equivalent
 6533 information from Pdelay_Resp messages is available, it may be substituted for Sync/Follow_Up
 6534 message information. However, measuring NRR using Pdelay_Resp messages is vulnerable to
 6535 additional error due to clock drift between the time NRR is measured, on receipt of the latest
 6536 Pdelay_Resp message, and use of the measurement during Sync message processing. This is
 6537 the reason using Sync/Follow_Up message information is preferable. It also means that a switch
 6538 to using Sync/Follow_Up message information as soon as possible is desirable. It is technically
 6539 possible to calculate a NRR using a combination of Pdelay_Resp and Sync messages but this
 6540 can be risky due to the potential for very short intervals between messages and resulting high
 6541 error due to timestamp errors, so it not recommended.

6542 It is the responsibility of implementers to decide whether and when to use Pdelay_Resp
 6543 message information and when to switch to using Sync/Follow_Up message information. The
 6544 normative requirements in this document are for operation after 32 Sync/Follow_Up messages
 6545 have been received and assume use of the algorithms in D.5.2 and D.5.3, or more effective
 6546 algorithms. Implementations that continue to use Pdelay_Resp message information to
 6547 calculate NRR after 32 messages have been received can find some of the normative
 6548 requirements difficult or impossible to meet.

6549 The following describes potential startup behaviour applicable to either Sync/Follow_Up or
 6550 Pdelay_Resp message information.

- 6551 a) At least two two messages must be received before calculating a NRR value.
- 6552 b) Prior to two messages being received, NRR = 1 (i.e., 0 ppm) should be used.
- 6553 c) Once two messages have been received, NRR should be calculated using the formula:

$$\text{2}^{\text{nd}} \text{ message: } mNRR = \left(\left(\frac{t_3(x)-t_3(x-1)}{t_4(x)-t_4(x-1)} \right) - 1 \right) \times 10^6 \quad (\text{D.11})$$

6554

6555 where

6556 $t_3(i)$ is the timestamp of the i^{th} Pdelay_Resp message on egress from the previous node ($n-1$), timestamped by that node's Local Clock, expressed in ns;

6558 $t_4(i)$ is the timestamp of the Pdelay_Resp message on ingress to the current node (n), timestamped by that node's Local Clock, expressed in ns.

6560

6561 d) When three to four messages have been received, NRR should be calculated using the
 6562 following formula:

$$\text{3}^{\text{rd}} \text{ message: } mNRR = \left(\left(\frac{t_{1outP}(x)-t_{1outP}(x-2)}{t_{2in}(x)-t_{2in}(x-2)} \right) - 1 \right) \times 10^6 \quad (\text{D.12})$$

$$\text{4}^{\text{th}} \text{ message: } mNRR = \left(\left(\frac{t_{1outP}(x)-t_{1outP}(x-3)}{t_{2in}(x)-t_{2in}(x-3)} \right) - 1 \right) \times 10^6 \quad (\text{D.13})$$

6563

6564 e) On arrival of the 5th Sync/Follow_Up message the first mNRRcalc and mNRRcalcT
 6565 calculations can take place and should be used for NRR:

$$mNRR_{\text{calc}}(x) = \left(\left(\frac{t_{s1outP}(x)-t_{s1outP}(x-4)}{t_{s2in}(x)-t_{s2in}(x-4)} \right) - 1 \right) \times 10^6 \quad (\text{D.14})$$

$$mNRRcalcT(x) = \frac{t_{s2in}(x) + t_{s2in}(x-4)}{2} \quad (\text{D.15})$$

5th Sync message: $mNRR = mNRRcalc(x)$ (D.16)

6566

6567 f) As the 6th, 7th and 8th messages arrive an average can be taken and used for NRR, so:

$$6^{\text{th}} \text{ message: } mNRR = \sum_{i=x-1}^x \frac{mNRRcalc(i)}{2} \quad (\text{D.17})$$

$$7^{\text{th}} \text{ message: } mNRR = \sum_{i=x-2}^x \frac{mNRRcalc(i)}{3} \quad (\text{D.18})$$

$$8^{\text{th}} \text{ message: } mNRR = \sum_{i=x-3}^x \frac{mNRRcalc(i)}{4} \quad (\text{D.19})$$

6568 g) For the 9th to the 31st message, the Formula (D.19) can be used.

6569

6570 Once the 32nd message arrives, the regular formulas with NRR drift tracking and error correction
6571 can be used.

6572 D.5.4 Algorithm for Tracking RR Drift

6573 A Sync or Follow_Ups message carries the rateRatio field, which informs each node of the
6574 previous node's estimate of its (the previous node's) Rate Ratio. This document also requires
6575 support for the Drift_Tracking TLV, which carries the rateRatioDrift field and informs each node
6576 of the previous node's estimate of its (the previous node's) Rate Ratio Drift.

6577 If the implementation of the Grandmaster PTP Instance means the ClockSource and Local Clock
6578 (at the Grandmaster PTP Instance) are linked such that the two are always operating at the
6579 same frequency, the rateRatio field received by the first node (Node 1) will always be 0 ppm
6580 and the rateRatioDrift field will always be 0 ppm/s. Thus, at Node 1, RR will equal NRR, RR
6581 Drift will equal NRR Drift, and therefore D.5.3 and D.5.3.2 describe how to calculate RR and
6582 RR Drift at Node 1.

6583 If the implementation of the Grandmaster PTP Instance means the ClockSource and Local Clock
6584 (at the Grandmaster PTP Instance) can operate at different frequencies, the implementation
6585 populates the rateRatio and rateRatioDrift field with values reflecting those differences.

6586 In either case all PTP Instances, other than the Grandmaster PTP Instance, calculate an
6587 estimate of the local Rate Ratio Drift when the latest Sync/Follow_Ups Message is received,
6588 based on the received rateRatioDrift field and the local measure of NRR Drift. The Rate Ratio
6589 Drift Rate from the previous node is in ppm/s relative to the timebase of its Local Clock (i.e.
6590 the "s" in "ppm/s"). For highest precision, this can be converted to the timebase of the current
6591 node's Local Clock.

$$\text{rateRatioDrift}(n) = \frac{\text{rateRatioDrift}(n-1)}{\left(1 + \frac{mNRR(n)}{10^6}\right)} + \text{NRRdriftRate}(n) \quad (\text{D.20})$$

6592

6593 where

6594 *rateRatioDrift* is the Rate Ratio drift rate, expressed in ppm/s.

6595

6596 However, given that adding ppm/s already lacks the precision of multiplying actual ratios, this
 6597 simplification delivers similarly accurate results.

$$\text{rateRatioDrift}(n) = \text{rateRatioDrift}(n - 1) + \text{NRRdriftRate}(n) \quad (\text{D.21})$$

6598

6599 D.5.5 Algorithm to Compensate for Errors in measured RR due to Clock Drift

6600 On receipt of a Sync or Follow_Up message, all PTP Relay Instances estimate a measured RR
 6601 ($mRR(n)$) based on the received rateRatio field ($mRR(n-1)$) and the local measure of NRR
 6602 ($mNRR(n)$). An $mRR(n)$ value is used to translate the sum of meanLinkDelay and
 6603 residenceTime from Local Clock timebase into Grandmaster timebase. An $mRR(n)$ value is
 6604 also passed in the transmitted Sync or Follow_Up message's rateRatio field to the next node.
 6605 Errors in these estimates due to clock drift can be reduced by taking account of RR Drift. Since
 6606 the optimal point in time for each estimate is different, the amount of applicable RR Drift is
 6607 different, and hence the estimates will be different.

6608 (For discussion of how different Grandmaster PTP Implementations affect the behaviour of a
 6609 PTP Relay Instance at Node 1 – or not – see D.5.4.)

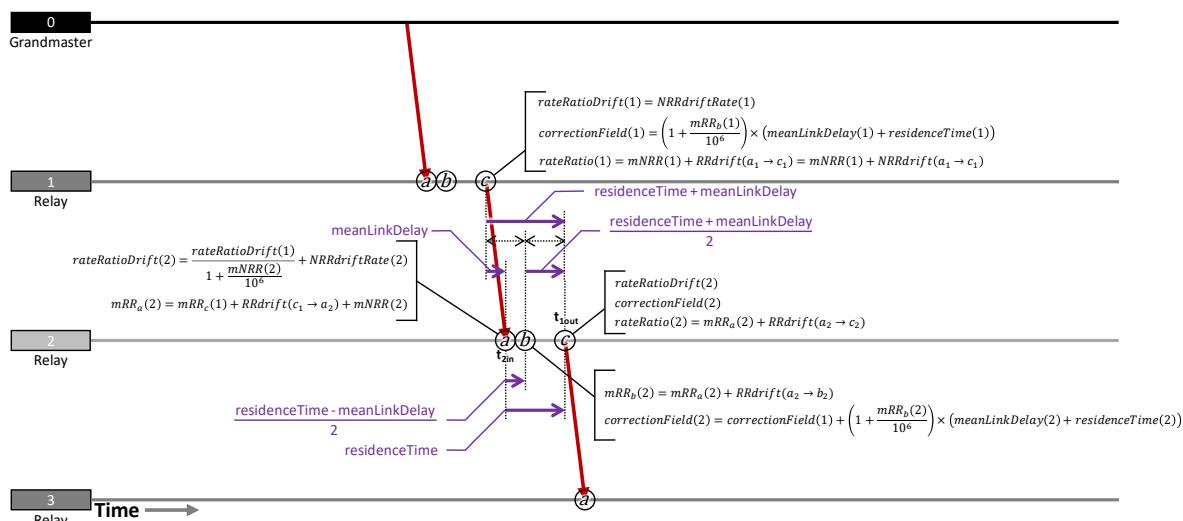
6610 A PTP End Instance is similar in that it estimates $mRR(n)$ on receipt of a Sync message,
 6611 subsequently uses an $mRR(n)$ value, and errors in the latter due to clock drift can be mitigated
 6612 by taking account of RR Drift. However, unlike a PTP Relay Instance, the $mRR(n)$ value is used
 6613 to keep the ClockTarget in line with the ClockSource and there is no need to transmit a rateRatio
 6614 field to a subsequent node.

6615 For a PTP Relay Instance there are three points in time of interest:

- Point a: Receipt of the Sync Message by the current node (Node n)
- Point b: Mid-point between transmission of the Sync message by the previous node (Node $n-1$) and transmission of the consequent Sync message by the current node (Node n)
- Point c: Transmission of the Sync Message by the current node (Node n)

6620

6621 Figure D.6 illustrates these points and the associated calculations.



6622

6623 **Figure D.6 – RR Drift Tracking and Error Compensation Calculations – PTP Relay**
 6624 **Instance**

6625 The estimate of RR when the Sync message arrives can be calculated as follows:

6626

$$mRR_a(n) = rateRatio(n - 1) + RRdrift(c_{n-1} \rightarrow a_n) + mNRR(n) \quad (D.22)$$

6627 $= rateRatio(n - 1) + \left(rateRatioDrift(n - 1) \times \left(1 + \frac{mNRR(n)}{10^6} \right) \times meanLinkDelay(n) \right) + mNRR(n)$

6628 where

6629 mRR_a is the estimate of RR when the Sync message arrives at node n , expressed in ppm;

6630 $RRdrift(c_{n-1} \rightarrow a_n)$ is the amount $rateRatio(n - 1)$ drifts between transmission of the Sync
6631 message at Node n-1 and reception at Node n, expressed in ppm/s.

6632

6633 $RRdrift(c_{n-1} \rightarrow a_n)$ is equivalent to $rateRatioDrift(n - 1)$ multiplied by $meanLinkDelay$ but, since
6634 $meanLinkDelay$ is measured in terms of Node n's Local Clock and $rateRatioDrift$ is in terms of Node n-
6635 1's Local Clock the former should be multiplied by the NRR at Node n for the highest accuracy.

6636 However, given that adding ppm/s already lacks the precision of multiplying actual ratios, the following
6637 simplification delivers similarly accurate results:

$$mRR_a(n) = rateRatio(n - 1) + (rateRatioDrift(n - 1) \times meanLinkDelay(n)) + mNRR(n) \quad (D.23)$$

6638

6639 Once the time when Node n transmits the consequent Sync message is known, the correctionField
6640 value can be calculated.

$$mRR_b(n) = mRR_a(n) + RRdrift_n(a \rightarrow b) \quad (D.24)$$

6641 $= mRR_a(n) + \left(rateRatioDrift(n) \times \frac{residenceTime(n) - meanLinkDelay(n)}{2} \right)$

6642 where

6643 $mRR_b(n)$ is the estimate of RR when Node n transmits the consequent Sync message,
6644 expressed in ppm.

6645

6646 The correctionField is calculated as follows:

$$correctionField(n) = correctionField(n - 1) + \left(1 + \frac{mRR_b(n)}{10^6} \right) \times (meanLinkDelay(n) + residenceTime(n)) \quad (D.25)$$

6647

6648 where

6649 $correctionField(n)$ is the value of the correction field transmitted by node n, expressed in
6650 ns.

6651

6652 The rateRatio field is calculated as follows:

6653 $rateRatio(n) = mRR_a(n) + RRdrift_n(a \rightarrow c)$

$$= mRR_a(n) + (RRdriftRate(n) \times residenceTime(n)) \quad (D.26)$$

6654

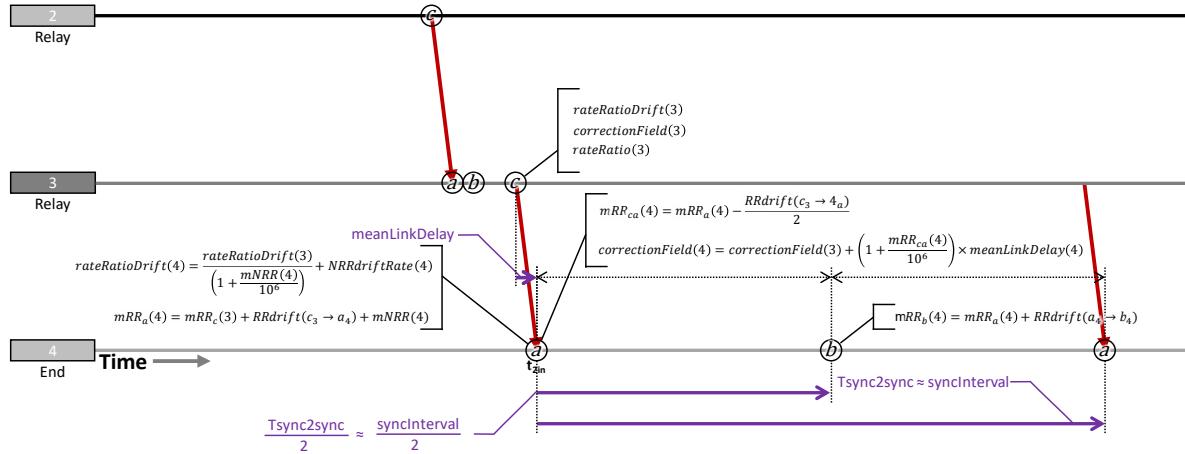
6655 where

6656 $rateRatio(n)$ is the value of the rateRatio field transmitted by node n , expressed in ppm.

6657

6658 D.5.6 Algorithm to Compensate for Errors in measured RR due to Clock Drift at PTP 6659 End Instance

6660 Figure D.7 illustrates a possible approach to applying similar RR drift tracking and error
6661 compensation at a PTP End Instance.



6662

6663 **Figure D.7 – RR Drift Tracking and Error Compensation Calculations – PTP End
6664 Instance**

6665 The initial calculations for rateRatioDrift and mRR_a are exactly the same as for a PTP Relay Instance.
6666 Instead of using RR to translate meanLinkDelay + residenceTime from the Local Clock timebase to
6667 the Grandmaster timebase – as is done at a PTP Relay Instance – a PTP End Instance uses mRR to
6668 translate meanLinkDelay to the Grandmaster timebase (there is no residenceTime at an End
6669 Instance), adding the result to the incoming correctionField to obtain an estimate of the ClockSource
6670 at the time the Sync message arrives, then uses mRR to keep its ClockTarget in line with the
6671 ClockSource until arrival of the next Sync message. The optimal mRR value for translating
6672 meanLinkDelay is halfway between meanLinkDelay's transmission (at c_{n-1}, i.e. point C at the previous
6673 node) and reception (at a_n, i.e. point A at the current node); in the formulas below, this value is
6674 referred to as mRR_{ca}.

$$6675 mRR_{ca}(n) = mRR_a(n) - \frac{RRdrift(c_{n-1} \rightarrow a_n)}{2}$$

$$= mRR_a(n) - \left(rateRatioDrift(n) \times \frac{meanLinkDelay(n)}{2} \right) \quad (D.27)$$

6676

6677 where

6678 $mRR_{ca}(n)$ is the estimate of RR calculated based upon one-half of the meanLinkDelay,
6679 expressed in ppm.

6680 The correction field at the PTP End Instance is given by:

$$6681 correctionField(n) = correctionField(n - 1) + mRR_{ca}(n) \times meanlinkDelay(n) \quad (D.28)$$

6682

6683 The optimal value of mRR for keeping the ClockTarget in line with the Clock Source is mRR_b, where
Point B is halfway between the most recently received Sync message and the next Sync message.

6684 Of course, the exact interval until the next Sync message's arrival (Tsync2sync in Figure D.7) can't be
 6685 known before it happens, but the Rate Ratio value is required as soon as possible after arrival of the
 6686 most recent Sync message. The solution is to use the nominal value of the interval, i.e. syncInterval,
 6687 which is 125 ms.

$$\begin{aligned}
 6688 \quad mRR_b(n) &= mRR_a(n) + RRdrift_n(a \rightarrow b) \\
 6689 \quad &= mRR_a(n) + \left(rateRatioDrift(n) \times \frac{syncInterval}{2} \right) \\
 6690 \quad &= mRR_a(n) + (rateRatioDrift(n) \times 0.0625) \tag{D.29}
 \end{aligned}$$

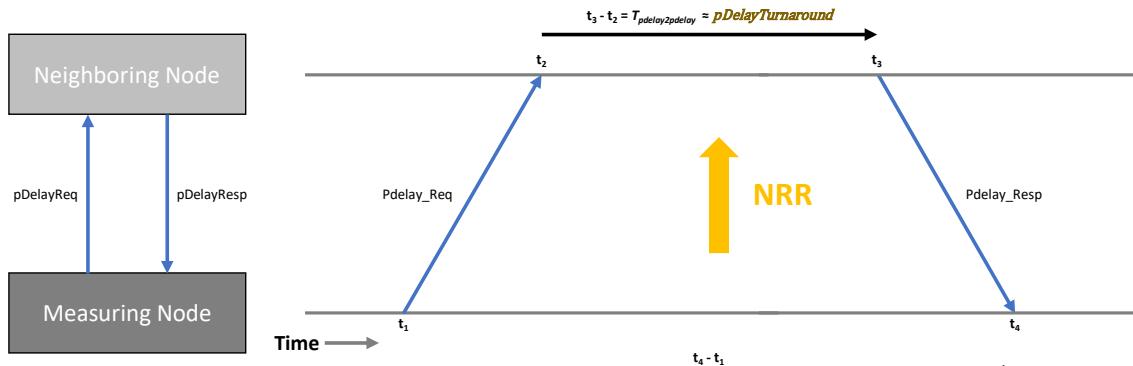
6690
 6691 where
 6692 *syncInterval* is the nominal value of the interval between sync messaged, expressed in ms.
 6693

6694 It is also possible to use more complex algorithms that repeatedly or continuously adjust the mRR
 6695 value between Sync messages, but such an approach is not addressed in this document.

6696 D.5.7 Mean Link Delay Averaging

6697 The actual Path Delay from one node to the next – for a wired connection – is very stable and
 6698 errors measuring it due to Timestamp Error average to zero. Thus, taking a long average or
 6699 applying a low-pass filter with a low bandwidth is an effective way to reduce error in
 6700 meanLinkDelay. Care needs to be taken during system startup or after any other initialisation
 6701 of the algorithm, to quickly converge on a stable value.

6702 The basic Pdelay calculation, used by the Common Mean Link Delay service, remains the same.
 6703 Figure D.8 illustrates it.



$$6704 \quad mPathDelay = \left(\frac{(t_4 - t_1) - \frac{(t_3 - t_2)}{NRR}}{2} \right) \tag{ns}$$

6705 **Figure D.8 – Signals and timestamps to measure path delay**

6706 Following each Pdelay_Req – Pdelay_Resp exchange, the measured path delay (mPathDelay) is
 6707 calculated.

6708 For the x^{th} message after initialisation...

$$mPathDelay(x) = \frac{(t_4 - t_1) - \frac{(t_3 - t_2)}{NRR}}{2} \tag{D.30}$$

6710 where

6711 $mPathDelay$ is the measured path delay between the measuring node and the neighboring
6712 node expressed in ns;

6713 t_1 is a measurement point as defined in Figure D.8, expressed in ns;

6714 t_2 is a measurement point as defined in Figure D.8, expressed in ns;

6715 t_3 is a measurement point as defined in Figure D.8, expressed in ns;

6716 t_4 is a measurement point as defined in Figure D.8, expressed in ns.

6717 ns

6718 The meanLinkDelay is then updated via an IIR (Infinite Impulse Response) filter. For the first
6719 measurement, the filter is initialized:

$$meanLinkDelay(x) = mPathDelay(x) \quad (D.31)$$

6720

6721 For the next few minutes after initialization (when $x < 1000$) the filter is in startup mode. It then
6722 transitions to steady-state mode.

6723 If $x < 1\ 000$ then $f = x$ else $f = 1\ 000$

$$meanLinkDelay(x) = \frac{(meanLinkDelay(x - 1) \times (f - 1)) + mPathDelay(x)}{f} \quad (D.32)$$

6724 For example...

$$meanLinkDelay(100) = \frac{(meanLinkDelay(99) \times 99) + pDelay(x)}{100} \quad (D.33)$$

6725

$$meanLinkDelay(5\ 836) = \frac{(meanLinkDelay(5\ 835) \times 999) + pDelay(x)}{1\ 000} \quad (D.34)$$

6726

6727 It is possible to automatically reinitialize the algorithm if an $mPathDelay$ value, or series of values,
6728 deviates too much from the $meanLinkDelay$, but the details are outside the scope of this document.

6729 The behaviour of timestamp error means that, for shorter actual link delays, $mPathDelay$ might be a
6730 negative value. It can seem tempting to reject negative values, since a negative delay is impossible.
6731 However, at a device level, including negative values of $mPathDelay$ in the input to the IRR filter
6732 results in a more accurate filter output, i.e. $meanLinkDelay$ value; values lower than the actual delay,
6733 even when negative, are balanced by values higher than the actual delay.

6734 Similarly, at a network level, using negative values of $meanLinkDelay$, i.e. the output of the IIR filter,
6735 results in a more accurate correctionField calculation at the PTP End Instance when there are many
6736 networking hops between it and the Grandmaster PTP Instance.

6737

6738

6739

Bibliography

6740

6741 IEEE Std 1588-2019, *IEEE Standard for a Precision Clock Synchronization Protocol for*
6742 *Networked Measurement and Control Systems*

6743 IEEE Std 802-2014, *IEEE Standard for Local and Metropolitan Area Networks: Overview and*
6744 *Architecture*

6745 IETF RFC 4210, Adams, C., Farrell, S., Kause, T., and Mononen, T., *Internet X.509 Public Key*
6746 *Infrastructure Certificate Management Protocol (CMP)*, September 2005, available at
6747 <https://www.rfc-editor.org/info/rfc4210>

6748 IETF RFC 6020, Bjorklund, M., *YANG: A Data Modeling Language for the Network Configuration*
6749 *Protocol (NETCONF)*, October 2010, available at <https://www.rfc-editor.org/info/rfc6020>

6750 IETF RFC 6242, Wasserman, M., *Using the NETCONF Protocol over Secure Shell (SSH)*, June
6751 2011, available at <https://www.rfc-editor.org/info/rfc6242>

6752 IETF RFC 7224, Bjorklund, M., *IANA Interface Type YANG Module*, May 2014, available at
6753 <https://www.rfc-editor.org/info/rfc7224>

6754 IETF RFC 8995, Pritikin, M., Richardson, M., Eckert, T., Behringer, M., and Watsen, K.,
6755 *Bootstrapping Remote Secure Key Infrastructure (BRSKI)*, May 2021, available at
6756 <https://www.rfc-editor.org/info/rfc8995>

6757 ITU-T Recommendation G.8260, *Definitions and terminology for synchronization in packet*
6758 *networks*

6759 ITU-T Series G Supplement 65, Simulations of transport of time over packet networks, Geneva,
6760 October 2018.

6761