ETSI GS F5G 013 V1.1.1 (2023-04)

Fifth Generation Fixed Network (F5G); F5G Technology Landscape Release 2

Disclaimer

The present document has been produced and approved by the Fifth Generation Fixed Network (F5G) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference
DGS/F5G-0013_Techno Land R2

Keywords
F5G, next generation protocol, requirements

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Table of figures

Table of tables

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Group Specification (GS) has been produced by ETSI Industry Specification Group (ISG) Fifth Generation Fixed Network (F5G).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The fixed network has developed to the 5th generation and many new use cases have been introduced. Some supporting technologies have been standardized and commercialized (e.g. XGS-PON and Wi-Fi® 6), but enhancement and optimization may be needed to implement the new use cases. These gaps need to be identified and addressed in corresponding technical specifications.

The present document studies the technology requirements for the F5G use cases R2, explores existing technologies, and perform the gap analysis. The technology landscape of F5G will be defined addressing also the relevant SDOs.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

[1] IEC 60529 (Edition 2.2/2013-08): "Degrees of protection provided by enclosures (IP Code)".

[2] Recommendation ITU-T G.8271: "Time and phase synchronization aspects of telecommunication networks".

[3] Recommendation ITU-T G.9807.1: "10-Gigabit-capable symmetric passive optical network (XGS-PON)".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] TM Forum: "AI Data Training Repository," Release 18.5.1, February 2019.

[i.2] TM Forum: "Autonomous Networks Technical Architecture," Version 1.0.0, November 2020.

[i.3] Recommendation ITU-T Y.3172 (June 2019): "Architectural framework for machine learning in future networks including IMT-2020".

[i.4] Recommendation ITU-T Y.3174 (February 2020): "Framework for data handling to enable machine learning in future networks including IMT-2020".

[i.5] ETSI White Paper No. #34: "Artificial Intelligence and Future Directions for ETSI," 1st Edition, June 2020.

[i.6] ETSI White Paper No. #4: "ETSI GANA as Multi-Layer Artificial Intelligence (AI) Framework for Implementing AI Models for Autonomic Management & Control (AMC) of Networks and Services; and Intent-Based Networking (IBN) via GANA Knowledge Planes (KPs)," August 2019.

[i.7] ETSI White Paper No. #40: "Autonomous Networks, supporting tomorrow's ICT business," 1st edition, October 2020.

[i.8] ETSI GS ZSM 002 (V1.1.1): "Zero-touch network and Service Management (ZSM); Reference Architecture".

[i.9] ETSI GR ZSM 005 (V1.1.1): "Zero-touch network and Service Management (ZSM); Means of Automation".

[i.10] ETSI GR ZSM 010: "Zero-touch network and Service Management (ZSM); General Security Aspects".

[i.11] ETSI GS ZSM 009-2: "Zero-touch network and Service Management (ZSM); Closed-Loop Automation; Part 2: Solutions for automation of E2E service and network management use cases".

[i.12] ETSI Whitepaper No. #44: "ENI Vision: Improved Network Experience using Experiential Networked Intelligence," 1st Edition, March 2021.

[i.13] ETSI GS ENI 005 (V2.1.1): "Experiential Networked Intelligence (ENI); System Architecture" work in progress.

[i.14] ETSI GR F5G 002 (V1.1.1) (February 2021): "Fifth Generation Fixed Network (F5G); F5G Use Cases Release #1".

[i.15] BBF TR-178: "Multi-service Broadband Network Architecture and Nodal Requirements", issue 2, September 2017.

[i.16] BBF TR-370: "Fixed Access Network Sharing - Architecture and Nodal Requirements (FANS)", issue 2, April 2020.

[i.17] BBF TR-386: "Fixed Access Network Sharing - Access Network Sharing Interfaces", January 2019.

[i.18] BBF TR-402: "Functional Model for PON Abstraction Interface", October 2018.

[i.19] ETSI TR 103 775 (V1.1.1): "Access, Terminals, Transmission and Multiplexing (ATTM); Optical Distribution Network (ODN) Quick Construction and Digitalization".

[i.20] IEEE 802.3AH™: "Media Access Control Parameters, Physical Layers, and Management Parameters for Subscriber Access Networks".

[i.21] IEEE 802.3AV™: "Physical Layer Specifications and Management Parameters for 10 Gb/s Passive Optical Networks".

[i.22] BBF TR-069: "CPE WAN Management Protocol (CWMP)".

[i.23] BBF TR-181: "Device Data Model for TR-069".

[i.24] BBF TR-369: "User Services Platform (USP)".

[i.25] IEEE 1905.1™: "Support of New MAC/PHYs and Enhancements".

[i.26] IETF RFC 8453: "Framework for Abstraction and Control of TE Networks (ACTN)".

[i.27] Recommendations ITU-T G.984 series: "Gigabit-capable passive optical networks (GPON)".

[i.28] Recommendation ITU-T G.987 series: "10-Gigabit-capable passive optical networks (XG-PON)".

[i.29] Recommendation ITU-T G.988: "ONU management and control interface (OMCI)".

[i.30] Recommendation ITU-T G.Sup51 (06/2017): "Passive optical network protection considerations".

[i.31] ETSI TS 101 573: "Access, Terminals, Transmission and Multiplexing (ATTM); General engineering of optical fibre cabling in buildings".

[i.32] ETSI EN 300 019-2-0: "Environmental Engineering (EE); Environmental conditions and environmental tests for telecommunications equipment; Part 2: Specification of environmental tests; Sub-part 0: Introduction".

[i.33] IEC 61158: "Industrial communication networks - Fieldbus specifications".

[i.34] IEEE 802.1AS™-2011: "Timing and Synchronization for Time-Sensitive Applications in Bridged Local Area Networks".

[i.35] Draft-ietf-rats-reference-interaction-models-01: "Reference Interaction Models for Remote Attestation Procedures".

[i.36] IETF RFC 9334: "Remote ATtestation procedureS (RATS) Architecture ".

[i.37] IEC 61753: "Fibre optic interconnecting devices and passive components - Performance standard".

[i.38] IEC 61754: "Fibre optic interconnecting devices and passive components - Fibre optic connector interfaces".

[i.39] 3GPP TR 38.801: "Study on new radio access technology: Radio access architecture and interfaces".

[i.40] IEEE 1588-2008™ (1588v2): "IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems".

[i.41] ETSI TS 136 104: "LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Base Station (BS) radio transmission and reception (3GPP TS 36.104)".

[i.42] ETSI TS 138 104: "5G; NR; Base Station (BS) radio transmission and reception (3GPP TS 38.104)".

[i.43] Recommendation ITU-T G.983 series: "Broadband optical access systems".

[i.44] ETSI GS ZSM 003: "Zero-touch network and Service Management (ZSM); End-to-end management and orchestration of network slicing".

[i.45] ETSI GS ZSM 008: "Zero-touch network and Service Management (ZSM); Cross-domain E2E service lifecycle management".

[i.46] MEF 6.3: "Subscriber Ethernet Services Definitions".

[i.47] MEF 10.4: "Subscriber Ethernet Service Attributes".

[i.48] BBF TR-383: "Common YANG Modules for Access Networks".

[i.49] BBF TR-385: "ITU-T PON YANG Modules".

[i.50] BBF TR-436: "Access & Home Network O&M Automation/Intelligence (AIM)".

[i.51] BBF WT-477: "CloudCO Enhancement - Access Node Hardware Disaggregation".

[i.52] IEEE 802.11ax™: "Enhancements for High-Efficiency WLAN".

[i.53] BBF TR-247: "Abstract Test Plan for GPON ONU Conformance".

[i.54] BBF TR-156: "Using GPON Access in the Context of TR-101".

[i.55] BBF TR-167: "GPON-fed TR-101 Ethernet Access Node".

[i.56] IEEE 802.1Q™: "Bridges and Bridged Networks".

[i.57] IETF RFC 2474: "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers".

[i.58] IETF RFC 3031: "Multiprotocol Label Switching Architecture".

[i.59] IETF RFC 7348: "Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks".

[i.60] IETF RFC 8402: "Segment Routing Architecture".

[i.61] IEEE 802.11ac™: "Enhancements for Very High Throughput for Operation in Bands below 6 GHz".

[i.62] IETF RFC 3580: "IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines".

[i.63] IETF RFC 2868: "RADIUS Attributes for Tunnel Protocol Support".

[i.64] IETF RFC 5176: "Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)".

[i.65] ETSI TS 124 244: "Universal Mobile Telecommunications System (UMTS); LTE; Wireless LAN control plane protocol for trusted WLAN access to EPC; Stage 3 (3GPP TS 24.244)".

[i.66] BBF TR-255: "GPON Interoperability Test Plan".

[i.67] Recommendation ITU-T G.709: "Interfaces for the optical transport network".

[i.68] BBF TR-384: "Cloud Central Office (CloudCO) Reference Architectural Framework".

[i.69] Carot et al: "Creation of a hyper-realistic remote music session with professional musicians and public audiences using 5G commodity hardware," in IEEE Computer Society, 2020.

[i.70] Carot et al: "Results of the fast-music project-five contributions to the domain of distributed music," IEEE Access, vol. 8, pp. 47925--47951, 2020.

[i.71] Rottondi et al: "An overview on networked music performance technologies," IEEE Access, pp. 8823--8843, 2016.

[i.72] Letz et al: "Jack audio server for multi-processor machines", in International Computer Music Conference, 2005.

[i.73] Lahderanta et al: "Edge computing server placement with capacitated location allocation", Journal of Parallel and Distributed Computing, vol. 153, pp. 130--149, 2021.

[i.74] 5G-ACIA - White Paper: "Integration of 5G with Time-Sensitive Networking for Industrial Communications", Feb. 2021.

[i.75] ETSI GR F5G 008 (V1.1.1): "Fifth Generation Fixed Network (F5G); F5G Use Cases Release #2".

[i.76] IEC/IEEE 60802: "TSN Profile for Industrial Automation", Draft D1.4, June 2022.

[i.77] Association for Advancing Automation: "GiGE Vision Version 2.1", August 2018.

[i.78] Association for Advancing Automation: "USB3 Vision Version 1.1".

[i.79] IEEE 1588™-2019 (1588v3): "Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems".

[i.80] PROFIBUS Nutzerorganisation e.V.: "PROFINET over TSN Guideline", Version 1.31, July 2021.

[i.81] Recommendation ITU-T G.873.1 (10/2017): "Optical transport network: Linear protection".

[i.82] Recommendation ITU-T Series G Supplement (06/2017): "Passive optical network protection considerations".

[i.83] PROFIBUS Nutzerorganisation e.V.

[i.84] ODVA EtherNet/IP™.

[i.85] EtherCAT® Technology Group.

[i.86] Sercos International e.V.

[i.87] Ethernet POWELINK Standardization Group.

[i.88] ETSI EN 300 019-1-0: "Environmental Engineering (EE); Environmental conditions and environmental tests for telecommunications equipment; Part 1-0: Classification of environmental conditions; Introduction".

[i.89] K. Löser: "Wi-Fi 6 in the Industry", White Paper, Siemens AG, 2020.

[i.90] E. Khorov, I. Levitsky, I. F. Akyildiz: "Current Status and Directions of IEEE 802.11be, the Future Wi-Fi 7", IEEE Access, vol. 8, pp. 88664-88688, May 2020.

[i.91] The Open XR Forum homepage.

[i.92] The Open XR Forum brochure.

[i.93] The IOWN Forum homepage.

[i.94] Recommendation ITU-T G.984.3: "Gigabit-capable passive optical networks (G-PON): Transmission convergence layer specification".

[i.95] IEEE 802.1CB™-2017: "Standard for Local and metropolitan area networks -- Frame Replication and Elimination for Reliability".

[i.96] IEEE 802.1Qcc™-2018: "Standard for Local and Metropolitan Area Networks -- Bridges and Bridged Networks -- Amendment 31: Stream Reservation Protocol (SRP) Enhancements and Performance Improvements".

[i.97] Recommendation ITU-T G.984.1: "Gigabit-capable passive optical networks (GPON): General characteristics".

[i.98] IEEE 802.3AZ™: "Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications Amendment 5: Media Access Control Parameters, Physical Layers, and Management Parameters for Energy-Efficient Ethernet".

[i.99] Recommendation ITU-T G.9806 (Amendment 2 - 05/2021): "Higher-speed bidirectional, single fibre, point-to-point optical access system (HS-PtP)".

[i.100] IEEE 802.3CP™-2021 - Amendment 14: "Bidirectional 10 Gb/s, 25 Gb/s, and 50 Gb/s Optical Access PHYs".

[i.101] IETF RFC 8231: "Path Computation Element Communication Protocol (PCEP) Extensions for Stateful PCE".

[i.102] ETSI TS 124 519: "5G; 5G System (5GS); Time-Sensitive Networking (TSN) Application Function (AF) to Device-Side TSN Translator (DS-TT) and Network-Side TSN Translator (NW-TT) protocol aspects; Stage 3 (3GPP TS 24.519)".

[i.103] ETSI TS 124 535: "5G; 5G System (5GS); Device-Side Time Sensitive Networking (TSN) Translator (DS-TT) to Network-Side TSN Translator (NW-TT) protocol aspects; Stage 3 (3GPP TS 24.535)".

[i.104] 3GPP TS 23.501 (V17.3.0): "System architecture for the 5G System (5GS) (Release 17)".

[i.105] IEEE 802.1Qca™: "IEEE Standard for Local and metropolitan area networks -- Bridges and Bridged Networks - Amendment 24: Path Control and Reservation".

[i.106] IEC 62439-3: "Industrial communication networks - High availability automation networks - Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR)".

[i.107] GSMA™ Cloud AR/VR Whitepaper.

[i.108] Recommendation ITU-T G709.1: "Flexible OTN short-reach interfaces".

[i.109] Recommendation ITU-T G709.2: "OTU4 long-reach interface".

[i.110] Recommendation ITU-T G709.3: "Flexible OTN long-reach interfaces".

[i.111] Recommendation ITU-T G709.4: "OTU25 and OTU50 short-reach interfaces".

[i.112] Recommendation ITU-T L.109: "Construction of optical/metallic hybrid cables".

[i.113] Recommendation ITU-T G.9804.1: "Higher speed passive optical networks - Requirements".

[i.114] IETF RFC 8641: "Subscription to YANG Notifications for Datastore Updates".

[i.115] IETF RFC 9232: "Network Telemetry Framework".

[i.116] draft-ietf-netconf-udp-pub-channel-03: "UDP based Publication Channel for Streaming Telemetry".

[i.117] draft-openconfig-rtgwg-gnmi-spec-01: "gRPC Network Management Interface (gNMI)".

[i.118] draft-song-opsawg-ifit-framework-19: "A Framework for In-situ Flow Information Telemetry".

[i.119] Draft-ietf-rats-eat-19: "The Entity Attestation Token (EAT)".

[i.120] Draft-ietf-rats-tpm-based-network-device-attest-14: "TPM-based Network Device Remote Integrity Verification".

[i.121] Draft-ietf-rats-yang-tpm-charra-21: "A YANG Data Model for Challenge-Response-based Remote Attestation Procedures using TPMs".

[i.122] GlobalPlatform GPD_SPE_009: "GlobalPlatform Technology TEE System Architecture Version 1.2".

[i.123] GlobalPlatform GPD_SPE_007: "GlobalPlatform Device Technology TEE Client API Specification Version 1.0".

[i.124] Recommendations ITU-T L.100 to L.199 are standards for optical fibre cables.

[i.125] Recommendations ITU-T L.200 to L.299 are optical infrastructure standards.

[i.126] Recommendations ITU-T L.300 to L.399 are maintenance and operation standards that include optical fibre cable maintenance.

[i.127] Recommendations ITU-T L.400 to L.429 focuses on passive optical devices standards.

[i.128] Recommendation ITU-T Q.3715: "Signalling requirements for dynamic bandwidth adjustment on demand on broadband network gateway implemented by software-defined networking technologies".

[i.129] BBF TR-144: "Broadband Multi-Service Architecture & Framework Requirements".

[i.130] ETSI TS 181 018: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Requirements for QoS in a NGN".

[i.131] ETSI TR 182 022: "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Architectures for QoS handling".

[i.132] ETSI GS MEC 002 (V1.1.1): "Mobile Edge Computing (MEC); Technical Requirements".

[i.133] ETSI GS MEC 003 (V2.2.1): "Multi-access Edge Computing (MEC); Framework and Reference Architecture".

[i.134] ETSI GS MEC 011 (V2.2.1): "Multi-access Edge Computing (MEC); Edge Platform Application Enablement".

[i.135] ETSI GS MEC 015 (V2.1.1): "Multi-Access Edge Computing (MEC); Traffic Management APIs".

[i.136] ETSI GS MEC 029 (V2.2.1): "Multi-access Edge Computing (MEC); Fixed Access Information API".

[i.137] ETSI GR MEC 024 (V2.1.1): "Multi-access Edge Computing (MEC); Support for network slicing".

[i.138] ETSI GS MEC-IEG 006 (V1.1.1): "Mobile Edge Computing; Market Acceleration; MEC Metrics Best Practice and Guidelines".

[i.139] ETSI White Paper No. 28: "MEC in 5G networks".

[i.140] 3GPP TS 23.548 (V17.1.0): "5G System Enhancements for Edge Computing; Stage 2 (Release 17)".

[i.141] ISO/IEC 23009-5: "Information technology -- Dynamic adaptive streaming over HTTP (DASH) -- Part 5: Server and network assisted DASH (SAND)".

[i.142] CTA-2066: "Streaming Quality of Experience Events, Properties and Metrics".

[i.143] IETF RFC 3945: "Generalized Multi-Protocol Label Switching (GMPLS) Architecture".

[i.144] IETF RFC 7138: "Traffic Engineering Extensions to OSPF for GMPLS Control of Evolving G.709 Optical Transport Networks".

[i.145] IETF RFC 7139: "GMPLS Signaling Extensions for Control of Evolving G.709 Optical Transport Networks".

[i.146] IETF RFC 7963: "RSVP-TE Extension for Additional Signal Types in G.709 Optical Transport Networks (OTNs)".

[i.147] Recommendation ITU-T G.Sup43: "Transport of IEEE 10GBASE-R in optical transport networks (OTN)".

[i.148] draft-ietf-ccamp-gmpls-otn-b100g-applicability-15: "Applicability of GMPLS for beyond 100 Gbit/s Optical Transport Network".

[i.149] IETF RFC 8795: "YANG Data Model for Traffic Engineering (TE) Topologies".

[i.150] draft-ietf-teas-yang-te: "A YANG Data Model for Traffic Engineering Tunnels, Label Switched Paths and Interfaces".

[i.151] draft-ietf-ccamp-otn-topo-yang: "A YANG Data Model for Optical Transport Network Topology".

[i.152] draft-ietf-ccamp-otn-tunnel-model: "OTN Tunnel YANG Model".

[i.153] draft-ietf-ccamp-l1csm-yang: "A YANG Data Model for L1 Connectivity Service Model (L1CSM)".

[i.154] draft-ietf-teas-ietf-network-slice-nbi-yang: "A YANG Data Model for the IETF Network Slice Service".

[i.155] draft-ietf-teas-ietf-network-slice-use-cases: "IETF Network Slice Use Cases and Attributes for the Slice Service Interface of IETF Network Slice Controllers".

[i.156] draft-ietf-teas-ietf-network-slices: "A Framework for IETF Network Slices".

[i.157] draft-ietf-ccamp-yang-otn-slicing: "Framework and Data Model for OTN Network Slicing".

[i.158] Recommendation ITU-T G.7044: "Hitless adjustment of ODUflex(GFP)".

[i.159] ETSI TS 122 104: "5G; Service requirements for cyber-physical control applications in vertical domains (3GPP TS 22.104)".

[i.160] IEEE 802.1Qbv™: "IEEE Standard for Local and metropolitan area networks -- Bridges and Bridged Networks - Amendment 25: Enhancements for Scheduled Traffic".

[i.161] IEEE 802.1Qbu™: "IEEE Standard for Local and metropolitan area networks -- Bridges and Bridged Networks -- Amendment 26: Frame Preemption".

[i.162] IEEE 802.1Qci™: "IEEE Standard for Local and metropolitan area networks -- Bridges and Bridged Networks -- Amendment 28: Per-Stream Filtering and Policing".

[i.163] IEEE 802.3™: "IEEE Standard for Ethernet".

[i.164] IEEE 802.11™: "IEEE Standard for Information technology -- Telecommunications and information exchange between systems Local and metropolitan area networks -- Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications".

[i.165] ETSI 122 261: "5G; Service requirements for the 5G system (3GPP TS 22.261)".

[i.166] SMPTE 259M: "For Television -- SDTV DigitalSignal/Data - Serial Digital Interface".

[i.167] SMPTE 292M: "Bit-Serial Digital Interface for High-Definition Television Systems".

[i.168] SMPTE 424M: "3 Gb/s Signal/Data Serial Interface".

[i.169] SMPTE ST-2082: "12 Gb/s Signal/Data Serial Interface -- Electrical".

[i.170] Recommendation ITU-T G.872: "Architecture of the optical transport network".

[i.171] Recommendation ITU-T G.798: "Characteristics of optical transport network hierarchy equipment functional blocks".

[i.172] Recommendation ITU-T G.8080: "Architecture for the automatically switched optical network".

[i.173] IEC 60079-0:2017: "Explosive atmospheres - Part 0: Equipment - General requirements".

[i.174] Recommendation ITU-T G.7703: "Architecture for the automatically switched optical network".

[i.175] IEEE 802.3df™: "400 Gb/s and 800 Gb/s Ethernet Task Force".

[i.176] IEEE 802.3ba™: "IEEE Standard for Information technology-- Local and metropolitan area networks -- Specific requirements -- Part 3: CSMA/CD Access Method and Physical Layer Specifications Amendment 4: Media Access Control Parameters, Physical Layers, and Management Parameters for 40 Gb/s and 100 Gb/s Operation".

[i.177] Recommendation ITU-T G.672: "Characteristics of multi-degree reconfigurable optical add/drop multiplexers".

[i.178] ISO/IEC JTC 1/SC 42: "Artificial intelligence".

[i.179] ETSI GS F5G 011: "Fifth Generation Fixed Network (F5G); Telemetry Framework and Requirements for Access Networks".

[i.180] ETSI GS F5G 016: "5th Generation Fixed Network (F5G); Data Models of Telemetry for Access Network".

[i.181] Recommendation ITU-T G.989: "40-Gigabit-capable passive optical networks (NG-PON2): Definitions, abbreviations and acronyms".

[i.182] Recommendation ITU-T G.Sup66: "5G wireless fronthaul requirements in a passive optical network context".

[i.183] Recommendation ITU-T X.509: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".

[i.184] Recommendation ITU-T G.9802: "Multiple-wavelength passive optical networks (MW-PONs)".

[i.185] Recommendation ITU-T G.9802.1: "Wavelength division multiplexed passive optical networks (WDM PON): General requirements".

[i.186] Recommendation ITU-T G.9802.2: "Wavelength division multiplied passive optical networks (WDM-PON): Physical media (PMD) and transmission convergence (TC) layer specifications".

[i.187] Recommendation ITU-T G.9804.2: "Higher speed passive optical networks - Common transmission convergence layer specification".

[i.188] Recommendation ITU-T G.9804.3: "50-Gigabit-capable passive optical networks (50G-PON): Physical media dependent (PMD) layer specification".

[i.189] Recommendation ITU-T G.9804.4: "50-Gigabit-capable Time and wavelength multiplexed passive optical networks (50G-TWDM-PON): Physical media (PMD) layer specification".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

PIN diode: type of photodiode with a wide, undoped intrinsic semiconductor region between a p-type semiconductor and an n-type semiconductor region

NOTE: The p-type and n-type regions are typically heavily doped because they are used for ohmic contacts.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

3GPP	3rd Generation Partnership Project
4G	Forth Generation
5G	Fifth Generation (fixed or Mobile)
AC	Alternating Current
ACIA	Alliance for Connected Industries and Automation
ACS	Auto-Configuration Server
ACTN	Abstraction and Control of Traffic Engineering (TE) Networks
AES	Advance Encryption Standard
AF	Application Function
AggN	Aggregation Network
AGV	Automated Guided Vehicles
AI	Artificial Intelligence
AIM	Automated and Intelligent Management
AN	Access Network
ANI	Access Network Interface
ANN	Artificial Neural Network
AP	Access Point
APD	Avalanche PhotoDiode
API	Application Programming Interface
APN	Access Point Name
AR	Augment Reality
ASI	Asynchronous Serial Interface
ASIC	Application Specific Integrated Circuit
ASON	Automatically Switched Optical Network
ATTM	Access, Terminals, Transmission and Multiplexing
AVB	Audio Video Bridging
AZ	Availability Zone

B2B	Business to Business
B2C	Business to Customer
BBF	BroadBand Forum
BBU	Base Band Unit
BSS	Basic Service Set
BSSID	Basic Service Set Identifier
BTV	Broadcast TV
BW	BandWidth
C&M	Control & Management
CAN	Controller Area Network
CE	Customer Equipment
CF	Collection Function
CFP2	C Form-factor Pluggable-2
CLI	Command Line interface
CMI	CNC-MDSC Interface
CNC	Customer Network Controller
CO	Central Office
COAP	Constrained Application Protocol
CPE	Customer Premises Equipment
CPN	Customer Premises Network
CPU	Central processing Unit
CRUD	Create, Read, Update, Delete
CT	Computed Tomography
CTA	Consumer Technology Association
CU	Central Unit
CWMP	CPE Wide Management protocol
DANE	DASH Aware Network Element
DASH	Desktop and mobile Architecture for System Hardware
DBA	Dynamic Bandwidth Allocation
DC	DataCentre
DCI	Data Centre Interconnect
DCN	Data Communication Network
DD	Double Density
DIM	Dynamic Integrity Measurement
DL	Deep Learning
DL/UL	DownLink/UpLink
DML	Directly Modulated Laser
DNS	Domain Name System
DPI	Deep Packet Inspection
DR	Digital Radiography
DS-TT	Device Side TSN Translators
DU	Distributed Unit
DVB	Digital Video Broadcasting
DWA	Dynamic Wavelength Assignment
E2E	End-to-End
EAT	Entity Attestation Token
EAU	Electrical Aggregation Unit
ECT	Equal Cost Tree
EE	Environmental Engineering
eFBB	enhanced Fixed Broadband
eMBB	5G enhanced Mobile BroadBand
EMC	Electric Magnetic Compatibility
EMI	Electro-Magnetic Interference
EML	Electro-absorption Modulated Laser
EMS	Element Management System
EN	European Norm
ENI	Experiential Networked Intelligence
EPC	Enhanced Packet Core
EPL	Ethernet Private Line
EPON	Ethernet Passive Optical Network
ER	Extended Range
ET	Explicit Tree

EVC	Ethernet Virtual Circuit
EVPL	Ethernet Virtual Private Line
FANS	Fixed Access Network Sharing
FDD	Frequency Division Duplexing
FDMA	Frequency Division Multiple Access
FEC	Feed-forward Error Correction
FFC	Full Fibre Connection
FIN	Fibre In-Premises
FoF	Factory of the Future
FP	Fabry-Perot laser diode
FRER	Frame Replication and Elimination for Reliability
FSAN	Full Services Access Network organization
FTTA	Fibre to the Antenna
FTTH	Fibre-To-The-Home
FTTR	Fibre-To-The-Room
FTTx	Fibre-To-The x
FWA	Fixed Wireless Access
GANA	Generic Autonomic Network Architecture
GCM	Galois Counter Mode
GE	Gigabit Ethernet
GI	Guard Interval
GIS	Geographic Information System
GM	Grand Master
GMPLS	Generalized Multiprotocol Label Switching
gNB	5G Node B
gNMI	Google Network Management Interface
GNSS	Global Navigation Satellite System
GPON	Gigabit Passive Optical Network
G-PON	Gigabit PON
GPU	Grapgic Processing Unit
GR	Group Report
GRE	Guaranteed Reliable Experience
gRPC	Google Remote Procedure Call
GSMA	Global System for Mobile Communication Association
GUI	Graphic User Interface
GVSP	GiGE Vision® Streaming Protocol
GW	Gateway
HD	High Definition
HMD	Head Mounted Display
HQ	HeadQuarters
HSP	High-Speed Passive
HTTP	HyperText Transfer Protocol
IBC	International Broadcasting Centre
ICT	Information & Communication Technology
ID	Identity
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IMT	International Mobile Telecommunications
InP	Infrastructure Provider
INT	Interoperability Testing
IOAM	In-situ Operations, Administration, and Maintenance
IoT	Internet of Things
IOWN	Innovative Optical and Wireless Network
IP	Internet Protocol
IPFIX	Internet Protocol Flow Information Export
IS	Intrinsic Safety
ISG	Industry Specification Group
IS-IS	Intermediate Station to Intermediate Station
ISO	International Organization for Standardization
IST	Internal Spanning Tree
IT	Information Technology
JTC1	Joint Technical Committee (ISO and IEC Joint Technical Committee)

KHz	KiloHertz
KPI	Key Performance Indicator
LAN	Local Area Network
LC	Little Connector
LiFi	Light Fidelity
LSP	Label Switched Path
LTE	Long-Term Evolution
LTE-A	Long Term Evolution - Advanced
M&C	Management and Control
MAAP	Multiple Access Aggregation over PON
MAC	Media Access Control
MANO	Management and Orchestration
MCA	Management, Control & Analytics
MD	Multi-Degree
MDSC	Multi-Domain Service Coordinator
MDT	MEC Deployment Trials
MEC	Multi-access Edge Computing
MEF	Metro Ethernet Forum
MIMO	Multiple-Input Multiple-Output
ML	Machine Learning
mMTC	massive Machine-Type Communications
MoCA	Multimedia over Coax
MP2MP	Multiple Point-to-Multi-Point
MPI	MDSC-PNC Interface
MPLS	Multiprotocol Label Switching
MQTT	Message Queuing Telemetry Transport
MR	Mixed Reality
MSA	Multi-Source Agreement
MSS	Maximum Segment Size
MSTI	Multiple Spanning Tree Instance
MU-MIMO	Multi User Multiple Input Multiple Output
MUX	Multiplexer
NBI	North Bound Interface
NE	Network Element
NFV	Network Functions Virtualisation
NG	Next Generation
NMS	Network Management System
NR	New Radio
NW-TT	Network Side TSN Translators
O&M	Operation and Maintenance
OAM	Operation, Administration and Management
ODN	Optical Distribution Network
ODU	Optical Data Unit
OFDMA	Orthogonal Frequency Division Multiple Access
OIF	Optical Internetworking Forum
OLT	Optical Line Terminal
OMCC	OMCI Communications Channel
OMCI	ONU Management and Control Interface
ONU	Optical Network Unit
OOK	On-Off Key
OOSE	One way Source to EAR
OPEX	OPeration EXpenditure
O-RAN	Open Radio Access Network
ORP	Optical Ring Passive
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
OSS	Operating Support System
OSU	Optical Service Unit
OTDR	Optical Time Domain Reflectometer
OTN	Optical Transport Network
OTT	Over the Top
OTU	Optical Transport Unit

OXC	Optical Cross-Connect
P2MP	Point-to-Multi-Point
P2P	Point-to-Point
PACS	Picture Archiving and Communication System
PCE	Path Computation Element
PCEP	Path Computation Element communication Protocol
PCR	Path Control and Reservation
PDH	Plesiochronous Digital Hierarchy
PDN	Public Data Network
PDV	Packet Delay Variation
PE	Provider Edge
PIN	Positive Intrinsic Negative (diode)
PKI	Public Key Infrastructure
PLOAM	Physical Layer Operation, Administration and Management
PMD	Physical Media Dependent
PNC	Provisioning Network Controller
PoC	Proof of Concept
PoE	Power over Ethernet
POL	Passive Optical LAN
PON	Passive Optical Network
PS	Project Stream
PTP	Precision Time Protocol
QAM	Quadrature Amplitude Modulation
QKD	Quantum Key Distribution
QinQ	Queue in Queue
QoE	Quality of Experience
QoS	Quality of Service
QSFP	Quad Small Form-factor Pluggable
RAM	Random Access Memory
RAN	Radio Access Network
RATS	Remote ATtestation ProcedureS
RF	Radio Frequency
RFC	Requests for Comments
RG	Residential Gateway
RH	Relative Humidity
RIS	Radiology Information System
RJ	Registered Jack
ROADM	Reconfigurable Optical Add/Drop Multiplexer
RP	Reference Point
RPC	Remote Procedure Call
RS	Reed Solomon
RSSI	Received Signal Strength Indication
RSVP	Resource Reservation Protocol
RTT	Round Trip Time
RU	Radio Unit
RUC	Use case Requirements [RUC#-xx]
SAND	Server and Network Assisted DASH
SC	Square Connector
SD	Standard Definition
SDH	Synchronous Digital Hierarchy
SDI	Serial Digital Interface
SDN	Software Defined Networking
SDO	Standard Organisation
SLA	Service Level Agreement
SME	Small and Medium Enterprise
SMF	Session Management Function
SMP	Service Mapping Point
SMPTE	Society of Motion Picture and Television Engineers
SNMP	Signalling Network Management Protocol
SR	Spatial Reuse
SRLG	Shared Risk Link Group
SRV	Service Record

ST	Standard
STA	Station
TC	Technical Committee
TC	Transmission Convergence
TCG	Trusted Computing Group
T-CONT	Traffic Container
TCP	Transmission Control Protocol
TDD	Time Division Duplexing
TDM	Time Division Multiplexing
TDMA	Time Division Multiple Access
TE	Traffic Engineering
TEAS	Traffic Engineering Architecture and Signaling
TEE	Trusted Execution Environment
TLS	Transport Layer Security
TM	TeleManagement (forum)
TPM	Trusted Platform Module
TR	Technical Report
TS	Timeslot
TSN	Time-Sensitive Networking
TT	TSN Translators
TV	TeleVision
TWDM	Time and Wave Division Multiplexing
TWT	Target Wake Time
UC	Use Case
UDP	User Data Protocol
UE	User Equipment
UHD	Ultra High Definition
UHDTV	Ultra High Definition TeleVision
UL	UpLink
UNI	User Network Interface
UPF	User Plane Function
UPnP	Universal Plug and Play
URLLC	Ultra Reliable Low Latency Communication
uRLLC	ultra-reliable and low-latency communications
USP	User Service Platform
V2X	Vehicle-to-everything
vAN	virtual Access Node
VCSEL	Vertical-Cavity Surface-Emitting Laser
vDBA	virtual Dynamic Bandwidth Allocation
VLAN	Virtual LAN
VM	Virtual Machine
VNO	Virtual Network Operator
VOD	Video On Demand
VP	Virtual Presence
VR	Virtual Reality
vRAN	virtual Radio Access network
VxLAN	Virtual Extensible LAN
WAN	Wide Area Network
WAVE	Web Application Video Ecosystem
WDM	Wavelength-Division Multiplexing
WFA	Wi-Fi® Alliance
WG	Working Group
WLAN	Wireless Local Area Network
WLCP	Wireless LAN Control Plane
WT	Working Text
XG	10 Gigabits
XGPON	10 Gigabit Symmetrical PON
XG-PON	10G PON
XGS-PON	10-Gigabit-capable Symmetric Passive Optical Network
xPON	(x = G, XG, XGS) PON
XR	Extended Reality
YANG	Yet Another Next Generation data modelling language

ZSM Zero-touch network and Service Management

4 Technology requirements and landscape

4.1 Overview

4.1.1 Introduction

This clause relies on the use cases defined in ETSI GR F5G 002 [i.14] and specifies per use case the technology requirements, the current available related standards, and describes the gaps in technology and standards to implement those use cases.

NOTE: Some clauses define requirements, standards, and gaps for several similar use cases together. Also a description of technologies, which can be used in many use cases is provided in clause 5.

The following use cases are included in the present document, refer to ETSI GR F5G 002 [i.14] for a detailed description of the use cases. In the following, only brief use case titles are given for reference:

- UC#1: Cloud Virtual Reality, clause 4.2.
- UC#2: High Quality Private Line, clause 4.3.
- UC#3: High Quality Low Cost private lines for SMEs, clause 4.4.
- UC#4: Fibre on-premises networking : Fibre-to-The-Room (FTTR), clause 4.5.
- UC#5: Passive optical LAN, clause 4.6.
- UC#6: PON for Industrial Manufacturing, clause 4.7.
- UC#8: Multiple Access Aggregation over PON (MAAP), clause 4.8.
- UC#10: Scenario Based Broadband, clause 4.9.
- UC#11: Telemetry-based Enhanced Performance Monitoring in Intelligent Access Network, clause 4.10.
- UC#13: Remote Attestation, clause 4.11.
- UC#14: Digitalized ODN/FTTX, clause 4.12.
- UC#15: Virtual Presence, clause 4.13.
- UC#16: Enterprise private line connectivity to multiple Clouds, clause 4.14.
- UC#17: Premium home broadband connectivity to multiple Clouds, clause 4.15.
- UC#18: Virtual Music, clause 4.16.
- UC#19: Next Generation Digital Twins, clause 4.17.
- UC#20: Media transport, clause 4.18.
- UC#21: Edge/Cloud-based visual inspection for automatic quality assessment in production, clause 4.19.
- UC#22: Edge/Cloud-based control of automated guided vehicles (AGV), clause 4.20.
- UC#23: Cloudification of Medical Imaging, clause 4.21.
- UC#24: F5G for Intelligent Mine, clause 4.22.
- UC#25: Enhanced optical transport network for Data Centre Interconnections, clause 4.23.

- UC#26: Enhanced Point to Point optical access, clause 4.24.
- UC#28: High-speed Passive P2MP Network Traffic Aggregation, clause 4.25.
- UC#30: Bandwidth on Demand, clause 4.26.
- UC#31: Intelligent Optical Cable Management, clause 4.27.
- UC#32: AI-based PON optical path diagnosis, clause 4.28.

4.1.2 Document structure overview

The remainder of clause 4 covers the use case itemized in clause 4.1.1. The structure of each use case is:

- Brief use case overview.
- Technology related to use case and associated requirements.
- Current standards relevant to the use case.
- Gaps in standards to meet the requirements.

The order of the use cases match that of the defined in ETSI GR F5G 002 [i.14] and the requirements are structure as [RUC#-xx] where UC# is the use case number defined in ETSI GR F5G 002 [i.14] and xx is the sequence number of the requirements. The Gaps have a similar structure [GapUC#-yy] and again UC# is the use case number defined in ETSI GR F5G 002 [i.14] and yy is the sequence number of the gaps. There should be a one to one correspondence between requirement and gap. If the requirements are already satisfied by current standards then the gap is labelled 'None' to indicate there is no gap.

Clause 5 elaborates on the state of play of the existing technologies. Clause 6 summarizes the requirements and associated gaps if any. It also maps the gaps to the SDO's that are or will work to resolve the gaps.

4.2 Cloud Virtual Reality

4.2.1 Use case briefing

The use case on Cloud Virtual Reality (VR) introduced cloud computing and cloud rendering technologies for VR services. In this use case, the Cloud VR content data are stored in the cloud when requested, Cloud VR content data are read, rendered, coded compressed and transmitted to user terminals through the network. The Cloud VR service will place stringent requirements on the network, such as bandwidth, guaranteed and deterministic latency, and low delay jitter and packet loss rate. To support multiple high definition Cloud VR applications and support a high quality of experience, the network should have high bandwidth (e.g. > 1,5 Gbps), low latency (e.g. < 8 ms), low delay jitter (e.g. < 7 ms) and low packet loss rate (e.g. $\leq 10^{-7}$).

This use case focuses on the use of OTN. It is acknowledged that there are alternative technical approaches in the industry, which are well-known (e.g. IP/Ethernet) and do not need further discussion.

4.2.2 Technical requirements

4.2.2.1 Cloud VR network performance requirements

The development of Cloud VR focuses on quality of experience, continuous improvement in image quality, interaction, and immersive experience. The synergy between content production and transmission, determines the grade of Cloud VR experiences. The quality of Cloud VR service experience can be ranked into the following four phases:

- fair-experience;
- comfortable-experience;
- ideal-experience;

- ultimate-experience phases.

The network requirements of Cloud VR for each phase are shown in Table 1.

NOTE 1: There are other sources, which mention similar network requirements e.g. GSMA Cloud AR/VR Whitepaper [i.107] In the public domain, bitrates related to VR streaming services are mentioned that are much lower. These likely refer to non-interactive (cloud-) VR services. This is left for further study.

Table 1: Expected Network requirements of Cloud VR in each phase

Cloud VR Phase	1	2	3	4
Typical full-view resolution	4K	8K	12K	24K~
Typical terminal resolution	2-3K	4K	8K	16K~
Traffic Bitrate	≥ 40 Mbps	≥ 65 Mbps	≥ 270 Mbps	≥ 770 Mbps
Recommended Network Bitrate	≥ 80 Mbps	≥ 130 Mbps	≥ 540 Mbps	≥ 1 540 Mbps
RTT requirement	20 ms	20 ms	10 ms	8 ms
Delay jitter requirement	< 15 ms	<15 ms	<10 ms	< 7 ms
Packet loss rate requirement	$\leq 10^{-5}$	$\leq 10^{-6}$	$\leq 10^{-7}$	$\leq 10^{-7}$

NOTE 2: The RTT requirement is the delay of the network and the delay jitter requirement is an additional varying delay.

NOTE 3: Cloud VR experience phases:

- Cloud VR Phase 1 (Fair Experience Phase): The content is represented by 4K VR. The terminal screen resolution is about 2K. The image quality is equivalent to that of 240 pixels or higher on a traditional TV.
- Cloud VR Phase 2 (Comfortable Experience Phase): The content is represented by 8K VR. The terminal screen resolution is about 4K. The video quality is equivalent to that of 480 pixels or higher on a traditional TV.
- Cloud VR Phase 3 (Ideal Experience Phase): Content is represented by 12K VR. The terminal screen resolution is about 8K. The development of the terminals and the content enables users to enjoy ideal experience. The picture quality is equal to that of 1 080 pixels or higher on traditional TV.
- Cloud VR Phase 4 (Ultimate Experience Phase): The content is represented by 24K. The terminal screen resolution is about 16K. The image quality is equivalent to that of 4K traditional TV.

[R01-1] The F5G network shall support configurations that satisfies the network performance requirements of the corresponding Cloud VR phases in Table 1.

4.2.2.2 High performance channel requirements

4.2.2.2.1 Home network performance

For any of experience phases mentioned in the previous clauses, the VR headset ("terminal") should be wirelessly connected, and this connection of course should meet the network requirements. In ideal and ultimate phase (phases 3 and 4), the bandwidth requirements are 540 Mbps and 1,5 Gbps. The theoretical data rate of Wi-Fi® 6 standard are shown in Table 2, and due to interference on the air interface, the actual achievable data rate may be reduced by 40 % or even lower than the theoretical rate. Normally, the terminal only has 2 antennas, which seriously limit the data rate of the terminal. To achieve good user experience, the terminal should have higher antenna specification. Wi-Fi® 6 can meet the bandwidth requirements of Cloud VR services and Wi-Fi® slicing technology can provide lower latency.

Table 2: Data rate of Wi-Fi® standards depending on the antenna configuration

IEEE Protocol	Frequency	Theoretical Data Rate
IEEE 802.11ax [i.52] (Wi-Fi® 6)	2,4/5/6 GHz	1,2 Gbps (2 × 2 MIMO, 80 MHz) 2,4 Gbps (2 × 2MIMO, 160 MHz) 4,8 Gbps (4 × 4 MIMO, 160 MHz) 9,6 Gbps (8 × 8 MIMO, 160 MHz)

In Table 2, latency and jitter are not mentioned as it is assumed they do not change for different antenna capabilities.

[R01-2] To meet the Cloud VR phases 3 and 4 the terminal shall support Wi-Fi® 6 with advanced antenna configuration.

[R01-3] To meet the Cloud VR phases 3 and 4 Wi-Fi® 6 slicing shall be supported.

4.2.2.2.2 Access network performance

In ideal and ultimate experience phases (phases 3 and 4), the average bit rate of a single channel of Cloud VR is 270 Mbps and 770 Mbps respectively. It can be seen in Table 3, that GPON under certain assumptions cannot satisfy the bandwidth requirement of Cloud VR in ideal and ultimate experience phases. It can also be seen in Table 3 that XG(S) PON should have a split ratio less than 1:16 to meet the ultimate experience phase. In addition, a low latency scheduling algorithm shall be used to reduce the latency and delay jitter of the Access Network segment.

Table 3: PON data rate and split ratio requirements

PON	Capacity (Gbps)	Available Load (Gbps)	Split Ratio	Actual Installation Rate	User Bandwidth (Mbps)
GPON	2,5	2,3	1:16	60 %	239
XG PON	10	8,6	1:16	60 %	896
XG PON	10	8,6	1:8	60 %	1 792

[R01-4] The F5G Access Network shall support XG(S) PON, ensuring the Cloud VR phases 3 and 4 are satisfied.

[R01-5] The F5G Access Network XG(S) PON shall support a split ratio of less than 1:16, ensuring Cloud VR phases 3 and 4 are satisfied.

[R01-6] The F5G Access Network shall support a low latency scheduling algorithms.

4.2.2.2.3 OLT Enhancement

Current OLTs are Ethernet based and all traffic is switched via a layer 2 switch, which is responsible for forwarding of traffic to and from the OLT. To achieve low latency and jitter Cloud VR traffic need to be identified and allocated a priority route to the cloud VR data centre. This route can be achieved by several approaches, via Ethernet or OTN.

The first approach implies remaining in the Ethernet domain and the Cloud VR service traffic shall be allocated priority routes to minimize latency and round trip delay. The Cloud VR traffic shall be identified and delineated via VLAN's or equivalent mechanism and isolated from other services traffic. It is also necessary to allocate appropriate priority and sufficient bandwidth to Cloud VR services exiting the OLT Ethernet uplink. To ensure quality of experience the priority Cloud VR routes shall be low latency and minimize round trip delay.

The alternative approach is to use OTN, this may require that the OLT be equipped with OTN line card(s) with connection to the Ethernet switch or an Ethernet connection to OTN equipment, the former is preferable to minimize delay. The connection from the Ethernet switch to the OTN card/equipment should have sufficient bandwidth to support all Cloud VR traffic, which are likely delineated via VLANs or equivalent mechanism. The OTN card/equipment shall support variable size containers to match the Cloud VR bit rate from 40 Mbits/s to 770 Mbits/s. Current ODUj (j = 0, 1, 2, 3, 4, flex) nominal minimum bit rate is 1,25 Gbits/s well in excess of that required by Cloud VR traffic. There is a need for a finer granularity container capable of supporting bit rates from 40 Mbits/s to 770 Mbits/s. It is also ideal that the OTN container size is flexible to match the variable capacity needs of the Cloud VR traffic demand. There is a new standardization project in ITU-T which introduces a new OTN container type. This new container is named the Optical Service Unit (OSU), which might support client rates from 2 Mbits/s to 1 Gbits/s, which is an efficient mechanism to transport Cloud VR traffic from the OLT to the Cloud VR data centre.

[R01-7] The F5G OLT should support OTN.

[R01-8] The F5G OTN Aggregation Network shall support variable size containers to match the Cloud VR bit rate from 40 Mbits/s to 770 Mbits/s.

4.2.2.2.4 Aggregation network performance

In ideal and ultimate phases, the bandwidth requirement of the aggregation network may be extremely high. For example, in the case of the aggregation edge node supporting 20 000 users, the traffic could reach 500 Gbps to 1,5 Tbps (assuming the penetration rate of 50 % and concurrency rate of 20 %) It is estimated that the port rate needs to evolve to 400 Gbps or even 1 Tbps.

Table 4: F5G Aggregation Network rate requirements

User Number	VR User Penetration Rate	Peak Concurrency Rate	Bit Rate (Mbps)	Data Rate Requirement (Gbps)
20 000	50 %	20 %	280 (Ideal Level)	560
20 000	50 %	20 %	770 (Ultimate Level)	1 540

The Cloud VR service places stringent requirements on the network, especially for the latency and delay jitter. Cloud VR in fair experience phases, require the RTT to be less than 20 ms. It can be transported with current Internet services, but the Cloud VR service experience needs committed bandwidth, guaranteed deterministic latency, and low packet loss. In comfortable, ideal and ultimate experience phases, much lower latency is required, to ensure an excellent Cloud VR experience. Therefore the Cloud VR traffic should be transported via an independent channel that ensures the desired performance and thereby isolates the traffic from existing internet services traffic. To implement this, an ONU identifies Cloud VR traffic and directs it to an independent channel. From the server side, Cloud VR traffic is transported via the same independent channel. When a cloud VR service is established the network should automatically recognize the change and allocate the bandwidth. This is true in the case of a single session, however if other users are using the same service then the slice bandwidth needs to be seamlessly increase without interfering with the established users. The reverse is true if the user releases a Cloud VR service the network should automatically recognize the change and deallocate the bandwidth. This again is true in the single user case however if other uses remain on the service then the slice bandwidth needs to seamlessly decrease without interference with the other users.

[R01-9] The F5G Aggregation network shall deploy OTN.

[R01-10] The F5G network shall support higher scheduling priority for Cloud VR service compared to other Internet services.

[R01-11] The F5G Access Network shall support high quality independent channels for the Cloud VR phase 3 and 4 services.

[R01-12] The F5G network shall automatically increase or decrease the bandwidth utilization for VR services to accurately meet the Cloud VR service bandwidth requirements.

4.2.2.3 Dynamic channel requirements

When the Cloud VR service is transported via a shared channel or an independent channel, an operational flow of actions for enabling high quality Cloud VR service is required. Once the VR service is setup, the network channel should meet the network requirement of the service. After the VR service ends, the resource of network channel can be released.

The current network channel consists of home network, Access Network, Aggregation Network and data centre segments. The data plane and management plane of each network segment is independent from each other. Hence, the channel setup mechanism of each network segment is also different and independent. To improve the efficiency of the network, these four network segments should support a mechanism that dynamically sets up the End-to-End channel when the Cloud VR service is setup by the users and releases the channel when the Cloud VR service ends.

Because there are several independent managements system, E2E bandwidth expansion or contraction is difficult to coordinate. There need to be a mechanism that supports these bandwidth changes without the need for coordination between the management systems, a low level handshake mechanism with minimal interaction with the management layer is ideal. The F5G network shall support dynamic set up and release of the high-quality network connection for Cloud VR services to guarantee the performance of Cloud VR service and increase the transmission efficiency of the F5G network.

[R01-13] The F5G network shall support dynamic set up and release of the high-quality network connection for Cloud VR service.

[R01-14] The F5G independent management systems should support a mechanism that dynamically sets up and releases the End-to-End connections.

[R01-15] The F5G network shall support a mechanism for dynamic bandwidth changes with minimal interaction with the management layer.

4.2.2.4 Efficient transport of cloud VR services

In order to carry a Cloud VR service with guaranteed performance and efficient resource utilization, the cloud VR service should be transported separately from other services via end-to-end hard slicing over PON and then either over IP/Ethernet or OTN, depending on which mechanism is chosen. To maximize transport efficiency, there should be accurate bandwidth matching between the Cloud VR service and its corresponding allocated E2E network slice. Based on Table 1, the four levels of VR experiences, require channel data rates from 40 Mbits/s to 770 Mbits/s. The slice bandwidth should be flexible with appropriate fine granularity. Here again if OTN is used then OSU is suitable for this purposes, matching the required Cloud VR rate and efficiently using the bandwidth of the OTN link. OTN links available today range from 2,5 G (OTU1) to 400 G+ (OTUCn) and should have minimum wastes of capacity and support a mixture of tradition ODUk as well as OSU traffic.

[R01-16] The F5G network shall support dedicated slices for Cloud VR traffic transport.

[R01-17] F5G slice shall match the Cloud VR bandwidth requirements.

[R01-18] The F5G management shall support coordinated E2E slice management.

4.2.3 Current related standard specifications

For the current related standard specifications refer to clause 5.

4.2.4 Gap analysis

4.2.4.1 Gap Context

In the present document the gaps refer to existing standards and not to technology in general. Some vendor's products that are not standardized could exist that implement the solutions described in the gaps.

4.2.4.2 Cloud VR network performance

The development of Cloud VR focuses on quality of experience, continuous improvement in image quality, interaction, and immersive experience. The network requirements for each of the Cloud VR phases are shown in Table 1. The following clauses elaborate on the potential gaps to meet these performance parameters.

[Gap01-1] None.

4.2.4.3 High performance channel requirements

4.2.4.3.1 Home network performance

Wi-Fi6 can meet the bandwidth requirements of Cloud VR services in each phase and Wi-Fi® slicing technology is available for lower latency, so no gap.

[Gap01-2] None.

To meet Cloud VR complete experience, the terminal should have advanced antenna capabilities, this will be satisfied by the user upgrading his equipment, so no technical gap.

[Gap01-3] None.

4.2.4.3.2 Access network performance

To achieve the bandwidth requirement of Cloud VR in ideal and ultimate experience, XG PON should be used with an appropriate split ratio if ideal experience phase and ultimate experience phase users are to be satisfied. The split ratio is a deployment issue so no gap. The Access Network supports a low latency scheduling algorithm so no gap.

[Gap01-4] None.

[Gap01-5] None.

[Gap01-6] None.

4.2.4.3.3 OLT Enhancement

Currently OLT's do not support OTN connectivity, this is a gap that need to be resolved in future deployments. OLT shall have direct uplink to OTN network in addition to current packet network. The OTN network need to support sub one gigabit data rate to be capable of supporting the Cloud VR service bit rates, which range from 40 Mbits/s to 770 Mbits/s. There is currently a gap in the OTN container efficiency, with the lowest bit rate available today being ODU0 with a nominal bit rate of 1,25 Gbits/s. The ODU0 could be used however its packing density efficiency for the Cloud VR bit rates range is 3,2 % to 62 %. However if an OSU is used the packing density efficiency for the Cloud VR bit rate range is 96 % to 99,7 %.

[Gap01-7] Currently OTN is not supported on the OLT.

[Gap01-8] OTN container with flexible and sub1G granularity to efficiently support Cloud VR traffic rates are currently not supported.

4.2.4.3.4 Metro network performance

For fair experience phases, the Cloud VR service can be transported by current Internet services, and it should have higher scheduling priority compared with other services, so no gap exists.

[Gap01-9] None.

For comfortable, ideal and ultimate experience phases, the Cloud VR service requires lower latency , low delay jitter, and a high quality independent channel is needed which would imply slicing is needed.

Assuming OTN is deployed in the aggregation network then there is no gap in technology deployment. The only available OTN container is nominally 1,25 Gbits/s, based on this an OTU4 could only carry 80 channels of Cloud VR traffic, and when moving towards the OTUCn links with 5G tributary slots it is still only 80 channels at 400 Gbits/s, by using muxing of ODU4 into ODUC4, up to 320 channels can be obtained, which is a very inefficient use of the aggregation network bandwidth, assuming all the traffic is of Cloud VR type. But the aggregation network shall support a variety of traffic bandwidth including 400GE. However if for example the Cloud VR bit rate of 40 Mbits/s is considered and using OSU then an OTU4 could carry around 2 380, and ODU0 (nominal rate 1,25 Gbits/s) can carry 30 channels.

[Gap01-10] OTN support for mixed traffic of ODUs and OSUs is currently not defined.

In general, home network, Access Network and aggregation network can meet the bandwidth requirements of Cloud VR services in each phase. The latency requirements is the main challenge.

[Gap01-11] The coordination of network slicing between home network, Access Network and Aggregation Network to form an end-to-end slice to meet end-to-end latency requirement is currently not supported.

The need for the network to recognize the establishment or release of Cloud VR service need to be developed. Assuming slicing is used as recommended then the slice bandwidth need to automatically increase or decrease seamlessly taking other users' bandwidth into account so as not to disturb their user experience.

[Gap01-12] The automatic bandwidth increase or decrease to accurately meet the bandwidth requirements of Cloud VR services in a seamlessly manner, is currently not supported.

4.2.4.4 Dynamic channel setup and release

The management plane for the home network, Access Network, Aggregation Network and data centre parts maybe independent of each other. So set up and tear down of the Cloud VR channel are different and independent for each of the management systems.

Based on the independent nature of the management system, the E2E on demand requests are difficult to coordinate. A simple handshake mechanism with minimal need for inter-management system coordination is missing.

[Gap01-13] Currently the F5G network does not support a coordinated management mechanism to setup or release a connection for Cloud VR services.

[Gap01-14] The independent management systems do not currently coordinate together to support a mechanism that dynamically sets up the End-to-End connections.

[Gap01-15] A simple mechanism for dynamic bandwidth changes with minimal need for coordinated management interaction is currently not supported.

4.2.4.5 Efficient transport of Cloud VR services

Today's network traffic can be delineated either on a packet or OTN network, but E2E service isolation via slicing is missing. The ability to identify Cloud VR traffic and carve out an E2E path via a slice is also missing. The ability to match the Cloud VR bandwidth in an efficient manner to the OTN container to establish the network slice is missing. The ability to easily satisfy bandwidth demand changes dynamically with minimal management involvement is missing making slice bandwidth control difficult.

[Gap01-16] E2E service isolation via slicing is currently not supported.

[Gap01-17] Currently OTN container bandwidth matching Cloud VR rates is currently not supported.

[Gap01-18] A simplified E2E slice management system is currently not supported.

4.3 High Quality Private Line

4.3.1 Use Case briefing

High quality Private Line needs to meet strict requirements on bandwidth, latency, availability, security, Cloud accessibility, service provisioning time, as well as operation and maintenance of the bearer network.

This use case focuses on the use of OTN. It is acknowledged that there are alternative technical approaches in the industry, which are well-known (e.g. Ethernet) and do not need further discussion.

The primary applications of high-quality Private Line are:

- Governments:
  - Interdepartmental communications.
  - Public services accessed by secure web sites.
  - Public service announcements.
- Large companies:
  - Inter-site department communications.
  - Data Centre connectivity.
  - Cloud connectivity.

- Financial institutions:
  - Banks:
    - Inter site and HQ communications.
    - Data centre connectivity.
  - Securities & futures.
- Medical institutions:
  - Public services.
  - Data Centre for medical records.

The above is not a complete list of applications of high-quality Private Line but mentions some typical examples.

These applications have common demands on a Private Line:

- Guaranteed bandwidth: The bandwidth shall be guaranteed based on an SLA, and match the users' needs, which may vary on time of year or time of day.
- Low latency: Some businesses demand ultra-low latency, e.g. stock exchange demands as low latency as possible.
- Five-nines availability: The network outage probability needs to be limited to $<10^{-5}$.
- Totally secured network: The private line services need to be immune to hacking.
- Access to Cloud services.
- Intelligent operation and maintenance of their connectivity.

4.3.2 Technology Requirements

4.3.2.1 General introduction

High quality Private Line services have strict requirements on bandwidth, latency, availability, security, Cloud accessibility, service provisioning time, as well as operation and maintenance of the bearer network.

OTN technology is well suited to provide private line services for large-scale enterprise networking. The capacity and performance of OTN can be tailored to match the current and future requirements.

4.3.2.2 Connection Overview

High quality Private Line has one or more point-to-point connections from one or more CPEs to the Central Office. The CPE supports the necessary site connectivity and services to match the user needs. Legacy services need to be supported, so mixed protocol support is necessary.

The OTN Aggregation Equipment will support OTUk (k = 0, 1, 2) and potentially OTU25/50-RS/OTU4 on the tributary card as depicted in Figure 1. The need for OTU25/50-RS/OTU4 will depend on customers' bandwidth needs. The OTN Aggregation Equipment line card will support OTU4 or OTUCn (n = 1, 2, 3, 4 …), depending on the deployment requirements. The OTN Aggregation Equipment supports hard isolation of user traffic via the use of separate ODUs. This ensures isolation of private line user traffic from other private line users and other users, guaranteed bandwidth, and dedicated ODUs per Private Line user are required. The management and control layer needs to be able to identify Private Line user traffic and route this traffic End-to-End appropriately. The management function should identify and manage different Private Line user services and via the use of different ODUs to develop a network of end-to-end service paths or slices via dedicated ODUs.

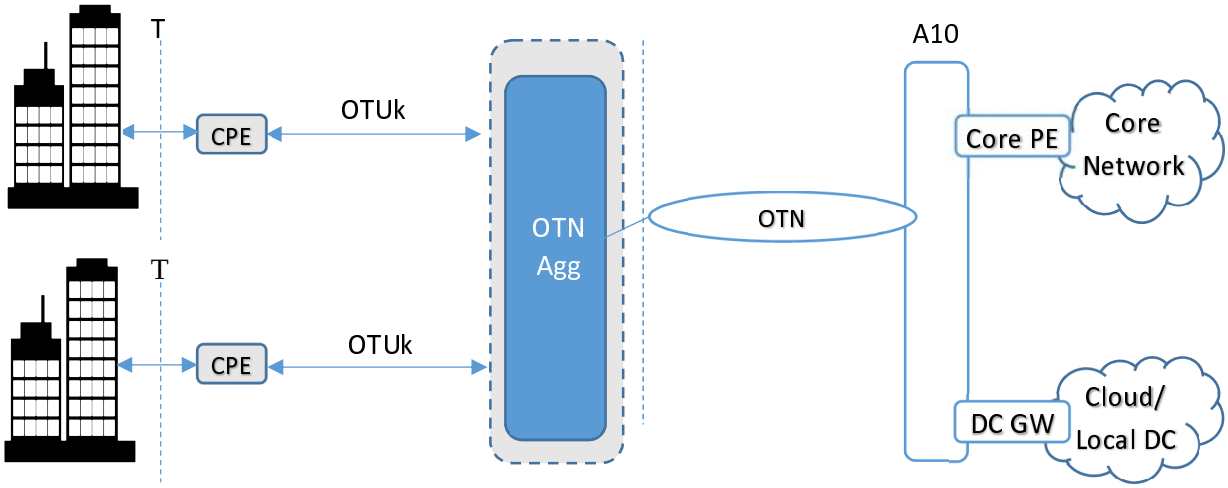


Figure 1: OTN Aggregation Equipment in the CO

4.3.2.3 Flexible Bandwidth

There shall be an agreed baseline or off-peak bandwidth guaranteed and the allowance for bursty traffic, and an absolute peak bandwidth limit, which will be part of the SLA. As an addition, it shall be possible for bandwidth requirements to change over time as the bandwidth usage expands or contracts. The bandwidth is customer dependent, and the range and granularity are for further study.

[R02-1] The F5G network should provide flexible bandwidth allocation.

4.3.2.4 Private line User Isolation

One Private Line shall be totally isolated from other private line and general traffic. This requires non-shared channels End-to-End. End-to-end connections are established across the network via multi-hop network equipment that is required to implement isolation paths across the network.

[R02-2] The F5G network should provide an end-to-end connection, which is isolated from other traffic.

4.3.2.5 On Demand Ordering

High quality Private Lines require efficient on-demand provisioning of end-to-end connections. Additional installations and services upgrades shall be supported by the provisioning system.

The provisioning system shall have the end-to-end connection up and running in the order of seconds when physical equipment is installed and available to be remotely configured.

[R02-3] The F5G network should provide an efficient on-demand connection provisioning and configuration system.

4.3.2.6 Guaranteed Reliability

End-to-end protection paths are required, such as cross-device dual-homing protection and fibre break protection, etc. The protection switching time shall reach the carrier-class of 50 ms, and the availability shall be higher than 99,999 %.

[R02-4] The F5G network should support availability greater than 99,999 %.

4.3.2.7 Low latency

Some Private Lines shall support low latency end-to-end connections that meet the following requirements:

- Low latency.
- Deterministic delay.

- Independent of network traffic load.

[R02-5] The F5G network should support deterministic low latency.

[R02-6] The F5G network should support low latency independent of traffic load.

4.3.2.8 Private DC and Cloud access

High quality Private Line shall allow dedicated access to:

- Private Data Centres of the users.
- Cloud services.

These end-to-end connections shall provide sufficient security, reliability, and bandwidth.

[R02-7] The F5G network should support dedicated access to the users private Data Centres.

[R02-8] The F5G network should support dedicated access to Cloud services.

4.3.2.9 Scalability

Both the line card and tributary card shall be configurable to match the current and growing needs of the Private Line users:

- The number of customers shall determine the Cross Connect capacity.
- Customer connectivity needs such as DC and Cloud services will determine the line card and tributary card bandwidth.

[R02-9] The F5G network should support configurable connectivity to match the user's current and future needs.

[R02-10] The F5G network should support efficient on-demand expansion or contraction of the provided connections.

4.3.3 Current related standard specifications

This use case focuses on OTN as the main technology to support high quality Private Line. To that end, an OTUk, (where k = 0, 1, 2), as well as OTU25-RS and OTU50-RS for higher bandwidth needs, will be used. These OTN point-to-point links can be used to support Private Line for both legacy TDM and Ethernet services. The Central Office should be equipped with OTN Aggregation Equipment, with high bandwidth links to the network such as OTU4 or OTUCn (n = 1, 2, 3, 4…) depending on required connectivity to the network. Different ODUs can be provisioned to separate Private Line user traffic.

Related standards include:

- Recommendation ITU-T G.709 [i.67].
- Recommendation ITU-T G.709.1 [i.108].
- Recommendation ITU-T G.709.2 [i.109].
- Recommendation ITU-T G.709.3 [i.110].
- Recommendation ITU-T G.709.4 [i.111].

4.3.4 Gap analysis

4.3.4.1 Gap Context

In the present document the gaps refer to existing standards and not to technology in general. Some vendor's products that are not standardized could exist that implement the solutions described in the gaps.

4.3.4.2 Flexible Bandwidth

This requirement in part is satisfied by the current OTN network. Once the bandwidth needs fit within fixed ODUk/ODUflex rates, and expansion of rates is currently possible by moving to the next higher standard rate.

However, there is a need for a more flexible bandwidth allocation. Current OTN containers are based on ODUk and ODUCn nominal rates such as of 1,25 Gbits/s, 2,5 Gbits/s, 10 Gbits/s, 25 Gbits/s, 40 Gbits/s, 50 Gbits/s, 100 Gbits/s, and any rate ≥ 1,25 Gbits/s. However, legacy services require lower rates and finer granularities. Not every Private Line customer's application matches the current OTN rates, so the ability to allocate multiple rates including sub-1G within the same domain is missing from the current OTN.

[Gap02-1] Currently sub-1G bandwidth granularity containers are not supported in OTN.

4.3.4.3 Private line User Isolation

Today's OTN provides hard isolation from other user traffic, however there is a growing need for not only connection isolation, but also service isolation. This requires the network to recognize different services and allocate dedicated paths or slices for these services. These services usually do not require equal bandwidth, and have different priorities for the customers. The network needs to allow for non-equal service usage.

[Gap02-2] Service-level slicing is currently not supported.

4.3.4.4 On Demand Ordering

OTN can support on-demand provisioning of the connection, however this will depend on the capabilities of the CPE and Edge node software. This may require upgrading of CPE and Edge node to support hitless upgrading of bandwidth to satisfy the on-demand request.

[Gap02-3] The on-demand ordering capability for both the CPE and Edge node is not currently supported.

4.3.4.5 Guaranteed Reliability

OTN can offer guaranteed availability once the necessary fibre connections are available from the CPE to allow for redundant connection. So OTN does satisfy this requirement.

[Gap02-4] None.

4.3.4.6 Low and deterministic Latency

As OTN is a TDM based approach, latency is deterministic and independent of traffic load.

[Gap02-5] None.

[Gap02-6] None.

4.3.4.7 Private DC and Cloud access

OTN can provide the necessary dedicated access to both private and public Data Centres.

[Gap02-7] None.

[Gap02-8] None.

4.3.4.8 Scalability

This scenario assumes the installation of OTN Aggregation Equipment in the Central Office.

The current OTN is a scalable network anywhere from 1,25 Gbits/s to 400 Gbits/s and beyond. The legacy services such as 100 Mbits/s Ethernet, PDH and SDH are supported via ODU0 with 1,2 G capacity, which is inefficient. There is a need for a more efficient packing density for legacy and low bandwidth services to be supported. A sub-1 Gbits/s level granularity is needed to allow for better scalability and more efficient use of bandwidth.

In the other direction, the need for higher bandwidth means that CPE needs to support services such as 10 GE, 25 GE, and above.

[Gap02-9] Currently OTN does not support finer OTN granularity below 1,25 Gbits/s.

[Gap02-10] Current CPE do not support higher speed interfaces.

4.4 High Quality Low Cost private lines for SMEs

4.4.1 Use Cases briefing

There are a large number of Small and Medium Enterprises (SMEs) and they are widely distributed. They are raising demands for networking with higher capacity and quality than those required by residential users. Traditional private line services provide high-quality networking services for enterprises, but at a relatively high price for SMEs, so a new type of private line with high quality and low cost needs to be delivered for these SMEs.

4.4.2 Technology Requirements

4.4.2.1 General introduction

Currently, mainstream technologies such as OTN and Ethernet private line are mature for large-scale enterprise networking, but they require dedicated infrastructures and the associated costs are high. In addition, both the capacity and performance of these technologies exceed SME requirements, leading to inefficient network resource utilization. SMEs are widely distributed geographically (many SMEs are located in residential areas) and they are very cost-sensitive. If the home access technology can be reused, the cost of SME private lines may be greatly reduced.

Currently, the mainstream fibre based home broadband access mode is PON-based FTTH, which features wide coverage and low cost. However, the private line service requirements of SMEs are different from those of home broadband. Currently, the PON network used for home broadband is not able to meet the functional and performance requirements of SMEs. If the traditional PON network can be optimized and enhanced to improve its guaranteed bandwidth, stability, and reliability to meet SME requirements, it will be advantageous to connect SMEs through the PON network.

4.4.2.2 CPN to support a large number of terminals

Generally, the CPN of a SME needs to support a large number of terminal devices including both wired and wireless devices. In most SMEs, numerous wireless terminals (such as laptops and mobile phones) are used, which usually work concurrently. In addition, wired devices, such as desktops, printers, phones, and production equipment, can be directly connected to the CPN, which is either connected to the CPE's network ports or through Ethernet switches.

While current Ethernet can support the required number of wired devices in an SME CPN, the number of devices that require concurrent wireless connections is growing significantly, often beyond what current wireless Access Points (APs) can handle. To solve this problem, multiple APs need to be deployed in the SME network. These APs need to support plug-and-play and support collaboration and seamless roaming. To further improve the high bandwidth and low latency requirements for multiple concurrent users, these APs need to support network slicing and multi-user MIMO.

[R03-1] The Wi-Fi® APs shall support plug-and-play setup and seamless roaming between APs.

[R03-2] The Wi-Fi® APs shall support multi-user MIMO.

[R03-3] The SME CPN shall support network slicing.

4.4.2.3 Quality assurance (bandwidth, latency, reliability)

SME users have higher bandwidth requirements than home broadband users such as high concurrent bandwidth and high requirements for upstream bandwidth. The SME private line can be configured to guarantee the total bandwidth of all services of an enterprise. The SME private line can also be configured to guarantee the bandwidth of only high-priority services selected by the enterprise. For example, the SME private line can guarantee the bandwidth of high-priority services such as voice, video live broadcast, video conference, video surveillance backhaul/query and cloud based services, and set remaining services to low priority. SMEs need to share the network infrastructure with home users, therefore, isolation between SMEs and home users is one of the key factors to ensure network service quality.

Network slicing and service identification and mapping are effective means to ensure Internet access service quality.

Network slicing is not a new technology. However, most network slices are soft slices, which are mainly reflected on the management plane. Actual resources can still be shared among different slices, and hardware resource reservation for high-priority services is not supported. Hardware slicing reserves dedicated hardware resources (such as buffers, CPU computing capabilities, Wi-Fi® air interface resources, and PON timeslots) for high-priority services that are not shared with low-priority services, to implement hard isolation between different priorities. E2E slicing is needed to be supported to isolate private line services from other users such as home broadband users and other SMEs for quality assurance. E2E slicing shall be supported to isolate different applications of a private line service for application quality assurance. In addition E2E slicing need to isolate a private line service from other traffic to ensure private line application quality.

[R03-4] Hardware slicing of the Wi-Fi®, CPE, and PON shall be supported.

[R03-5] E2E slicing shall be supported isolating different users.

[R03-6] E2E slicing shall be supported isolating different applications.

4.4.2.4 Quality of Experience for cloud based services

With the development of digitization, more and more enterprises choose to use cloud based information systems (IT systems, big data storage, and office applications) and even core systems (production control systems and core data processing systems). This requires high bandwidth and better than 99,99 % reliability with low latency and jitter. In order to guarantee the performance requirements, the network needs to manage the traffic from the device to the cloud or from the device to the cloud service provider peering point.

[R03-7] The SME private line network shall support high quality communication to cloud platforms of different providers.

[R03-8] The interface between the network service provider and the cloud provider shall be open and interoperable.

4.4.2.5 Low cost based on reusing residential Access Network

Many SMEs are located in residential areas. Therefore, the SME network needs to share the access and aggregation networks with home broadband users. This sharing of the Access Network can also take advantage of off-peak traffic between commercial users and home users to make more efficient use of the infrastructure and reduce the cost of SME private lines.

To ensure the SLA of SME private lines, the carrier network needs to isolate enterprise private line users from home broadband users to provide differentiated services. The SME private line management system needs time-of-day based SLAs, to take advantage of the different traffic profiles of business and residential customers.

[R03-9] SME private line services should be supported on the same infrastructure as residential services.

[R03-10] The SME private line management system should support time-of-day based SLAs. .

4.4.2.6 High availability and reliability

SMEs require higher network reliability than home broadband users. Protection technologies are needed to improve network reliability to achieve a network availability of 99,99 %.

[R03-11] The F5G Network should support protection to achieve network availability of 99,99 %.

4.4.2.7 Fast provisioning and highly efficient management and operation

SME private line services should be provisioned quickly, in the order of days or even minutes in case of immediate hardware availability. The intelligent management system provides an open North Bound Interface (NBI) to interconnect the upper-layer OSS with the intelligent management system and enables quick provisioning of private line services and automatic and fast provisioning of cloud network services as well.

Technologies needed to enable:

1) Private line CPE plug-and-play.

2) Automatic and fast fault detection, demarcation, isolation and correction.

3) Network operating SLA indicator or SLA visualization Apps for enterprise users.

[R03-12] The F5G network shall support fast provisioning of SME private line service, which includes private line CPE and multi-APs systems plug-and-play.

[R03-13] The F5G network shall support automatic fault detection, demarcation, isolation and correction.

[R03-14] The F5G network management system should support the visualization of network operation SLA indicators to SMEs and operators.

4.4.3 Current related standard specifications

BBF TR-178 [i.15] has specified L2VPN and L3VPN services for business customers. Access Network and Aggregation Network are implemented by Carrier Ethernet and IP MPLS to support these services.

Refer to clause 5.1 for the Wi-Fi® technology status. Beyond that, Wi-Fi® Alliance® has defined EasyMesh™ for multiple APs.

Wi-Fi® EasyMesh™ is a certification program that defines home and small office Wi-Fi® networks with multiple APs that are easy to install and use, self-adapting, and multi-vendor interoperable. This technology brings both the consumers and the service provider's additional flexibility in choosing Wi-Fi® EasyMesh™ devices for home deployment.

Wi-Fi® EasyMesh™ uses a controller to manage the network, which consists of the controller plus additional APs, called agents. Establishing controllers to manage and coordinate activity among the agents ensures that each AP does not interfere with the other, bringing both expanded, uniform coverage and more efficient service.

4.4.4 Gap analysis

4.4.4.1 Gap Context

In the present document the gaps refer to existing standards and not to technology in general. Some vendor's products that are not standardized could exist that implement the solutions described in the gaps.

4.4.4.2 CPN to support a large number of terminals

Wi-Fi® Alliance has developed Wi-Fi® CERTIFIED EasyMesh™ that supports AP plug-and-play and mobility of Wi-Fi® clients. However, the performance of roaming among APs needs to be further improved.

IEEE 802.11 [i.164] has defined multi-user MIMO, which supports up to 128 devices concurrently.

[Gap03-1] Improvement of EasyMesh™ technology for supporting better roaming performance is currently unavailable.

[Gap03-2] The slicing and quality guaranteed services for multi-AP scenarios are currently not standardized.

[Gap03-3] Slicing in the CPN to meet the high quality requirements of SMEs is currently not defined.

4.4.4.3 Quality assurance (bandwidth, latency, reliability)

1) Traffic identification and mapping

At CPE and access node, the private line service traffic needs to be classified differently from other services and forwarded via a high-priority data channel. A service identification rule and forwarding policy may be statically configured at CPE and access node according to 5-tuple information based on the IP and MAC address of a packet, or a VLAN attached to a fixed port. Although this solution is stable and reliable, it is complex and inflexible. It is difficult to respond to user or application requirements dynamically and in real time.

AI-based intelligent service traffic identification and service flow mapping can automatically identify and set forwarding rules to respond to users' high-priority service requirements dynamically and in real time. Currently, mature AI architectures and algorithms are available in the industry. However, their functions, configurations, and management interface standards need to be defined based on the actual application requirements.

[Gap03-4] Hard slicing of Wi-Fi®, CPE, and PON is currently not supported.

[Gap03-5] AI based traffic identification support to distinguish private line service from other users as well as to identify different applications of a private line service is currently not supported.

2) End-to-End slicing

Existing slicing standards mainly define a soft slicing solution for Access Network. The embodiment is the slicing of the data plane that is mainly designed from the management perspective. In fact, network resources are still shared among slices, while hardware resources such as computing capacity, buffer, PON line resources, and Wi-Fi® air interface resources are not exclusively designated and reserved for high-priority services.

An enhanced slicing solution is reserving hardware resources exclusively for high-priority services to ensure that enterprise users and home broadband users share network resources, with hard isolation between home broadband and enterprise services. Thereby ensuring that the enterprise services are not affected by the home broadband services.

In this case, network devices should support at least two slices to separate home broadband and enterprise services. To further differentiate applications inside enterprise or home broadband services, for example, isolating video services from internet services, more slices need to be supported.

[Gap03-6] E2E slicing mechanism including management standards for fixed network are currently not defined.

4.4.4.4 Quality of Experience for cloud based services

The network architecture shall be able to support traffic steering and enable high quality communication to cloud platforms of different providers.

[Gap03-7] None.

[Gap03-8] The interface between the F5G network and the cloud network for guaranteed services, specifically in cases where the cloud provider and the network operator are in different administrative domains is currently not specified.

4.4.4.5 Low cost based on reusing residential Access Network

Usually the infrastructure can be re-used, however, the management and control system differs due to the different requirements of the market segments. The management of SME private line service is missing.

[Gap03-9] None.

[Gap03-10] Time-of-day based SLA management interface and data models are currently not supported to the required level.

4.4.4.6 High availability and reliability

There are protection mechanisms for Access Network and Aggregation Network, and so there is no gap for the technology.

[Gap03-11] None.

4.4.4.7 Fast provisioning and high efficient management and operation

Self-installation and efficient provisioning are usually supported for residential services, but are not supported for SME private line services due to the more complex SME environment.

[Gap03-12] Fast provisioning of private line services including private line CPE and multi-APs systems plug-and-play are currently not defined.

[Gap03-13] Automatic fast fault detection, demarcation, isolation, and correction are currently not defined.

[Gap03-14] Visualized SLA indicators for network operation are currently not supported.

4.5 Fibre on-premises networking: Fibre-to-The-Room (FTTR)

4.5.1 Use case briefing

The current connections in the house are mostly copper or wireless based, and they suffer from limited capacity due to the restricted frequency range and limited spectrum resource. In this case, users would like to deploy new media for the on-premises network. Fibre is a preferred upgrade choice for the on-premises network due to its future proof capabilities.

The other case is for business and corporate LAN. In general, these LANs are composed of multi-port switches (providing P2P links over Ethernet copper cable) connected to WAN routers. The cable infrastructure is very complex and the size of multi-port device is larger in these LANs. With passive optical devices, such as optical splitter, the Fibre In-Premises (FIN) system would have several advantages, i.e. simple fibre deployment, wider coverage, immunity to Electro-Magnetic Interference (EMI), low power, and long life cycle.

NOTE: This use case is using Local Area Networks (LANs) for small areas. See the use case on passive optical LAN in clause 4.6, where the LAN is covering a larger area.

4.5.2 Technical requirements

4.5.2.1 General introduction

Although PON has been accepted and deployed in the market as a major solution for optical Access Networks, the on-premises applications are quite different from that in an Access Network. This is leading to distinct technical requirements for network topology, optical components parameters, physical and data link layer protocols, network configuration and management. All of those topics should be addressed for the fibre-based on-premises network.

4.5.2.2 Variety of data rate profile

A variety of devices connect to the home network and to the business & corporate LAN using different services. With the rapid home digitalization, more connected devices are emerging. For example, for an IoT application, the environmental sensor detects the physical conditions and communicates the data. High resolution television requires bandwidths of 10 to several 100 of Mbps per video stream. AR/VR applications require 100 Mbps to 1 Gbps data rate. Dense connection in Small & Medium Enterprise (SME) require up to 10 Gbps aggregated data rate. In the future, new services (e.g. holographic communications) and network devices may require 10 or even several 100 of Gbps network capability.

With the evolution of technologies, it is obvious that multiple generations of network technologies could coexist in the same network. The fibre-based on-premises network should be capable to adapt to this co-existence.

[R04-1] The fibre-based on-premises network shall support multiple profiles (in terms of data rate) for different types of network device.

[R04-2] The fibre-based on-premises network shall support up to 10 Gbps date rate.

4.5.2.3 Lower optical link budget

In a FIN system, the optical link budget depends on 3 factors, the fibre length, the split ratio and the number of connectors. It is important to focus on the first two as they impact the architectural choice.

For fibre on-premises networking, the fibre length is expected to be less than 1 km, therefore the related attenuation is small. Therefore the main factor becomes the split ratio, which depends on the number of connected points. For most apartments and detached houses, a split ratio of 1:16 is considered to be sufficient and lower than that deployed in the Access PON Network, which means the optical link budget can be much lower than that of a typical Access PON Network.

For an apartment building or SME LAN, using FIN technology, the split ratio could be 1:32 which is still lower than that of an Access PON FTTH scenario (the typical value is 1:64). Since on-premises fibre length is shorter than in an Access PON Network, again the link budget primarily depends on the split ratio.

[R04-3] The fibre-based on-premises Residential network shall support a split ratio of 1:16.

[R04-4] The fibre-based on-premises apartment building or SME network shall support a split ratio up to 1:32.

4.5.2.4 Seamless roaming support for Wi-Fi® connection

Wi-Fi® is the most widely used technology for connecting end user devices. Mobility of users may require switching the connection between different Access Points (APs). The APs are connected by the fibre-based on-premises network for high capacity. If the switching time between APs exceeds that imposed by the QoS requirements of the service, this will result in poor user experience. In case a fibre-based on-premises network is used as a backhaul network, Wi-Fi® handover requires priority.

In the handover process, a sequence of handover protocol messages are exchanged between access points. Any potential loss of the message will cause the handover process to stop or to retry, especially when Wi-Fi® is used as the backhauling link for the AP. To achieve a guaranteed or robust exchange of handover messages, it is better to choose a fibre connection to minimize the transmission latency. In addition, the handover process also requires successful communication between AP and stations (STA) in time. This needs an end-to-end coordination over fibre and wireless link.

[R04-5] The fibre-based on-premises network shall support a dedicated high-priority channel for exchanging signalling messages.

[R04-6] The fibre-based on-premises network should support a mechanism, to provide a guaranteed intercommunication channel for APs.

[R04-7] In order to avoid any potential message contention in the fibre backhaul link between P-ONU and E-ONU and wireless fronthaul link between ONU and STA, The fibre-based on-premises network shall define a coordinated mechanism for different nodes in the network.

4.5.2.5 Support of diversified transceiver

For fibre-based on-premises networks, the fibre is deployed over a short distance. For most houses or enterprise buildings, tens to hundreds of metres are sufficient. The short transmission distance results in lower optical insertion loss. The transceiver profile could be quite different from that of the current Access Network PON transceivers. For example, VCSEL based transmitter and PIN based receiver could be used for such distances. Besides single mode fibre, multi-mode fibre or plastic fibre are candidates for the fibre infrastructure.

[R04-8] The transceiver profile shall be optimized to match the fibre deployment (including fibre topology, fibre and connector types).

4.5.2.6 Network security

The on-premises network needs to be protected against cyber-attacks, in particular in view of the increasing number of connected devices and amount of accessible sensitive data. For business users, the network security is even more important than for residential users. Authentication of new devices needs be supported on the on-premises network to ensure that all devices in the network are known and safe. The following are the minimum requirements that an on-premises network should comply with in terms of security.

[R04-9] The on-premises network should support authentication of all new devices connecting to the network.

[R04-10] The on-premises network should support data encryption.

4.5.2.7 Fibre infrastructure

In most buildings, fibre infrastructure is not available and needs to be deployed. Easy and low cost solutions should be considered for on-premises fibre deployments. In the traditional fibre installation, splicing is used to join fibre segments. Pre-connectorized optical cables, which are now commonly used, do simplify the procedure of fibre deployment.

For small houses, fibre to each room could be connected directly to the residential gateway, however this will be challenging for multi-floors houses. In this scenario, an uneven optical splitting method could be used to enable optical splitting on each floor so that the fibre infrastructure is further simplified. In addition, to reduce the difficulty of fibre deployment, an optical and electrical hybrid cable could be used.

NOTE: The uneven optical splitting method in a cascaded ODN topology and is defined as follows. It contains at least an optical power splitter, which has at least one trunk branch, which connects to the next stage of splitters. And it has at least one ONU branch, which connects to one or more ONUs. The split ratio between these is at least two, branches are unequal to each other, and usually the trunk branch has a higher split ratio than an ONU branch's split ratio.

In a cascaded ODN topology, an optical power splitter, which has at least one trunk branch connecting to the next stage of the splitter, and at least one ONU branch which connects to an ONU, while the split ratio between these is at least two, branches are unequal to each other, normally the trunk branch has a higher ratio than an ONU ratio.

[R04-11] Fibre with pre-connectorized optical cable should be used in the on-premises network.

[R04-12] The on-premises network shall be P2MP topology.

[R04-13] The on-premises network should support the use of uneven optical power splitter should in multi-floor buildings.

[R04-14] The on-premises network should support the use of optical and electrical hybrid cable for Wi-Fi® AP devices.

4.5.2.8 Power saving and management

Smart home services are considered to be one of the most important applications for the home network. These services include a variety of different, frequently battery-powered, IoT sensors and actuators, communicating with an IoT hub. The IoT hub may also be battery powered, acting as a gateway between the IoT network and the Residential Gateway (RG). While the communication between the IoT hub and the sensors/actuators is on a radio channel, the IoT hub could be conveniently connected to the RG by fibre. In this case the on-premises fibre network should support a low power mode.

Some IoT services, e.g. a fire alarm, may require low latency communication, and the fibre on-premises network should guarantee these requirements. Since the triggering of some IoT events is coming from the sensor, the IoT hub shall be able to control the low power modes.

[R04-15] The fibre-based on-premises network shall support a low power mode for IoT applications.

[R04-16] The fibre-based on-premises network shall enable the IoT hub to manage the coordination between the IoT hub and the residential gateway in low power mode.

4.5.2.9 Support of network QoS

Customer experience depends on the QoS supported by all the network segments in the end-to-end connection, and also on that of the on-premises network. The support of a given QoS may require control of different parameters (such as data rate, latency and packet loss, etc.).

[R04-17] The fibre-based on-premises network shall define a QoS related transmission mechanism.

4.5.2.10 Support of East-to-West data streaming

East-to-West data communication is needed for the on-premises network. The traditional PON network does not support the direct communication between ONUs. Generally, an Ethernet switch is necessary for packet routing, which will add delay. Direct node-to-node communication may be needed to better support East-to-West data streaming.

[R04-18] The fibre-based on-premises network shall support East-to-West data communication.

[R04-19] The fibre-based on-premises network shall support symmetric transmission data rate between P-ONU and E-ONU.

4.5.3 Current related standard specifications

4.5.3.1 IEEE

IEEE 802.3AH [i.20] is the EPON standard in which Ethernet and PON technology are combined. Based on the passive optical network architecture, a new physical layer specification is defined (mainly addressing optical interfaces). 10G-EPON is defined as the next generation of EPON by IEEE 802.3AV [i.21]. Table 5 shows the basic optical power budget and wavelength allocation requirement of 10G-EPON. The lowest loss budget is 20 dB for 10 km and the highest loss budget is 29 dB for 20 km. A cooled EML shall be used for downstream and a DML shall be used for upstream. The requirements seem to be too strict for the FTTR and POL use cases.

Table 5: Optical power budget and wavelength allocation requirement of 10G-EPON

Description	Low Power Budget		Medium Power Budget		High Power Budget		Units
	PRX10	PR10	PRX20	PR20	PRX30	PR30	
Number of fibres	1						-
Nominal downstream line rate	10,3125						GBd
Nominal downstream wavelength	1,25	10,3125	1,25	10,3125	1,25	10,3125	GBd
Downstream wavelength tolerance	-2, +3						nm
Nominal upstream line rate	1 577						nm
Nominal upstream wavelength	1 310	1 270	1 310	1 270	1 310	1 270	nm
Upstream wavelength tolerance	±50	±10	±50	±10	±50	±10	±10
Maximum reach	≥ 10		≥ 20		≥ 20		km
Maximum channel insertion loss	20		24		29		dB
Minimum channel insertion loss	5		10		15		dB

4.5.3.2 ITU-T

GPON was first proposed by the FSAN in September 2002, then ITU-T Q2/SG15 (Optical Access Network) standardized the GPON series Recommendation ITU-T G.984 series [i.27]. GPON has a downstream capacity of 2,488 Gbits/s and an upstream capacity of 1,244 Gbits/s that is shared among users. XG-PON is the ITU-T's next generation standard following on from GPON. Asymmetric 10G-PON is specified as XG-PON: 10 Gbits/s downstream and 2,5 Gbits/s upstream (nominal line rate of 9,95328 Gbits/s downstream and 2,48832 Gbits/s upstream).Symmetric 10G-PON is also proposed as XG-PON2 with 10 Gbits/s upstream, but would require burst-mode lasers on Optical Network Units (ONUs) to deliver the upstream transmission speed. The following table shows the different optical path loss classes for XG(S)-PON. The lowest optical path loss class is 29 dB and the highest is 35 dB. It is stricter than the IEEE standard. Besides, the differential distance requirement is 20 km and 40 km which is also stricter than the IEEE standard.

Table 6: Different optical path loss classes for XG(S) PON

	'Nominal1' class (N1 class)	'Nominal2' class (N2 class)	'Extended1' class (E1 class)	'Extended2' class (E2 class)
Minimum loss	14 dB	16 dB	18 dB	20 dB
Maximum loss	29 dB	31 dB	33 dB	35 dB

The same wavelength allocation for 10G-EPON is applied to XG(S)-PON, which means similar optics as in 10G-EPON can be used for XG(S) PON. However, the optical power budget of XG(S) PON is higher, so the requirements of the transceiver is also higher.

For the internal management channel, the control, Operation, Administration and Management (OAM) information in an ITU-T PON system is carried in three ways:

- embedded OAM, Physical Layer Operation, Administration and Maintenance (PLOAM); and
- ONU Management and Control Interface (OMCI).

The embedded OAM and PLOAM channels manage the functions of the PMD and TC layers. OMCI provides a uniform system for managing higher (service-defining) layers. The embedded OAM and PLOAM functions are specified in the TC recommendation of each PON generation. For example, the embedded OAM and PLOAM of XG-PON system is specified in Recommendation ITU-T G.987.3. The OMCI functions are specified in Recommendation ITU-T G.988 [i.29] which provides plenty of functions for ONU management.

ITU-T Q16/SG15 has been working on Recommendation ITU-T L.109 [i.112], which is an optical-electronic composite cable standard for the FTTA (fibre to the antenna) scenarios. Currently there is no standard for optical-electronic composite micro-optical cables for the FTTR scenarios.

In addition, ITU-T Q18/SG15 (home network) initiate G.fin project (High speed fibre-based in-premises transceivers) for the FTTR scenario. Four recommendations, including system architecture, physical layer, data link layer and network management are planned for the G.fin project. Two corresponding technical paper ("Architecture, function and service of home network" and "Use case & requirements of Fibre-To-The-Room (FTTR)") have been published in 2021. A supplement document on FTTR use cases for small and medium enterprise (SME) has been published in 2022. The group is now focusing on specifying the system architecture of FTTR technology before defining the protocols.

4.5.3.3 Broadband Forum (BBF)

The Broadband Forum (BBF) specifies the application layer protocol BBF TR-069 [i.22] for remote management and provisioning of Customer-Premises Equipment (CPE)) network. The protocol provides a series of functions, including auto-configuration, software or firmware image management, status and performance managements, diagnostics etc. Figure 2 shows the CWMP remote management in an E2E architecture. As can be seen, the protocol is defined as the communication between the Auto-Configuration Server (ACS) and the CPE (such as residential gateway, set-top box, Wi-Fi® AP, etc.). The corresponding device data model is also specified, for example, in BBF TR-181 [i.23]. This protocol could be extended to manage the fibre-based on-premises network.

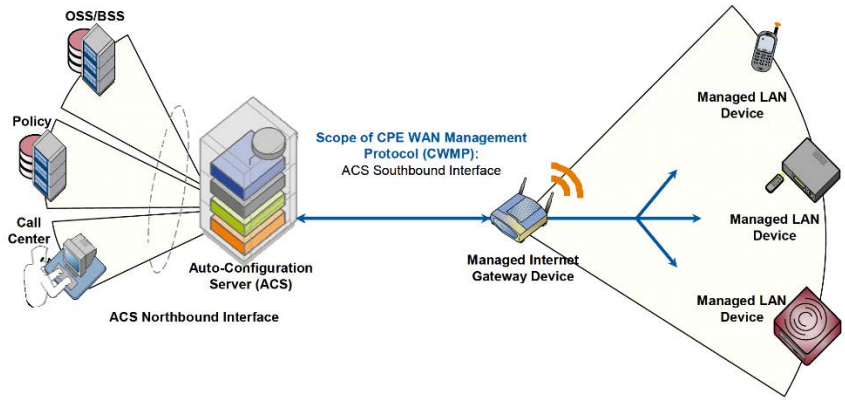


Figure 2: CWMP remote management in E2E architecture

As the natural evolution of CWMP protocol, BBF TR-369 [i.24] - universal service platform has been developed to build up the management relationship as controller and agent, extending to a global management system. Specifically, a couple of light weight transport protocols are supported (such as COAP, MQTT, etc.), which enable the protocol to be suitable for IoT applications.

4.5.3.4 Wi-Fi® alliance (WFA)

Wi-Fi® EasyMesh™ is a certification program in the Wi-Fi® Alliance that defines a Multi-Access Point specification for forming a Wi-Fi® backhauling network. The protocol is based on IEEE 1905.1 [i.25] and the extension of the interface facilitates new functionalities such as installation, self-adaptation, and multi-vendor interoperability. EasyMesh™ uses a controller to manage the network, which consists of the controller plus additional APs, called agents. Allowing the controllers to manage and coordinate activity among the agents, ensures that each AP does not interfere with the other, bringing both expanded, uniform coverage and more efficient service.

4.5.4 Gap analysis

4.5.4.1 Gap Context

In the present document the gaps refer to existing standards and not to technology in general. Some vendor's products that are not standardized could exist that implement the solutions described in the gaps.

4.5.4.2 General

The fibre-based on-premises network should consider the practical network requirements with respect to on-premises and business LAN. It is not easy to directly use PON systems in such applications. There are still gaps that need to be filled before such deployments are feasible.

4.5.4.3 Variety of data rate profile

The current PON system supports only On-Off Key (OOK) modulation. Different generations of PON systems enable data rate upgrade by increasing the modulation bandwidth with another wavelength. Flexible data rate profile in a single wavelength is valuable to support various complex device requirements. Higher modulation may be utilized to make good use of the channel capacity with ample link budget in short range optical communication.

[Gap04-1] A variety of data rate profiles for fibre-based on-premises network in terms of modulation bandwidth, high modulation scheme, etc. are not currently available.

[Gap04-2] None.

4.5.4.4 Lower optical link budget

The typical optical link budget is 29 dB or higher for the Access Network in the current recommendations, while 20 dB may be enough for on-premises networks. By considering the different requirements for specific scenarios, multiple optical link budget classes should be defined for the different scenarios.

[Gap04-3] The optical link budget from 0~23 dB is currently not specified for Residential networking.

[Gap04-4] None.

4.5.4.5 Seamless roaming support for Wi-Fi® connection

EasyMesh™ is defined by the Wi-Fi® Alliance® (WFA) to facilitate multi-AP for LAN interconnection. The protocol is based on IEEE 1905.1 [i.25] and supports interconnection of both wireline and wireless technology. Moreover, the protocol is built above the physical layer and MAC layer, thus the exchange of the protocol message is not bound to the transmission technology itself. Obviously, this is not optimized for the protocols.

[Gap04-5] The high-priority channel for roaming is currently not supported.

[Gap04-6] The mechanism to recognize network signalling and protocols is currently not supported.

[Gap04-7] The fibre and wireless coordination mechanism is currently not supported.

4.5.4.6 Diversified transceiver and fibre types

Different fibre deployments will lead to distinct requirements for the transceiver design. Of course, re-use of the current optical components in the new design needs to be considered. For new on-premises networks, there is no need to consider the coexistence with legacy generations in the past. However, the future coexistence is an important issue. The new transceiver specifications should consider but is not limited to the following items:

- Light source type (e.g. VCSEL, FP laser, DML, EML, etc.).
- Detector type (e.g. PIN diode or APD).
- Wavelength plan (e.g. re-use PON wavelength (downstream@1490nm/ upstream@1310nm, downstream@11577nm/ upstream@1270nm), or use new wavelength (850 nm, downstream 1330nm/ upstream@1270)).
- Transmission power.
- Receiver sensitivity.
- Fibre type: single mode fibre, multi-mode fibre, plastic fibre, optical and electrical hybrid fibre.

It should be noted that the specifications of these above items usually depend on the optical power budget requirement, the maturity of the industry supply chain, future evolution ability and so on.

[Gap04-8] Optimized transceivers parameters (such as transmission power, receiver sensitivity, dispersion, etc.) for single mode fibre and new parameters of P2MP transceivers for multi-mode fibre and plastic fibre are currently not supported.

4.5.4.7 Network security

For traditional PON systems, device authentication and data encryption are supported. There are different authentication methods and AES-128 is supported for data encryption in PON systems. As the fibre-based on-premises network is used in residential area or business building, the users may not be knowledgeable of the detailed security configuration.

[Gap04-9] Simplified authentication process is currently not supported.

[Gap04-10] None.

4.5.4.8 Fibre infrastructure

Different kinds of passive distribution device and components can be used for different scenarios. Current fibre connectors are too large and not suitable for deploying them through ducts. Current optical and electrical hybrid cables are mainly used for 5G small cells. The size of the cable and connector is large, and the power supply capability is more than enough for on-premises application.

[Gap04-11] Small size connectors with good protection is currently not standardized.

[Gap04-12] None.

[Gap04-13] None.

[Gap04-14] Small size optical and electrical hybrid cable with appropriate bend radius as well as the connectors are currently not defined.

4.5.4.9 Power saving and management

Many of the wireline communication technologies have defined a power saving mode in the ITU-T/IEEE standards. PON technology also specify the power saving mode in two ways: sleep mode and listening mode. However, in PON technology, the power mode selection is determined by the Optical Network Unit (ONU). In addition, the power saving mode is not often used since the ONU is not a low power device. For connecting the IoT device by using the fibre-based on-premises network, a new power saving mode is required to fulfilling the technical requirements of the IoT service.

[Gap04-15] None.

[Gap04-16] A mechanism for IoT hub to manage the coordination in low power mode between the IoT hub and the RG needs to be defined.

4.5.4.10 Support of network QoS

In communication technologies priority queuing in the MAC layer is used to achieve differentiating packet transmission opportunities, resulting in providing methodologies to target network QoS requirements. In PON technology, a transmission data rate related parameter (T-CONT) is used to specify the demand on the data rate. However, only one factor reflecting the date rate is not enough to satisfy the network QoS. The protocol should define multi-dimension QoS parameters for dedicated service.

[Gap04-17] The transmission QoS mechanism that allows for multi-dimension network parameters, such as data rate, round trip delay, packet error rate, etc. is currently not standardized.

4.5.4.11 Support of East-to-West data streaming

East-to-West data communication is needed for the on-premises network. The traditional PON network does not support the direct communication between ONUs. Generally, an Ethernet switch is necessary for packet routing, which will add delay. Direct node-to-node communication may be needed to better support East-to-West data streaming.

[Gap04-18] A direct node-to-node communication method on layer 2 for fibre-based on-premises network is currently not defined.

[Gap04-19] Symmetric transmission data rate is not supported in 2,5 Gbps data rate profile.

4.6 Passive optical LAN

4.6.1 Use case briefing

Local Area Networks (LANs) are widely deployed in a variety of business scenarios, such as campus, high-rise buildings, hotel, school, hospital, stadium, shopping centres, etc., providing connection to end-users and transporting digital business data for both south-to-north and east-to-west directions. The connection to end devices could be wireless (Wi-Fi®) and wireline (Ethernet). The backhauling of the LAN traditionally uses Layer 2 switches, Layer 3 routers and connected media by using copper Ethernet cable, e.g. CAT5 cable. This deployment approach has many shortcomings. One of which is the missing support for emerging business needs, while others include the complexity of the cable deployment, the bottleneck to upgrade the transmission data rate due to the copper medium, and the high power consumption.

An optical fibre infrastructure is an ideal approach to replace the traditional copper-based deployments. Benefits of the fibre approach are long lifetime, smaller diameter cable compared to copper Ethernet cable, low transmission loss, low emissions, less active equipment, and low power consumption. Enterprises are adopting passive optical LAN (POL) solutions based on PON technology for LAN deployment.

4.6.2 Technical requirements

4.6.2.1 General introduction

PON technology is a very successful technology in access network for FTTH scenario, and is continuously being upgraded with higher throughput (for example, from GPON, to XG(S)-PON, to 50G-PON). It is advantageous to leverage PON technology for POL deployment. However, according to the characteristics of business services, it is necessary to adapt the PON technology for the POL application.

The FTTR requirements as specified in clause 4.5.2 shall apply also for this use case.

4.6.2.2 Network slicing

Business scenarios, like campus deployments, usually have multiple sub-networks for different services: typically an internal network (Intranet), public Internet access and intelligent service network (a network for dedicated campus services, such as security, IoT, surveillance). POL shall be capable of recognizing the different network types and allocate appropriate network resources to ensure that the service priority and network operation is satisfied.

In order to guarantee the transmission requirements for the various kinds of services, network slicing is indispensable in a POL system, which will partition the whole POL network into different sub-networks. One physical OLT can be sliced into different slices that can be allocated to each sub-network. There may be multiple slices allocated to each sub-network depending on the required priority of the traffic within a sub-network. Each network slice has its own reserved network resources, e.g. different sub-networks using different VLANs, slice demarcation based on MAC address resources, slice by forwarding plane. In POL, the management plane may not be sliced, because it is under the control of a single administrative entity. Typically, the business scenario like campus has a private team for network management.

There are a number of network slicing technologies, which provide both control-plane and user-plane isolations. Slicing granularities are showed in Table 7.

NOTE: The slicing functions and requirements are similar to the Industrial PON use cases as described in clause 4.7.2.

Table 7: Different Slicing Granularities

Slicing granularity	Detailed description
Line-card level slicing	Each OLT line-card can be configured as a sub-network
PON port level slicing	Each PON port on the OLT line-card can be configured as a sub-network
ONU level slicing	Different ONUs within the same OLT line-card port can be configured as a sub-network
ONU port level slicing	Different ONU interfaces within the same ONU can be configured as a sub-network

[R05-1] POL technology shall support network slicing functionality.

[R05-2] The POL slicing functionality should support the multiple granularities as defined in Table 7.

4.6.2.3 Network security and reliability

There are many business scenarios, including bank, government, hospital, etc., that require security, protection and reliability (> 99,99 %) for continuous service operation. It is also necessary to implement PON protection switching technology (including Type B and Type C PON protection [i.98]) to ensure the stability of applications and deal with service interruptions caused by network failures.

[R05-3] POL technology should support data encryption in L2 layer.

[R05-4] POL technology should support PON protection Type B and Type C as defined in IEEE 802.az [i.98].

4.6.2.4 Centralized access control

Wi-Fi® is the most widely used technology for connecting end user devices. Mobility of devices require dynamic switching of connections among different Access Points (APs). The behaviour of multiple AP should be centrally controlled. For example, seamless roaming can enable stable connection and service continuity under centralized control.

A large number of APs are deployed in LANs using the POL solution (such as to deploy AP in rooms of campus, hotel, school, hospital, etc.). An Access Controller (AC) is normally used in POL. Many functionalities are moved from the AP to the access controller, like authentication, security key exchange, determination of roaming, etc. In this case, a "Fit AP" type (having only the encryption and radio functions) is preferred to deploy with less complexity. In general, the "Fit AP" need to be maintained and managed by the AC and cannot work alone.

[R05-5] The POL OLT should support a centralized control function for the Wi-Fi® access in the POL network.

[R05-6] The ONU should support "Fit AP" mode, controlled by the access controller.

4.6.2.5 Power over Ethernet (PoE)

The ONUs in POL could provide direct links to other devices like security camera, deployed around the building, and surrounding areas. For many of those scenarios, it is difficult to have localized power available. Hence it is essential that the ONU supports PoE/PoE+/PoE++ functionality on the Ethernet ports.

[R05-7] The POL ONU should support PoE/PoE+/PoE++ functionality.

4.6.3 Current related standard specifications

4.6.3.1 ITU-T PON standards

For PON standard in ITU-T SG15 Q2 refer to clause 4.5.3 of the present document.

4.6.3.2 Broadband Forum

There are several standards defined by BBF on Access Network slicing technologies. As BBF TR-370 [i.16] targets a business case for sharing an Access Network by multiple Virtual Network Operators (VNOs), where Access Network is sliced by Infrastructure Provider (InP) and operated by multiple VNOs. And BBF TR-386 [i.17] defines management interface to support the roles of VNOs and InP.

4.6.4 Gap analysis

4.6.4.1 Gap Context

In the present document the gaps refer to existing standards and not to technology in general. Some vendor's products that are not standardized could exist that implement the solutions described in the gaps.

4.6.4.2 Network slicing

Network slicing in POL needs to be supported for sub-network partitioning and for the isolation of different services according to the business scenarios.

[Gap05-1] Slicing standards are not currently defined for the POL scenarios

[Gap05-2] The granularities and requirements of network slicing for POL are currently not supported.

4.6.4.3 Network security and reliability

The standardized PON technology has built-in network security functions, including network access control and data encryption. The PON protocol defines lower layer transmission, i.e. PMD and TC. The data encryption takes place in the PON TC layer. PON protection solutions are well known and adopted. Different methodologies, including Type A/B/C/D are defined.

[Gap05-3] None.

[Gap05-4] None.

4.6.4.4 Centralized access control

The centralized control function is typically vendor specific. The exact functionality of centralized access control is not well specified.

[Gap05-5] The functionality requirements and technologies of centralized access control are currently not specified for POL.

[Gap05-6] The "Fit AP" functional requirements of the corresponding ONU are currently not specified for POL.

4.6.4.5 Power over Ethernet (PoE)

PoE is widely applied in LAN deployments. IEEE 802.3 [i.163] is working on this subject for quite a long time. The corresponding testing standards are also well addressed.

[Gap05-7] None.

4.7 PON for Industrial Manufacturing

4.7.1 Use Cases briefing

Passive Optical Network (PON) with its high bandwidth, low deployment cost, smart operation functions and capability for easy upgrade, has been the dominant choice of fibre Access Network solutions. It has been deployed worldwide to provide various Fibre-To-The-X (FTTX) services, to fulfil the broadband access demands of both residential and enterprise customers.

On the other hand, the evolution of modern industrial manufacturing defines new demands of the wired network within the factory, which cannot easily be achieved with existing copper based industrial Ethernet network solutions.

By introducing the PON solution to the industrial manufacturing scenarios, a network can have higher performance, lower cost, better industrial adaption and easier operation for the industrial customers.

There can be three major use case catalogues for PON in the industrial manufacturing:

i) Industrial process data sub-network: PON is used as the underlying network to carry intra-plant process data. Machines with various industrial interfaces (RS232, RS485, etc.) and protocols (Modbus, Profinet, etc.) can be connected to upper layer manufacturing management and control systems via PON, proprietary industrial data format can be transmitted via PON.

ii) Office sub-network: Factories always have an office network along with industrial manufacturing networks, and the data flows between these two sub-networks are very busy. It is much more cost effective when one single solution can be deployed for both networks, as it provides no obstacles for the data flows, and a unified solution means easier network management and lower total cost. The PON solution is an excellent choice for the enterprise users, and is used to extend the office network into the factory without any additional modifications.

iii) Surveillance sub-network: Industrial customers have strong requirements on video monitoring and environmental sensing services. PON can provide a versatile network solution for these applications. PON ONU can have RJ-45 with Power over Ethernet (PoE) interfaces to provide power delivery to the video cameras, and wireless sensors can be connected by PON ONUs build-in or stand-alone Wi-Fi® APs.

4.7.2 Technology Requirements

4.7.2.1 Unified multi-service support

Factories usually have multiple sub-networks for different services, as the aforementioned three types of sub-networks. PON shall be capable of realizing an all-in-one multi-service network solution.

In order to carry these various kinds of services, the industrial PON system needs to provide effective mechanisms to partition the whole PON network into different sub-networks, and the control planes for these sub-networks shall also be separated.

One technology for implementing service isolation is network slicing, it is designed to address these requirements. One physical OLT can be sliced into different slices that are used to carry each sub-network within the factory. Each network slice has its own reserved network resources, and can be managed and controlled individually without knowing the existence of other slices.

For example, network slicing can be realized by VLAN schemes, where different sub-networks are assigned different VLAN IDs, and those sub-networks are isolated on the L2 network.

There are also network slicing technologies, which provide both control-plane and user-plane isolations. Mainstream industrial PON system vendors can provide three types of slicing granularities as shown in Table 8.

Table 8: Different Slicing Granularities

Slicing granularity	Detailed description
Line-card level slicing	Each OLT line-card can be configured as a sub-network
PON port level slicing	Each PON port on the OLT line-card can be configured as a sub-network
ONU level slicing	Different ONUs within the same OLT line-card port can be configured as a sub-network

[R06-1] The industrial PON system shall support network slicing functionality.

4.7.2.2 Deterministic network performance

The manufacturing process requires stringent latency and jitter, and the PON network shall provide deterministic performance. There are requirements for the PON system to partially or fully support the features as defined by the IEEE 802.1 standards group for Time Sensitive Network (TSN) standards.

PON systems can provide similar or even better features as TSN without supporting native TSN, when used as the E2E network for the manufacturing system, where deterministic latency is required. However, if PON is used as part of an E2E deterministic network, where TSN is used, interworking functions need to be supported between PON and TSN.

Different types of applications in the industrial network require different network performance, as shown in Table 9.

Table 9: Different Network Performance characteristics

Types	Periodicity	Data delivery guarantee	Tolerance to interference	Tolerance to loss	Criticality	Supported by PON
Isochronous	Periodic	Deadline	0	None	High	Partial supported
Cyclic	Periodic	Latency	≤ latency	Typical 1-4 frames	High	Fully supported
Events	Sporadic	Latency	n.a.	Yes	High	Fully supported
Network control	Periodic	Bandwidth	Yes	Yes	High	Fully supported
Config & Diagnostics	Sporadic	Bandwidth	n.a.	Yes	Medium	Fully supported
Best effort	Sporadic	None	n.a.	Yes	Low	Fully supported
Video	Periodic	Latency	n.a.	Yes	Low	Fully supported
Audio/voice	Periodic	Latency	n.a.	Yes	Low	Fully supported

[R06-2] The industrial PON system shall support different deployment scenarios, with scenario-dependent latency, jitter and bandwidth requirements.

[R06-3] The industrial PON system should support interworking functions between the industrial PON system and TSN.

4.7.2.3 Industrial interface and protocol support

There are various proprietary interfaces and protocols for conventional industrial processes. Different interfaces and/or protocols comply with different standards. Industrial PON can provide interfaces for various industrial machines. Different protocols can be supported with stand-alone industrial gateways connected to a PON ONU or with a gateway integrated ONU.

For the ONUs with built-in industrial interfaces, the industrial protocols could be interpreted by the ONU with corresponding functions. For the ONUs without industrial interfaces, the industrial data is interpreted by the stand-alone industrial gateways before sending the data to the ONU, or the data is just tunnelled over the PON network.

The industrial PON ONU should support built-in industrial physical interfaces (at the UNI) other than RJ-45, including but not limited to RS-232, RS-485, and CAN.

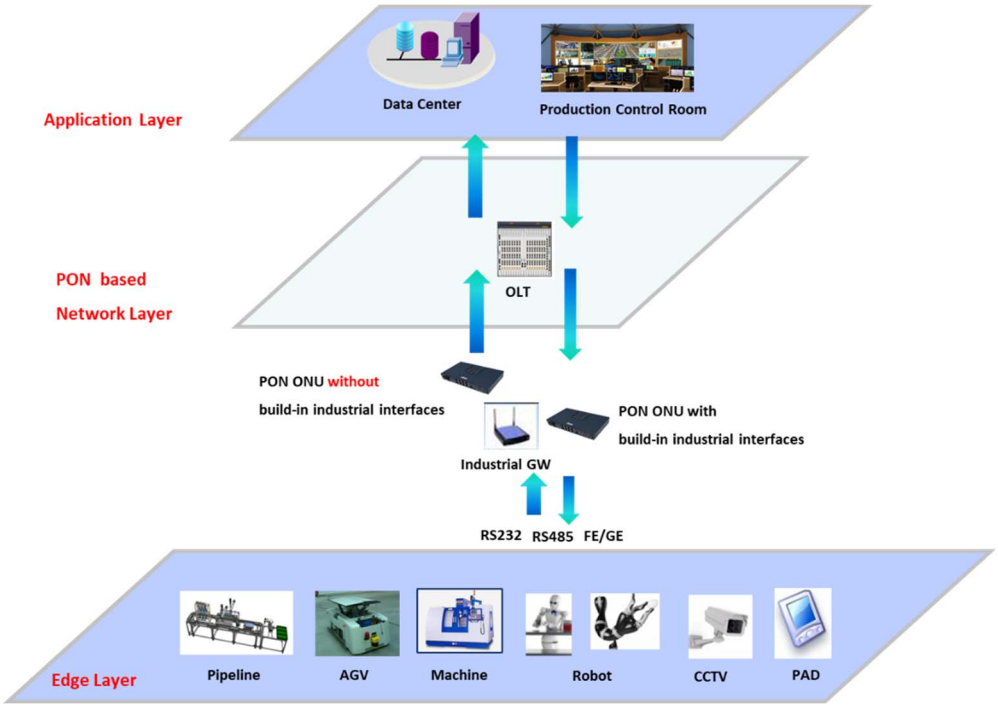


Figure 3: The architecture of the industrial interfaces and protocols carried by a PON system

[R06-4] The industrial PON system should support carrying industrial protocols and satisfy the performance requirements of these protocols.

[R06-5] The industrial PON ONU should support built-in industrial physical interfaces.

4.7.2.4 Stronger network resilience

Network reliability is a top requirement for industrial clients. PON can provide different grades of network resilience, implemented with different protection schemes. Additionally, some new protection schemes have been developed for the industrial scenarios. For example, the dual-OLT protection, which uses two hot stand-by OLTs with 2:N optical splitters and two optical modules on the ONU, to provide a full backup connection.

[R06-6] The industrial PON system shall support protection schemes that cover the OLT, the ODN and the ONU.

4.7.2.5 Higher network security

Industrial clients require higher network security. PON has multiple built-in ONU authentication methods, and no ONU can access the PON network without correct authentication. PON supports AES and other encryption functions to provide a safe data link among different elements within the factory.

[R06-7] The industrial PON system shall support ONU authentication.

[R06-8] The industrial PON system shall support AES data encryption functionality.

4.7.2.6 Smart management

The PON system is configured and managed by network operator personnel experts in the residential and enterprise scenarios. However, in the industrial manufacturing scenario, as the PON is a private network, clients prefer to configure and manage the network themselves so as to have a quicker response to network problems and not to reveal sensitive data of the company to other people.

PON should provide a smart and easy-to-use network management system for the clients, so they can easily operate the PON system without knowing technical details of the system.

This smart management system should be based on standard north-bound protocols, in order to provide an open and interoperable platform for different PON systems from multiple vendors.

EXAMPLE: NETCONF/YANG is nowadays the dominant solution for the smart management system, supported by typical industrial PON solution providers and major PON vendors.

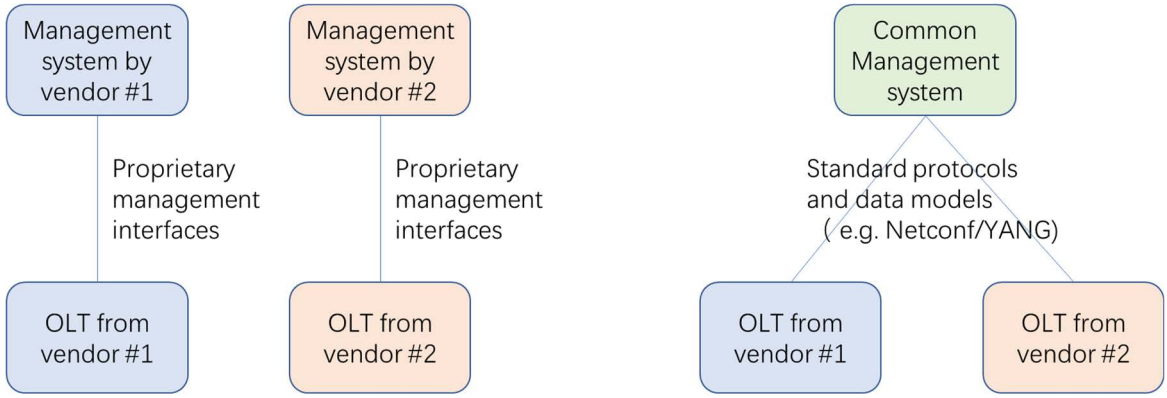


Figure 4: The comparison of vendor-specific management system and standard protocols based management system

[R06-9] The industrial PON system should support standard management protocols and data models.

[R06-10] The industrial PON system shall support a GUI-based user-friendly network management system.

4.7.2.7 Harsh environment adaptation

PON ONUs for industrial manufacturing scenario would usually be deployed in harsh environments, thus the hardware of the ONU should be enhanced to meet requirement on working temperature range, resistance for water, dust, high humidity, and EMC, etc.

[R06-11] The industrial PON ONU shall meet the environmental requirements of the corresponding deployment scenarios.

4.7.2.8 Edge computing

As the manufacturing workshops are becoming smarter, new applications such as computer vision, deep learning on the edge computing platform require less latency and faster computing speed. Therefore, the integration of the edge computing platform into the PON system can fulfil the requirements for speed and latency. A practical solution is an embedded line-card plugged into the OLT chassis.

If the edge computing platform is stand-alone, the system may not fulfil the requirements of an industrial PON system.

Edge computing in the industrial manufacturing scenario usually involves 3rd party applications such as manufacturing control application, pipeline video surveillance and image processing applications, etc.

[R06-12] The industrial PON OLT should support embedded edge computing.

[R06-13] The edge computing module should support 3rd party applications.

4.7.3 Current related standards

4.7.3.1 IEEE

IEEE 802.3AH [i.20] is the EPON standard where Ethernet and PON technology are combined. Based on the passive optical network architecture, a new physical layer (mainly optical interface) specification is defined. 10G-EPON is defined as the next generation of EPON by IEEE 802.3AV [i.21].

These standards define basic Layer 2 standards and essential management and operation protocols for the EPON system.

IEEE 802.1 Time-Sensitive Networking (TSN) task group defines series of standards of synchronization, latency, reliability and resource management of the TSN system.

4.7.3.2 ITU-T

ITU-T standardized GPON series Recommendations ITU-T G.984 series [i.27], and G.987 series [i.28] is the ITU-T's next generation standard for 10G-PON following on from G-PON.

These standards define physical layer, TC layer for the GPON system, and Recommendation ITU-T G.988 [i.29] defines the OMCI related management layer standards.

ITU-T also defined PON system protection schemes as Recommendation ITU-T G.Sup51 [i.30].

4.7.3.3 ETSI

ETSI TC ATTM (Access, Terminals, Transmission and Multiplexing) standardized ETSI TS 101 573 [i.31], which give guidance to the design and construction of the industrial PON optical distribution networks.

ETSI TC EE (Environmental Engineering) ETSI EN 300 019-2-0 [i.32] Specification of environmental tests, gives the guidance of environmental adaption standards for industrial PON.

4.7.3.4 IEC

The International Electrotechnical Commission's IEC 61158 [i.33] standard covers digital data communications for measurement and control in industrial scenarios, which is also the dominant standards for industrial communication technologies.

4.7.4 Gap analysis

4.7.4.1 Gap Context

In the present document the gaps refer to existing standards and not to technology in general. Some vendor's products that are not standardized could exist that implement the solutions described in the gaps.

4.7.4.2 Unified multi-service support

Network slicing is a major solution for unified multi-service networks. The functionality of "slicing" was addressed for various purposes in Access Network. There are several standards defined by BBF on Access Network slicing technologies. As BBF TR-370 [i.16] targets a business case for sharing an Access Network by multiple Virtual Network Operators (VNOs), where Access Network is sliced by Infrastructure Provider (InP) and operated by multiple VNOs. And BBF TR-386 [i.17] defines management interface to support the roles of VNOs and InP.

However, slicing is different in industrial networks. There are most likely no VNOs that share InP's Access Network in this scenario, and industrial clients emphasize on the network resource isolation capability. Thus, new related standards need to be defined to meet the requirements in industrial scenarios. Accordingly, the granularity of the network slice, the management and control function requirements, and the network resource allocations should be further studied.

[Gap06-1] Industrial slicing scenarios, including granularity of the network slice, the management and control function requirements, and the network resource allocations are currently not standardized.

4.7.4.3 Deterministic network performance

The manufacturing process requires stringent latency and jitter, and the PON system shall provide deterministic performance. The industrial PON system can be optimized for its performance on latency and jitter. However, different vendors nowadays are using different solutions to achieve the same goal. There are strong demands for the vendors to provide a unified standard methods of a deterministic network solution in PON systems.

And there are strong requirements for the PON system to fully support the features of the TSN (Time Sensitive Network) standards. Industrial PON system now supports part of this group of standards features, such as the IEEE 802.1AS [i.34], and fully supporting the features of TSN standards is still under study by the PON community.

So far there is no standard to support interworking between PON and TSN.

[Gap06-2] The PON system optimization to support TSN features is currently not supported.

[Gap06-3] The interworking of PON and TSN is currently not supported.

4.7.4.4 Industrial interface and protocol support

There are various independent industrial networking and data protocols within the industrial networks. Even machines in the same workshop may use different protocols or have different physical interfaces. This introduces problems when the clients want to integrate all the machines with different protocols into one manufacturing management system, the protocols need to be converted into one converged format.

Industrial PON partially solve those problems with build-in or stand-alone industrial gateways and corresponding protocol interpretation software. However, there are still gaps between productions and standards, as currently a common architecture and technical standards of the industrial PON ONU with industrial interfaces and protocol interpreting functions is missing.

[Gap06-4] Industrial PON ONU with industrial interfaces and protocol interpreting functions are currently not available.

[Gap06-5] Same as [Gap06-4].

4.7.4.5 Stronger network resilience

Current PON standards provide different grade of protection schemes for different scenario, and there can be a balance of cost and reliability. There are no urgent needs for new amendments to current standards.

[Gap06-6] None.

4.7.4.6 Higher network security

As mentioned in above context, the industrial PON system has complete multiple built-in network security functions, which cover network access control and data encryption.

The PON system mainly works on Layer 2 of the OSI network architecture, while higher layers can enhance the network security with their own measurements. Thus there is currently no new requirements on the network security issues of the PON standards.

[Gap06-7] None.

[Gap06-8] None.

4.7.4.7 Smart management

BBF defines PON related YANG modules, and open-source communities provide key frameworks for the realization of smart management systems for industrial PON.

There are still some key points to be standardized, including a common telemetry technology, which provides faster and less resource consuming methods to monitor the network, and automatic network resource allocation and configuration enabled by AI based functions within the PON system.

[Gap06-9] Industrial PON telemetry, automatic network resource allocation and configuration enabled by AI based functions within the PON system is not currently defined.

[Gap06-10] None.

4.7.4.8 Harsh environment adaption

There are no urgent needs for new amendments to current standards. The hardware of industrial PON system can be further enhanced if new extreme working conditions appear.

[Gap06-11] None.

4.7.4.9 Edge computing

Edge computing in industrial scenarios do not emphasize NFV or SDN based functionality, but it is about 3rd party compute intensive applications such as image processing and AI related computing.

The same application may have a very different execution time on different computing platforms, and there is the risk that the same 3rd party software may have very different performance or user experience on different edge computing platforms.

Thus, it is necessary to define a computing power metric for edge computing platforms from different PON vendors, such as the requirements on the performance of CPUs, the capacity of the RAM etc., in order to prevent the fragmentation of edge computing solutions, and provide a unified user experience for the industrial clients.

[Gap06-12] The definition of compute power for edge computing platforms in Industrial PON is currently not defined.

[Gap06-13] None.

4.8 Multiple Access Aggregation over PON (MAAP)

4.8.1 Use Cases briefing

PON technology is mostly used for the Residential Market, however some operators are also using it for the Enterprise Market and as transport solution for Mobile Backhaul, commonly providing services all together in the same PON. Different markets, transport solutions or services, fixed and mobile have different requirements and challenges to face. With current OLT/ONU solutions, there is some evidence that PON technology will need to be improved to overcome those challenges.

Regarding the mobile traffic transport, it should be considered that the evolution from 4G to 5G and vRAN architectures will bring additional challenges due to the several splitting options and BBU decomposition in three parts (CU, DU and RU). In this context and for MAAP specific use case, it is crucial to understand the requirements and architectures for PON networks to support the main 5G transport scenarios, based on different RAN functional splits (defined in 3GPP TR 38.801 [i.39]):

- Backhaul - connection from Central Unit (CU) to 5G core
- Midhaul - connection between Central Unit (CU) and Distributed Unit (DU)
- Fronthaul (see note) - connection from Distributed Unit (DU) to transmitter Remote Unit (RU)

NOTE: The Fronthaul scenario has additional opportunities, but also complexities when analysed from a PON perspective. This will be addressed in a specific use case in the future and is for further study.

Therefore, this use case has the main goal of not only address the support of the new emerging services with tight definitions, but also transport them simultaneously with mobile xHaul within the same PON interface.

4.8.2 Technology requirements

4.8.2.1 General introduction

Having in mind that it is intended to have an access solution to allow the aggregation of all types of traffic, it is mandatory that the evolution of PON technologies, such as XG-PON, XGS-PON, NG-PON2, and 50G-PON, addresses not only high bit rates but also other requirements. As far as it is predictable today, the most demanding requirements are those associated with 5G transport and, therefore, if the technology supports these requirements, it will naturally support the Residential and Enterprise market as well.

The main challenges in addressing the support for these new features and services, are the demands for higher data rates, higher coverage and densification, higher and stratified QoS, ultra-low latency, and tighter time synchronization, higher security, and higher availability (protection). This is irrespective of whether it is an FTTH Fixed services or a Mobile xHaul based services.

Network Densification
Brownfield GPON Access Network's reuse of the extensive Optical Distribution Network (ODN) is a key factor in 5G's business case implementation, and this gains more relevance if the forecasted number of cells (especially small cells) are 10x to 100x larger.

Meaning that whenever the location of new cell sites coincides with the FTTH footprint already deployed and supporting Business-to-Consumer (B2C) and/or Business-to-Business (B2B) services, there are advantages in reusing the same PON infrastructure to transport all services, which increases the pressure on PON bandwidth and other performance requirements.

Network QoS
With the increasing usage of network resources, QoS becomes fundamental for new implementations at the OLT as well as the ONU level, since it also enables shared use of multiple applications and very divergent requirements (Residential Market, Enterprise Market and Mobile Transport). Additionally, it is necessary to add the required flexibility and scalability to meet these requirements.

As mentioned, new features to support higher data rates, ultra-low latency, tighter time synchronization and security, as well as physical path protection need to be established so that multiservice aggregation could be achieved within the same PON interface.

Network Availability
Network availability is ultimately given by the level of end-to-end protection of equipment and paths to connect them. If for the residential market, protection in the Access Network, may not be essential, when connecting cell sites or enterprise services with stringent SLAs, it is mandatory to have effective network protection and resilience options with auto recovery configurations from failover, achieving immediate restoration and availability of 99,999 % (5 nines).

The technical requirements for Multiple Access Aggregation over PON use case are addressed in the next points.

4.8.2.2 Bandwidth

Clearly, the explosion of new types of services like Online Video, UHDTV, OTT, VR, Cloud Gaming, etc., is driving today's increase in bandwidth demand.

Since the increase in bandwidth is already a huge challenge to address, it is an even greater challenge in shared networks such as PON, which can aggregate 64 or more end customers in a single physical interface.

To reinforce that challenge, the added fixed bandwidth reserved for the OMCC channels of each ONU is higher than desirable.

With current GPON, and even with new XGS-PON implementations, some improvements can be made in order to enhance the OMCC bandwidth allocation and inter-gap allocations (guard band, preamble and delimiter), without detriment of ONU's inband management and bandwidth map assignments, freeing up PON upstream bandwidth for end customer services.

Table 10: Default bandwidth allocation on current xPON technologies

	UL BW consumed by OMCC + inter-gap per ONU	UL BW left w/ 64 ONUs per PON	UL BW free per ONU w/ 64 ONUs per PON (equitable distribution)
GPON (2,5 G/1,25 G)	7 Mbps	750 Mbps (62 %)	11 Mbps
XG-PON (10 G/2,5 G)	22 Mbps	1,1 Gbps (44 %)	17 Mbps
XGS-PON (10 G/10 G)	90 Mbps	4,2 Gbps (42 %)	65 Mbps

Moreover, if an FEC is used for error correction, an additional 15 % reduction in total PON upstream bandwidth shall be considered when performing average bandwidth calculations for access endpoints, limiting the maximum useful bandwidth/throughput for XGS-PON to 8,5 Gbps bidirectional.

Figure 5 shows the maximum average bit rate per access and the forecast of PON average traffic per access. Looking at the current PONs traffic consumption behaviour and the expected growth of average bitrate per client/access (typically for B2C clients due to the FTTH mass market and the overall traffic demand), it is possible to infer that XGS-PON technology is unlikely to be able to provide additional bit rate greater than 4 Gbps while guaranteeing an average of 50 Mbps per client for 64 clients.

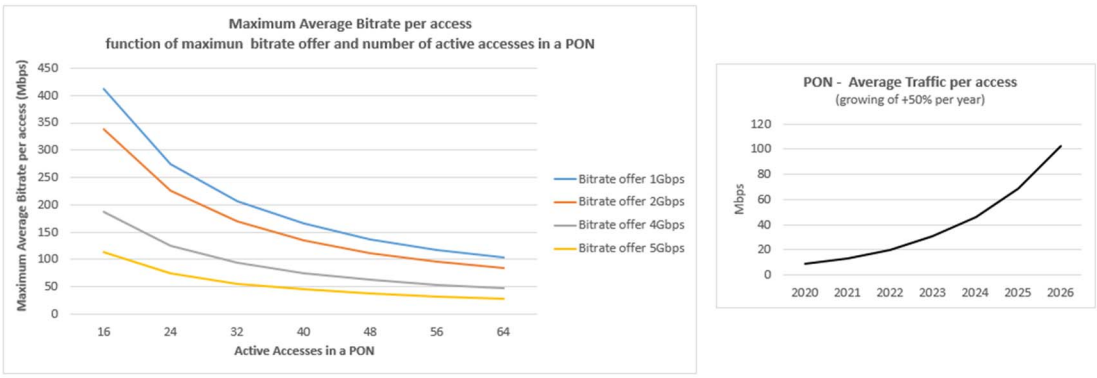


Figure 5: Maximum average bit rate per access and Forecast of PON average traffic per access

NOTE: Considering XGS-PON with FEC active and assuming 500 Mbps for Multicast traffic.

If in addition to mobile xHaul of 5G, the support of eMBB services is considered on the same PON interface, the following typical bandwidth usage scenarios need to be considered, which may be different depending on the type of geographic dispersion.

Table 11: Typical bandwidth requirements for cell site types

	High density NR 3,6 GHz 100 MHz TDD Active Antenna (64T64R/sector) ---- 1 700 Mbps/sector	**Mid density NR 3,6 GHz 100 MHz TDD Passive Antenna (8T8R/sector) ---- 550 Mbps/sector**	**Low density NR 700 MHz 2x10 MHz FDD Passive Antenna (4T4R/sector) ---- 100 Mbps/sector**	**Small Cells NR (FR1 sub-6 GHz TDD/FDD Passive Antenna ---- up to 4 Gbps**
Backhaul Transport	3 960 Mbps	1 440 Mbps	270 Mbps	4,8 Gbps
Midhaul Transport	4 Gbps	1 454 Mbps	273 Mbps	4,85 Gbps

In the future, with mmWave bands (26 GHz), it will be possible to achieve 8 Gbps peak rate for eMBB, considering that each operator will be allocated 400 MHz bandwidth. Today, the main business driver for this band is Fixed Wireless Access (FWA).

Therefore, the 8.5Gbps supported by the XGS-PON technology may be a solution in the short term, but it is clear that in the future it will show its bandwidth limitations.

Due to the complexity (inside plant operationalization and OSS developments - inventory, provision and diagnostic) to include new PON technologies, it is mandatory that the OLT/ONU evolution addresses a seamless integration of these new technologies. For GPON, XG(S)-PON and future generation PON systems the OMCC bandwidth allocation and inter-gap allocations shall be optimized to reduce fixed bandwidth reserved for the OMCC channels.

[R08-1] The F5G Access Network shall support OMCC bandwidth allocation and inter-gap allocation optimization.

[R08-2] The F5G Access Network PON infrastructure shall support high capacity solutions as defined in table 10 for MAAP.

[R08-3] The F5G Access Network PON technologies shall support a seamless upgrade and integration with the existing deployed PON ecosystem.

[R08-4] The F5G Access Network PON technologies shall support multiple services (B2B, B2C and mobile xHaul) over the same PON infrastructure.

4.8.2.3 Protection

To address high levels of availability needed for the Enterprise market and 5G Midhaul and Backhaul, network protections and restoration schemes shall be implemented or optimized.

The field implementations are extremely dependent of ODN duplication and corresponding business cases to support that investment, but the technology should support the scenarios below for Layer 2 protection. The two schemes in Figure 6 below shall apply to PONs of the same OLT, different OLTs and whether they are co-located or not.

If PONs are in the same OLT, the features associated with PON switching can be applicable in a monolithic or a SDN/NFV solution. When PONs belong to different OLTs (co-located or not) these features shall be implemented by SDN/NFV solutions.

The switching process shall have minimal impact on the active services and shall allow configurable thresholds based on bandwidth management, latency, delays, power levels, optical errors, traffic discards or other performance parameters related to service slicing.

The protection solution shall allow a backup option for ONU, namely the option of having one or two ONUs at Client/Cell site. The protection switching shall be automatic based on network failures or performance degradation.

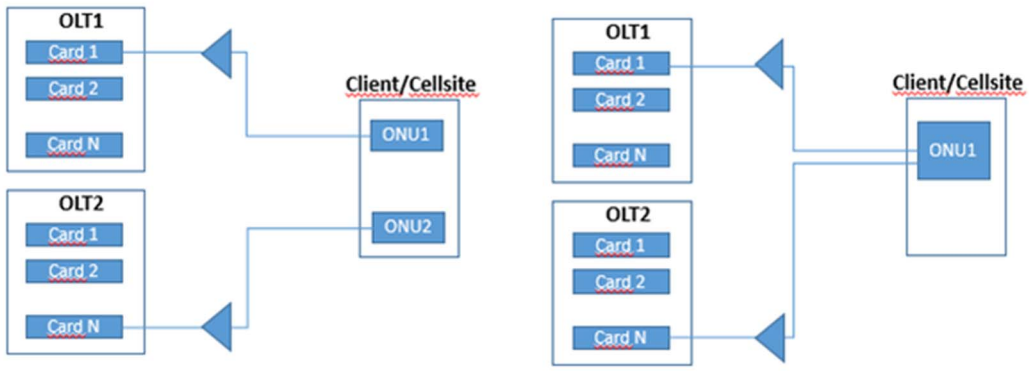


Figure 6: Protection schemes

[R08-5] The F5G Access network PON infrastructure shall support protection mechanisms for MAAP between two distinct OLT, using single or dual ONU.

[R08-6] The F5G Access network PON infrastructure shall support automatic protection switching for MAAP.

4.8.2.4 Latency

Ultra-low latency and low jitter communication is becoming an important requirement for future mobile Access Networks, mainly for URLLC and mMTC services. PONs are known to be a resource efficient and low cost technology for the fixed Access Networks. But the current drawbacks in latency and jitter, as a result of Dynamic Bandwidth Allocation (DBA) implementations for upstream transmission, can cause delays in the order of milliseconds and the delay can vary in time.

Future networks are not just about sensors and smart meters, it also includes applications such as connected vehicles (V2X), smart traffic management, remote video monitoring, industrial robotics, which can demand very low latency (< 1 ms in some cases).

Alternative DBA implementations can have an average delay in the order of 600 µs, in upstream transmission, providing better service experience. Nevertheless, to accomplish the ultra-low latency requirements for 5G (naming the Industry Control Sensors use case), new or optimized algorithms shall be implemented.

Table 12: Latency measures in current GPON/XGS-PON implementations

		UL upstream profile	
		100 Mbps	10 Gbps
UL	min	10 µs	10 µs
	average	500 µs	100 µs
	max	1 000 µs	500 µs
DL	min	10 µs	10 µs
	average	15 µs	15 µs
	max	50 µs	50 µs

An additional key challenge with traditional PON solutions that has an impact on latency and time synchronization is the quiet windows to add new ONUs to the PON.

Recent trends of network slicing and virtualization are providing unprecedented opportunity to increase the level of control, and once implemented in software, virtualization enables network functions to be split and replicated with different algorithms and purposes. This is especially important in 5G networks, which need to support a large number of highly heterogeneous services.

PON virtualization has also progressed beyond the basic "softwarization" of the DBA, by designing new mechanisms that allow running multiple independent DBAs in parallel, managed by a common low level engine. For example, this enables running a DBA for one set of users (e.g. residential broadband) and another DBA for low-latency applications (e.g. 5G URLLC services).

Several new DBA technics may be considered to achieve better low-latency and jitter performance:

- Single-frame Multi-burst technology: achieving better overall performance if grants are allocated in small size.
- Dual-wavelength technology: one for ranging and eMBB services the other for uRLLC services.
- Disaggregated DBA applications for service differentiation: separation of DBA algorithm from common merging engine, with the creation of virtual DBA (vDBA), implementing different algorithms for service differentiation.
- Cooperative DBA for mobile fronthaul applications (though not further detailed in this use case), with more restrictive delay requirements, bypasses the high-latency report/grant process of typical DBAs. Enabling communication between the schedulers of BBU and PON possibly allows for issuing grants based on DBA calculations.

The solution may not be just one isolated technique, but the combination of several.

Table 13: KPI Targets for latency in future XGS-PON or Next-PON implementations

KPI	2020	2021	2022+
Bandwidth	GPON/XGS-PON	XGS-PON or Next-PON	XGS-PON or Next-PON
Latency	Upstream: 400 µs Downstream: 50 µs	Upstream: 200 µs Downstream: 50 µs	Upstream: 100 µs Downstream: 50 µs

[R08-7] The F5G Access network PON infrastructure shall support distinct service types based on different latency, jitter and bandwidth requirements.

4.8.2.5 Timing & Synchronization

Although there are different, and sometimes complementary, network time synchronization methods for RAN, one that shall be addressed when used in PON Access Networks is IEEE 1588v2 [i.40].

Presently, DBA's implementations, aligned with latency gaps already mentioned, have also drawbacks related to time precision clock synchronization with high impact on new 5G services with URLLC requirements, as well as with current 4G LTE-A.

Figures 7 and 8 show the phase discrimination measurements made on GPON and/or XGS-PON with traditional DBA implementations. The figures show that the LTE time accuracy requirements will not be satisfied if no further features are added to the OLT and ONU. Here, the major influence comes from high Packet Delay Variation (PDV) on Delay Request packets (Tp2 measurements) in the upstream when using IEEE 1588v2 [i.40]/PTP for network time synchronization.

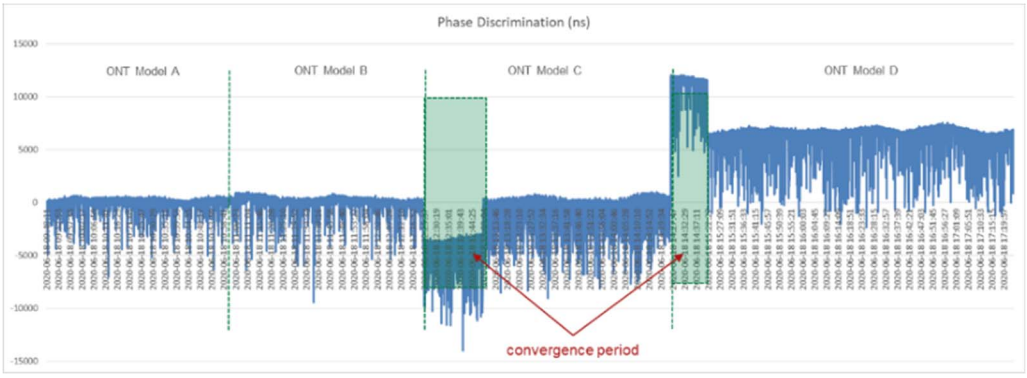


Figure 7: Example of phase discrimination measured in a GPON solution

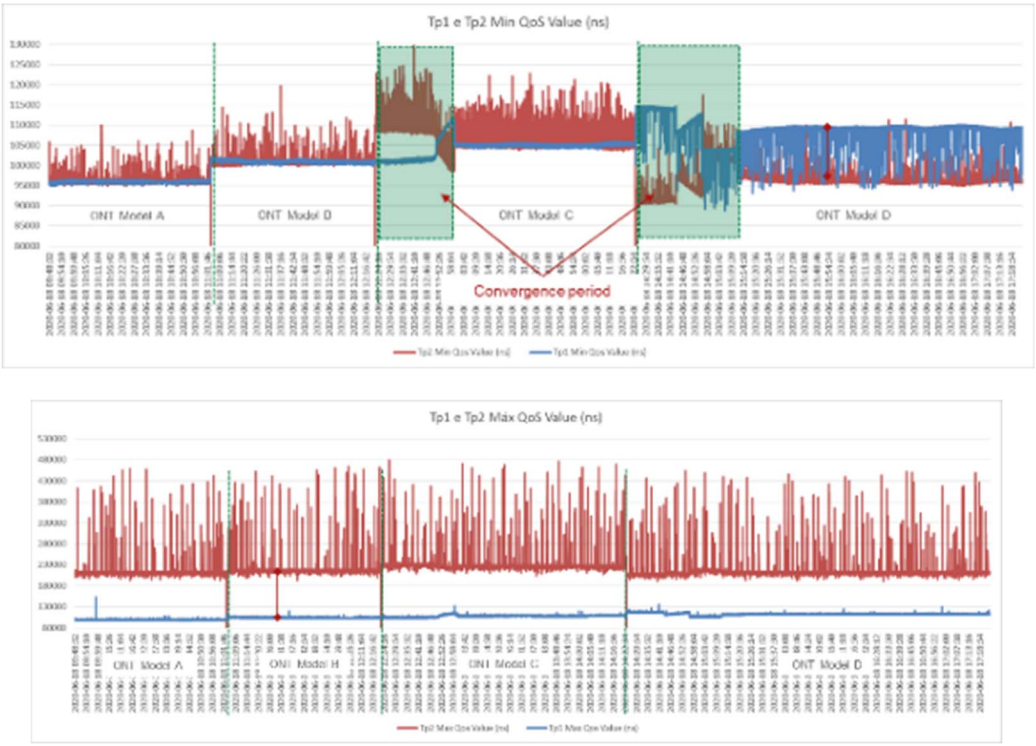


Figure 8: Example of PDV for downlink (Tp1) and uplink (Tp2) measured in a GPON solution

4G LTE-A is the first example in which specific and tight synchronization requirements are set for the end-to-end time accuracy of ±1,5 µs, limiting the transport to ±1,1 µs and ±0,4 µs for the RAN.

5G's first phase implementation specific for eMBB have similar time accuracy requirements as 4G LTE-A, but further 5G services have more severe requirements with time accuracy limited to ±130 ns (Recommendation ITU-T G.8271 [2], clause 6.5.23.1 of ETSI TS 136 104 [i.41], and clauses 6.5.3 and 9.6.3 of ETSI TS 138 104 [i.42]), not supported by current GPON/XGS-PON implementations.

[R08-8] The F5G Access network PON infrastructure shall support 5G end-to-end time accuracy and synchronization requirements for MAAP.

4.8.2.6 Slicing

Service transport provides a limited form of isolating a service within a common infrastructure, usually based on a simple L2 VLAN cross connection with a common and shared DBA per PON interface, with proven limitations on quality of data transmission for time-sensitive and mission-critical services.

In this sense, network slicing at the Access Node, as a point of aggregation for FTTH Fixed and xHaul Mobile based services, is a vital feature that will allow carriers to create virtual data pipelines for each of its data type of services, assuring the proper QoS, latency and jitter, with the proper mapping for an end-to-end service.

Figure 9 shows an example of how different techniques could be combined to implement a top level end-to-end slice, with the implementation of AI Engines to steer the traffic to the proper vDBA and/or Virtual Extensible LAN (VxLAN), depending on each service's specific demand for bandwidth, latency and packet jitter, with the more suitable mapping to the service slice type and traffic isolation processes.

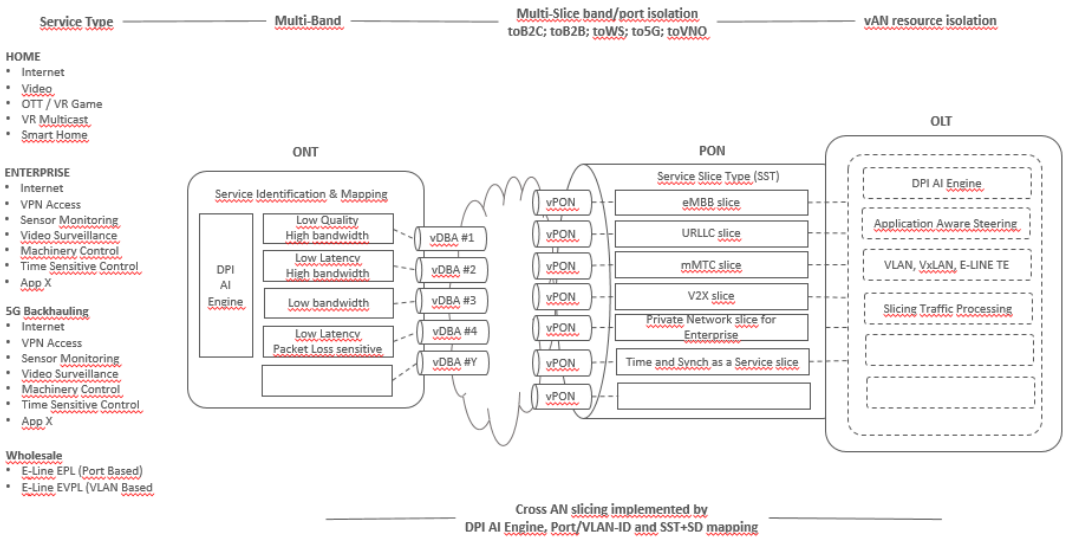


Figure 9: Example of an Access Network slicing model

[R08-9] The F5G Access network PON infrastructure shall support network slices for different mobile and fixed service levels in the MAAP solution.

4.8.2.7 Protocol transparency

A gap in some of today's PON implementations is the support of full transport transparency of any protocol data traffic across ONU and OLT. Although present implementations support the forwarding models based on VLAN-ID or Port-based mappings, they are not fully transparent, meaning that some protocol frames are still going to the CPU.

Future Access Network implementations should support full transparency similar to that defined for an E-Line type of service defined by MEF (MEF 6.3 e MEF 10.4) for EPL (Ethernet Private Lines) all to one bundling port based and EVPL (Ethernet Virtual Private Lines) EVC identified by VLAN ID, with no additional processing done at ONU and/or OLT.

EPL shall be fully transparent, filtering only pause frames, EVPL is required to peer or drop most of the Layer 2 control protocols. All other protocol types shall flow with no further processing.

[R08-10] The F5G Access network PON infrastructure shall support protocol transparency for MAAP.

4.8.3 Current related standard specifications

4.8.3.1 ITU-T

ITU-T defines the standards for GPON in the Recommendation ITU-T G.984 series [i.27].

Its evolution, XG-PON standards are published in the Recommendation ITU-T G.987 series [i.28].

There is also a companion ITU-T standard defining a management and control interface for administering optical network units, referred to by the Recommendation ITU-T G.987 [i.28].

Recommendation ITU-T G.983 series [i.43], defines standards for Dynamic Bandwidth Allocation (DBA) in PON systems

ITU-T also defined PON system protection schemes as Recommendation ITU-T G.Sup51 [i.30].

In 2018, ITU-T established the High-Speed Passive (HSP) optical network project to define the next generation PON. 50-Gbits/s PON has been selected as a primary technology in the new G.HSP standard project series. This G.HSP series of standards include the following standards:

- Recommendation ITU-T G.9804.1 [i.113], describing the HSP requirements includes overall system requirements, evolution and coexistence, and supported services and interfaces of high-speed PON systems. The standard achieved consent in July 2019 and was officially approved in November 2019.
- Recommendation ITU-T G.9802 [i.184], describing the Physical Media Dependent (PMD) layer specifications based on 50-Gbits/s time-division multiplexing PON (TDM PON).
- Recommendation ITU-T G.9802.1 [i.185], describing the PMD layer specifications of time-and-wavelength-division multiplexing PON (TWDM-PON) with per-channel data rate at up to 50 Gbits/s. This standard is under development.
- Recommendation ITU-T G.9802.2 [i.186], describing the common Transmission Convergence (TC) layer specifications of the HSP series, such as TC layer architecture, physical adaptation layer, business adaptation layer, management process, and message definition etc. This standard is still under development.
- Recommendations ITU-T G.9804.1 [i.113], G.9804.2 [i.187], G.9804.3 [i.188] and G.9804.4 [i.189], describing Point-to-Point (P2P) wavelength-division multiplexing PON (WDM-PON) with over 40 total wavelength channels for both directions at up to 25 Gbits/s per wavelength channel. This standard is still under development.

Also, ITU-T has been making Recommendation ITU-T G.989 [i.181] Amendments to support cooperative Dynamic Bandwidth Allocation (DBA) by adding in the TC layer the delay and jitter requirements and guidance on how to build a DBA engine with proper controls. The Open Radio Access Network (O-RAN) alliance is working on a specification for the cooperative transport interface, while the G.989 Amendments provide all the protocol elements needed to communicate with the OLT. Moreover, ITU-T is working on Recommendation ITU-T G.sup.66 [i.182] for 5G applications in a PON context, and specifying the needed interfaces such as the F1 and Fx interfaces in the O-RAN terminology.

4.8.3.2 3GPP

One of the goals of this use case is to have a PON network able to support all the B2C and B2B services along with the main 5G transport scenarios, based on different gNB functional splits.

3GPP TR 38.801 [i.39] specifies the several functional blocks and potential split points on the signal processing chain in the upstream and downstream of both 4G and 5G.

4.8.3.3 IEEE

IEEE 1588v2 [i.40] on Precision Time Protocol addresses network time synchronization methods for RAN.

4.8.3.4 ETSI

ISG NFV defines the major SDN/NFV specifications that meet the needs of the industry, namely the NFV architecture and the NFV-MANO (Management and Orchestration) framework.

ISG ZSM develops the architectural, functional and operational requirements for end-to-end network and service automation, namely specifying solutions and management interfaces for the orchestration and automation of the emerging E2E network slicing technology (ETSI GS ZSM 003 [i.44]) and E2E cross-domain service orchestration and automation (ETSI GS ZSM 008 [i.45]).

ISG ENI is defining a Cognitive Network Management architecture, using Artificial Intelligence (AI) techniques and context-aware policies to adjust offered services based on changes in user needs, environmental conditions and business goals, specifying a framework for automated service provision, operation, and assurance, as well as optimized slice management and resource orchestration.

4.8.3.5 MEF

MEF 6.3 [i.46] defines several Subscriber Ethernet Service Types that are used to create Point-to-Point, Multi-Point-to-Multi-Point, and Rooted-Multi-Point Ethernet Services that are either Port or VLAN based.

MEF 10.4 [i.47] describes Service Attributes for Subscriber Ethernet Services provided to an Ethernet Subscriber by an Ethernet Service Provider. The Service Attributes describe behaviours observable at an Ethernet User Network Interface and from Ethernet User Network Interface to Ethernet User Network Interface.

4.8.3.6 BBF

BBF TR-402 [i.18] defines the PON abstraction interface and use cases for time-critical applications such as Dynamic Bandwidth Allocation (DBA) and Dynamic Wavelength Assignment (DWA). BBF TR-402 [i.18] addresses disaggregation of algorithm and PON interface, so that multiple DBA algorithms on a common engine can be supported.

4.8.4 Gap analysis

4.8.4.1 Gap Context

In the present document the gaps refer to existing standards and not to technology in general. Some vendor's products that are not standardized could exist that implement the solutions described in the gaps.

4.8.4.2 Overall gap analysis

Based on the analysis above, enhancements and modifications are needed in the next-generation PON to meet the key technical requirements such as high bandwidth, reliable protection, low latency, accurate timing & synchronization, the ability to perform slicing, and protocol transparency.

4.8.4.3 Bandwidth

Based on Table 10, 5G xHaul requires backhaul and midhaul interface bit rates of 4 Gbits/s. When a PON system is used to aggregate 16, 32 and 64 such interfaces, the required net data rates are 64 Gbits/s, 128 Gbits/s and 256 Gbits/s, respectively, which are beyond XGS-PON and the upcoming 50G-PON. Thus, further increasing of the throughput of next-generation PON is needed to better meet the bandwidth requirement.

[Gap08-1] Increase in PON throughput via new technologies such as high-order modulation and wavelength-division multiplexing is currently unavailable.

[Gap08-2] Same as [Gap08-1].

[Gap08-3] None.

[Gap08-4] None.

4.8.4.4 Protection

Based on Figure 6, mission critical services such as 5G services require reliable protection such as 1+1 protection for both the OLT and the ONU. Automatic switching between the working path and the protection path needs to be provided. Also, the switching needs to be seamless, not causing any interruption of the mission critical services. This would require the delay compensation between the working path and the protection path. This has not been specified in current PON systems.

[Gap08-5] None.

[Gap08-6] Automatic protection switch with delay compensation between the working path and the protection path to avoid service interruption is currently unavailable.

4.8.4.5 Latency

Based on Table 12, current PON upstream latency is variable and can be greater than 500 µs, which is insufficient to support ultra-low latency requirements from 5G (for use cases such as the Industry Control Sensors). Thus, improved DBA algorithms shall be implemented.

[Gap08-7] Improved DBA to support low-latency upstream transmission with latency below 100 µs is currently unavailable.

4.8.4.6 Timing & Synchronization

Future 5G services require accurate timing & synchronization in the order of ±130 ns. Enhancements in future PON systems are needed to meet the accurate timing & synchronization requirements.

[Gap08-8] Enhanced timing & synchronization for future PON systems to ensure end-to-end requirements are met is currently unavailable.

4.8.4.7 Slicing

Network slicing is an important feature to meet a diverse set of requirements with optimal resource utilization. AI Engines need to be implemented to steer the traffic to the proper vDBA and/or VxLAN, depending on each service's specific demand for bandwidth, latency and packet jitter, etc.

[Gap08-9] Slicing in PON with suitable mapping of the vDBA and/or VxLAN to the service slice type and traffic isolation processes is currently not supported.

4.8.4.8 Protocol Transparency

Current PON implementations do not support full transport transparency of any protocol data traffic across ONU and OLT. Future Access Networks implementations should support full transparency with no unnecessary protocol processing done at ONU and/or OLT.

[Gap08-10] Protocol transparency in PON throughput via new technologies such as Ethernet Private Lines (EPLs) and Ethernet Virtual Private Lines (EVPLs) is currently not supported.

4.9 Scenario Based Broadband

4.9.1 Use Cases briefing

The scenario based broadband use case describes the required broadband network capabilities to support a guaranteed experience in the context of multiple scenarios for both residential and business users. Applications and services in different scenarios may have different SLA requirements.

Applications with higher SLA requirements should be recognized by the network components with their embedded Artificial Intelligence (AI) capability.

Different network actions could be taken according to the application, in particular the application's quality of service requirements. For instance, on-line gaming requires large bandwidth and low latency from the terminal to the gaming cloud, while education broadband requires low bi-directional latency, low jitter and packet loss. Different network resources should be allocated to different broadband applications so as to guarantee the broadband user experiences.

4.9.2 Technology Requirements

4.9.2.1 General introduction

The key requirement of the scenario based broadband use case is a network based capability for accurate and automatic broadband applications identification and experience guarantee.

In order to support the scenario based broadband applications in the network, different applications could be identified by the network with the capability of distinguishing the traffic features of one application from another. The appropriate network resources will be allocated to the identified applications, including the home network segment. To support the flexible changes of the broadband application, the scenario based broadband network should also be designed to autonomously adapt to new broadband applications.

4.9.2.2 Application identification

Different broadband applications are required to be recognized by the network in order to guarantee the application experience.

Application identification could be implemented based on an artificial intelligence mechanism. The legacy method for application identification is based on packet analysis, such as Deep Packet Inspection (DPI). To protect the privacy of broadband users, it is recommended to use AI to analyse the differences between external features of the traffic model of different applications instead of using packet analysis such as DPI.

[R10-1] The F5G network shall support application type (video, file transfer, Internet browsing, etc.) identification.

[R10-2] The F5G network should support AI based application type identification.

4.9.2.3 Broadband application feature database establishment and updates

The network based AI engine communicates with the feature database to acquire the features of the various broadband applications running in the network and to take actions for a guaranteed experience. The establishment of the feature database should be based on Big Data and on AI learning processes for automatic and continuous update. The establishment and the updates of the feature database could be implemented in real time or periodically.

[R10-3] The application feature database for AI should be established and updated in real-time or periodically.

4.9.2.4 Network slicing and application acceleration.

The network needs to be sliced into multiple logical network slices with different service characteristics to support the differentiation of applications. The slice should be implemented both to Home Network, Access Network and Aggregation Network to guarantee the End-to-End network service characteristics. High value and latency sensitive applications such as Cloud Gaming, Cloud VR, On-line Education, telemedicine and so on should be accelerated on the network transport by allocating a slice with the appropriate characteristics.

[R10-4] The F5G network shall support slicing with different service characteristics.

4.9.2.5 QoE evaluation

The network shall be able to evaluate current QoE performance and verify whether the SLA of the service is satisfied. The evaluation of QoE is service oriented, which means different services may have different approaches. The network shall at least be able to evaluate the QoS of a certain service of the network, including but not limited to the application throughput, packet loss, latency, jitter, video resolution change, video frame loss, etc.

[R10-5] The F5G network shall support measurement mechanisms for QoS evaluation.

[R10-6] The F5G network should support measurement mechanisms for QoE evaluation.

4.9.2.6 Potential application and user discovery

The AI enabled network is capable of discovering network usage and demands of different applications, including discovering usage of demanding applications, which may require acceleration. The AI enabled network uses this knowledge to generate indications of application needs to the network operator to enable the latter to allocate available resources.

A link to individual users should be avoided where possible unless this service is explicitly included in the user's service level agreement. As an example of the former, AI-identified application and user might link to a virtual group of users rather than to individual users.

[R10-7] The F5G network should support identification of application network usage, which potentially have acceleration requirements.

[R10-8] The F5G network should support the allocation of available resources.

[R10-9] The F5G network should avoid links to individual user usage of applications unless this service is explicitly included in the user's SLA. Otherwise, linking should be restricted to an anonymized group of users.

4.9.2.7 The network capacity monitoring and expansion prediction

The network is capable of monitoring the utilization of the overall network resources and associated health status, such that the application SLAs can be checked, by adjusting network resources.

[R10-10] The F5G network shall support the monitoring of network resource utilization and health status.

4.9.3 Current related standards

4.9.3.1 ITU-T

Recommendation ITU-T Y.3172 [i.3] specifies an architectural framework for Machine Learning (ML) in future networks including IMT-2020. A set of architectural requirements and specific architectural components needed to satisfy these requirements are presented. These components include, but are not limited to, an ML pipeline as well as ML management and orchestration functionalities. The integration of such components into future networks including IMT-2020 and guidelines for applying this architectural framework in a variety of technology-specific underlying networks are also described.

4.9.3.2 BBF

BBF TR-370 [i.16] defines three different models for resources sharing or slicing:

1) Management System based, which performs network slicing at management system level and not directly in the equipment itself.

2) Virtual Access Node based, which extends the capabilities of physical access and aggregation nodes to support multiple, virtual functions, each containing ports and forwarding resources directly managed by a Virtual Network Operator (VNO).

3) The SDN-based approach relies on vAN and vAggN instances which are Management and Control (M&C) Plane entities accessed by VNOs to manage their virtual network resources via the mediation of SDN M&C elements. The Data Planes of all VNOs' virtual Access Networks remain respectively within the physical Access Nodes and the Aggregation Switches/Switch Fabrics.

4.9.3.3 ETSI

ETSI TC MEC works on:

1) Increasing the accessibility and adoption of MEC specifications by exposing OpenAPI™ (as known as Swagger) compliant MEC API descriptions via the ETSI Forge site and associated mirror sites.

2) Exploring availability and initiation of Open Source initiatives relating to a reference design for entities within the MEC System, e.g. the MEC Platform, focusing on facilitating MEC application development.

3) Enabling operator adoption and interoperability by developing and maintaining specifications relating to testing, including guidelines and API conformance specifications.

4) Showcasing MEC through webinars and support for Proof of Concepts (PoCs), MEC Deployment Trials (MDT), Hackathons and Plugtests.

4.9.3.4 Artificial Intelligence

Refer to clause 5.6 about current status of AI.

4.9.4 Gap analysis

4.9.4.1 Gap Context

In the present document the gaps refer to existing standards and not to technology in general. Some vendor's products that are not standardized could exist that implement the solutions described in the gaps.

4.9.4.2 Traffic or application classification

There are already multiple applications running in the broadband network before F5G. Multiple services are already a feature supported in the so-called "multi-play" networks. In the existing network the traffic classification is normally defined with the different segment of the data packet, e.g. physical port number, PON ID, VLAN tag, MAC address, IP address. In very few circumstances are the Quintuple or Deep Packet Inspection (DPI) used to identify the traffic of different services. This kind of mechanism may distinguish different types of services whose packet segment features is clearly known. When there is only partial information known or there are multiple kinds of applications with the same packet segment, it will be quite difficult to distinguish them. Furthermore, the traffic classification rules are programmed in the network in advance to implement the traffic identification. When there are new rules that need to be added, the network software has to be upgraded somehow which is normally complicated in a working network.

To implement the scenario based broadband, the identification granularity has to be changed from traffic type level to broadband Apps level. It cannot be based on the segments of Layer 2 or Layer 3 packets whose information is not sufficient to identify a specific App. The Quintuple or DPI is not recommended for data privacy protection reason.

Artificial Intelligence is one of the options for application identification. Artificial Intelligence is needed to be considered here to learn the outer shape features of a specific application when samples are used to train the AI data model. The longer the AI identification process is executed, the greater the potential improvement on the accuracy of the AI identification.

There could be other possibilities for the operators owned application, Cloud VR, for instance. Dedicated signalling process may be designed for these applications.

There are several AI architectures available, that need to be evaluated in order to determine which are adequate for F5G network application identification. Applying a proper AI architecture to the F5G network and support application identification also needs to be studied.

[Gap10-1] An application type identification mechanism is currently not supported.

[Gap10-2] Use of AI for application identification in a F5G network is currently not supported.

4.9.4.3 Application list or database setup

There has to be an application list or database stored in the network for the applications which are needed to be identified. In the existing multi-play network, in which the multiple services are supported, any kinds of rule table items are maintained as the rules for the traffic identification, such as Layer 2 or Layer 3 forwarding or filtering table, Quintuple table or DPI table. When the reused table needs to be adjusted, add, delete or modification actions have to be taken by the network operators. The application list or data base is setup statically with fixed rules.

When Artificial Intelligence is used for application identification, an application feature database entry may be setup based on Big Data and machine learning mechanisms. They are setup and self-optimized automatically while in use.

The establishment and the updates of the feature database could be implemented on-line in real time or off-line periodically.

[Gap10-3] The dynamic creation and updates of application feature database entries using Big Data and Machine Learning mechanisms is currently not supported.

4.9.4.4 Network slicing and SLA

QoS mechanisms are a set of actions applied to the processing of identified packets. The Diffserv model is a typical way to guarantee the QoS for different services or traffic flows. The typical technologies include labelling, priority, buffering, queueing, scheduling, etc. They are all based on a shared physical and logical network. The QoS of different network segments are also managed and controlled separately without integrated operation. For instance in an E2E broadband network composed of multiple physical technologies such as, Wi-Fi®, PON and OTN, the QoS mechanisms are totally different on each of them.

To implement the scenario based broadband, the focus of the quality management has to be changed from the QoS of the traffic to the Quality of Experience (QoE) of an application. Physical or logical network slicing needs to be used to manage the application QoE. The improved mechanism may include a slice in all the physical technologies of Wi-Fi®, PON and OTN, dual network planes of packet and OTN, separation of application and network, etc.

End to end slicing on multiple network segments with different physical technologies and how to guarantee a consistent SLA shall be studied.

[Gap10-4] Mechanisms for F5G End-to-End slicing with consistent SLA on multiple network segments with different physical technologies is currently not supported.

4.9.4.5 QoE improvement effect automatic evaluation

Although there are QoS mechanisms in the existing multi-play broadband network before F5G, it is still lacking the evaluation scheme of technical solutions for the quality of services. The network operator may monitor the transportation of the traffic with the packet statistical parameters in the network. However, the network statistical parameter does not reflect to the QoE directly. The existing QoS parameters are usually defined for network operator technicians with good network expertise, and not designed for the other related parties, either the broadband users or the broadband application providers.

A series of QoE evaluation system should be defined to the specific application instead of QoS of data traffic flow. Different kinds of QoE views should also be provide automatically for the concerns of different parties.

[Gap10-5] None.

[Gap10-6] Evaluation schemes for QoE of specific applications are not currently supported.

4.9.4.6 Potential application and subscriber discovery

The current network can identify a user's usage of the network in real time. In order to find potential demands for network acceleration, namely from heavy users and demanding applications, the network also needs to be able to identify and distinguish each application for a certain user. However, this solution is not available yet.

[Gap10-7] Mechanisms to identify application network usage, which potentially have acceleration requirements are currently not supported.

[Gap10-8] None.

The F5G network needs to avoid links to individual user applications usage unless this service is explicitly included in the user's SLA. Otherwise, linking should be restricted to an anonymized group of users. The linking to specific applications is currently not supported, so the need to avoid links to individual user's applications usage has not arisen yet.

[Gap10-9] Same as [Gap30-4].

4.9.4.7 Network status monitoring

Prior to F5G, the network behaviour has to be defined and programmed accurately to react to any changes in the network. The accuracy can be managed thoroughly but it is not self-manageable and not capable to handle the unpredicted changes if not programmed.

In the circumstances of the scenario based broadband, all the network behaviour should be managed and controlled by the network Artificial Intelligence engine throughout the life cycle of the network. All the network actions should be taken automatically under the indication of the AI engineer, including application identification, network resource allocation, QoE evaluation, network heathy status inspection, proactive network optimization, etc.

For timely reaction of the automated management and control, real-time status reports from the network are needed. Today's monitoring and configuration solutions are based on the Element Management System (EMS) polling (regularly read) information from the devices, however, this is a reactive approach and is not well-suited for AI-based control and management. A novel approach is streaming the device status, from an error, performance, and counter perspective, to the AI engine to react in real time or near real time. This approach needs data models that support streaming telemetry, enabling the management system to understand the streamed data. The management system needs to be able to subscribe to the needed monitoring data, and the devices need to have the capacity for large amounts of management and control data to be streamed to the EMS and AI functionality. This new approach needs further study and standardization of the protocols and data models in the fixed network domains.

[Gap10-10] Mechanisms for near real-time monitoring of F5G network resource utilization and health status are currently not supported.

4.10 Telemetry-based Enhanced Performance Monitoring in Intelligent Access Network

4.10.1 Use Case briefing

The network performance monitoring of traditional Access Networks is mainly based on SNMP and/or CLI (Command-Line Interface) schemes, the sampling intervals of these poll-based data collection mechanisms are limited to the order of minutes, which can be acceptable for conventional traffic monitoring of webpage browsing based services.

However, as more and more novel high bandwidth and latency sensitive services (AR, VR, online gaming, etc.) becoming popular, end users may pose more demands on Access Network qualities, and network operators shall have the capabilities to monitor the traffic variation in order of seconds, as to discover the instant traffic peaks and adjust the network configuration accordingly.

Thus, it is necessary to improve the traditional traffic monitoring scheme, and introduce novel analysis tools for network monitoring, to fulfil the network quality demands of novel applications.

There can be two major use cases for enhanced traffic monitoring and network control in intelligent Access Networks:

i) Performance monitoring of large scale Access Networks, which requires less resource consuming network monitoring techniques, the ability of elastic scaling. This is a better solution for Access Network in populated areas.

ii) Real-time and precise traffic monitoring can improve the traditional traffic monitoring techniques by providing in the order of second traffic sampling, and higher precision collection of traffic data. This is a better solution for dedicated subscriber monitoring.

4.10.2 Technology Requirements

4.10.2.1 Telemetry based network performance monitoring

Enhanced Access Network monitoring can be realized by telemetry techniques, which can provide a lower resource utilization solution for network monitoring, and can archive real-time, shorter interval, finer granularity monitoring capabilities.

Telemetry encompasses various techniques for remote data generation, collection, correlation, and consumption from physical and virtual network elements. The network elements actively report their performance data via 'push mode', comparing to conventional 'pull mode' in SNMP and CLI schemes.

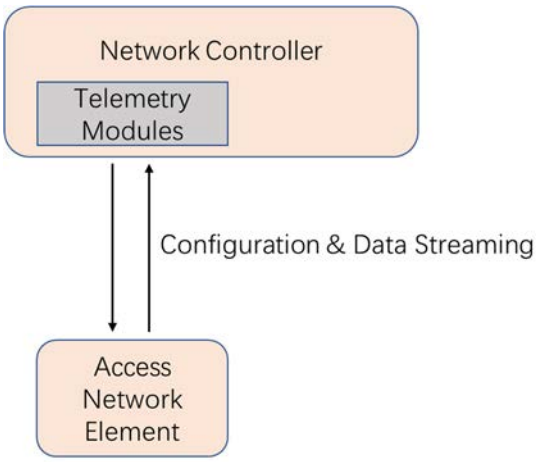


Figure 10: Telemetry based network monitoring scheme

The push mode can avoid unnecessary interaction between controller and network elements, and can effectively reduce processing and bandwidth consumption for routine monitoring. Also, the push mode enables second-level or even sub-second-level sampling intervals for large scale networks.

Network telemetry is intended to be an umbrella term covering a wide spectrum of techniques, and may refer to but not limited to gRPC, YANG-push, IPFIX, IOAM, etc. Telemetry-based performance monitoring is providing better quality of experience since the frequency of telemetry data collection is increased compared to traditional monitoring.

[R11-1] The F5G Access Network shall support telemetry-based network performance monitoring techniques.

4.10.2.2 Network abstraction and configuration schemes for telemetry

Telemetry is a model-driven monitoring technology. The telemetry configuration is usually delivered to network elements via protocols such as NETCONF, etc., in cooperation with specific telemetry YANG models.

Tools and technologies such as YANG models of the Access Network, and NETCONF and/or gRPC based interactive protocols, are necessary for realizing telemetry-based performance monitoring. Currently, there is no standard data model for the telemetry function in Access Network.

[R11-2] The F5G Access Network should define data models for configuration and data collection.

4.10.3 Current related standards

4.10.3.1 BBF

BBF defines the Access Network YANG models, such as BBF TR-383 [i.48] and BBF TR-385 [i.49], and other standards related to other type of Access Network systems. However, as yet there is no telemetry data model for Access Network defined.

BBF also defined telemetry related standards as BBF TR-436 [i.50] and BBF WT-477 [i.51]. BBF TR-436 [i.50] has introduced a Collection Function (CF) as one AIM Basic Components. CF supports collecting data of telemetry, in a general and high-level manner. Logical subsystems defined in TR-436 are required to support consuming telemetry data.

BBF WT-477 [i.51] has started discussion of telemetry, which is specific mapping of BBF TR-436 [i.50] into D-AN architecture.

4.10.3.2 IETF

IETF defines telemetry related framework, and gRPC and UDP based standards for telemetry.

Tables 14 and 15 show the related RFC and several working group drafts related to telemetry, and it should be noted that working drafts are not yet finalized RFCs and they are prone to be updated and may have a possibility of not successfully becoming an RFC, thus the following tables are only for informational use.

Table 14: Telemetry related RFC

Related RFCs	Description
IETF RFC 8641 [i.114]	Subscription to YANG Notifications for Datastore Updates
IETF RFC 9232 [i.115]	Network Telemetry Framework

Table 15: Telemetry related IETF working drafts

Related IETF working drafts	Description
draft-ietf-netconf-udp-pub-channel-03 [i.116]	UDP based Publication Channel for Streaming Telemetry
draft-openconfig-rtgwg-gnmi-spec-01 [i.117]	gRPC Network Management Interface (gNMI)
draft-song-opsawg-ifit-framework-19 [i.118]	A Framework for In-situ Flow Information Telemetry

4.10.3.3 Related open-source project

Open source projects such as gRPC (https://grpc.io/), provide a universal RPC framework, which can be used for traffic monitoring and telemetry in Access Networks.

4.10.4 Gap analysis

4.10.4.1 Gap Context

In the present document the gaps refer to existing standards and not to technology in general. Some vendor's products that are not standardized could exist that implement the solutions described in the gaps.

4.10.4.2 Telemetry technology supporting and evolution in Access Network

Telemetry is so far not widely supported in Access Networks. SNMP and CLI based technics still dominated a large part of the Access Network systems.

For those that support telemetry, the mainstream telemetry technology in Access Networks is gRPC, it has the merit of open source, universal adaption and multiple programming language support. However, the number of devices in Access Network may be very large, even though gRPC is a high-performance telemetry framework, the efficiency and availability may be affected as the number of managed elements grow. Novel lightweight telemetry technology such as UDP-based telemetry should be further studied and deployed.

[Gap11-1] Specification for a lightweight Telemetry technology, such as UDP based telemetry, for the F5G Access Network telemetry is currently not supported.

4.10.4.3 Data model supporting network quality monitoring

Currently there are no dedicated data models for performance monitoring and data collection in Access Network, it is necessary to standardize these data models.

[Gap11-2] Development and specification of a dedicate data model for performance monitoring and data collection for the F5G Access Network are not currently available.

4.11 Remote Attestation

4.11.1 Use Cases briefing

The trustworthiness of network elements (e.g. OLT, ONU) in the Access Network and Transport Network determines the security of the whole F5G network. Remote attestation is a reliable technique for these network elements to prove their trustworthiness to a challenger in a trusted way.

The two best practices for remote attestation are measured boot and Dynamic Integrity Measurement (DIM). Measured boot focuses on authentication of the boot sequence at start-up while dynamic integrity measurement aims at validation of the real-time status of the network elements. By measuring the boot sequence or system runtime data and receiving the measured value securely, the administrator can determine whether the firmware or the running system have been tampered with.

4.11.2 Technology Requirements

4.11.2.1 General introduction

In recent years, attacking techniques are evolving dramatically. Telecommunication network elements, such as OLT and ONU elements, are vulnerable to different kinds of attacks, from physical to cyber-attacks. It is therefore necessary to have efficient methods to detect the malware installed on network elements. Remote attestation is a very reliable method to enable a network management system (the challenger) to determine the level of trust in the integrity of the network elements (attestator) that constitute the F5G network.

4.11.2.2 Secure measurement data generating, storing and reporting

A telecommunication network consists of a large number of different network elements. It is necessary for a challenger to obtain the status of trustworthiness of these network elements. Remote attestation is a reliable technique to achieve this goal. Remote attestation has three major steps:

- Step 1 - Generating measurement data:
  - The status data generating process need to be verified to make sure the data generated is trusted.
- Step 2 - Storing status data:
  - The status data should be securely stored to defend against data tampering.
- Step 3 - Reporting status data:
  - The status data should be securely sent to the challenger.

[R13-1] F5G network elements should support the generation of security measurement data, store it securely and securely report its integrity status.

4.11.2.3 Remote attestation support for network elements with multiple hardware architectures

The hardware architecture of a network element can be implemented in several ways: a single slot network element, a multi-slots network element, or a multi-chassis network elements. Remote attestation should be appropriately supported by network elements s with different hardware architectures.

Remote attestation in a single-slot network element is straight-forward since such kind of network element only contains one single blade. This blade should provide proofs of the integrity status of the network element to the challenger, on demand.

In a multi-slot network element, each blade contains independent hardware running its own operating system. Thus the trustworthiness of the network element depends on the evidence provided by all the blades it contains. Among these blades, only the main blade can communicate with the challenger while the others cannot. However, the main blade should collect the evidence of the other blades, and produce the final evidence of the whole network element.

In a multi-chassis network element, a main chassis cascades with multiple sub-chassis, each running an independent system. Each sub-chassis communicates with the main chassis through a network cable. Herein the main chassis should act as a proxy, collecting the evidence from each sub-chassis and producing the evidence for the whole network element cluster.

[R13-2] F5G network elements should prove its trusted status to the challenger, which should be suitable for its own hardware architecture.

4.11.2.4 Remote attestation support for network element booting and running

Attacks can occur at every stage during a network element's life cycle. Boot and run-time are two typical stages during which hackers can engage and drive the system away from its normal operations. Firmware tampering is one of the classic attack methods to inject malware or involve vulnerabilities to the network element. Secure boot can be helpful to defend against the hacker by verifying the boot firmware and to prevent the system from executing either accidentally or maliciously modified firmware while network administrator cannot get enough information about the attack event. Trusted Boot, enabled by remote attestation, provides another way to demonstrate the integrity of the firmware while keeping the system working.

Run-time is another stage when most of the cyberattacks can occur. The attacker can exploit the software running on the network element to hijack the execution flow or injecting malicious codes. Remote attestation enables the network management system (challenger) to determine the level of trust in the software integrity of a running network element (attestator).

[R13-3] F5G network elements should support the function to prove the evidence of its trusted boot.

[R13-4] F5G network elements should support providing the status of its trustworthiness during run-time.

4.11.3 Current related standards

4.11.3.1 IETF

IETF Remote ATtestation ProcedureS (RATS) working group has published several standard drafts on remote attestation architecture as well as relative protocols:

Table 16: IETF RATS draft briefing

Documents	Summary
IETF RFC 9334 [i.36] Remote Attestation Procedures Architecture	This document defines a flexible architecture consisting of attestation roles and their interactions via conceptual messages.
Draft-ietf-rats-eat-19 [i.119] The Entity Attestation Token (EAT)	This document defines the Entity Attestation Token (EAT), a signed set of claims that describe state and characteristics of an entity, used in remote attestation procedures.
Draft-ietf-rats-reference-interaction-models-01 [i.35] Reference Interaction Models for Remote Attestation Procedures	This document describes interaction models for remote attestation procedures. Three conveying mechanisms - Challenge/Response, Uni-Directional, and Streaming Remote Attestation - are illustrated and defined.
Draft-ietf-rats-tpm-based-network-device-attest-14 [i.120] TPM-based Network Device Remote Integrity Verification	This document describes a workflow for remote attestation of the integrity of firmware and software installed on network devices that contain Trusted Platform Modules [TPM1.2], [TPM2.0] as defined by the Trusted Computing Group (TCG).
Draft-ietf-rats-yang-tpm-charra-21 [i.121] A YANG Data Model for Challenge-Response-based Remote Attestation Procedures using TPMs	This document defines a YANG RPC and a minimal data store required to retrieve attestation evidence about integrity measurements from a device following the operational context defined in Draft-ietf-rats-tpm-based-network-device-attest-14 [i.120].

4.11.3.2 Global Platform

GlobalPlatform Trusted Execution Environment (TEE) Committee is a working group focused on defining an open security architecture for network devices using a Trusted Execution Environment (TEE). They have published several specifications on TEE system architecture and TEE client APIs as below.

Table 17: Trusted Execution Environment specifications briefing

Documents	Summary
TEE System Architecture v2.1 [i.122]	This document explains the hardware and software architectures behind the TEE. It introduces TEE management and explains concepts relevant to TEE functional availability in a device.
TEE Client API Specification 1.0 [i.123]	This document defines the communication between applications running in a rich operating environment and the applications residing in the TEE.

4.11.4 Gap analysis

4.11.4.1 Gap Context

In the present document the gaps refer to existing standards and not to technology in general. Some vendor's products that are not standardized could exist that implement the solutions described in the gaps.

4.11.4.2 Secured measurement data generating, storing and reporting

Recently, IETF Remote ATtestation ProcedureS (RATS) working group has published draft-ietf-rats-reference-interaction-models-01 [i.35] to illustrate a workflow for remote attestation of the integrity of firmware and software on network devices that contain Trusted Platform Modules. This standard draft covers both secure data storing and reporting.

According to the draft, the measurement values are securely stored in a Trusted Platform Module (TPM), a small embedded security module that helps enable tamper-resistant data encryption. The interface provided by TPM for data storing and logging should also be controlled and used in a Trusted Execution Environment (TEE). GlobalPlatformTEE Committee has spent plenty of time studying TEE and published several documents on TEE system requirements as well as TEE client APIs, which has been well developed and commercially used all around world (e.g. Arm® TrustZone®, Intel™ Software Guard Extension).

However, the secured generation of measurement data has not yet been revealed in any of existing standard drafts. Theoretically, the code block used for device artifacts measuring can also be tampered. As a result, the data, which has been securely stored and reported is potentially untrusted at the source. There should be a trusted mechanism, such as secured boot, to verify the integrity of the measurement module before generating data. An appropriate method for security measurement data generation has been requested to be studied and IETF RATS WG is considered as the suitable place to take over this task.

[Gap13-1] An appropriate method for security measurement data generation is currently not supported.

4.11.4.3 Remote attestation support for devices with multiple hardware architectures

IETF RFC 9334 [i.36] published by IETF RATS working group has already covered the conceptual data flow of remote attestation for a composite device with either multi-slot or chassis. According to the draft, a lead attester should be selected to collect the evidence of all other attesters and then generate the evidence of the whole network element. The guidance depicted in this draft can be applied to F5G network elements.

[Gap13-2] None.

4.11.4.4 Remote attestation support for network element booting and running

Currently, most existing remote attestation solutions focus on the integrity of the firmware during boot time. However, carrier-level network elements are in running status most of their life time. Therefore cyber-attacks are more likely to happen during the running moment. Remote attestation should be deployed in run time network element attesting.

Running data stored in the system is vulnerable to cyberattacks such as the notorious buffer overflow attack. The binary file stored in the file system as well as the code loaded in memory is a popular target of an attacker. Thus, file integrity measurement and memory data measurement shall be supported to determine the trustworthiness of the network element.

Unlike at boot time, attesting during which boot sequence is measured and stored as a one-time effort, dynamic integrity measurement, focused on run-time data protection, needs real-time feedback during the whole running cycle. Network elements shall be periodically challenged by the challenger to form the up-to-date status of the network elements. An appropriate method for remote attestation support in F5G network elements running period has been requested to be studied and ETSI TC Cyber is considered as the suitable place to take over this task.

[Gap13-3] An appropriate method for remote attestation support in F5G network elements while running is currently not supported.

[Gap13-4] Same as [Gap13-3].

4.12 Digitalized ODN/FTTX

4.12.1 Use case briefing

PON has been deployed as the main solution for the FTTx Access Network for a long time. With large-scale deployment, costs of PON systems and optical components are greatly reduced. This brings the possibility of replacing some legacy networks (e.g. Ethernet-based networks) with PON systems to a wide range of industries. Therefore, 10G-PON can be used as a basic technology to implement "fibre to everything everywhere" in the F5G generation. The Optical Distribution Network (ODN) is the basis of the FTTx optical Access Network. It connects OLTs and ONUs to form an all-optical Access Network. Typical ODN construction is slow, costly and raises several challenges on resource management being an inevitable issue in the industry. Therefore, fast and flexible ODN construction and efficiently manageable ODN networks have become the core goal and technology development trend of the F5G generations.

This use case describes the digital ODN network and compares it with the traditional ODN network solution. The digital labels and prefabricated connectors of the ODN products enable quick construction and visualization of the entire ODN network, greatly improving the construction efficiency and O&M of the ODN network.

4.12.2 Technology Requirements

4.12.2.1 General introduction

FTTx has been recognized by the majority of fixed network operators worldwide as a strategic approach for the deployment of broadband networks. As the basic infrastructure of FTTx, ODN construction and management consumes the largest part of network investments by operators. It also takes a long time for the construction and significant OPEX costs for operation and maintenance. An ODN network technical solution for fast network construction and digital management can effectively address these issues.

4.12.2.2 ODN digital management

The ODN network structure is complex and involves complex fibre routing management. ODN is a pure passive network, which does not contain any active parts and therefore the connection relationship is usually captured by paper or plastic labels. After the connection is made, the relationship will be recorded manually, hence it is prone to human errors, and labels are prone to detaching, getting lost, and damaged. Moreover, for ODN troubleshooting, a technician shall remotely access the database to retrieve the connection data and look for the corresponding labelled fibre. This makes the management and operation of ODNs dependent on non-reliable network data. The digital management system implements end-to-end ODN management based on image recognition and ODN digitalization, achieving accurate resource management, quick service provisioning, and improving network O&M efficiency.

The following features are required to implement efficient ODN management:

[R14-1] The F5G Access Network shall support the digitization of the physical ODN labels of the various components.

[R14-2] The F5G Access Network Controller shall support the construction and maintenance process, by automatically capturing the ODN information, and visualizing the ODN networks.

[R14-3] The F5G Access Network Controller shall support troubleshooting by remotely accessing the F5G ODN database by technicians.

4.12.2.3 Digitized ODN construction based on pre-connection

To support digitized ODN construction, there are some requirements for pre-connection:

[R14-4] Pre-connecterisation shall be supported for different types of F5G ODN connectors and boxes (including outdoor adapters) and in various environments (indoor, outdoor, simple and complex).

[R14-5] The F5G ODN connectors and boxes (including outdoor adapters) shall meet the appropriate Ingress Protection (IP) level depending on the deployment scenario (such as ingress protection rating IP68 and IP65 [1]).

[R14-6] The connectors shall support low insertion loss to meet the link loss requirements of the F5G ODN.

The digitized ODN connection and installation process long-term reliability test requirements are for example, 2 000-hour, and dual 85-hour test for closures. The digitized ODN connection and installation process mechanical test requirements are for example, optical cable tension and strain requirements.

[R14-7] The digitized ODN connection and installation process shall meet the long-term reliability test requirements and mechanical test requirements during onsite construction and deployment.

4.12.3 Current related standards

4.12.3.1 IEC

IEC 61753 [i.37] is the test standard for all ODN products (including boxes, cables, and connectors). IEC 61754 [i.38] specifies the interface and performance standards for common connectors (such as SC and LC). These standards are product-level design and test standards for traditional ODN networks, there is also no long-term reliability standard requirements, which are quite different from digital ODN scenarios. The related standards cannot be used in the digital ODN solution, and there is no framework standard at the ODN network solution level.

4.12.3.2 ITU-T

Recommendations ITU-T L.100 to L.199 [i.124] are standards for optical fibre cables, including cable structure and characteristics, cable evaluation, guidance and installation technique; Recommendations ITU-T L.200 to L.299 [i.125] are optical infrastructure standards, focusing on infrastructure including node elements (except cables), general aspects and network design. Recommendations ITU-T L.300 to L.399 [i.126] are maintenance and operation standards that include optical fibre cable maintenance, infrastructure maintenance, operation support and infrastructure management and disaster management. Recommendations ITU-T L.400 to L.429 [i.127] focuses on passive optical devices standards.

In conclusion, similar to IEC, the ITU-T standardizes the single-point product solution and corresponding test requirements for optical fibres, cables, and node boxes. The Optical Time Domain Reflectometer (OTDR) and reflector detection solutions are used in traditional ODN network construction and maintenance.

4.12.3.3 ETSI

ETSI also lacks standards for the architecture and product standardization of intelligent ODN and pre-connected ODN [i.19]. It only defines indicators and routine test requirements for some traditional products, such as optical splitter.

4.12.4 Gap analysis

4.12.4.1 Gap Context

In the present document the gaps refer to existing standards and not to technology in general. Some vendor's products that are not standardized could exist that implement the solutions described in the gaps.

4.12.4.2 Introduction

Considering the large-scale deployment of FTTx networks around the world, the digital quick ODN aims to improve ODN deployment and management efficiency, and reduce the total cost of the End-to-End ODN network.

4.12.4.3 ODN digital management

The new approach of a digitalized ODN management system, needs to be standardized including the ODN management system architecture and its interfaces, labels for the components, and the requirements for the terminals used by the workforce to capture installation data, access ODN network information, and visualize the ODN network.

[Gap14-1] The digitalized ODN management system as part of the F5G Access Network controller, is currently not standardized.

[Gap14-2] Same as [Gap14-1].

[Gap14-3] Same as [Gap14-1].

4.12.4.4 Digitized ODN construction based on pre-connection

In the traditional ODN network construction, a lot of connection points are mainly realized by fusion or mechanical splicing on site. This procedure is very time consuming and needs well-trained technicians, which impact the ODN construction efficiency and cost a lot. High quality and high reliability connectors and assemblies shall be manufactured in the factory avoiding onsite fibre splicing and enable plug-and-play features during onsite construction. The standards for quality and reliability of connectors and assemblies shall be specified.

The ODN network environment is complex, including aerial, underground, and duct scenarios. Traditional pre-connection connectors cannot be used in harsh environments, like outdoor. Special designs and standards are required for connection nodes (optical cable connectors and adapters of boxes and box products) of pre-connected ODN products to ensure appropriate link budgets, IP protection level, and service life. The criteria shall be defined for different ODN deployment scenarios.

[Gap14-4] Special designs required for connection nodes are currently not standardized.

[Gap14-5] Same as [Gap14-4].

[Gap14-6] Same as [Gap14-4].

[Gap14-7] Same as [Gap14-4].

4.13 Virtual Presence

4.13.1 Use Case briefing

Virtual presence can be defined as a user experience where something or someone seems to be present, but in reality is not. EXtended Reality (XR)-based virtual presence is another step towards further removing the barriers of distance.

Extended Reality (XR) comprises Virtual, Augmented and Mixed Reality. In all cases, users wear some type of head-mounted-display (HMD) which provides the user with a surround view of some virtual elements. In Virtual Reality (VR), the entire environment is virtual, whereas in AR and MR, parts of the environment may correspond to elements in the (local) real world.

For example, people who want to socially connect to each other over a distance may do so using VR-assisted technology. With each iteration of virtual reality technology at the present the rate of advances, people may feel increasingly as if they are present in the same virtual space. They feel like they are virtually present.

Current state-of-the-art Virtual Presence technology relies on real-time transmission of spatial representations of users. This includes video, audio as well as other related sensory media such as haptic feedback.

In the following clauses it will be explained that providing Virtual Presence (VP) services with sufficient QoS requires dynamic allocation of both upstream and downstream bandwidth, as well as strict requirements on latency. The aforementioned dynamicity in requirements is caused not only by a varying number of users making use of VP, but also by varying requirements during VP sessions. Note that for the downstream bandwidth requirements, this use case is similar to the Cloud VR use case (see clause 4.11).

4.13.2 Technology Requirements

4.13.2.1 General introduction

In general, enabling technologies for virtual presence are oriented at handling the large volume of data which needs to be transmitted and processed. Some of these technologies (such as encoding/decoding) incur a latency penalty, while the user experience demands that latency is kept at a minimum.

4.13.2.2 High performance bi-directional channel requirements

Virtual presence requires bi-directional communication. In order to facilitate this, a bi-directional communication channel needs to be provided by the network. Typically, bandwidth requirements for upstream data traffic are lower than for downstream data traffic. The PON access network needs to be provisioned with appropriate bandwidth for upstream and downstream traffic in order to provide sufficient service for the Virtual Presence use case. The following table defines a number of service levels or network requirements as a set of incremental phases for Audio or (spatial) Video communication with increasing number of users and improved VR user experience.

Table 18: Virtual Presence Phases and network performance requirements

Virtual Presence Phase	1	2	3	4
# parallel users	4	10	16	32
Upstream bandwidth per user	5 Mbits/s	10 Mbits/s	50 Mbits/s	250 Mbits/s
Downstream bandwidth per user	25 Mbits/s	50 Mbits/s	500 Mbits/s	2 Gbits/s
Motion-to-photon latency requirement	< 250 ms	< 150 ms	< 50 ms	< 10 ms
Packet loss rate requirement	< 2 %	< 1 %	< 0,5 %	< 0,5 %

[R15-1] The F5G network shall meet the corresponding network performance requirements of a given Virtual Presence Phase.

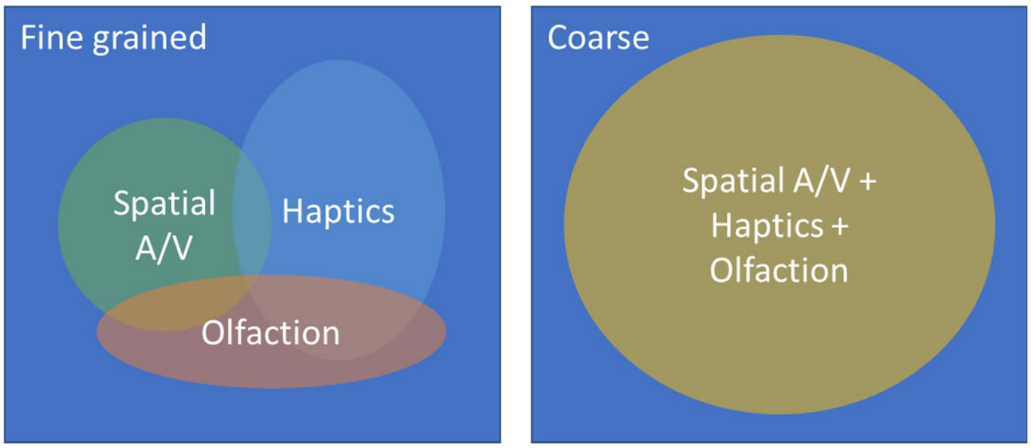
Client applications need to be able to discover the maximum service level which may be provided by the network at a given time. This allows client applications to adapt their streaming strategies to the network capabilities, enabling a faster convergence to optimal, stable resource allocation and an improved user experience as a result.

[R15-2] The F5G network shall support the enabling of applications to discover what service level(s) the network can provide.

4.13.2.3 Virtual Presence slices

The network needs to guarantee that a certain set of QoS parameters is met. These parameters may consist of upper bounds of bandwidth usage and a maximum allowed latency. Network slicing may provide the technology for providing such guarantees from the network. The F5G network needs to support traffic slicing according to specifications which consist of a subset of at least the following parameters: bandwidth, latency, packet jitter, packet loss.

[R15-3] The F5G network shall support traffic slicing for specified network parameters.



NOTE: To the left an allocation with many fine-grained slices, to the right the convex hull of the left allocations as a single slice. Note that the total area of the latter is greater than the total area of the former.

Figure 11: A schematic impression of a resource space allocation

Virtual presence requires the use of multiple different types of input and output systems in parallel e.g. for spatial audio/video, haptics and olfaction with corresponding traffic flows. As such, an application may be able to provide fine-grained information on the desired set of slices for these individual traffic flows, as shown in Figure 11.

EXAMPLE: An application could request for the same usage scenario the following sets of slices, with the following indicative bandwidth figures:

1) Fine-grained slices:

   a) Audio/Spatial Video: 10 Mbits/s up, 50 Mbits/s down, maximum network delay 150 ms, packet loss < 1 %.

   b) Haptics: 5 Mbits/s up, 5 Mbits/s down, maximum network delay 5 ms, packet loss < 0,1 %.

   c) Olfaction: 200 Kbit/s up, 1 Mbits/s down, maximum network delay 200 ms, packet loss < 10 %.

2) Coarse slice (convex hull of fine-grained slices):

   a) Virtual Presence: 15,2 Mbits/s up, 56 Mbits/s down, maximum network delay 5 ms, packet loss < 0,1 %.

As illustrated by the example above: Compared to a coarse slice, a set of fine-grained slices will allow network operators to make more efficient use of their resources, as some of the more stringent requirements apply to only a small amount of traffic. Therefore, less resources have to be allocated and/or reserved, increasing the likelihood that these and other guarantees can be made and kept. To enable efficient and effective use of F5G network resources, the F5G network shall support multiple parallel slices that each support specific requirements of a specific application.

[R15-4] The F5G network shall support multiple parallel slices that each support specific requirements of a specific application.

Cross-layer signalling between the application and network layers is needed in order for applications to be able to request allocation and adjustment of appropriate network slices. E.g. a virtual presence session orchestrator may assist in negotiating a slice on behalf of client devices on the network.

[R15-5] The F5G network shall support a control interface with the application layer.

[R15-6] The F5G network shall support on-demand application and service requests, to dynamically setup, release and adapt F5G network slices.

User experience may be improved by continuously adjusting slice and application parameters based on network conditions. To facilitate this, both the network and the application need to be able to share QoE metrics.

[R15-7] The F5G network shall support the bi-directional exchange of real-time QoE metrics with the applications and services.

The network operator may offer network slices for specific VP applications and/or VP systems only.

[R15-8] The F5G network shall support authentication and authorization specific to VP applications and/or VP systems for a configurable set of services.

[R15-9] The F5G network shall support authentication and authorization to specific VP applications and/or VP systems for a configurable set of allocated network slices.

Moreover, the network requirements may change during a virtual presence session. For instance, the scene may change, or users may join or leave a shared session. Furthermore, changes may be triggered by the network, e.g. when more or less bandwidth becomes available, the network may advise client applications.

[R15-10] The F5G network should support dynamic adjustment of slice parameters.

4.13.2.4 Edge computing and compute offloading

Virtual Presence may benefit greatly from using edge computing technology. Edge computing extends cloud computing by enabling additional compute resources closer to the end-user, i.e. closer to the edge of the network. Depending on the scenario, the edge may be in the same neighbourhood, radio cell, city, or country as the user. A PON operator may consider providing edge computing services directly connected to the PON. Alternatively, the edge may be accessible by a user within the PON, but the edge itself may be located outside of said PON.

One of the main uses for edge computing in the Virtual Presence use case is the offloading of computation tasks to a central or edge cloud. Client devices that are capable of offloading to an edge require less powerful hardware and become cheaper as a result.

Another use case for edge computing is the acceleration of application functions beyond that of the capabilities of the client device (e.g. due to dedicated hardware such as GPUs, ASICs, Quantum computers, or AI accelerator units). In such scenarios, edge computing is no longer optional, and becomes vital to providing any user experience at all.

[R15-11] The F5G network should support edge computing functionality integrated with the OLT.

[R15-12] The F5G network shall support edge computing services.

Offloading of computation tasks to a central cloud environment instead of the edge may be preferred in some use cases such as those with less stringent latency or higher computation requirements. In other cases, insufficient edge resources may be available, and some computation tasks need to be offloaded to the cloud instead. In all these cases the application still needs bandwidth guarantees from the network. Such requirements may need a different priority than regular traffic by the application. The F5G network should support slices with different QoS/priority levels to support compute offloading to a cloud environment.

[R15-13] The F5G network should support slices with different QoS/priority levels.

4.13.2.5 Privacy and security

The Virtual Presence use case requires users to be recorded. Users may not be fully aware or in control of the data which is being sent by the application they are using. Moreover, some of the data recorded by virtual presence systems may be considered biometric (e.g. body proportions/head rotation/eye-gaze/haptics). Great care needs to be taken to properly handle the user data, and to prevent misuse of sensitive information. The VP application needs to ensure that sensitive traffic is end-to-end encrypted i.e. from client device to application server.

[R15-14] The F5G network shall support encryption of user data traffic flows.

[R15-15] The F5G network shall prevent side-channel attacks on the encrypted user traffic itself.

Virtual Presence requires the allocation and use of (a potentially large amount of) network resources. Misconfigured or malicious applications may reserve more resources than is needed.

[R15-16] The F5G network should prevent applications from allocating excessive proportion of F5G network resources.

[R15-17] The F5G network should prevent applications from failing to release F5G network resources.

4.13.3 Current related standard specifications

4.13.3.1 ITU-T

Recommendation ITU-T Q.3715 [i.128] (produced by ITU-T Question 5 of Study Group 11) provides an architectural recommendation including signalling requirements to implement dynamic bandwidth adjustment (increase/decrease) based on user's demand with the help of Software Defined Networks (SDNs). The proposed architecture consists of a service platform, a controller and network gateway. The controller is connected to operational support system and a billing system. The subscriber directly requests the service platform to adjust his/her bandwidth. The controller receives this request from service platform, assesses if such a request can be fulfilled and acts accordingly.

4.13.3.2 BBF

BBF TR-144 [i.129] provides a set of requirements that an architecture shall comply with in order to support bandwidth on demand.

BBF TR-369 [i.24] provides a generic platform for agents to consume services provided by controllers. Moreover, the standard contains discovery mechanisms for discovery of controllers, as well as message protocols and formats for signalling and data exchange. The framework of BBF TR-369 [i.24] may fulfil some of the requirements for application/network cross-communication.

4.13.3.3 ETSI

ETSI TS 181 018 [i.130] and ETSI TR 182 022 [i.131] identifies the capabilities required of a network for providing QoS guarantees. Appendix A.4 outlines how the specified capabilities may be used to request a given amount of bandwidth for some time. This example may be trivially extended to include other network parameters as well. Such a service may provide a step towards providing a full Virtual Presence service by the network.

ETSI GS MEC 002 (V1.1.1) [i.132] provides general requirements for a system which implements edge computing. Although oriented at Mobile edge computing, many of the requirements also apply to general edge computing.

ETSI GS MEC 003 (V2.2.1) [i.133] describes a framework and a reference architecture for Mobile Edge Computing.

ETSI GS MEC 011 (V2.2.1) [i.134] describes various APIs and architectures for the interaction between applications and the network for managing edge computing services.

ETSI GS MEC 015 (V2.1.1) [i.135] describes APIs, messages and architectures wherein Mobile Edge Applications can request bandwidth from the network. ETSI GS MEC 015 [i.135] focuses on bandwidth allocation only, and not on other network parameters. The describe message formats cover distinctions between upstream and downstream bandwidth. Traffic may be allocated on a per-session or per-application basis.

ETSI GS MEC 029 (V2.2.1) [i.136] describes a Fixed Access Information Service, which provides APIs and messages for discovering available Fixed Access technologies. Moreover, the messages described in ETSI GS MEC 029 [i.136] allow API users to discover a basic set of network capabilities.

ETSI GR MEC 024 (V2.1.1) [i.137] provides details on network slicing state-of-the-art at the time of writing of said document (2019). More details are provided on how to achieve edge computing across multiple networks, what guarantees can be provided in such cases and when.

ETSI GS MEC-IEG 006 (V1.1.1) [i.138] provides an overview of network metrics which may be relevant for taking into account end-user QoS/QoE when assigning slices.

ETSI White Paper No. 28 [i.139] "MEC in 5G Networks" summarizes the ETSI GS MEC specifications. The white paper provides details a variety of Edge Computing architectures, tailored to 5G. Moreover, a number of use cases are described which show how Edge Computing can be used with such architectures.

4.13.3.4 3GPP

3GPP TS 23.548 (V17.1.0) [i.140] specifies how Edge Application Servers may be discovered. 3GPP TS 23.548 [i.140] provides additional details on how to set-up and initialize edge computing applications.

3GPP TS 23.501 (V17.3.0) [i.104] has a clause on how network slicing may be implemented in a 3GPP 5G system. Details include slice management, client management and allocation, and slice characteristics.

4.13.3.5 ISO/IEC

ISO/IEC 23009-5 [i.141] (DASH-SAND) describes a reference architecture where clients communicate with a DASH-Aware Network Element (DANE) which is capable of managing and assigning available bandwidth to clients. Moreover, ISO/IEC 23009-5 [i.141] describes messages which allow clients to communicate media-oriented QoS constraints.

4.13.3.6 CTA WAVE

CTA-2066 [i.142] has been developed by CTA R04 WG20 Streaming Media Quality of Experience. CTA-2066 [i.142] outlines a standardized set of media playback metrics and APIs. CTA-2066 [i.142] is aimed at consumption of 2D (potentially live) media.

4.13.3.7 IETF

In its draft-teas-ietf-network-slices-19 [i.156] on network slicing use cases (Network Slicing Use Cases: Network Customization and Differentiated Services), engineers from IETF explain what slicing entails in 3GPP terms. The document describes the current state of affairs with respect to standardization. The document concludes with "*There is need for a uniform framework for End-to-End network slicing specifications that spans across multiple technology domains and can drive extensions in those technology-areas for support of Network slices.*", suggesting that more standardization efforts may still be required.

4.13.4 Gap analysis

4.13.4.1 Gap Context

In the present document the gaps refer to existing standards and not to technology in general. Some vendor's products that are not standardized could exist that implement the solutions described in the gaps.

4.13.4.2 High performance bi-directional channel requirements

Expected network requirements can be serviced by current-gen PON networks.

[Gap15-1] None.

There are no standards for exchanging the service level(s) explicitly. However, most of these metrics are typically determined on a reactive basis (e.g. by running a speed test, monitoring packet loss) in current applications. Some of the required technology for this gap may be available in the 3GPP 5G slice management APIs.

ETSI GS MEC 029 (V2.2.1) [i.136] describes a Fixed Access Information Service, which allows i.e. to retrieve the maximum capabilities of the network.

[Gap15-2] A Standard for explicitly discovering application-oriented service levels provided by the network is currently not defined.

4.13.4.3 Virtual Presence slices

The above may be implemented using a DiffServ architecture. However, application-oriented specifications for an integrated architecture are lacking. Slicing is most extensively covered by the 3GPP 5G specification from a 5G network perspective. Although the support for the mentioned metrics may be available through a slice with specific control-plane and user-plane functions, there is still a gap where these metrics may be explicitly specified.

BBF TR-144 [i.129] specifies requirements for guaranteeing a set QoS, bandwidth, latency or packet loss. However, BBF TR-144 [i.129] does not specify any mechanisms on how that should be achieved.

[Gap15-3] Explicit slicing mechanism for slicing networks according to a combination of bandwidth, latency, packet jitter, packet loss, is currently not supported.

This requirement adds an additional requirement to Gap15-3 solutions wherein an application shall be able to request multiple slices.

The 3GPP 5G specification places an explicit limit on the number of parallel slices served to a single client. As such, there is a gap where users are running multiple multi-slice applications. The network capability to offer a (practically) unbounded number of parallel slices is currently not supported. Some of these requirements may be fulfilled using service discovery mechanisms such as DNS (SRV) and UPnP.

[Gap15-4] The F5G network capability to support a practically unbounded number of parallel slices is currently not supported.

The 3GPP MEC and 5G specifications cover this aspect.

[Gap15-5] None.

No explicit protocols exist for application/network integration (e.g. (how) can the application signal slice change requests?). Some of the APIs and architecture from the ETSI MEC standards may be useful to construct a full solution, but such a specification is lacking.

Recommendation ITU-T G.9807.1 [3] requires dynamic bandwidth allocation mechanisms to be available. This may be suitable for the implementation of higher-level implementations/effectuation of slices.

[Gap15-6] API and system architecture to allow applications to dynamically request and release network slices are currently not supported.

DASH-SAND provides messages and mechanisms for the network to communicate QoE metrics. Moreover, the CTA-2066 specification also provides directions for standardized media QoE metrics.

ETSI GS MEC-IEG 006 (V1.1.1) [i.138] also provides details on what kind of metrics may be useful to monitor QoE in MEC systems. However, no mechanism or service is described where these QoE metrics are routinely collected and exchanged as a service.

An integration effort for the above standards may pave the way to fulfilling this gap.

[Gap15-7] Mechanisms for clients to exchange application-related QoE metrics with the network are currently not supported.

PKI-based authentication and authorization infrastructure technologies such as Recommendation ITU-T X.509 [i.183], TLS and e.g. Kerberos are widely available.

[Gap15-8] None.

PKI-based authentication and authorization infrastructure technologies such as Recommendation ITU-T X.509 [i.183], TLS and e.g. Kerberos are widely available.

[Gap15-9] None.

Application-initiated slice parameter adjustment is not included in either the MEC or 3GPP 5G slicing standards.

[Gap15-10] Same as [Gap15-6].

4.13.4.4 Edge computing and compute offloading

No standard exists for optical networks. However, ETSI MEC standards may serve as detailed inspiration and partial implementation of a future Optical Edge Computing standard.

[Gap15-11] Same as [Gap15-12].

Support for slicing should suffice for fulfilling this gap. An application wishing to use an external edge computing solution may request (one or more) dedicated slices for edge computing data and orchestration traffic.

[Gap15-12] A Standard for edge computing integrated within optical F5G networks is not currently defined.

ETSI MEC standards do not support slices with different QoS/priority levels to support compute offloading to a cloud environment. Part of this scheduling technology is included as part of the Kubernetes control plane. Intel Telemetry-Aware Scheduling may fill most of this gap.

[Gap15-13] Prioritization of slices is not currently supported.

4.13.4.5 Privacy and security

Encryption of user data traffic flows may be implemented using existing security mechanisms, algorithms and standards.

[Gap15-14] None.

Existing standards do not address the need for privacy of VP users. This can be an important aspect, for instance if a user requests to lower the bandwidth for the weekend since they are not at home, the compromise of such information could lead to problems to the user. In another example, the intelligent network might realize that the user is starting to stream a high-quality video and would increase the bandwidth temporarily. However, such information about the user should be anonymized. In yet another example, the intelligent network might realize that the user is starting to stream haptics data and would change the latency service level temporarily. However, such information about the user should be anonymized.

[Gap15-15] Same as [Gap30-4].

The resource allocation services need to support authentication and authorization in order to prevent unauthorized allocation requests. For example, an adversarial actor may attempt to request expensive resources in order to incur costs to end-users or network operators alike. In another example, an adversarial actor requests on behalf of a user that computation is moved to their device, leading to an inefficient use of resources such as draining their battery or hampering the user device in performing its regular functions.

Many implementations of governed resource allocation exist. For example, Kubernetes has an architecture in place for role-based allocation and release of resources.

[Gap15-16] None.

Application-initiated dynamic bandwidth allocation comes with a number of inherent security risks. For example, misconfigured or rogue applications may lay claim more resources than required, this then prevents legitimate users from receiving the best possible QoE. Likewise, the resource allocation service needs to be resilient to malfunctioning applications which e.g. fail to actively request release of previously claimed resources. An adversarial actor may also attempt to disrupt automated resource allocation algorithms by generating malicious traffic (either a targeted set of payloads, or simply a large amount of traffic).

[Gap15-17] Mechanisms to prevent the requesting and use of more F5G network resources than required by applications are not supported currently.

NOTE: [Gap15-17] is related to [Gap15-6].

4.14 Enterprise private line connectivity to multiple Clouds

4.14.1 Use Case briefing

Enterprise private line services require high quality network performance, such as on-demand guaranteed bandwidth, low latency, high secure isolation, and high availability. In addition, enterprises are gradually migrating their applications to different clouds. This further requires flexible private line connectivity to access these multiple clouds, to meet different customer service requirements. This use case requires the carrier network to provide high quality and flexible Point-to-Multi-Point or Multi-Point-to-Multi-Point connectivity to multiple clouds.

4.14.2 Technology Requirements

4.14.2.1 General introduction

Enterprise private line services have strict performance requirements on the carrier network.

OTN is a TDM-based technology. Unlike the packet store and forward technologies, OTN does not have oversubscription, and queuing and buffering is not necessary when using OTN to transport service traffic. Therefore, OTN naturally has the characteristics of guaranteed bandwidth, low deterministic latency and low packet jitter, high security, high availability and traffic isolation. OTN is well suited to be the carrier network for these services.

4.14.2.2 Single-point/Multi-point access to multiple Clouds

Single-point/Multi-point access to multiple Clouds.

Typically different Cloud Data Centres (DCs) can provide different application services (e.g. storage or cloud computing services). An enterprise needs to access multiple cloud DCs for different application services. An enterprise normally has one headquarter and may have one or multiple branches. If all the enterprise branches access the Cloud DCs through the enterprise headquarter, the OTN carrier network is required to support Point-to-Multi-Point (P2MP) service access. If the enterprise headquarters and its branches are each directly connected to multiple Cloud DCs (e.g. each branch selects the nearest Cloud DC to access), the OTN carrier network is required to support Multiple Point-to-Multi-Point (MP2MP) service access.

[R16-1] The F5G OTN edge nodes shall support P2MP and MP2MP connectivity to cloud services.

4.14.2.3 Service driven

For the enterprise private line connectivity to single or multiple clouds scenarios, an enterprise may request access to a new cloud DC for a new cloud application.

To reduce the service enabling time and improve the enterprise's experience, the connectivity for the requested cloud service should be provisioned automatically. This requires the OTN carrier network to recognize such service request, and to trigger the OTN carrier network to provision the connection for the requested service.

[R16-2] The F5G OTN edge nodes shall support recognizing the cloud service request and its SLA requirements.

[R16-3] The F5G OTN edge nodes shall support on-demand OTN connection creation, modification and deletion based on the cloud service requirements.

4.14.2.4 Flexible bandwidth

For the enterprise private line connectivity to single and multiple clouds scenario, different enterprises and different cloud application services may require very different bandwidths from tens of Mbps to several Gbps. For example, the required bandwidths are normally less than 100 Mbps for the government cloud services, about 200 Mbps ~ 10 Gbps for remote healthcare services and about 1 Gbps ~ 10 Gbps for cloud education service for a campus.

To improve the resource utilization of the OTN carrier network, the bandwidth per OTN connection should match the bandwidth requirements of the cloud services. This requires the OTN to support both fine granularity connectivity and course granularity connectivity.

[R16-4] The F5G network shall support OTN container that match the bandwidth requirements of the various enterprise cloud services.

Furthermore, an enterprise may have different bandwidth requirements in different time period. For example, the enterprise may request to increase the bandwidth of its private line service temporarily at the end of a month for stock audit, or banks doing reconciliations between banks. When adjusting the bandwidth of the OTN connection, the existing service traffic shall not be affected.

[R16-5] The F5G OTN shall support dynamic bandwidth adjustment of an OTN connection.

[R16-6] Same as [R23-2].

4.14.2.5 Slicing

For enterprise private line connectivity to multiple clouds scenarios, different enterprises' data to and from the clouds needs to be isolated from other user traffic, without affecting or being affected by other user traffic. This provides the enterprise user with a secure connection. To achieve this an enterprise specific slice can be set up, to channel the service traffic.

In addition, enterprises may use their own private addresses (e.g. IP addresses) for their private line services. To avoid conflict of private addresses between different enterprises, private address isolation shall also be supported for enterprise data transmission.

Furthermore, to provide efficient and dynamic operation and maintenance of the OTN carrier network, the OTN network slices need to be managed and controlled automatically.

[R16-7] The F5G E2E OTN shall support network slicing.

[R16-8] The F5G E2E OTN shall support the management and control of network slices.

4.14.2.6 Service scalability

In the past, private line services were mainly used by large-scale enterprises to interconnect their headquarters and branches. There is a trend that more and more enterprises, including large-scale enterprises and Small and Medium Enterprises (SMEs), are migrating their applications to Cloud DCs, and requesting more and more private line services to connect to the clouds. Therefore, the total number of OTN connections for these private line services will be increasing.

The OTN carrier network shall be configurable to match the current and increasing needs of the cloud services. Especially, to control the increasing number of the OTN connections, the scalability of the connection control needs to be considered.

[R16-9] The F5G E2E OTN should provide scalable connection control to match the increasing number of connections.

4.14.2.7 Deterministic protection and restoration

The reliability between the OTN carrier network and the Cloud DCs is extremely important, because all the cloud services will be affected if the communication between the OTN carrier network and the Cloud DCs is interrupted. Dual-homing protection mechanisms could be used for the cloud interconnection, i.e. a Cloud DC cloud interconnect with the dual-homed active and standby Cloud PEs (Provider Edge) in the OTN carrier network.

Protecting the OTN connections against network failures within the carrier network is also needed to improve the availability of the services. Protection (e.g. 1+1 or 1:1 protection) or restoration (e.g. rerouting) mechanisms may be used.

Restoration mechanism has much higher resource utilization than protection mechanism, especially when there are a large number of cloud service. The performance of the restoration time is critical. To minimize the impact on the enterprise's service traffic, the restoration time is normally required to be several hundreds of milliseconds, which should not become significantly longer when there are a large number of connections to be rerouted at the same time. In this way, the service interruption time can be short and deterministic, and the availability of the service could be guaranteed.

[R16-10] The F5G E2E OTN should support protection mechanisms to resolve network failures to the Cloud DCs.

[R16-11] The F5G E2E OTN connection protection mechanisms should resolve single or multiple network failures.

[R16-12] The F5G E2E OTN should support connection restoration mechanisms to resolve single or multiple network failures in OTN, with deterministic restoration performance.

4.14.3 Current related standard specifications

4.14.3.1 ITU-T

ITU-T has standardized the OTN series of Recommendations, see clause 4.4.3 of the present document.

ITU-T also standardized the management and control architecture of the Optical Transport Network, see clause 5.5.4 of the present document.

4.14.3.2 IETF

IETF has defined the GMPLS architecture for the control plane of different types of transport networks, and has made protocol extensions to support the control of the OTN.

- IETF RFC 3945 [i.143] which defines the architecture of the GMPLS.
- IETF RFC 7138 [i.144] which specifies the OSPF-TE routing protocol extensions to support GMPLS control of OTN.
- IETF RFC 7139 [i.145] which provide extensions to GMPLS signalling to control the full set of OTN features specified in Recommendation ITU-T G.709 (2012) [i.67], including ODU0, ODU4, ODU2e, and ODUflex.
- IETF RFC 7963 [i.146] which provides further extensions to RFC 7139 to support additional signal types (ODU1e, ODU3e1 and ODU3e2) defined in Recommendation ITU-T G.Sup43 [i.147].
- draft-ietf-ccamp-gmpls-otn-b100g-applicability-15 [i.148] which examines the applicability of using existing GMPLS routing and signalling mechanisms to set up ODU connections over ODUCn links as defined in Recommendation ITU-T G.709 (2020) [i.67].

IETF is now developing a set of YANG data models for the TE networks, and the augmentation of these YANG data models for OTN:

- IETF RFC 8795 [i.149] which defines the YANG data model for representing, retrieving and manipulating TE topologies.
- draft-ietf-teas-yang-te [i.150] which defines the YANG data model for the provisioning and management of TE tunnels, LSPs and interfaces.
- draft-ietf-ccamp-otn-topo-yang [i.151] which defines the YANG data model to describe the topologies of the OTN.
- draft-ietf-ccamp-otn-tunnel-model [i.152] which defines the YANG data model for tunnels in OTN TE networks.
- draft-ietf-ccamp-l1csm-yang [i.153] which provides a YANG data model for Layer 1 Connectivity Service Model (L1CSM).

Furthermore, IETF is working on the YANG data models for network slicing, and the augment of these YANG data models for OTN:

- draft-ietf-teas-ietf-network-slice-nbi-yang [i.154] which defines the YANG model for the IETF Network Slice service.
- draft-ietf-teas-ietf-network-slice-use-cases [i.155] which describes the use cases of IETF Network Slice, and analyses the functionalities for the NBI of the IETF Network Slice Controller.
- draft-ietf-teas-ietf-network-slices [i.156] which defines a framework of network slicing in the context of networks built from IETF technologies.
- draft-ietf-ccamp-yang-otn-slicing [i.157] which defines a framework for OTN network slicing and a YANG data model augmentation of the OTN topology model.

4.14.4 Gap analysis

4.14.4.1 Gap Context

In the present document the gaps refer to existing standards and not to technology in general. Some vendor's products that are not standardized could exist that implement the solutions described in the gaps.

4.14.4.2 Single-point/Multi-point access to multiple Clouds

Traditional OTN provides Point-to-Point (P2P) service access and transparent service transmission.

In addition to support P2MP and MP2MP access for enterprise services, the OTN edge nodes need to determine the destination information of the service traffic, and know which OTN edge node the service traffic is destined for. In this way, the correct OTN connection can be determined, with the correct destination OTN edge node, to transmit the service traffic.

The source and destination of the service traffic are from/to the enterprise-side access nodes (e.g. enterprise CEs (Customer Edge)) and the Cloud DC gateways, which may or may not be in the same IP segment.

If the enterprise-side access nodes and the Cloud DC gateways are in the same IP segment, the VLAN ID could be used to differentiate the different service traffic, and the OTN edge nodes need to learn the VLAN information in both enterprise-side access nodes and Cloud DC gateways.

If the enterprise-side access nodes and the Cloud DC gateways are in the different IP segments, the IP addresses could be used to differentiate the different service traffic, and the OTN edge nodes need to learn the IP addresses in both user-side access nodes and Cloud DC gateways.

The OTN edge nodes need to support the automatic learning of the cloud-side and enterprise-side service address information (e.g. Layer-2 VLAN ID and Layer-3 IP address, etc.), and support mapping service packets with different service addresses into different OTN connections.

[Gap16-1] The mechanism to automatically learn the cloud-side and enterprise-side service address information in the OTN edge node is not currently supported.

4.14.4.3 Service driven

Traditional OTN connections are used to transmit the service traffic transparently. The creation of the OTN connection is normally triggered by the network operator, or by the network management and control system.

When an enterprise needs to connect to a new Cloud DC, or to modify the bandwidth of an existing cloud private line service, a service request (including the SLA requirements of the service) will be sent to the OTN management and control system, so that the OTN management and control system can trigger the creation or modification of the OTN connection.

A YANG data model is needed on the northbound interface of the OTN management and control system, which is under development in draft-ietf-ccamp-l1csm-yang [i.153].

[Gap16-2] Standardized YANG data models for the cloud service requests and their SLA requirements are not currently supported.

Once a new service request is identified, the OTN carrier network could run the existing signalling protocol in its control plane to create the OTN connection, e.g. the GMPLS RSVP-TE protocol specified in IETF RFC 7139 [i.145].

[Gap16-3] None.

4.14.4.4 Flexible bandwidth

Currently OTN supports an ODUflex container with a bandwidth of approximately 1,25 Gbps. To support any rate traffic above 1,25 Gbps, ODUflex can be used with the bandwidth of N × 1,25 Gbps. For enterprise cloud service whose bandwidth requirement is lower than 1,25 Gbps, an OTN connection with 1,25 Gbps has to be provisioned, which is suboptimal wasting resources.

The current OTN supports lossless bandwidth adjustment for ODUflex connections with the bandwidth of N × 1,25 Gbps, see Recommendation ITU-T G.7044 [i.158]. The current OTN also support dynamic lossless bandwidth adjustment of ODUflex by the cooperation of the OTN data plane and control plane, see IETF RFC 7139 [i.145]. However, there is no OTN standard to support dynamic lossless bandwidth adjustment below 1 Gbps or seamlessly across the 1,25 Gbps boundary.

See clause 4.16.4.1 of the present document.

[Gap16-4] Same as [Gap23-1].

[Gap16-5] The dynamic bandwidth adjustment for sub-1 Gbps OTN connections is currently not supported.

[Gap16-6] Same as [Gap23-2].

4.14.4.5 Slicing

OTN supports hard isolation between different connections, because it is based on TDM technologies.

[Gap16-7] None.

On the management and control aspects, the OTN management and control system needs to manage each OTN slice and maintain their information. A set of YANG data models for the northbound interface of the OTN management and control system is needed, which is under development in draft-ietf-ccamp-yang-otn-slicing [i.157].

[Gap16-8] The YANG data models for the management and control of the OTN slice are currently not standardized.

4.14.4.6 Service scalability

The current OTN signalling protocol, as defined in IETF RFC 7139 [i.145], is designed to control the OTN with the granularity of 1,25 Gbps. For finer granularity bandwidth (e.g. Mbps-level) in OTN, the number of the connections could be multiple order of magnitude greater than that of existing network.

Traditional OTN signalling protocol may face a scalability problem to control a large number of OTN connections. For example, it may take much longer time to restore a large number of OTN connections, due to the congestion in the OTN Data Communication Network (DCN) when sending a large number of restoration signalling messages simultaneously.

[Gap16-9] There is a short fall in the current OTN signalling protocol performance when controlling a large number of OTN connections

4.14.4.7 Deterministic protection and restoration

To protect the communication between the OTN carrier network and the Cloud DCs, OTN dual-homing protection mechanism is needed.

When the dual-homing protection is used, the destination nodes of the OTN working path and protection path within the OTN carrier network will be different. For example, in Figure 12, the destination nodes of the OTN working path and protection path are Cloud PE_1 and Cloud PE_2 respectively.

In the existing protection mechanisms such as 1+1 or 1:1, the destination nodes of the working and protection path are always the same. New protection mechanism is needed to support the case where the destination node of the OTN protection path is different from that of the working path.

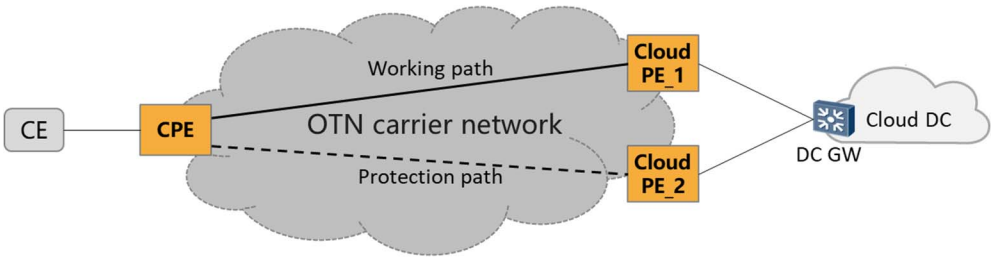


Figure 12: Example of OTN dual-homing protection

[Gap16-10] Current OTN protection mechanisms do not support the case where the destination node of the OTN protection path is different from that of the working path.

To protect the OTN connections against one or multiple network failures within the carrier network, protection or restoration mechanisms (or a combination of them) could be used. Existing OTN 1+1 or 1:1 protection mechanisms are still applicable, while the existing dynamic restoration (also known as dynamic rerouting) mechanism may face the scalability and performance problem when restoring a large number of connections, see clause 4.15.4.5 of the present document.

[Gap16-11] None.

[Gap16-12] Same as [Gap16-9].

4.15 Premium home broadband connectivity to multiple Clouds

4.15.1 Use Case briefing

Premium home broadband services such as high quality video and Cloud VR have become increasingly popular, driving the need for upgrading of the home network technologies. High bandwidth, high reliability, low packet jitter, and low latency are key indicators of high quality video transport networks. In Cloud VR, as an example, when a home terminal user of the Cloud VR service accesses a VR application and goes online, the carrier network needs to dynamically schedule services to different cloud nodes based on the VR cloud nodes allocated by the VR service management and scheduling platform.

4.15.2 Technology Requirements

4.15.2.1 General introduction

Premium home broadband services impose stringent requirements on both the Access and Aggregation Networks, such as high bandwidth, low latency, and low packet loss rate. In addition, the need for on-demand network scheduling and flexible connectivity bandwidth provisioning, supporting the Cloud VR service requirements, is required. The traffic route is defined by the location of Cloud VR active server node, to which a particular user is assigned.

In the Access Network, PON technology is used to carry the high-quality cloud services. In the Aggregation Network, the high-quality cloud services from the OLTs to the Cloud DCs could be transmitted by OTN connections, as the OTN naturally support guaranteed bandwidth and low latency and jitter, but other technologies could also apply.

Note that different home users connected to the same OLT and accessing to the same Cloud DC may use the same OTN connection in the Aggregation Network. This significantly reduce the total number of OTN connections in the network.

4.15.2.2 Single-point/Multi-point access to multiple Cloud DCs

Typically different Cloud DCs can provide different application services. For premium home broadband, a very large number of home broadband users may need to access multiple Clouds via a large number of OLTs. So the connectivity model between the OLTs and the Cloud DCs can be Point-to-Multi-Point or Multi-Point-to-Multi-Point, both of which need to be supported by the OTN Aggregation network.

[R17-1] Same as [R16-1].

4.15.2.3 Service-driven optical network

For the home broadband services connectivity to single or multiple clouds scenarios, a home user may request access a new or additional cloud DC for a new cloud application.

To reduce the service enabling time and improve the home user's experience, the connectivity for the requested cloud service needs to be provisioned automatically. This requires the OLT node to be aware of cloud service application type, service requests and their SLA requirements, and to trigger the OTN aggregation network to provision the connection for the requested service.

NOTE 1: How an OLT is aware of the service information is an internal function of the OLT, which does not need to be standardized, and therefore no standard requirement is needed.

The OLT may interact with the OTN Aggregation Network at the controller level, or the Network Element (NE) level. For the former case, the OLT interacts with the OTN Aggregation Network through its Access Network Controller, to request the OTN connection for the service.

[R17-2] The OLT shall support the coordination of service request with OTN through the Access Network Controller.

For the latter case, the OLT directly sends the service request, to trigger the OTN aggregation network to create OTN connections based on service request.

[R17-3] The OLT shall support triggering the OTN edge node, to create OTN service based connections.

Once the OTN Aggregation Network receives the OTN connection request, the edge node of the OTN needs to perform on-demand OTN connection provisioning for the requested service.

[R17-4] The F5G OTN edge nodes shall support on-demand OTN connection creation, modification and deletion based on the cloud service requirements.

NOTE 2: The edge node of the OTN needs to create the connection, which is triggered by the OLT.

In the case that an OTN connection in the Aggregation Network is used for premium home broadband services from the same OLT to the same Cloud DC. The OLT needs to monitor the real-time traffic of the premium home broadband services from its PON port, and to determine the required bandwidth based on the application traffic model. In the OTN Aggregation Network, the OTN connection bandwidth needs to be adjusted automatically based on the actual application traffic or the number of users using that OTN connection.

[R17-5] The OLT shall support triggering the automatic bandwidth adjustment of the OTN connection.

NOTE 3: How an OLT monitors the service traffic and determines the bandwidth are internal functions of the OLT, which do not need to be standardized, and therefore no standard requirement is needed.

4.15.2.4 Flexible bandwidth adjustments for DC connections

For the home broadband user connectivity to single and multiple clouds scenario, different home broadband users and different cloud application services may require very different bandwidths from tens of Mbps to several Gbps. For example, the required bandwidth of Cloud VR Phase 1 to Phase 4 vary from 80 Mbps to 1,5 Gbps (see Table 1 in clause 4.2.2.1 of the present document).

To improve the resource utilization of the OTN aggregation network, the bandwidth per OTN connection needs to match the bandwidth requirements of the cloud services as close as possible in order to maximize the bandwidth utilization. This requires the OTN technology to support fine granular containers.

[R17-6] Same as [R16-4].

Furthermore, the OTN connection needs to be adjustable based on the increasing or decreasing number of home users from the same OLT and accessing to the same Cloud DC.

[R17-7] Same as [R16-5].

[R17-8] Same as [R23-2].

4.15.2.5 Slicing

For home broadband service connectivity to multiple clouds scenarios, different services have different requirements on network Key Performance Indicators (KPIs).

PON slicing and OTN slicing technologies need to be supported, so that these premium home broadband services can be scheduled and directed to the high-priority slices, to guarantee their KPIs.

[R17-9] The F5G network shall support PON slicing, for premium home broadband services.

NOTE: [R08-9] in the present document introduces the requirement about PON slicing for both mobile and fixed services. [R17-9] is similar to [R08-9] on PON slicing, but focusing only on the slicing for premium home broadband services, which belong to fixed services.

[R17-10] Same as [R16-7].

[R17-11] Same as [R16-8].

4.15.2.6 Service scalability

Emerging applications such as cloud education and cloud gaming have become popular, which requires more and more service connections with different service requirements between OLTs and Cloud DCs. Therefore, the total number of OTN connections used for premium home broadband services will significantly increase, and the scalability of the connection control needs to be considered.

[R17-12] Same as [R16-9].

4.15.2.7 Deterministic protection and restoration

The nodes and the links interconnecting the OTN aggregation network and the Cloud DCs need to have high availability. Dual-homing protection mechanisms could be used for the cloud interconnection, i.e. a Cloud DC cloud interconnect with the dual-homed active and standby Cloud PEs in the OTN aggregation network.

[R17-13] Same as [R16-10].

Similarly, the reliability between the OTN aggregation network and the OLT equipment also needs to be considered. For example, an OLT may be connected to two OTN nodes to protect the home user's services from network failure between the OLT and the OTN.

[R17-14] F5G network protection mechanisms should resolve network failure between the OLT and OTN.

Clause 4.13.2.7 of the present document, describes the protection or restoration mechanisms for the OTN connections against network failures within the carrier network.

[R17-15] Same as [R16-11].

[R17-16] Same as [R16-12].

4.15.3 Current related standard specifications

4.15.3.1 ITU-T

ITU-T has standardized a set of PON related standards, see clause 4.7.3.1 of the present document.

ITU-T has standardized the OTN series of Recommendations, see clause 4.3.3 of the present document.

ITU-T also standardized the management and control architecture of the Optical Transport Network, see clause 5.5.4 of the present document.

4.15.3.2 IETF

IETF has defined the GMPLS architecture for the control plane, and has made protocol extensions to support the control of the OTN. IETF is also developing a set of YANG data models for OTN. See clause 4.14.3.2 of the present document.

4.15.4 Gap Analysis

4.15.4.1 Gap Context

In the present document the gaps refer to existing standards and not to technology in general. Some vendor's products that are not standardized could exist that implement the solutions described in the gaps.

4.15.4.2 Single-point/Multi-point access to multiple Clouds

Similar to the description in clause 4.13.4.1 of the present document, to support P2MP and MP2MP access for home broadband services, the OTN edge nodes need to support the automatic learning of the cloud-side and user-side service address information (e.g. VLAN ID, MAC address and IP address), and support generating the mapping table and mapping the service packets with different service addresses into different OTN connections according to the mapping table.

[Gap17-1] The mechanism to learn the cloud-side and user-side service address information and automatically build the mapping table in the OTN edge nodes, are not currently supported.

[Gap17-2] The mechanism to automatically generate the mapping table from service addresses to OTN connections is not currently supported.

4.15.4.3 Service-driven optical network

A home user may need to connect to a new Cloud DC, or to modify the bandwidth of an existing cloud home broadband service.

The Access Network needs to interact with OTN to trigger the creation or modification of the OTN connection. Such interaction may be in the controller level, or the Network Element level.

In the former case, the OLT sends the service request to its Access Network Controller, and then the Access Network Controller interacts with the Optical Transport Controller (maybe through the E2E Orchestrator), to request the creation or modification of the OTN connection for the service. A YANG data model is needed to convey the service request by the northbound interfaces of both Access Network Controller and the Optical Network Controller.

[Gap17-3] Same as [Gap16-2].

In the latter case, a new mechanisms is needed for the OLT to interact with the OTN edge node to trigger the OTN connection creation, modification or deletion.

[Gap17-4] A standardized interaction process between the OLT and the edge OTN node for the cloud service requests and their SLA requirements is currently not defined.

In addition, when a large number of user's services go online simultaneously during network peak hours, all services need to be created quickly to ensure the users' experience. This requires the OTN signalling protocol to efficiently handle a large number of connection control tasks almost simultaneously.

[Gap17-5] Same as [Gap16-9].

4.15.4.4 Flexible bandwidth

The bandwidth requirement of the home broadband service is possibly lower than 1,25 Gbps (e.g. for Cloud VR see above). Using an existing OTN connection with the bandwidth of 1,25 Gbps is suboptimal due to bandwidth not used and therefore allocated and wasted.

As described in clause 4.13.4.3 of the present document, the current OTN only supports ODUflex connections with a bandwidth capability of N × 1,25 Gbps. There is no OTN standard to support sub-1 Gbps containers, and therefore no support of dynamic lossless bandwidth adjustment below 1,25 Gbps.

[Gap17-6] Same as [Gap23-1].

[Gap17-7] Same as [Gap16-5].

[Gap17-8] Same as [Gap23-2].

4.15.4.5 Slicing

The OLT supports priority slicing and high-priority QoS scheduling for high-quality services. Network slicing is an important feature to meet a diverse set of requirements with optimal resource utilization. AI Engines may be used to steer the traffic to the proper vDBA and/or VxLAN, depending on each service's specific demand for bandwidth, latency and packet jitter, etc.

[Gap 17-9] Same as [Gap08-9].

For the Aggregation Network, the gaps of the OTN network slicing and the management and control of it are the same as that in clause 4.13.4.4 of the present document.

[Gap17-10] None.

[Gap17-11] Same as [Gap16-8].

4.15.4.6 Service scalability

Same as clause 4.13.4.5 of the present document.

[Gap17-12] Same as [Gap16-9].

4.15.4.7 Deterministic protection and restoration

To protect the communication between the OTN Aggregation Network and the Cloud DCs, and between the OLT and the OTN Aggregation Network, OTN dual-homing protection mechanism is needed. In such a case, the source or destination nodes of the OTN working and protection path within the OTN aggregation network will be different, as shown in Figure 13. Similar to [Gap16-10], the current OTN protection mechanisms do not support the case where the source nodes and/or the destination nodes of the working and protection paths are different.

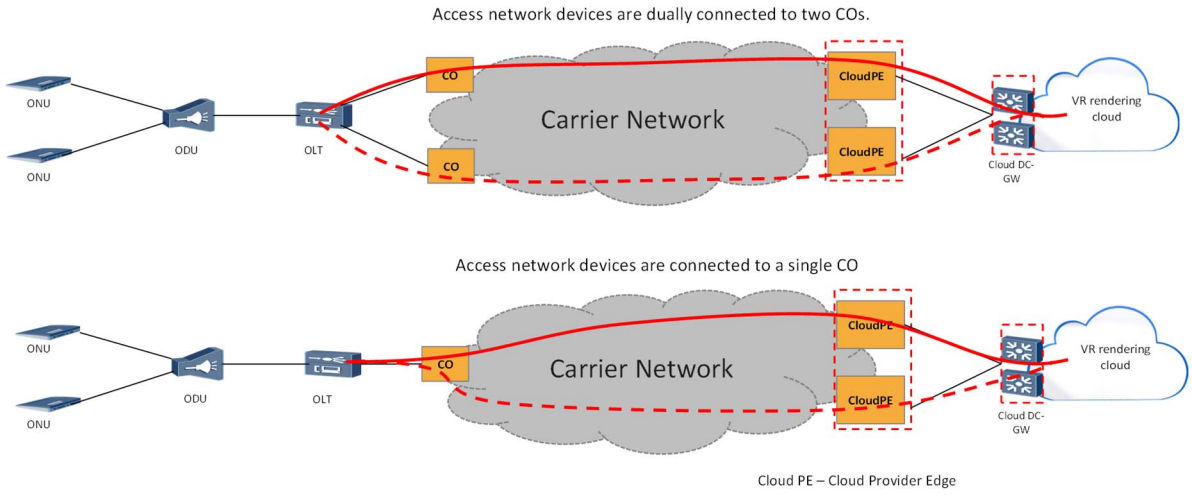


Figure 13: Example of OTN dual-homing protection (Source: Figure 70 of ETSI GR F5G 008 [i.75])

[Gap17-13] Same as [Gap16-10].

[Gap17-14] Current OTN protection mechanisms do not support the source node of the OTN protection path being different from that of the working path.

Within the OTN Aggregation Network, existing OTN 1+1 or 1:1 protection mechanisms are still applicable.

[Gap17-15] None.

For OTN dynamic restoration (also known as dynamic rerouting), existing mechanism may face scalability and performance problems when restoring a large number of connections, see clause 4.13.4.6 of the present document.

[Gap17-16] Same as [Gap16-9].

4.16 Virtual Music

4.16.1 Use Case briefing

Virtual music is a way of sharing and creating music via internet in real time with different parties that are not in the same location. Virtual music can be used in different ways with persons at geographically different locations, e.g. in a virtual orchestra (conductor, musicians, audience), virtual music classes (teacher, student(s)), virtual studio (musicians) and virtual concerts (musicians, audience).

Virtual music is based on client-server or peer-to-peer communication topologies. For a good experience, a reliable low latency audio connection is required. An additional video channel will enhance the experience of creating and sharing music together e.g. for virtual orchestra. In cases such as virtual concert where audience are involved, the synchronization between audio and video is critical.

The virtual music service puts stringent requirements on the network such as guaranteed and deterministic latency (round trip delay < 20 ms), low delay jitter (< 5 ms), and bandwidth (20 Mbps for audio, up to 40 Mbps or 65 Mbps for 4K/8K full view video).

Today, musicians can create music together via cloud-based virtual studio services on the best-effort Internet with no guaranteed performance. F5G networks overcome the limitations that currently make it in practice difficult to interactively create music together through a remote connection via cloud-based virtual music services.

4.16.2 Technology Requirements

4.16.2.1 General introduction

Virtual music imposes strict requirements on latency and jitter, specifically for audio traffic. Musicians can be connected to each other either in a client-server model or in a peer-to-peer model. In case of a client-server model, each performer is connected to a central entity referred to as an audio server. This audio server processes these inputs and sends a common output to each performer. In case of a peer-to-peer model, there is no central entity, but a copy of the music generated is sent from each party to every other party The focus of the present document is on the client server model as it is easier to manage especially when the number of participants increase [i.69] and [i.70], however the requirements are applicable for peer to peer model as well.

The scope of the present document is on the requirements for the audio channel between participants in a virtual music use case. The video between the musicians can be sent across a separate channel which will have to meet the requirements relevant for streaming video, AR or VR which are out of scope for this clause. For instance, the clause on (cloud) VR provides relevant requirements to support high quality user experience. The synchronization between the audio and video is also out of scope of the present document.

4.16.2.2 Ultra-low latency and jitter for increased distance between musicians

To enable a virtual music service, the delays created by the network should not be more than the maximum delay experienced by the musicians due to distance between them in real life. The network needs to provide the lowest possible latency such that a virtual music service may cover larger distances between the musicians. The main parameter for virtual music performance experience is the One-way Source-to-Ear (OOSE) delay.

Typical values for OOSE tolerance are: below 10 ms - 15 ms is ideal, between 10 ms - 15 ms and 20 ms - 25 ms is good, between 25 ms - 60 ms is acceptable (i.e. degradation becomes perceivable) and above 60 ms performance is heavily impaired.

The value of 10 ms - 15 ms is chosen as the lower threshold and 50 ms - 60 ms as the upper threshold for OOSE as this maximum one way delay allows the musicians to play effectively [i.71]. OOSE delay between the musicians is made up of delays caused by various components connecting the musicians. Significant delays in the End-to-End chain are caused by three components:

a) Latency caused by the soundcard and other components in the device connecting music instruments to the network.

b) Latency added by the central server referred to as audio server in client server architecture.

c) Latency caused by network transmission as seen in Figure 14.

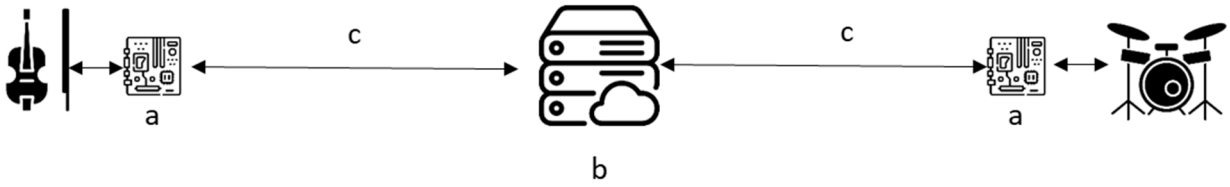


Figure 14: End to end latency caused at various points between the musicians

By using dedicated hardware connecting to the music device, latency at the first component (a) can be reduced to as low as 1 ms - 2 ms [i.72]. Specialized software and sometimes hardware can be used in the central audio server to reduce the latency added in the second component (b) in the order of microseconds.

It is assumed that the components contributing to latency of network transmission (c) are the in-home network technology, the E2E network architecture and the physical/geographical distance between the users.

Home network with Fibre-To-The-Room (FTTR) or usage of ultra-low latency Wi-Fi® can help reduce the latency for the communication between user's device and the ODN/Access Network. Next generation F5G network should be able to reduce latency in the network connecting the musicians to audio server (c).

Assuming that the above-mentioned implementations are used together with uncompressed audio streaming, the budget of the latency and jitter available for the network transmission can be maximized. To support this, sufficient bandwidth is needed, see clause 4.14.2.4.

Table 19: Latency, jitter and bandwidth requirements for different types of user experience

User experience	Excellent	Good	Fair
One-way Source-to-Ear latency	< 15 ms	15 ms - 25 ms	25 ms - 60 ms
One-way E2E network latency	< 13 ms	13 ms - 23 ms	23 ms - 58 ms
E2E time jitter	< 2 ms	< 5 ms	< 10 ms
Bandwidth	20 Mbps	20 Mbps	20 Mbps

[R18-1] The F5G network should support constant/deterministic low latency.

[R18-2] The F5G network shall meet the latency requirements in Table 19 between any pair of musicians or participants.

NOTE: The ability of the network to meet these latency and time jitter requirements depends on the latency and time jitter introduced in active network components and the latency of the end-to-end data transmission over optical links (bound by speed of light in optical fibres which is approximately 200 km/ms). The end-to-end latency depends on the network topology and the total fibre length, related to the physical distance between endpoints and the central virtual music server.

In case of peer to peer model, these latency requirements are for a direct connection between the musicians, in case of client server model, the End-to-End connection involves a central server along the path between two musicians.

4.16.2.3 Dynamic set up of audio channel

Virtual music is based on ad-hoc sessions for sharing and creating music, meaning that participants may start, join or leave the session dynamically. When a virtual music session is started via a shared channel or an independent channel, an operational flow of actions for enabling the ad-hoc virtual music session is required. Once the virtual music session is setup, the network channel should meet the network requirement of the service. After the virtual music session ends, the resources of the network channel can be released.

For a cloud-based virtual music session the end-to-end network consists of multiple parts i.e. home networks of musicians, access networks, aggregation network and data centre network.

[R18-3] The F5G network shall support dynamic set up and release of the high-quality end-to-end network channel for virtual music audio sessions between multiple musicians.

4.16.2.4 Guaranteed bandwidth

To minimize the latency induced by buffers in the network components, the network should be able to provide guaranteed bandwidth of 20 Mbps for the audio channel [3]. Audio compression may be used to reduce the required bandwidth but this introduces an additional latency (up to 10 ms) and is therefore not considered in this analysis.

[R18-4] The F5G network should guarantee a bandwidth of 20 Mbps for the audio channel.

NOTE: The bandwidth requirement for an accompanying video channel are left out of scope as stated in the introduction clause.

4.16.2.5 Edge computing capability

In case of a client-server model, the audio server is placed on the edge of the network to minimize latency. Note that in case of the peer to peer model, an audio server is not required. The selection of the geographical location of the audio server for the client server model plays an important role in reduction or optimization of the overall end-to-end latency between the musicians. All musicians involved in a virtual music session have to setup a data connection to the central server to join a session and to exchange audio and video streams. The individual audio streams may be merged in a single stream by the central server or can be shared directly between musicians. The virtual music service may support the dynamic selection of a server in the edge i.e. with minimal (average) latency and as close as possible to the musicians involved in a session. The selection of the location of the edge server depends on the relative latency that is assumed to be mainly related to location of the clients (but it could also relate to specific network implementation). It thus requires a flexible or on-demand allocation (in terms of location) to cater to the dynamic needs of the musicians. Such a feature will benefit the musicians greatly. Optimal allocation mechanisms for the placement of the edge server specified in literature such as in [i.73] can help achieve a low End-to-End latency between the musicians.

At present, existing audio servers are fixed across a set of locations, per region (e.g. Europe, North America). Choosing an audio server from a fixed set of 15-20 audio servers located globally will not always provide optimum placement of musicians and the selected audio server.

[R18-5] The F5G network should support dynamic (re)allocation of a central server ensuring optimized End-to-End latency.

In order to have an efficient audio server that achieves lowest possible latency, specialized software needs to be part of the edge server.

[R18-6] The edge server should support 3rd party applications.

4.16.3 Current related standard specifications

4.16.3.1 General introduction

The current standards for edge computing are considered in clause 4.16.3. For the current related standard specifications of low latency communication, refer to clause 5.

4.16.3.2 ETSI

ETSI GS MEC 003 [i.133] specifies the standards for Multi-access Edge Computing (MEC). It provides details about the overall architecture along with various functional elements. The host that provides the edge computing capability is referred to as MEC host. MEC applications are virtual instances on the MEC host which offer MEC related services. The MEC orchestrator is responsible for MEC system level management.

4.16.3.3 3GPP

3GPP TS 23.548 [i.140] contains the specifications for the enhancements to 5G system to support of edge computing. It contains the procedures supporting relocation of edge server. Using such procedures, user plane path can be re-configured to obtain optimized configuration. The relocation is triggered by AF (Application Function) of F5G based on various triggers, for instance when the maximum allowed user plane latency requirement is exceeded. The SMF will then relocate the edge server to a new UPF that matches the allowed latency requirement. The UE (user equipment) will then have to perform re-discovery procedure to the new edge server.

4.16.4 Gap analysis

4.16.4.1 Gap Context

In the present document the gaps refer to existing standards and not to technology in general. Some vendor's products that are not standardized could exist that implement the solutions described in the gaps.

4.16.4.2 Ultra-low latency and jitter for increased distance between musicians

This use case assumes OTN based aggregation network is used. OTN with hard isolation will result in deterministic latency.

[Gap18-1] None.

Latency measured in GPON/XGS-PON implementations in upstream or downstream will cause a maximum additional latency of < 1 ms. So, the required latency requirement can be achieved, for instance using GPON FTTH deployments.

[Gap18-2] None.

4.16.4.3 Dynamic set up of audio channel

The set up and release of the audio channel for virtual music shows similarities to the channel setup and release for cloud VR in clause 4.2. The following gap is therefore derived from [Gap 01-13]

[Gap18-3] Currently each F5G network segment does not support the coordinated management mechanism to dynamically set up and release of a high-quality end-to-end network channel for audio.

4.16.4.4 Guaranteed bandwidth

With existing standards, it is possible to offer the guaranteed bandwidth of 20 Mbps.

[Gap18-4] None.

4.16.4.5 Edge computing capability

Using the current standards mentioned by ETSI and 3GPP, it is possible to re-locate the edge server.

A third party can send requests to a MEC orchestrator as specified in ETSI GS MEC 003 [i.133] to specify the location where the third-party application needs to be active. The edge server can be relocated based on the procedures specified in 3GPP TS 23.548 [i.140] based on the user plane latency requirement. When the latency between a UE and the UPF exceeds this requirement, the network component (AF) triggers the relocation of the UPF.

However, the optimal geographic placement of the edge server based on dynamic locations of multiple virtual music participants is missing in the current standards.

[Gap18-5] On demand allocation of a central server based on an overall End-to-End latency optimization is currently not standardized.

The MEC applications run as virtual machines with the help of virtualization provided by MEC host as specified in ETSI GS MEC 003 [i.133]. The third-party application that is necessary to run an audio server can be an MEC application.

[Gap18-6] None.

4.17 Next Generation Digital Twin

4.17.1 Use Case Briefing

A digital twin refers to a digital replica of physical assets, processes and/or systems. Digital twins integrate artificial intelligence, machine learning, and data analytics to create living digital simulation models that are able to learn and update as well as represent and predict the current and future conditions of physical counterparts. Digital twins that are truly *decisive*, i.e. that have the autonomy to make decisions without interaction of the operator, are called *next generation digital twins*. These digital twins are currently on the horizon with challenges around resiliency, autonomy, and privacy. In the *next generation digital twin use case*, a set of digital twins could work together, with each digital twin having a well-defined objective on its own.

Digital twin technology has applications in many different domains, such as the manufacturing or process industry, intelligent transport systems, power grids and smart cities. The underlying F5G network infrastructure - with a mix of optical network in LAN, access, aggregation and core networks - shall support high-performance data exchange for digital twins. In this use case, the focus is on digital twin technology for industrial automation (also referred to as Factory of the Future (FoF) or Industry 4.0). For Next Generation Digital Twin the following generic requirements for the F5G network infrastructure are applicable:

- One or more locations in the network where a distributed cloud (on-premises, edge, central) is deployed that is capable of supporting multiple interconnected digital twins in terms of compute, storage and networking.
- A highly available, (near-) real-time network between the real-world object(s) and the location(s) in a distributed cloud architecture where the digital twins are realized.
- Support of multiple digital twins over the same network.

4.17.2 Technology Requirements

4.17.2.1 Next generation digital twin technology for industrial automation

The main motivation behind the usage of next generation digital twin technology in industrial automation is to improve the performance of assets, systems or processes. The technology is based on digital replica (with autonomous or decisive systems) of physical counterparts in production processes. Digital twins rely on data exchange for control and monitoring e.g. real-time control of robots in automated or autonomous manufacturing systems supported by video streams and sensor data for monitoring.

Industrial automation solutions are demanding for the convergence of information technology and operation technology (e.g. manufacturing robots) into a single infrastructure for enabling digital twin applications and augmented reality, centralization of controllers and virtualization in enterprise data centres.

A next generation digital twin is expected to be deployed on a distributed cloud computing infrastructure to collect, process and store information for autonomous operations, and this distributed cloud is interconnected via a high-performance reliable F5G network infrastructure.

Part of the requirements to support data exchange for industrial automation over an F5G network are also covered in related use cases (ETSI GR F5G 008 [i.75]), i.e. PON for Industrial Manufacturing (clause 6.6) and Cloud-based visual inspection for automatic quality assessment in production (clause 7.7).

For industrial automation different traffic types need to be supported [i.74] and examples of traffic types and service requirements are shown in Table 20. These are based on ETSI TS 122 104 [i.159] and IEC/IEEE 60802 [i.76].

Table 20: Example of different traffic types and service requirements in industrial automation

Traffic type	Periodic/sporadic	Typical period	Typical data size (bytes)	Criticality
Isochronous	Periodic	100 µs - 2 ms	Fixed: 30 - 100	High
Cyclic	Periodic	500 µs - 20 ms	Fixed: 50 - 1 000	High
Events	Sporadic	10 ms - 50 ms	Variable: 100 - 200	High
Network control	Periodic	50 ms - 1 s	Variable: 50 - 500	High
Audio/video	Periodic	Frame rate	Variable: 1 000 - 1 500	Low

4.17.2.2 Interworking with Ethernet/TSN networks

Today, industrial Ethernet and/or Time Sensitive Networks (TSN) are widely used in industrial automation. An example of an industrial PON network to connect production locations to a data centre is shown in Figure 15. The industrial PON network supports connecting industrial automation applications, via TSN-networks to the ONU or via the industrial (optical) network to the ONU.

NOTE: The assumption for the scenario is that it shows only local compute infrastructure. Other scenarios are for further study.

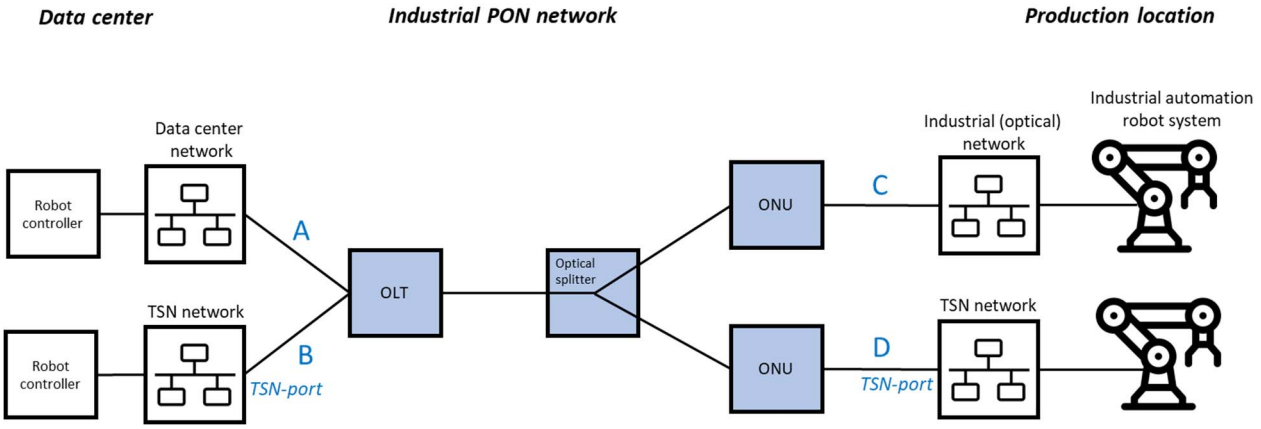


Figure 15: Industrial- PON network, with and without integration with TSN networks

For industrial automation different traffic types need to be supported, as described in Table 20. These traffic types are supported on Ethernet-based networks via additional TSN features in IEEE 802.1 (e.g. strict priority via IEEE 802.1Q [i.56], redundancy via IEEE 802.1CB [i.95], time synchronization via IEEE 802.1AS [i.34], scheduled traffic via IEEE 802.1Qbv [i.160], frame pre-emption via IEEE 802.1Qbu [i.161], per-Stream Filtering and Policing via IEEE 802.1Qci [i.162] and TSN configuration via IEEE 802.1Qcc [i.96]).

PON systems can provide similar features as TSN without supporting native TSN. PON could integrate TSN switching functionality, interface with TSN switches and even replace parts of the TSN network to further reduce cost and complexity. In Figure 15 two options are illustrated: Industrial PON offering TSN features without integration with TSN networks (path A-C) and with integration with TSN networks (path B-D).

However, if PON is used as a part of a deterministic network where TSN is used, interworking functions need to be supported between PON networks and TSN networks.

[R19-1] The F5G network should support connectivity between TSN ports on-premises and in data centre(s) in such a way that TSN functionality is preserved.

In TSN networks, latency information from individual ports of TSN switches connected through an F5G network is needed, e.g. latency information of the network connection from TSN-port on interface B to TSN-port on interface D in Figure 15. An interface between the TSN network (control plane) and the F5G network can provide this information via a standardized interface.

NOTE: The standardized interface is for further study.

[R19-2] The F5G network shall provide latency information of the F5G connection between TSN switches connected through an F5G network to the TSN control plane.

To support TSN features between TSN switches interconnected via an F5G network, a gateway or translator function is required between the TSN network and the F5G network (e.g. on interfaces B and D in Figure 15). This function can interpret TSN traffic in optical (terminating) equipment in F5G networks, to enable QoS and timing information being passed on to the F5G network, which the F5G network should then use to support TSN features.

[R19-3] The F5G network shall support a gateway function between the F5G network and TSN network for interpreting TSN traffic in optical (terminating) equipment in F5G networks.

[R19-4] The F5G network shall support Ethernet and TSN traffic stream filtering and policing.

[R19-5] The F5G network shall support the mapping of Ethernet and TSN traffic streams to F5G-specific QoS flows.

4.17.2.3 Deterministic network performance and mix of traffic

In the next generation digital twin use case a guaranteed level of service quality is desired for prioritized traffic with most stringent timing requirements for deterministic network traffic.

A QoS flow can be established for IP or Ethernet flows in such a way that each packet of a given flow is forwarded across the F5G network in the same way (e.g. for scheduling and admission control). These flows can be associated with different priority levels, packet delay budgets, and tolerable packet error rates. These priority levels can be used to prevent that lower priority traffic can have a performance degradation impact on the hard-real-time traffic.

To meet the timing requirements, the F5G network shall support time-aware scheduling with configurable absolute cyclic time boundaries with latency down to 100 μs over 5 hops, and maximum transmission period of 0,5 ms for prioritized traffic flows in both directions.

[R19-6] The F5G network shall support a mix of traffic, both deterministic latency traffic following a time-aware schedule and lower priority traffic.

[R19-7] The F5G network shall support time-aware scheduling with guaranteed maximum latency of 100 μs over 5 hops.

4.17.2.4 Stronger network resilience

Network reliability via redundant transmissions between customer premises and data centres is a top requirement for the next generation digital twin technology in the industry. PON can provide different grades of network resilience, implemented with different protection schemes (see Recommendation ITU-T G.Sup51 [i.30]). Additionally, some new PON protection schemes have been developed for the industrial scenarios. For example, the dual-OLT protection, which uses two hot stand-by OLTs with 2:N optical splitters and two optical modules on the ONU, to provide a full backup connection.

[R19-8] The F5G PON access network shall support network protection mechanisms.

4.17.2.5 Time synchronization

Accurate time synchronization of network elements is crucial to meet the stringent requirements on tolerance of latency (none for isochronous) for closed-loop control in a distributed architecture for industrial automation. In case TSN networks are supported the profile for use of IEEE 1588 [i.79] for time synchronization over a virtual bridged local area network, as defined by IEEE 802.1AS [i.34], should be supported.

[R19-9] The F5G network shall support TSN element clock synchronization as defined in IEEE 802.1AS [i.34].

[R19-10] The F5G network shall support clock synchronization of network elements to a main clock with an accuracy better than 1μs.

To support time critical services within the F5G network, timing redundancy is needed, to enable the use of an F5G network for time critical services in collaboration with or as a backup to other timing solution such as loss or degradation of GNSS reference timing.

[R19-11] The F5G network shall support timing redundancy.

4.17.3 Current related standard specifications

4.17.3.1 ITU-T

4.17.3.1.1 GPON

ITU-T defined the xPON series in recommendations, ITU-T G.984.x [i.27] and G.987.x [i.28] on XG(S)-PON, where XG(S)-PON and above is in scope of F5G.

ITU-T protection schemes of a PON system are defined in Recommendation ITU-T G.Sup51 [i.30].

ITU-T Study Group 15 Question 13 studies network synchronization and time reference distribution performance (this includes the distribution of both precision time and frequency). The requirements are based on new network architectures and applications e.g. as related to the IoT, IMT2020/5G, IMT-2020/5G evolution, industrial automation and new emerging applications that may require accurate timing such as support for enhanced security solutions, SDN/NFV, AI/ML, or Quantum Key Distribution (QKD).

4.17.3.1.2 OTN

ITU-T OTN standards are:

- Recommendation ITU-T G.709 [i.67].
- Recommendation ITU-T G.709.1 [i.108].
- Recommendation ITU-T G.709.2 [i.109].
- Recommendation ITU-T G.709.3 [i.110].
- Recommendation ITU-T G.709.4 [i.111].

4.17.3.2 IEEE

4.17.3.2.1 Time Sensitive Networks

IEEE 802.1 Time-Sensitive Networking (TSN) task group - formed in November 2012 by renaming the existing Audio Video Bridging Task Group - defines a series of standards of synchronization, latency, reliability and resource management of the TSN system, e.g.:

- Extensions to IEEE 802.1Q [i.56] for the TSN bridge model with bridge ID, traffic forwarding information, traffic class related information, per-stream filtering and policing information (Qci) and bridge enhancements for support of scheduled traffic (Qbv) and stream reservation protocol (Qcc). IEEE 802.1Qca [i.105] Path Control and Reservation (PCR) specifies extensions to the Intermediate Station to Intermediate Station (IS-IS) protocol to configure multiple paths in bridged networks. IEEE 802.1Qca [i.105] integrates control protocols to manage multiple topologies, configure an explicit forwarding path (a predefined path for each stream), reserve bandwidth, provides data protection and redundancy, and distribute flow synchronization and flow control messages. These are derived from Equal Cost Tree (ECT), Multiple Spanning Tree Instance (MSTI) and Internal Spanning Tree (IST), and Explicit Tree (ET) protocols.
- IEEE 802.1AS [i.34] for TSN time synchronization.
- IEEE 802.1CB [i.95] redundancy for highly reliable communication (Frame Replication and Elimination for Reliability (FRER). IEEE 802.1CB [i.95] Frame Replication and Elimination for Reliability (FRER) sends duplicate copies of each frame over multiple disjoint paths, to provide proactive seamless redundancy for control applications that cannot tolerate packet losses. FRER requires centralized configuration management and needs to be used with IEEE 802.1Qcc [i.96] and IEEE 802.1Qca [i.105]. Industrial fault-tolerance High-availability Seamless Redundancy (HSR) protocol and Parallel Redundancy Protocol (PRP) for Ethernet specified in IEC 62439-3 [i.106] are supported.

4.17.3.2.2 Precise Timing Protocol

IEEE 1588-2008 [i.40] (IEEE 1588v2) is also known as Precise Timing Protocol (PTP) version 2.
IEEE 1588-2019 [i.79] (1588v3) was published in November 2019 and includes backward-compatible improvements to the 2008 publication. IEEE 1588-2009 include a profile concept defining PTP operating parameters and options. Several profiles have been defined for applications including audio-visual applications.

IEEE 802.1AS-2011 [i.34] is part of the IEEE Audio Video Bridging (AVB) group of standards, further extended by the IEEE 802.1 Time-Sensitive Networking (TSN) Task Group. It specifies a profile for use of IEEE 1588-2008 [i.40] for time synchronization over a virtual bridged local area network (as defined by IEEE 802.1Q [i.56]). In particular, IEEE 802.1AS [i.34] defines how IEEE 802.3 [i.163] (Ethernet), IEEE 802.11 [i.164] (Wi-Fi), and MoCA can all be parts of the same PTP timing domain.

IEEE 1588-2019 [i.79] defines the Precision Clock Protocol for Networked Measurement and Control Systems.

4.17.3.3 3GPP

4.17.3.3.1 Industrial Automation: 5G and Industry 4.0

In ETSI TS 122 104 [i.159] (Service requirements for cyber-physical control applications in vertical domains) requirements are defined of use cases (30+) in various vertical domains (e.g. Factories of the Future, electric power distribution and smart grid, connected hospitals, positioning). The requirements cover:

a) network performance (with multiple traffic types, clock synchronization, timing resilience, positioning performance);

b) support for Ethernet applications; and

c) support for direct device-to-device connectivity.

4.17.3.3.2 5G and Time Sensitive Communications

The 'Vertical_LAN' work item, in 3GPP Release-16, introduces the support for Time Sensitive Communications by seamlessly integrating the 5G system as a bridge to IEEE TSN. 5G Time Sensitive Communication is a service that supports deterministic and/or isochronous communication with high reliability and availability and is included in the 5G architecture (see 3GPP TS 23.501 [i.104]). It provides packet transport with Quality of Service (QoS) characteristics such as bounded latency and reliability, where end systems and relay/transmit nodes can be strictly synchronized. 3GPP supports TSN time synchronization, by considering the entire end-to-end 5G system as an IEEE 802.1AS [i.34] "time-aware system". Only the TSN Translators (TTs) at the edges of the 5G system need to support the IEEE 802.1AS operations. UE, gNB, UPF, NW-TT and DS-TTs are synchronized with the 5G GM (i.e. the 5G internal system clock) which keeps these network elements synchronized.

In ETSI TS 124 519 [i.102] the Time-Sensitive Networking (TSN) Application Function (AF) to Device-Side TSN Translator (DS-TT) and Network-Side TSN Translator (NW-TT) protocol aspects are specified.

ETSI TS 124 535 [i.103] defines (g)PTP message delivery in different modes of operation:

a) a time-aware system, for which the 5G network needs to support implementation of (g)PTP requirements (see IEEE 802.1AS [i.34]);

b) a boundary clock, for which the 5G network needs to support implementation of PTP requirements (see IEEE 1588 [i.79]);

c) a peer-to-peer transparent clock, for which the 5G network needs to support implementation of PTP requirements (see IEEE 1588 [i.79]); and

d) an end-to-end transparent clock, for which the 5G network needs to support implementation of PTP requirements (see IEEE 1588 [i.79]). Within a 5G network, a (g)PTP message is delivered over the user plane.

In ETSI TS 122 261 [i.165] (clauses 6.36 and 7.8) timing resilience requirements of a 5G system are defined for TSN.

4.17.3.4 IEC

IEC/IEEE 60802 [i.76] covers a Time-Sensitive Networking Profile for Industrial Automation.

4.17.3.5 5G-ACIA

The 5G Alliance for Connected Industries and Automation (5G ACIA) has released several white papers on 5G technology for industrial automation e.g. [i.74].

These white papers give an overview of use cases, requirements and solutions with 5G mobile networks to support connected industries and automation. This information is also valuable to support these use cases and service requirements over optical F5G networks in LAN, access, aggregation and core.

4.17.4 Gap analysis

4.17.4.1 Gap Context

In the present document the gaps refer to existing standards and not to technology in general. Some vendor's products that are not standardized could exist that implement the solutions described in the gaps.

4.17.4.2 Interworking with Ethernet/TSN networks

To support high-performance Ethernet/TSN-based applications over optical LAN, access, aggregation and core networks interworking is required to support Ethernet/TSN services end-to-end over an optical network with a mix of technologies such as PON and OTN. Ethernet/TSN switches can be interconnected over PON and/or OTN networks.

[Gap19-1] None.

Latency information can be exchanged in a time-aware network by using PTP (IEEE 1588-2019) [i.79] or gPTP (IEEE 802.1AS [i.34]). Recommendation ITU-T G.987.1 [i.28] (Appendixes IV and V) describes how IEEE 1588 master and slave functionality between OLT and ONU is distributed and forwarded to external connected devices, i.e. via network synchronization to OLT and UNI synchronization from ONU. However, these appendices are not an integral part of Recommendation ITU-T G.987.1 [i.28] and do not include support of gPTP (IEEE 802.1AS [i.34]) and IEEE 1588-2019 [i.79].

[Gap19-2] Support of gPTP and IEEE 1588-2019 [i.79] in PON to exchange latency information to Ethernet/TSN switches interconnected via PON is missing.

[Gap19-3] Same as [Gap04-17].

[Gap19-4] Same as [Gap04-17].

[Gap19-5] A TSN gateway or translator function on OLT or ONU may be needed to support specific TSN features e.g. for time synchronization via IEEE 802.1AS [i.34]/gPTP or topology discovery of logical ports/bridges (IEEE 802.1Qcc [i.96]).

4.17.4.3 Deterministic network performance and mix of traffic

Service differentiation via QoS is supported over PON and OTN optical networks, see other use cases. PON and OTN are TDM-based and do support deterministic delay independent of the network load.

[Gap19-6] None.

An Ethernet/TSN network isolates time-critical flows, and maintains their cycles, with constant latency and low jitter. PON networks shall support strict priority for a low-latency MAC layer and jitter compensation options for scheduled time-bound traffic e.g. as described in [i.2].

The support in PON network to isolate time-critical Ethernet/TSN flows and maintain their cycles, with constant latency and low jitter, is limited. Enhancements may be needed, including time-aware scheduling per flow with configurable time boundaries with latency down to 100 μs over 5 hops.

[Gap19-7] The F5G PON access network support for time-aware scheduling is not sufficient to support this use case.

4.17.4.4 Stronger network resilience

Recommendation ITU-T G.984.1 [i.97] specification outlines several topologies for achieving redundancy; these have been named Type A, Type B, Type C and Type D. There are quite a few PON protection architectures defined in PON standards both by ITU-T and IEEE based on these 4 types. The difference between these different protection schemes depends on what is being protected: feeder fibre; feeder and drop fibres; OLT equipment; OLT and ONU equipment; or a mix and match between them. Recommendation ITU-T G.Sup51 [i.30] provides considerations on passive optical network protection. Compared with transport networks, access networks are very cost sensitive because only a few subscribers need to share all the costs associated with the protection. Thus, presently there is a lack of deployment of PON protection systems, largely because of cost considerations.

IEEE TSN task group has specified two extensions to IEEE 802.1Q [i.56] for fault tolerance, IEEE 802.1Qca [i.105] Path Control and Reservation (PCR) and IEEE 802.1CB [i.95] Frame Replication and Elimination for Reliability (FRER). Both IEEE solutions can be used on top of the protection schemes of PON.

[Gap19-8] None.

4.17.4.5 Time synchronization

TSN requires a common network time base to operate each switch according to a global schedule. Synchronization is achieved through the IEEE 802.1AS generalized Precision Time Protocol (PTP) profile, which requires any two time-aware devices separated by 7 or fewer hops to be synchronized within 1 µs peak-to-peak accuracy. IEEE 802.1AS [i.34] (clause 7.5) describes the differences between PTP (IEEE 1588-2019 [i.79]) and gPTP (IEEE 802.1AS [i.34]) are explained.

PON access networks support time synchronization via several use cases (Recommendation ITU-T G.987.1 [i.28], Annex 3) based on IEEE 1588v3 [i.79] PTP and/or SyncE. For end-to-end time synchronization in a mix of optical networks, boundary clocks may be used on optical nodes at the boundaries of a (transport) network. The gPTP Relay Instances for time synchronization of TSN networks may be used in PON or OTN network elements.

[Gap19-9] An update of Recommendation ITU-T G.987.1 [i.28] is needed to support gPTP (IEEE 802.1AS [i.34]) and IEEE 1588-2019 [i.79] in ONU and OLT in PON networks.

GNSS can provide a time signal accurate to better than 100 ns. When using network-based timing in a time-aware network with (generalized) Precision Time Protocol (gPTP) an accuracy to just several hundred of nanoseconds can be achieved using and the operational complexity can be significantly simplified compared to GNSS. Timing accuracy can be improved by using advanced transfer techniques, boundary clocks and limiting the number of optical nodes in an end-to-end network. PON networks support clock synchronization better than 1µs. The ongoing work of ITU-T Study Group 15 Question 13 addresses improvements on accuracy of clock synchronization over PON and OTN networks.

[Gap19-10] None.

Timing resilience is included in IEEE 802.1AS [i.34] and IEEE 1588-2019 [i.79]. If these standards are supported, no additional specifications are needed.

[Gap19-11] None.

4.18 Media transport

4.18.1 Use case briefing

Live broadcast of large-scale events is evolving from on-site production to remote and Cloud-based production. The live video is captured in real-time and sent to the International Broadcasting Centre (IBC) or to the remote studio production centre for further editing and processing. The advantages are obvious, with low cost, high efficiency and better quality video production. The rapid development of global UHD (Ultra-High Definition) video industry provides the end users with an upgraded audio-visual experience. The exponential growth of live video data delivery puts strict requirements on the media transport in terms of bandwidth, latency, packet loss, driving the media transport network evolution in both architecture and technology.

4.18.2 Technical requirements

4.18.2.1 General introduction

The live video media generation normally supports multiple format, including SD (Standard Definition, e.g. 480P) HD (High Definition, e.g. 1080P) and UHD (Ultra-High Definition, e.g. 4K and 8K). The real-time transportation of these data formats requires the transport network to provide enough network capability, such as guaranteed bandwidth, low latency with low packet jitter, low packet loss rate, service security and high reliability to ensure efficiency and quality delivery of the live video content. Full fibre connection is the key characteristic of F5G. OTN is one of the technologies for transport network in the E2E F5G network. Compared to other F5G transport technologies, like Ethernet/IP network, OTN has several advantages, including end-to-end transparent connection, increased spectral efficiency, deterministic, hard isolation, and lower packet loss and large-capacity transmission for long-haul. The ideal technology for media transport should be OTN. Thus, this clause mainly focuses on OTN.

4.18.2.2 Flexible media interface

There are mainly three types of live video signals. The first live video signal is uncompressed raw video data. This live video signal maintains the complete fidelity for remote production, flexible post-production, and multi-party production. The typical data interface formats is SDI. The second live video signal is shallow compression to reduce the cost of transmission and storage. The typical interface is an Ethernet port. The third live video signal is deep compression for direct video transport. The typical data interface data formats are DVB-ASI and Ethernet port. The optical transport network should be flexible and support the different applications interface.

[R20-1] OTN for media transport shall support the interfaces (SD-SDI, HD-SDI, 3G-SDI, 12G-SDI) to transport the uncompressed raw video signal.

[R20-2] OTN for media transport shall support the interfaces (GE, 10GE, 25GE) to transport the shallow compressed video signal.

[R20-3] OTN for media transport shall support the interfaces (DVB-ASI, GE) to transport the deeply compressed video signal.

4.18.2.3 Guaranteed high bandwidth

E2E guaranteed bandwidth is an important feature for media transport. The architecture of OTN includes wavelength add/drop multiplexing/demultiplexing implemented at Layer 0 (L0), while ODUk/OSU service grooming is implemented at Layer 1 (L1). Therefore, OTN can enable different types of network slicing techniques for real-time transmission of various video signal to avoid contention with other services.

[R20-4] OTN for media transport shall support L0 network slicing by applying wavelength-based hard isolation technologies to provide > 100 Gbps data rate.

[R20-5] OTN for media transport shall support L1 network slicing by using ODUk/OSU-based hard isolation technologies to enable flexible data rate up to 100 Gbps.

4.18.2.4 Deterministic and low latency

UHD video including 4K/8K broadcast TV (BTV) and video on demand (VOD) require deterministic and low latency. According to the processing site in OSI model, if the process takes place in lower layer, the smaller the processing latency will be. OTN mainly focus on L0 and L1 layer, the processing latency of L0 NEs is in order of nanoseconds (ns) and for L1 NEs is in Microseconds (μs) level (see Table 21). The traditional Ethernet switching works on L2 or L3, leading to 1~10 Milliseconds (ms) latency. Moreover, another advantage of OTN is the independency of different network payload, thus OTN is one of the mainstream communication technologies for achieving low latency transmission, close to the physical limit of transmission and committing deterministic latency.

Table 21: The latency comparison of OSI layer network model

OSI Layer	Network Element	Latency
L0	Photonic component (MUX/DEMUX, ROADM, Amplifier and etc.)	ns ~ 100 ns level
L0		5 μs/km
L1	OTN	10 μs ~ 100 μs level, independent to network payload
L2	L2 Packet Switch	ms ~ 10 ms level, related to network payload
L3	Router, L3 Packet Switch	ms ~ 10 ms level, related to network payload

[R20-6] OTN for media network transport shall support deterministic and low transmission latency with load-independent, satisfying the particular video signal type requirements.

4.18.2.5 Ultra-low packet loss

The traditional Ethernet/IP networks for video transport includes media gateway, L2/L3 data switching, etc. The video data are processed by multiple equipment nodes, introducing the probability of additional packet loss. OTN can provide E2E ODUk/OSU hard pipe from the video capturing events to the IBC/Production Centre with one-hop transmission. With the advancement of Forward Error correction (FEC) with high symbol error correction capability, the packet loss rate in OTN will be much lower than that of the traditional bearing network.

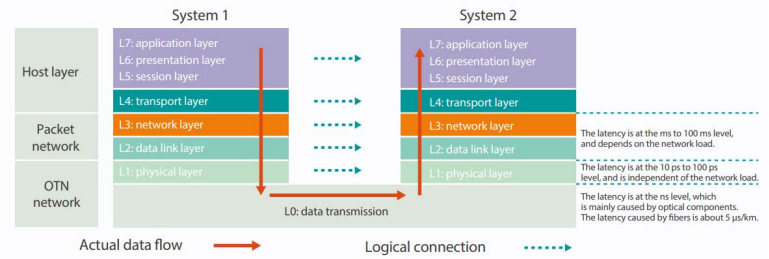


Figure 16: Example of video transmission flow in OTN

[R20-7] OTN for media transport shall support < 10^{-5} packet loss rate for 4K video transmission.

[R20-8] OTN for media transport shall support < 10^{-6} packet loss rate for 8K video transmission.

4.18.2.6 Service Security

Protecting the security of live video streaming is an important aspect to preserve the business value of the content and not allow interception by others. OTN can applies popular encryption mechanisms, e.g. Advanced Encryption Standard - Galois Counter Mode (AES-GCM), to the live video data for media service transmission, to reduce the risk of intruder attacks.

[R20-9] OTN for media transport shall support ODU/OTU level encryption.

4.18.2.7 High Reliability

Link failure will cause disruption of live video communication, affecting the continuity of video service. OTN should support network protection capability to counter act fibre failure, such as fibre cut. In some sensitive and important scenarios, there may be higher requirements for the protection with multiple fibre failure support over multiple links.

[R20-10] OTN for media transport shall provide service-level 1+1/1:1 protection in dual-path scenarios.

[R20-11] OTN for media transport shall support protection switching time < 50 ms.

[R20-12] OTN for media transport shall support fast multi-route protection and restoration capabilities based on ASON.

4.18.3 Current related standard specifications

4.18.3.1 Society of Motion Picture and Television Engineers (SMPTE)

SMPTE is an international standard organization, defining the SDI interface, see Table 22.

Table 22: SDI interfaces and their relevant standards

No.	Service Type	Service Rate	Standard
1	SD-SDI	270 Mbits/s	SMPTE 259M [i.166]
2	HD-SDI	1,49 Gbits/s	SMPTE 292M [i.167]
3	3G-SDI	2,97 Gbits/s	SMPTE 424M [i.168]
4	12G-SDI	12 Gbits/s	SMPTE ST-2082 [i.169]

4.18.3.2 ITU-T

ITU-T SG15 has worked on a series of OTN standards over the past decade. Many of them have been well adopted by the industry and widely deployed, see Table 23.

Table 23: OTN recommendation in ITU-T SG15

Standard	Description
G.709 [i.67]	Interfaces for the Optical Transport Network (OTN)
G.872 [i.170]	Architecture of optical transport networks
G.798 [i.171]	Characteristics of optical transport network hierarchy equipment functional blocks
G.873.1 [i.81]	Optical Transport Network (OTN): Linear protection
G.8080 [i.172]	Architecture for the automatically switched optical network
G.709.1 [i.108]	Flexible OTN short-reach interfaces

4.18.4 Gap analysis

4.18.4.1 Gap Context

In the present document the gaps refer to existing standards and not to technology in general. Some vendor's products that are not standardized could exist that implement the solutions described in the gaps.

4.18.4.2 General

OTN is one of the ideal networks for media transport. Fibre link provides high and stable throughput. One-hop connection low provides latency.

4.18.4.3 Flexible media interface

For the transport of uncompressed raw video signal and deeply compressed video signal from camera and codec which are electrical signal, then O/E conversion is needed for converting electrical signal to optical signal.

[Gap20-1] None.

[Gap20-2] None.

[Gap20-3] None.

4.18.4.4 Guaranteed Bandwidth

Optical Service Unit (OSU), a new path layer network in OTN is in development to support sub 1G services transmission. OSU is very flexible in adapting to the requirements of different live video service.

[Gap20-4] None.

[Gap20-5] The standardization of L1 network slice OSU (Optical Service Unit) in not currently defined.

4.18.4.5 Deterministic and low latency

[Gap20-6] None.

4.18.4.6 Ultra-low packet loss

[Gap20-7] None.

[Gap20-8] None.

4.18.4.7 Service security

Recommendation ITU-T G.709.1 [i.108] specifies the encryption and authentication of the Flexible Optical Transport Network (FlexO) frame structures on a FlexO interface. Currently there is no standard specifying the ODU/OTU level encryption.

[Gap20-9] The ODU/OTU level encryption is not currently standardized.

4.18.4.8 High reliability

[Gap20-10] None.

[Gap20-11] None.

[Gap20-12] None.

4.19 Edge/Cloud-based visual inspection for automatic quality assessment in production

4.19.1 Use Case briefing

This use case looks at a specific application of industrial communication in the context of automated quality assessment in production based on processing of sensor information in edge cloud environments. The use case covers edge/Cloud-based visual inspection in the production environments using AI-assisted video analytics. Industrial-grade video cameras monitor produced objects in the visual inspection stations embedded in production lines. These video streams are transported to an edge data centre and processed by AI-assisted video analytics edge/Cloud services in order to evaluate the produced part quality metrics. Based on these metrics, automatic quality control measures are taken on the factory shop floor, such as controlling robotic actors to handle the defect parts. Basically, the use case describes the full control loop from the acquisition of sensor information (e.g. from video cameras) on the factory shop floor, the transmission of that information to the data centre, the processing of the sensor information and finally the transmission of derived control signals back to machines and robots on the factory shop floor.

4.19.2 Technology Requirements

4.19.2.1 General introduction

This clause describes the technology requirements for the transport network between factory shop floor and data centre (in the following referred to as F5G network). Depending on the location of production and data centre sites, urban or regional scenarios may apply with respect to the distances between the sites. The following scenarios are considered:

1) On-Premise Edge: < 10 km.
2) Urban area colocation/public edge: < 50 km.
3) Regional area colocation/public edge: < 80 km.

For more information on the use case itself, refer to use case #21 in ETSI GR F5G 008 [i.75].This use case shares several technology requirements with the following related use cases "#6 PON for Industrial Manufacturing" (clause 4.6) and "#19 Next Generation Digital Twin" (clause 4.15) from the ETSI ISG F5G Use Cases Release #2 document [i.75]. The shared technology requirements are referenced in the respective clauses below.

4.19.2.2 Deterministic network performance

This use case requires low latency and deterministic data exchange between cameras, data centre (edge cloud) and actuators/robots on the factory shop floor. Typical vision inspection applications require a maximum cycle time of 5 ms - 10 ms, while some very time-critical vision inspection scenarios may require 2 ms or less. In order to assure these cycle times, there needs to be a guaranteed upper bound on the latency. For example Time Sensitive Networking (TSN) provides a standard for timing and synchronization for time-sensitive applications and profiles specifically tailored for industrial automation (IEC/IEEE 60802 [i.76]). Concerning the interworking between F5G network and TSN some options have been described in the "Next Generation Digital Twin" use case clause of the present document (clause 4.15).

[R21-1] The F5G network should support functionality and performance requirements for industrial automation.

NOTE: One example of such requirements is provided by the industrial automation profile IEC/IEEE 60802 [i.76] for TSN.

[R21-2] Same as [R19-1].

[R21-3] The F5G network shall support cyclic communication with configurable cycle time boundaries in the range of 2 ms - 10 ms

[R21-4] Same as [R19-7].

4.19.2.3 Time Synchronization

Industrial grade video cameras for vision inspection are based on the GiGE Vision® [i.77] and USB3 Vision™ [i.78] standards. To time synchronize the cameras, these standards use IEEE 1588 [i.40] Precise Time Protocol (PTP).

[R21-5] The F5G network should support GiGE Vision® and USB3 Vision™ time synchronization.

4.19.2.4 Industrial interface and protocol support

There are a number of real-time capable industrial Ethernet protocols, such as ProfiNET®, EtherNet/IP™, EtherCAT®, Sercos® III and Ethernet POWERLINK™. There are ongoing activities for integration with TSN, e.g. ProfiNET® over TSN [i.80]. Furthermore, industrial grade video cameras are standardized according to GiGE Vision® and USB3 Vision™ which partly also define protocols for streaming.

[R21-6] The F5G network should support transport of industrial Ethernet protocols.

[R21-7] The F5G networks should support the performance requirements of industrial Ethernet protocols

[R21-8] The F5G network should support GiGE Vision® Streaming Protocol (GVSP).

4.19.2.5 Upstream bandwidth

The required upstream bandwidth per vision inspection station can be as high as 20 Gbits/s.

[R21-9] The F5G network should support upstream bandwidth $\geq$ 20 Gbits/s per vision inspection station.

4.19.2.6 Network resilience

The reliability of the communication over the F5G network between factory shop floor and data centre is of utmost importance for industrial use cases. Both OTN and PON can provide different grades of network resilience, implemented with different protection schemes such as e.g. automatic protection switching [i.81] and different PON protection architectures [i.82].

[R21-10] Same as [R19-9].

4.19.2.7 Network security

The security of data communication over the F5G network between factory shop floor and data centre is of utmost importance for industrial use cases. The data that is communicated over the F5G network needs to be protected against potential attacks. Therefore, the network should secure data integrity by AES link protection while at the same time minimize the impact on latency in order to not compromise the cycle time boundaries [R21-3].

[R21-11] The F5G network shall provide AES link protection.

4.19.2.8 Harsh environment adaptation

F5G network terminals (e.g. ONUs) that are deployed in industrial manufacturing scenarios can face harsh environments with respect to temperature, humidity, dust and exposure to fluids and chemically or mechanically active substances. Therefore, F5G network terminals should be hardened against such environmental effects depending on the deployment scenario.

[R21-12] Same as [R06-11].

4.19.3 Current related standards

4.19.3.1 GiGE Vision® and USB3 Vision™

GiGE Vision® [i.77] and USB3 Vision™ [i.78] standards define device control, device discovery and streaming protocols for industrial grade video cameras that are relevant for vision inspection.

4.19.3.2 IEC/IEEE

The IEC/IEEE 60802 [i.76] as a joint project of IEC SC65C/WG18 and IEEE 802 defines TSN profiles for industrial automation, which select features, options, configurations, defaults, protocols, and procedures of bridges, end stations, and LANs to build industrial automation networks. These profiles also serve as a basis for integration with industrial Ethernet protocols such as ProfiNET® [i.80].

4.19.3.3 Industrial Ethernet

There are a number of real-time capable industrial Ethernet protocols, such as ProfiNET® [i.83], EtherNet/IP™ [i.84], EtherCAT® [i.85], Sercos® III [i.86] and Ethernet POWERLINK™ [i.87].

4.19.3.4 ETSI

ETSI TC EE (Environmental Engineering) ETSI EN 300 019-1-0 [i.88] specify environmental conditions and environmental tests for telecommunications equipment to operate in different environments including harsh environments that can possibly be met in industrial manufacturing.

4.19.4 Gap analysis

4.19.4.1 Gap Context

In the present document the gaps refer to existing standards and not to technology in general. Some vendor's products that are not standardized could exist that implement the solutions described in the gaps.

4.19.4.2 Deterministic network performance

Currently, the features of the industrial automation profile IEC/IEEE 60802 [i.76] or similar/equivalent features are not fully supported. Additionally, time-aware scheduling with absolute cycle time boundaries of < 10 ms (loose scenario), < 5 ms (medium scenario), or < 2 ms (challenging scenario) is not yet supported.

[Gap21-1] TSN features of the industrial automation profile IEC/IEEE 60802 or similar/equivalent features are currently not fully supported.

[Gap21-2] None.

[Gap21-3] Time-aware scheduling with absolute cycle time boundaries is currently not supported.

[Gap21-4] Same as [Gap19-7].

4.19.4.3 Time Synchronization

Time synchronization according to the IEEE 1588 [i.79] Precise Time Protocol (PTP) as required by GiGE Vision® can already be supported.

[Gap21-5] None.

4.19.4.4 Industrial interface and protocol support

Current networks do not natively support the transport of industrial Ethernet protocols and their performance requirements e.g. with respect to cyclic communication requirements.

[Gap21-6] Native support for transport of industrial Ethernet protocols is currently not available.

[Gap21-7] Performance requirements of these protocols is currently not fully supported.

GVSP runs on the UDP protocol and is supported in Ethernet networks.

[Gap21-8] None.

4.19.4.5 Upstream bandwidth

The F5G network should support upstream bandwidth of up to 20 Gbits/s per vision inspection station. In scenarios with multiple vision inspection stations, the resulting aggregated upstream bandwidth demand can reach well in excess of 50 Gbits/s and more. In case the F5G network is realized by a PON, such bandwidth demands are not yet supported by current PON standards (Recommendation ITU-T G.9804.1 [i.113] peaking off at 50 Gbits/s) but are available for OTN. Therefore, the following gap applies to PON based access to the vision inspection stations.

[Gap21-9] Upstream bandwidth in excess of 50 Gbits/s is not yet standardized for PON.

4.19.4.6 Network resilience

Both OTN and PON can provide different grades of network resilience, implemented with different protection schemes such as e.g. automatic protection switching (Recommendation ITU-T G.873.1 [i.81]) and different PON protection architectures (Recommendation ITU-T Series G Supplement [i.82]).

[Gap21-10] Same as [Gap19-9].

4.19.4.7 Network security

Both PON and OTN are able to support AES protection, even post-quantum secure AES encryption methods are available.

[Gap21-11] AES link protection is currently not standardized for OTN.

4.19.4.8 Harsh environment adaptation

Network terminals which are hardened against environmental effects are available.

[Gap21-12] None.

4.20 Edge/Cloud-based control of Automated Guided Vehicles (AGV)

4.20.1 Use Case briefing

Edge/Cloud-based control of Automated Guided Vehicles (AGV) is another industrial communication use case. AGVs, i.e. small mobile transport robots, are essential to distribute materials and production parts inside the factory and between different buildings on an industrial campus. The use case considers that navigation, guidance control system, and other services of the AGVs are moved to the edge cloud and identifies requirements for the communication network between AGVs and the data centre. For more information on the use case itself (refer to use case #22 in ETSI GR F5G 008 [i.75]).

4.20.2 Technology Requirements

4.20.2.1 General introduction

This use case shares several technology requirements with the following related use cases "#6 PON for Industrial Manufacturing" (clause 4.6), "#19 Next Generation Digital Twin" (clause 4.15) and "#21 Edge/Cloud-based visual inspection for automatic quality assessment in production" (clause 4.16) from the ETSI ISG F5G Use Cases Release #2 document (ETSI GR F5G 008 [i.75]). The shared technology requirements are referenced in the respective clauses below.

4.20.2.2 Interworking with wireless networks

On the factory shop floor, the AGVs are operating in a wireless network. The options listed in the use case are 5G campus network, Wi-Fi® access network and LiFi access network. The F5G network should support interworking with at least one of these three options.

[R22-1] The F5G network should support interworking with 5G campus networks.

[R22-2] The F5G network should support interworking with Wi-Fi® 7 access networks.

[R22-3] The F5G network should support interworking with LiFi access networks.

4.20.2.3 Deterministic network performance

This use case requires low latency and deterministic data exchange between AGVs, data centre (edge cloud) and actuators/robots on the factory shop floor. In order to assure defined cycle times, there needs to be a guaranteed upper bound on the latency. For example Time Sensitive Networking (TSN) provides a standard for timing and synchronization for time-sensitive applications and profiles specifically tailored for industrial automation [i.76]. Concerning the interworking between F5G network and TSN some options have been described in the "Next Generation Digital Twin" use case clause of the present document (clause 4.15).

[R22-4] Same as [R21-1].

[R22-5] Same as [R19-1].

[R22-6] Same as [R21-3].

[R22-7] Same as [R19-7].

4.20.2.4 Network availability

Due to safety reasons, the availability of the network between the AGV and the data centre, where navigation and control algorithms are running, needs to be extremely high.

[R22-8] The F5G network availability between AGV and data centre should be > 99,9999 %.

4.20.2.5 Network resilience

The reliability of the communication over the F5G network between AGV and data centre is of utmost importance for this use case. Both OTN and PON can provide different grades of network resilience, implemented with different protection schemes such as e.g. automatic protection switching [i.81] and different PON protection architectures [i.82].

[R22-9] Same as [R21-10].

4.20.2.6 Network security

The security of data communication over the F5G network between AGV and data centre is of high importance for this use case. The data that is communicated over the F5G network needs to be protected against potential attacks. Therefore, the network should secure data integrity by Layer 1 AES protection while at the same time minimize the impact on latency in order to not compromise the cycle time boundaries [R21-3].

[R22-10] Same as [R21-11].

4.20.3 Current related standards

4.20.3.1 3GPP

See 3GPP description in "Use Case Next Generation Digital Twin" (clause 4.17.3.3) in the present document.

4.20.3.2 Wi-Fi® 6 (IEEE 802.11ax) and Wi-Fi® 7 (IEEE 802.11be)

Wi-Fi® 6 and Wi-Fi® 7 are potential options for industrial wireless networks:

- Wi-Fi® 6 already implemented several functions, which are relevant for industrial deployment scenarios. For example, the Target Wake Time (TWT) feature enables longer runtime of battery-powered AGVs and at the same time enables planned access to the communication channel [i.89].
- Wi-Fi® 7 is expected to provide support on bounded latency and TSN features [i.90].

4.20.4 Gap Analysis

4.20.4.1 Gap Context

In the present document the gaps refer to existing standards and not to technology in general. Some vendor's products that are not standardized could exist that implement the solutions described in the gaps.

4.20.4.2 Interworking with wireless networks

Interworking with some wireless network options is already implemented. For example, current generation Wi-Fi® 6 access points, LiFi access points and 5G small cells can be served by ONUs. Support for Wi-Fi® 7 that is expected to provide support on bounded latency and TSN features is still missing.

[Gap22-1] None.

[Gap22-2] Interworking with next-generation Wi-Fi® 7 is currently not supported.

[Gap22-3] None.

4.20.4.3 Deterministic network performance

[Gap22-4] Same as [Gap22-1].

[Gap22-5] None.

[Gap22-6] Same as [Gap21-3].

[Gap22-7] Same as [Gap19-7].

4.20.4.4 Network availability

The required > 99,9999 % availability can be achieved in current networks by appropriate redundancy, restoration and resilience mechanisms.

[Gap22-8] None.

4.20.4.5 Network resilience

Both OTN and PON can provide different grades of network resilience, implemented with different protection schemes such as e.g. automatic protection switching [i.81] and different PON protection architectures [i.82].

[Gap22-9] Same as [Gap19-9].

4.20.4.6 Network security

Both PON and OTN can support AES protection, even post-quantum secure AES encryption methods are available.

[Gap22-10] Same as [Gap21-11].

4.21 Cloudification of Medical Imaging

4.21.1 Use Case Briefing

The cloudification of medical imaging uses systems such as Picture Archiving and Communication System (PACS) or Radiology Information System (RIS). To ensure optimal experience, the imaging system requires that the network accessing the Cloud to provide high bandwidth, low latency, low packet loss rate, high security, high reliability, and flexible scheduling capabilities. Medical image Cloud provides services for remote consultation, specialist imaging diagnosis, image teaching, mobile image reading/consultation, and image big data analysis services. These services enable medical personnel to quickly query and search medical records, improving their work and scientific research efficiency. For more detail on this use case number 23 see ETSI GR F5G 008 [i.75].

For the equation there are three parameters that affect the TCP throughput, which are Round trip delay (Rtt), percentage packet loss (p), and the Maximum Segment Size (MSS).

$$\text{Throughput} = \text{MSS/Rtt} \times 1/\sqrt{p}$$

As an example assume the maximum upload rate is 50 Mbits/s, Table 24 gives an example of experimental data for the uploading rate for the same image file from the local image system to the image cloud under different cloud network latency and packet loss rates.

Table 24: Example of experimental data for uploading time for different delays on the cloud access network

Image Type	RTT(ms)	Packet loss rate	Upload Rate (Mbps)	Upload Time(s)
CT	3	0,1 %	47,49	22
	+200	0,1 %	↓ 20,09	↑ 52
	+1 000	0,1 %	↓ 5,04	↑ 207
MR	3	0,1 %	37,43	8
	+200	0,1 %	↓ 17,57	↑ 17

- When the latency of the cloud access network is low enough (for example, 3 ms), the actual transmission rate is close to the maximum value of the image system.
- When the latency of the cloud access network increases to 200 ms, the actual transmission rate deteriorates by more than 50 %.

To ensure the upload experience, the packet loss rate of the cloud network should be as close as possible to 0 %. Table 25 gives an example of the uploading rate for different packet loss rates with Rtt set to 3 ms for the same image file. Otherwise, the upload rate deteriorates by more than 90 %

Table 25: Example of experimental data for uploading time for different packet loss rates on the cloud access network

Image Type	RTT(ms)	Packet loss rate	Upload Rate (Mbps)	Upload Time (s)
CT	3	0,1 %	47,49	22
	3	2 % in both directions	↓ 4,25	↑ 258
MR	3	0,1 %	37,43	8
	3	2 % in both directions	↓ 4,04	↑ 78
DR	3	0,1 %	51,26	1
	3	2 % in both directions	↓ 4,14	↑ 13
	3	10 % in both directions	↓ 1,77	↑ 37

So to ensure a satisfactory user experience for the uploading of medical imaging, the network round trip should be in the low milliseconds range typically 3 ms. The packet loss should be as close to zero as possible and a typical value is 0,1 %

4.21.2 Technology Requirements

4.21.2.1 General introduction

The content of the medical image service flow is mainly patient image data. The network delay between the medical image Cloud and the display terminal should be in the millisecond range. The amount of medical image data varies according to the patient type and imaging equipment used. The medical image data can vary from tens of megabytes to 2 GBytes. The number of outpatients can vary depending on the size of the hospital as well and the country in question, so it can vary from several hundreds to as large as 20 000 for level 3 hospital for example. The bandwidth of the network accessing the image Cloud will also vary depending on whether the access is from a large hospital to a doctor's surgery from megabytes to double digit gigabytes. To ensure that healthcare workers can perform their work efficiently when examining and analysing patient's medical condition, the image Cloud network needs to guarantee the bandwidth and isolation of multiple patient's data from each other. Therefore, the medical image Cloud network should have large bandwidth, low latency, ultra-low packet loss rate, and high reliability.

There are several technologies that can be used to achieve image transport, however this use case will focus on OTN as the transport protocol. This does not imply it is the only approach, just that it is the focus of this use case.

OTN has been widely used in government, in finance and in large enterprise to provide premium private line network services. Therefore, the technical capabilities and performance of OTN are also very suitable to the medical industry and can meet the high-quality network requirements for the medical image Cloud.

Figure 17 shows an example for networking of the medical image Cloud service to different end users. On the top of Figure 17 there is a large hospital with a large number of patients. In the middle a small or regional hospital with moderate to low patient numbers. At the bottom a doctor's office or small doctors surgery with a small number of patients. The large hospital is connected to the medical image cloud via a CPE with a large bandwidth capacity. The small or regional hospital is connected to the medical image cloud via a CPE with a lower bandwidth capacity. The doctor's office is connected to the medical image cloud via an ONU over a PON network with a much lower bandwidth capacity. Each path either connected directly to the aggregation OTN network or in the case of the doctor via an OTN connection from the local OLT. The connection topology between the large and small medical institutions and the medical image Cloud is point to point. While the doctor's office is via Point-to-Multi-Point PON network. The CPE connects to the egress network device of the large and small medical institutions, usually via layer-3 switch or a campus router, and the CPE implement the mapping of the medical image service flow into the preconfigured ODUk (k = 0, 1, 2, 3, 4, flex) links. This enables high-quality transmission of service flows to/from each hospital over OTN. While the doctor office connect is to the ONU via a residential gateway and a predefined channel, this traffic is mapped into a sub 1G container on the egress of the OLT. Again enables high-quality transmission of service flows over OTN.

OTUk links with appropriate bandwidth (k = 0, 1, 2, 3, 4) are selected based on the bandwidth requirements of the service flow in the hospital. The doctor's office PON connection will support the appropriate bandwidth capacity and the predefined sub 1G OTN container will match the doctor office capacity needs. The OTN aggregation nodes need to be well coordinated to map the service flows to an appropriately dimensioned independent ODUk/ODUflex. This ensures end-to-end hard isolation of service flows and guarantees the network bandwidth of service flows for each medical scenario.

The management and control plane need to be able to identify the traffic of the image Cloud for different medical scenarios. In the case of the hospital end-to-end physical links (including working and protection links) from each hospital to the medical image Cloud are automatically calculated based on the link requirements (bandwidth, latency, and reliability) managed by the network administrator. This is also true for the doctor surgery scenario through the OTN aggregation network. It is unlikely that the doctor surgery has redundant links on the PON segment of the connection, but this is a cost and deployment choice, not a technical choice. In this way, the links between the medical institutions and the medical image Cloud can be automatically generated and removed.

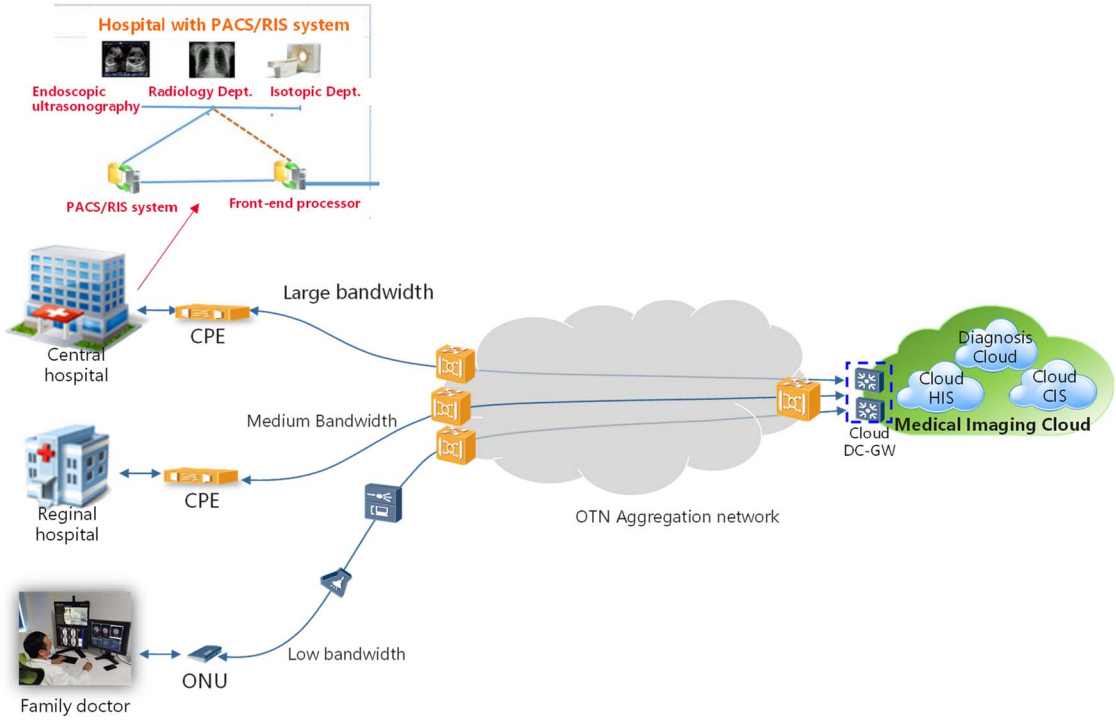


Figure 17: Example of a medical image Cloud network

4.21.2.2 Flexible Bandwidth

There are peak and off-peak hour's bandwidth requirements in each scenario. To better satisfy the service requirements and improve the bandwidth utilization of the medical image Cloud network, the network shall support SLA capabilities such as basic bandwidth, burst bandwidth, and absolute peak bandwidth guarantees for each connection. To meet the requirements the users, the network committed bandwidth shall support different values for different time of day segments according to pre-defined rules. When the bandwidth of a connection is adjusted, no packet loss shall occur. As stated above the images size can vary from hundreds of megabytes to 2G bytes. These images should be transported using OTN container that match the image size to maximize bandwidth efficiency.

[R23-1] The F5G network shall support OTN containers that match the bandwidth requirements of the various medical image formats and sizes.

[R23-2] The F5G network shall support non service affecting bandwidth adjustment.

It was shown in the use case #23 in ETSI GR F5G 008 [i.75] that the hospital bandwidth requirements vary dependent on the size of the hospital. In Table 17 of ETSI GR F5G 008 [i.75] the range is from 792 Mbits/s to 15,840 Gbits/s. So the minimum link capacity is 25 Gbits/s for the large hospital, but this does not leave much room for expansion in the future. A more future proof value would be 50 Gbits/s or 100 Gbits/s for the larger hospitals. In the case of doctor's surgeries, the bandwidth would be 10 Mbits and growing depending on the number of patients and number of doctors per surgery.

[R23-3] The F5G network should support lossless bandwidth adjustment from 2 Mbits/s to 100 Gbits/s.

4.21.2.3 Hard isolation based on service flows

Medical image flows shall be hard isolated, so that concurrent flows do not affect each other, this ensures patient privacy and ensure quality of experience for medical personnel. This requires an end-to-end non-shared channel between the source and destination nodes of the medical image flows, passing through multiple network nodes in the network.

[R23-4] The F5G network shall support hard isolation on end-to-end service flows.

4.21.2.4 On-demand Network Management

High-quality medical image Cloud private lines shall support efficient end-to-end connection and on-demand provisioning. This implies that, private lines between the source and destination nodes of the image Cloud can be ordered/provisioned on demand. In addition, the ordering/provisioning system should support additional line installations and service upgrades.

Once the required fibres are laid and physical devices are installed and can be remotely configured, the tenants can provision private lines for the image Cloud network in the management system within seconds.

[R23-5] The F5G network management system shall support on demand configuring and provisioning of private line services.

Smart phones, tablets and laptops all support applications to monitor such things as power consumption, health monitoring, even cooking monitoring, etc. Then it should not be surprising that users would like to monitor their network for such things as latency, failure, congestion, bandwidth usage and other SLA parameters.

[R23-6] The F5G network management system should support user applications for non-intrusively monitoring of their SLA parameters indicators.

4.21.2.5 Reliability

The image Cloud network shall provide end-to-end network-level protection capabilities, such as cross-device dual-homing protection and fibre cut protection. The protection switching time shall meet the operator-level performance requirement of 50 ms. The reliability of the network should be 99,999 %.

[R23-7] The F5G network shall support 99,999 % reliability.

4.21.2.6 Latency

The image Cloud network should support the agreed SLA latency for the end-to-end connections, which is independent of network traffic load.

[R23-8] The F5G network shall support the agreed SLA latency.

[R23-9] The F5G network latency should be independent of traffic load.

4.21.2.7 Private Data Centre and Cloud access

The image Cloud network should support dedicated access connections to:

- Private Cloud Data Centre.
- Cloud Services.

These end-to-end dedicated connections should have sufficient security, reliability, and bandwidth.

[R23-10] The F5G network shall provide dedicated connections to the user's private Data Centre.

[R23-11] The F5G network shall provide dedicated connections to access Cloud service.

4.21.3 Current related standard specifications

This option focuses on OTN as the main technology to support high quality Private Line. To that end, an OTUk, (where k = 0, 1, 2), as well as OTU25-RS and OTU50-RS for higher bandwidth needs, will be used. These OTN point-to-point links can be used to support Private Line both legacy TDM and Ethernet services. The Central Office should be equipped with OTN Aggregation Equipment, with high bandwidth links to the network such as OTU4 or OTUCn (n = 1, 2, 3, 4…) depending on required connectivity to the network. Different ODUs can be provisioned to separate Private Line user traffic.

Related standards:

- Recommendation ITU-T G.709 [i.67].
- Recommendation ITU-T G.709.1 [i.108].
- Recommendation ITU-T G.709.2 [i.109].
- Recommendation ITU-T G.709.3 [i.110].
- Recommendation ITU-T G.709.4 [i.111].

4.21.4 Gap analysis

4.21.4.1 Gap Context

In the present document the gaps refer to existing standards and not to technology in general. Some vendor's products that are not standardized could exist that implement the solutions described in the gaps.

4.21.4.2 Flexible Bandwidth

The existing OTN network meets this capability requirement. If the service traffic capacity to be carried is greater than 1 Gbps, existing OTN systems can support efficiently packed OTN containers with minimal capacity wastage. In addition, OTN container bandwidths can be flexibly and support hitless bandwidth adjustment.

However, for a service flow less than 1 Gbits/s (which may be referred to as a sub-1 Gbits/s service), only 1,25 Gbits/s containers can be allocated in the existing OTN network. As a result, for sub 1 Gbits/s services, the OTN container bandwidth is sub-optimal.

Therefore, the current OTN network does not support the capability of allocating correctly dimensioned OTN container for sub-1 Gbits/s traffic.

OTN supports non-service-affecting bandwidth adjustment for container greater than 1 Gbits/s. Currently there is no support for non-service-affecting bandwidth adjustment below 1 Gbits/s.

[Gap23-1] The support for sub 1 Gbits/s bandwidth granularity OTN containers is not currently supported by OTN.

[Gap23-2] The support for non-service-affecting bandwidth adjustment below 1 Gbits/s is not currently supported by OTN.

An OTN network can support lossless bandwidth adjustment from 1,25 Gbits/s to 100 Gbits/s. There is currently a standardization process in ITU-T Q11 to create a Sub 1G OTN container, which will support bandwidths from 10 Mbits/s to 1,25 Gbits/s. As part of this standardization process this Sub 1 G container will support lossless bandwidth adjustment from 10 Mbits/s to 1,25 Gbits/s. However when the boundary of 1,25 Gbits/s is reached a different mapping scheme is used to map user traffic into OTN for 1,25 Gbits/s and above using ODUflex. If the bandwidth requested is close to the 1,25 Gbits/s boundary (for example 750 Mbits/s) then ODUflex could possibly be used instead of a Sub 1G container. However this will waste bandwidth from the chosen point up to 1,25 Gbits/s.

[Gap23-3] The support for lossless bandwidth adjustment from 2 Mbits/s to 100 Gbits/s is not currently supported by OTN.

4.21.4.3 Implements hard isolation based on service flows

Currently OTN provides hard connection isolation between tenants, but individual services of a given tenant cannot be hard isolated. This requires the OTN network to identify different service types and allocate dedicated connections or slices to these services end-to-end. Generally, these services have different bandwidth requirements and have different customer priorities.

Therefore, OTN needs to allocate hard pipe connections or slices based on service flows end-to-end, and allow different service priorities between service flows.

[Gap23-4] The support of hard service flow isolation is not currently supported by OTN.

4.21.4.4 On-Demand network management

OTN needs to support on-demand connection provisioning, but this depends on the software capabilities of the network equipment (CPE's and ONU) installed on the customer premises and OTN edge nodes. The customer network equipment and OTN edge node functions may need to be upgraded to enable on-demand provisioning of private line services between tenant access points and the image Cloud to carry services in a timely manner.

[Gap23-5] The support of on-demand private line provisioning for customer network equipment and edge nodes is not currently supported.

It is not unrealistic for a user to expect to have an application on a smart devices to monitor their SLA.

[Gap23-6] The F5G network management support of user applications for non-intrusively monitoring their SLA parameters is not currently supported.

4.21.4.5 Reliability

The network can support high reliability if redundant connections between the customer network equipment (CPE's and ONU) and the cloud are supported. Therefore, it is recommended that the network supports redundant connections. OTN supports redundant paths so there is no gap on the OTN side. PON does support redundant connection but it is more a deployment choice based on cost and not technology.

[Gap23-7] None.

4.21.4.6 Latency

Because OTN is a TDM-based network technology, network delay is deterministic and independent of traffic load.

[Gap23-8] None.

[Gap23-9] None.

4.21.4.7 Private Data Centre and Cloud access

OTN provides private and public Data Centres with the necessary connection access.

[Gap23-10] None.

[Gap23-11] None.

4.22 F5G for Intelligent Mining

4.22.1 Use Case Briefing

The 10G PON has many advantages such as mature technology, simple structure, high reliability, and cost effective, and has been widely deployed in FTTH networks. These also make 10G PON optimal for industry digitalization, such as intelligent mine networks.

The use case of F5G for intelligent mining describes implementation of 10G PON in intelligent mining network infrastructure. In this case dual optical fibre based ring network architecture is used to provide high reliability, large bandwidth, and low latency network services for mine intelligent transformation, and dramatically improve the electrical safety, service safety, construction safety, and maintenance safety of the underground network.

4.22.2 Technology Requirements

4.22.2.1 General introduction

The intelligent mine services include industrial control, environment monitoring, video surveillance, and personnel positioning services. These are essential to the normal operation of a mine production, risk of security incident will increase and be out of control in case of network outage. Therefore, a high reliability network infrastructure is a necessity for the underground and opencast.

In the production environment of underground or opencast mines, high concentration of combustible and explosive gases, large amount of dust and high humidity exist in the air. Therefore, the network equipment deployed in the above-mentioned environment shall be explosion-proof and robust and meet safety regulations required by management authorities.

Optical fibres cable should be capable of quick connected and avoid needs of field splicing and fusing, this also improves deployment efficiency and reduces working time in harsh environments. The optical fibre network infrastructure should be visualized and managed by Network Management System (NMS). This means NMS should be able to quickly and accurately locate the position in case of there is a fault in the cable, and guide the technician to repair the fibre quickly.

4.22.2.2 High-reliability networking

The F5G network shall adopt Type-C dual-homing protection networking defined in Recommendation ITU-T G.984.1 [i.97], with optical fibre redundancy protection being connected to each ONU. When a fault occurs at network device, optical splitter, or optical fibre cable, the system can be switched to the standby link within 30 ms and services can be recovered accordingly.

[R24-1] The F5G mining network shall support Type-C dual-homing protection.

[R24-2] F5G mining network shall support switching to the standby link within 30 ms.

4.22.2.3 Industrial grade equipment

The network equipment deployed in the well and opencast mines shall be installed in the special explosion-proof box or Intrinsic Safety (IS) box to meet the requirements of IP65 ingress protection requirements, as specified by IEC 60079-0:2017 [i.173]. The circuit design and electronic components used for network equipment shall meet the explosion-proof requirements of mine safety regulations of the management authorities and obtain corresponding safety certificates. The network equipment shall be capable of operating normally under an ambient temperature ranging from -40 °C to 70 °C and a relative humidity of 95 % (non-condensing).

[R24-3] The F5G mining network shall meet IP65 protection requirements.

[R24-4] The F5G mining network shall be installed in explosion-proof box or intrinsic safety box.

[R24-5] The F5G mining network shall support fully functional operation in an environment of temperature ranging from -40 °C to 70 °C and a relative humidity of 95 % (non-condensing).

4.22.2.4 Fast fibre connection

It is applicable to ODN connectors and boxes (including outdoor adapters) in various complex environments in wells and opencast mines. The connection shall meet the ingress protection level of IP65. Long-term environmental reliability test (such as 2000-hour test of 85 °C temperature and 85 % Relative Humidity (RH) on the connector box) and mechanical test (such as cable tension and strain requirements) are also recommended. Quick connection and installation should be implemented during onsite construction and deployment.

[R24-6] The F5G mining network fibre connection shall meet IP65 ingress protection.

[R24-7] The F5G mining network shall use pre-connectorized fibre segments for optical fibre deployment.

4.22.2.5 Intelligent optical O&M management

The ODN network infrastructure and deployment environment are complex, which make the ODN management complicated. In the prior art, paper or plastic labels are manually attached to the fibres and manually recorded. The records and its updates might not be able to be recorded timely. In addition, these labels are easily damaged and therefore no longer be identifiable. When a fault occurs, the corresponding link cannot be quickly located hence be repaired in time. The intelligent ODN management, which was illustrated in F5G Use Cases Release #1 (ETSI GR F5G 002 V1.1.1 [i.14]) and ETSI TR 103 775 [i.19] (Optical Distribution Network (ODN) Quick Construction and Digitalization), should be implemented to record, display fibre connections and topology in a digitalized and intelligent mode. When a fault occurs, the fault can be quickly located and the remote fibre fault diagnosis technology can be used to quickly locate the fault point.

[R24-8] The F5G Network Management System (NMS) should support visualization and management of the optical fibre network infrastructure.

[R24-9] The F5G mining network should support a digitalized intelligent ODN management system.

4.22.3 Current standard

4.22.3.1 ITU-T

Recommendation ITU G.987 [i.28] defined 10G PON technical specifications and technical requirements, but does not describe how F5G is applied to intelligent mining scenarios.

4.22.3.2 IEC

IEC 61753 [i.37] is the test standard for the full range of ODN products (including boxes, cables and connectors). The IEC 61754 series [i.38] of standards specifies the interface and related performance standards of common connectors (SC/LC, etc.). These standards are aimed at normal scenarios, which cannot be used for harsh environment such as underground mine network. The standards for long-term reliability of ODN product design and testing for the mining industry, which are quite different from the scenarios of above, are also needed.

4.22.4 Gap analysis

4.22.4.1 Gap Context

In the present document the gaps refer to existing standards and not to technology in general. Some vendor's products that are not standardized could exist that implement the solutions described in the gaps.

4.22.4.2 General

The traditional mining network solution uses multiple 10GE/100GE aggregation switches to form an aggregation ring network, with multiple 10GE/100GE access switches in a chain network connected to the aggregation ring. Taking mining industry as an example, this kind of network scheme is more and more difficult to meet the requirements of intelligent network development in mining.

4.22.4.3 Networking reliability

The F5G network should adopt Type C dual-homing protection which is defined in Recommendation ITU-T G.984.1 [i.97], and optical fibre redundancy protection should be used to connect to the ONU. When a network device, optical splitter, or optical fibre is faulty, the system can switch to the standby link within 30 ms, and services can be automatically recovered. This form of network formation can greatly improve the reliability of the mine network.

[Gap24-1] None.

[Gap24-2] The F5G mining network support for switching times better than 30 ms and with Type-C dual-homing protection is currently not defined.

[Gap24-3] None.

4.22.4.4 Electrical safety

In the passive all-optical network based F5G mining network, the Optical Ring Passive (ORP) network infrastructure replaces the aggregation switch and its explosion-proof box. The ORP is made of antistatic and flame retardant materials which meet the requirements of mine safety regulations. Compared with the traditional network solution, the use of explosion-proof devices and explosion-proof boxes is reduced, and the risk of electric sparks in the underground mine is effectively reduced. IEC 60079-0:2017 [i.173] specifies the general requirements for construction, testing and marking of Ex Equipment (Equipment that has been classified as safe for use in hazardous areas) and Ex Components (components that have been classified as safe for use in hazardous areas) intended for use in explosive atmospheres, which covers the requirements of intelligent mining networks.

[Gap24-4] None.

[Gap24-5] None.

[Gap24-6] None.

4.22.4.5 Fast fibre connect

The traditional optical fibre network deployment in mines is accompanied by a large number of high-temperature fibre splicing and fusing operations. In the environment with high concentration of explosive gas, these operations are very risky. The fibre pre-connected fibre technology which eliminates on-site fibre splicing and fusing should be adopted by F5G mining network to ensure safety and improve the efficiency.

[Gap24-7] The support for more reliable and faster fibre connection technologies for the mining industrial is currently not defined.

4.22.4.6 Intelligent optical O&M management

When a fault such as fibre cut occurs in the fibre network, technicians need to locate the fault and repair it, which is difficult and of low efficiency in the mine environments when no digitalized ODN infrastructure management system exist. The digitalized intelligent fibre management technology, which provide digitalized ODN connection information and can solve the problems of fibre deployment and O&M.

[Gap24-8] None.

[Gap24-9] None.

4.23 Enhanced optical transport network for Data Centre Interconnections

4.23.1 Use case briefing

Cloud services are usually supported by multiple interconnected Data Centres (DCs). This Data Centres interconnection needs a Data Centre Interconnect (DCI) infrastructure with requirements on high bandwidth, low latency, high reliability, and flexible scheduling. In use case # 25, two typical applications scenarios, Availability Zone (AZ) DCI and regional DCI are introduced. The corresponding requirements for the interconnecting network for each scenario are discussed and potential technologies are analysed in the present document. (For more detail on use case # 25, see ETSI GR F5G 008 [i.75], F5G Use case, Release 2.)

4.23.2 Typical scenarios and services of DCI

4.23.2.1 Scenarios introduction

There are two typical DC concepts:

1. Availability Zone (AZ)

An AZ is a logical Data Centre in a region and consists of multiple discrete data centres with redundant and separate power supplies, networking, and connectivity to provide highly available, fault tolerant, and scalable cloud services. There are typically 2~5 AZs in a region of a public cloud.

One typical AZ scenario is DCI for Intra-city DCs, which communicate with each other via the intra-city DCI network to meet the high availability requirements. The active-active and Virtual Machine (VM) migration services which require low latency are provided by this intra-city DCI network. The intra-city DCI network supports the public and/or the private cloud services, such as video streaming, gaming, cloud based virtual desktops, and cloud Internet cafe services. To ensure low latency, the intra-city DCI network is deployed in the same city or in the greater city surrounding area. The distance of intra-city DCI is typically less than 100 km and more likely less than 50 km. One city may have several large DCs.

The active-active, synchronization, VM migration operations, and disaster recovery and backup services between intra-city DCs require tens of terabytes/second transmission capacity. Due to insufficient optical fibre resources and high costs associated with deploying new fibres, the single fibre transmission capacity need to be enhanced.

2. Region

A region is a geographic area within a cloud infrastructure that contains multiple data centres. In a public cloud infrastructure, a region can cover multiple provinces or even multiple countries. In a private cloud infrastructure, a region may cover just one DC or a few DCs within a short distance (e.g. tens of kilometres) from each other. Inter-city connections within a region may be in range of 100 km to 1 500 km.

In region DCI scenario, remote DC which are located in a low cost rural region may be used to provide disaster recovery and backup, for example, backing up data from a large city DC. Some service, such as commercial services, have no particular requirement on latency. However, to improve interaction efficiency as well as service experience, the latency is still expected to be as low as possible. Figure 18 shows the service flow between the remote DC's and the large city DC cluster.

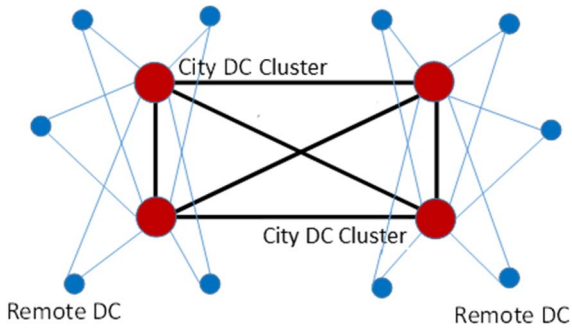


Figure 18: Example of regional DC with remote DCs and city DC clusters

4.23.2.2 DCI Service functionality

DC interconnection needs to be an all optical connectivity to meet the high-speed interconnection requirements between DCs. Below are some DCI service functionalities:

- Active-active operation: Active-active operation needs at least two data centres. Each DC serves as an active site for the other. This means that an application continues to be accessible even if parts of the network or servers fail unexpectedly.
- Remote storage: Remote data storage provide reliable, secure, redundant, connectivity and space for storage of important data.

- Virtual Machine (VM) migration: VM migration is the process of moving a running virtual machine or application between different physical machines without disconnecting the client or application. Memory, storage, and network connectivity of the virtual machine are transferred from the original guest machine to the destination.

- Disaster recovery and backup: Disaster recovery is the plan and process for quickly restabilising access to applications, data and resources after an unexpected outage. Backup is the process of making an extra copy of data

These functions require high-bandwidth and low-latency communications, and high availability to meet the high reliability requirements.

4.23.3 Technical requirements

4.23.3.1 Network bandwidth

DCI network introduces huge bandwidth demand. Currently available technology support 96 × 50 GHz-spaced channels, with 200 Gbits/s - 400 Gbits/s per channel (400 Gbits/s in short reach less than 100 km for intra-city DCI and 200 Gbits/s for up to 1 500 km for inter-city DCI). In order to meet the ultrahigh capacity requirements, two aspects should be considered:

- one is to increase bandwidth of each channel;

- the other is to increase the number of channels over each fibre, for example, to increase number of channels to 120 in C-band and/or L-band.

Hence the combination of these two approaches will achieve transmission bandwidth in the order of 64 Tbits/s.

[R25-1] The data rate for intra-city DCI shall support 800 Gbits/s per channel, with range up to 100 km.

[R25-2] The data rate for inter-city DCI shall support 400 Gbits/s per channel, with range from 100 km to 1 500 km.

[R25-3] DCI equipment shall support Extend C-band and L-band to support up to 120 × 50 GHz-spaced channels.

4.23.3.2 Fibre infrastructure and distance for intra-city DCI

Intra-city fibre network between DCI concerns high density areas where fibre infrastructure can be provided using a combination of dark fibre offers on various leasing models and lit fibre (dedicated fibre) by the DCI operator. This combination of fibre infrastructure segments allows to reach a distance up to 100 km. In this context, the opportunity to use single fibre transmission allows to simplify network operation and to save required fibres along the path between DCIs.

[R25-4] The DCI should support bidirectional transmission over two fibres or single fibre.

4.23.3.3 Ultra-long-haul transmission distance for intercity DCI

Regional DCI needs to connect DCs located in cities which may be up to 1 500 km from each other. To realize a low latency, green DCI network, an all optical transparent connection up to 1 500 km without optical-electronic-optical conversions is needed.

[R25-5] Inter-city DCI shall support an all optical transparent connection for distances up to 1 500 km.

4.23.3.4 Optical-layer wavelength grooming

Large service nodes need to support simultaneous grooming of multiple optical directions with high capacity. Optical Cross-Connect (OXC) can be used to support optical-layer wavelength grooming without electrical layer switching, effectively reducing latency, electrical-layer switching costs, and power consumption, and hence more environmentally friendly. Advanced OXC techniques can be applied to improve integration density and achieve "zero" manual fibre connections to save site space and reduce operating cost. This will also help to achieve low latency and jitter.

[R25-6] DCI shall support optical layer wavelength grooming.

4.23.3.5 High reliability

It is essential to support highly reliable DCI for cloud services. With advanced optical transport network protection and automatic recovery technologies, services can still run properly even when multiple fibre cuts occur in the DCI network. ASON/GMPLS (Recommendation ITU-T G.7703 [i.174]/IETF RFC 3945 [i.143]) provides protection and recovery functions which can achieve this requirements.

[R25-7] DCI network elements shall support protection and automatic recovery functions.

4.23.3.6 High flexibility

The DCI traffic profile (e.g. Bandwidth, route, traffic pattern) might change frequently depending on the DC workloads and operational task, therefore the changes of traffic profiles needs to be flexibly allocated.

[R25-8] DCI should support dynamic allocation of bandwidth, route and traffic profile.

4.23.3.7 Latency measurement and control

Introduction of photonic cross connection helps reducing latency especially in long haul link by the need for E-O-E conversion. To further guarantee latency for applications over DCI network, online delay measurement and optical routing according to the measurement result can improve the DCI latency and jitter.

[R25-9] DCI should support online delay measurement and visualization, and traffic allocation based on that measurement.

4.23.4 Current related standard specifications

4.23.4.1 General

800 G and above interfaces are being studied and progressed in ITU-T, OIF and IEEE organizations.

4.23.4.2 ITU-T

Metro 800G OTN interface is in the scope of ITU-T. Related applications and requirements have been discussed in ITU-T, including multi-vendor client-side interfaces (2 km ~ 40 km grey optics), multi-vendor line-side interfaces (80 km for DCI and 450 km for metro), and single vendor line-side interfaces (1 500 km for long haul).

4.23.4.3 IEEE

At present, IEEE has an active work item 800 GE and 1,6 Tbits/s Ethernet interfaces under 40 km, for example IEEE 802.3df [i.175] which defined 800GE SR/DR/FR/LR/ER.

4.23.4.4 OIF

OIF is mainly focus on 10 km/80 km 800 G interface for DCI (LR/ZR).

4.23.5 Gap analysis

4.23.5.1 Gap Context

In the present document the gaps refer to existing standards and not to technology in general. Some vendor's products that are not standardized could exist that implement the solutions described in the gaps.

4.23.5.2 Network bandwidth

The current standards for intra-city DCI (for long distance up to 100 km) could support up to 400 Gbits/s channel. However 800 Gbits/s per channel standard for intra-city DCI is missing.

[Gap25-1] The intra-city DCI support for 800 Gbits/s per channel standard for up to 100 km is currently not supported.

The current standards for inter-city DCI (for long distance up to 1 500 km) could support up to 200 Gbits/s per channel. However 400 Gbits/s per channel standard for inter-city DCI is missing.

[Gap25-2] The inter-city DCI support 400 Gbits/s per channel standard for up to 1 500 km is currently not supported.

The current DCI standard supports up to 96 × 50 GHz-spaced channels. Standard which Extend C-band and L-band to support up to 120 × 50 GHz-spaced channels in each band is missing.

[Gap25-3] The DCI support for extend C-band and L-band to support up to 120 × 50 GHz-spaced channels in each band is currently not supported.

4.23.5.3 Fibre infrastructure and distance for intra-city DCI

Bidirectional single fibre for 100 Gbits/s is defined by IEEE 802.3ba [i.176], However for line rate at 200 Gbits/s, 400 Gbits/s and 800 Gbits/s are missing.

[Gap25-4] The standard for bidirectional transmission over two fibres or single fibre for data rate up to 800 Gbits/s is currently not defined.

4.23.5.4 Ultra-long-haul transmission distance for intercity DCI

The current ultra-long-haul (Up to 1 500 km) WDM all-optical network standard supports 200 Gbits/s per channel and 80 channels over each fibre. This use case requires 400 Gbits/s ultra-long-haul (Up to 1 500 km) WDM all-optical network. 200 Gbits/s per channel should be increased to 400 Gbits/s per channel. The optical spectrum needs to be extended from the C band to the C+L band. The current DCI standard for all optical transparent connection up to 1 500 km, supports up to 200 Gbits/s per channel. 400 Gbits/s per channel standard for all optical transparent connection up to 1 500 km is missing.

[Gap25-5] Standard for 400 Gbits/s per channel standard for all optical transparent connection up to 1 500 km is currently not defined.

4.23.5.5 Optical-layer wavelength-level grooming

The classification and the characteristics of multi-dimensional reconfigurable optical add/drop multiplexers (MD-ROADMs) has been standardized in Recommendation ITU-T G.672 [i.177]. However Recommendation ITU-T G.672 [i.177] cannot meet the DCI requirements in terms of integration, volume, power consumption, and OAM any more. A Standard is needed to define the function model of integrated photonic cross-connects based on backplane with higher integration, smaller size, lower power, zero manual fibre connection.

[Gap25-6] Standard for function model of integrated photonic cross-connecting with higher integration, smaller size, lower power, zero manual fibre connection is currently not defined.

4.23.5.6 High Reliability

The current OTN protection and restoration standards specify linear protection, shared ring protection, shared mesh protection, subnetwork connection protection and ASON restoration.

[Gap25-7] None.

4.23.5.7 High flexibility

Currently OTN standard Recommendation ITU-T G.709 [i.67] defined ODUflex container which enables OTN connections with flexible rate, furthermore Recommendation ITU-T G.7044 [i.158] defined hitless adjustment of ODUflex. IETF RFC 7139 [i.145] defined the signalling protocol for dynamical creation, remove and adjustment of ODUflex connections.

[Gap25-8] None.

4.23.5.8 Latency measurement and control

Standards to specify online delay measurement and visualization, and traffic allocation based on the measurement result to achieve deterministic and low latency are missing.

[Gap25-9] Standards to specify online delay measurement and visualization, and traffic allocation based on the measurement are currently not defined.

4.24 Enhanced Point to Point optical access

4.24.1 Use case briefing

Optical Access Networks use either Point-to-Multi-Point (based on PON) or Point to Point interfaces (based on Ethernet). All these interfaces may be supported on the Optical Line Terminal (OLT) shelf with dedicated cards and ports. The focus of this use case is P2P access connections between the OLT and the customers such as enterprises and mobile antennas. The existing OLT P2P market is focused on mobile backhaul (OLT linked to cell site gateway) and business (OLT linked to business gateway). Another promising market could be the mobile fronthaul (between the Digital Unit (DU) and the Radio Unit (RU)) through an OLT. With the evolution of bit rate and power reduction of P2P interfaces, the existing interfaces should be upgraded and replaced to higher performance versions.

4.24.2 Technical requirements

4.24.2.1 General introduction

Due to the fibre installed base of single fibre to many locations for enterprises and mobile base stations, bidirectional optical communication shall be enabled on a single fibre.

[R26-1] The F5G Access network shall support Bi-directional P2P fibre technologies.

4.24.2.2 Network Supervision

The purpose of access network supervision is to reduce the operational expenditure of the transport systems, without significantly increasing the capital expenditure, by including as much test and diagnostic capability as possible in the network nodes. Naturally, this should be achieved without compromising the service availability such as bandwidth shortfall.

[R26-2] The F5G P2P Access Network test and diagnostics technologies shall not be service affecting.

[R26-3] The F5G P2P Access Network RSSI (Received Signal Strength Indication) resolution, accuracy, repeatability and response time shall be appropriate for high-performance supervision algorithms.

[R26-4] The F5G P2P Access Network monitoring and optical medium health check should differentiate optical medium failures from transport system failures.

[R26-5] The F5G P2P Access Network key performance indicators shall be provided by the F5G Access network controller to the E2E F5G orchestrator in an abstract way.

4.24.2.3 Point to point link performance

Consideration need to be given to the fact that the OLT is located in a central office. The reach of the F5G Access network technology is defined by the Optical Distribution Network (ODN) fibre length. The length is typically dependent on the density of homes or other users like mobile base station and enterprises in the area around the central office. Therefore, the F5G P2P Access Network technology reach requirements are deployment dependent.

[R26-6] The F5G P2P Access network technology shall support up to 10 km for highly dense areas.

[R26-7] The F5G P2P Access network technology shall support up to 20 km for moderately dense areas.

[R26-8] The F5G P2P Access network technology shall support up to 60 km for low density areas.

[R26-9] The F5G P2P Access network technology shall support P2P bidirectional bit rates up to 100 Gbits/s.

[R26-10] The F5G P2P Access network technology shall support energy saving mechanisms.

4.24.3 Current related standard specifications

4.24.3.1 ITU-T

Recommendation ITU-T G.9806 [i.99] describes a higher speed bidirectional single fibre point-to-point optical access system than the data rate in existing ITU-T point-to-point access systems. It supports 10 Gbits/s for the optical access services including the Optical Distribution Network (ODN) specification, the physical layer specification, services requirements and the Operation, Administration and Maintenance (OAM) specification. Amendment 1 added support for 25 Gbits/s and amendment 2 adds support for 50 Gbits/s.

Due to its effectiveness, the watchful sleep mode has been approved to be included in the Recommendation ITU-T G.984 [i.27] (G-PON) and Recommendation ITU-T G.987 [i.27] (XGPONs) standards.

4.24.3.2 IEEE

IEEE has defined the bi-directional access for 10 Gbits/s, 25 Gbits/s, and 50 Gbits/s in IEEE 802.3AZ [i.98]. Also it includes various energy saving mechanisms specified in Recommendation ITU-T G.9806 [i.99].

4.24.4 Gap analysis

4.24.4.1 Gap Context

In the present document the gaps refer to existing standards and not to technology in general. Some vendor's products that are not standardized could exist that implement the solutions described in the gaps.

4.24.4.2 General

Different specifications for bi-directional access network technologies exist in Recommendation ITU-T G.9806 [i.99] or IEEE 802.3CP [i.100].

[Gap 26-1] None.

4.24.4.3 Network Supervision

The F5G P2P Access Network already supports test and diagnostics technologies that does not affect service quality and availability.

[Gap 26-2] None.

The F5G P2P Access Network uses Received Signal Strength Indication (RSSI) measurements, the resolution, accuracy, repeatability and response time depends on the implementation and depending on the supervision algorithms the requirements for the metrics might be different.

[Gap 26-3] Exporting F5G P2P Access Network metrics to a controller is currently not standardized.

The F5G P2P Access Network monitoring and optical medium health check should be able to differentiate optical medium failures from transport system failures. Some of that is implementation dependent.

[Gap 26-4] None.

The F5G P2P Access Network key performance indicators shall be provided from the controller to the E2E F5G orchestrator in an abstract way.

[Gap 26-5] The interface and data model is currently not standardized.

4.24.4.4 Point to point link performance

Consideration need to be given to the fact that the OLT is localized in a central office. The coverage of this central office is defined by the Optical Distribution Network (ODN) and therefore the reach of the technologies can be derived from that.

The P2P access network technology needs the support up to 10 km, 20 km, or 60 km depending on the density of the area. Those are supported by the technologies.

[Gap 26-6] None.

[Gap 26-7] None.

[Gap 26-8] None.

The P2P access network technology is expected to support P2P bidirectional bit rates up to 100 Gbits/s. 50 Gbits/s is specified in amendment 2 of Recommendation ITU-T G.9806 [i.99].

[Gap 26-9] P2P bidirectional 100 Gbits/s is under study and needs to be specified.

Energy saving features are specified in Recommendation ITU-T G.9806 [i.99], providing energy saving mechanisms such as sleep periods as specified in IEEE 802.3AZ [i.98] and the watchful sleep mechanisms as specified in PON. In addition line rates can be switch in low duty times.

NOTE: The watchful sleep mode has been included in Recommendation ITU-T G.9806 [i.99] (G-PON) and Recommendation ITU-T G.987 [i.28] (XGPONs) standards.

[Gap 26-10] None.

4.25 High-speed Passive P2MP Network Traffic Aggregation

4.25.1 Use Case briefing

In the F5G Aggregation Network (AggN), the network topology is typically Point-to-Multi-Point (P2MP). High-speed passive P2MP network traffic aggregation is a novel approach to implement such network segments that offers benefits in terms of cost, complexity, and power consumption. Telecommunication networks have leveraged the benefits of Point-to-Multi-Point optics for decades in passive optical networks and within datacentres. PON networks have a single OLT optical interface that distributes bandwidth to multiple ONUs. Within the datacentres, optical breakout cables are used to reduce the spine port count. The total cost benefits of Point-to-Multi-Point in these applications extend beyond equipment costs to include more efficient use of space and power. If the same concepts can be adapted to coherent optics the potential benefits would be significant for mobile xHaul, aggregation and access networks.

Traffic aggregation such as OLT backhaul, mobile xHaul or enterprise access necessitates multiple edge nodes to be bi-directionally connected to a central node. In the traditional implementation, Point-to-Point (P2P) optical links connect N edge nodes with their corresponding central node via an Electrical Aggregation Unit (EAU). In such an implementation, 2*N optical transceivers are needed for the P2P connections between the edge nodes and the EAU and 2 full-band (aggregated bandwidth) transceivers are required for the P2P connection between the EAU and the central node. In addition, the EAU itself requires an additional power supply and an equipment room with sufficient ventilation or even air conditioning. As the aggregation network plays a major role in the overall network deployment, reducing its complexity is highly desirable to improve the cost effectiveness and energy efficiency of the network.

This use case describes a high-speed passive P2MP network traffic aggregation, where the central node is connected to multiple edge nodes through a passive optical splitter. In addition, this P2MP connection approach reduces the number of optical transceivers by half compared to the traditional P2P connection approach. With this approach, there is no requirement for the EAU and its associated power supply and equipment room. Thus achieving a simplified and energy-efficient aggregation network.

NOTE: The following description is focused on the scenario of mobile xHaul as this is a challenging application. However, other scenarios are interesting as well, including the F5G Aggregation Network.

4.25.2 Technology Requirements

4.25.2.1 Technology Description

The described use case brings with it several needs or requirements. Especially for mobile xHaul, best effort transport will not be sufficient.

The following features are required to implement high-speed passive P2MP network traffic aggregation:

First, a minimum total bidirectional throughput can be derived. This is different to a traditional backhaul infrastructure implemented with point to point links. Here, the capacity of the central note shall be designed sufficiently large to handle the aggregate traffic of all participants in the Point-to-Multi-Point architecture.

[R28-1] The total bidirectional throughput of the central node shall be sufficient for the deployment scenario.

Second, the system shall support a sufficient number of edge nodes for a given deployment scenario. This can be defined by the number of antenna sites in an area that is connected to a central node.

[R28-2] The total number of edge nodes supported shall be sufficient for the deployment scenario.

Third, in xHaul scenarios there will be a large throughput per antenna site. As a result the edge nodes shall support a large throughput in the order of up to 100 Gbits/s for 5G deployments.

[R28-3] The maximum throughput of each edge node shall be sufficient for the deployment scenario.

However, as antenna sites differ in number of antennas and overall bandwidth, the respective bandwidth requirements will differ significantly. Therefore, the edge nodes shall offer sufficient granularity to efficiently use the total capacity of the central node.

[R28-4] The bandwidth granularity of each edge node shall be sufficient for the deployment scenario.

As distances to antenna sites vary depending on densely populated or more rural areas, transmission distances of up to 20 km can easily occur. The maximum transmission distance between central nodes and edge nodes shall therefore be sufficient to cover a variety of scenarios.

[R28-5] The maximum transmission distance between the central node and an edge node shall be sufficient for the deployment scenario.

With Point-to-Multi-Point systems comes an additional challenge in configuring the edge nodes and connecting them to the central node. Among others, wavelength and frequency bands have to be configured and timing has to be aligned. This should occur mostly automatic to avoid increased complexity and additional truck rolls. Therefore, the system shall provide a control and management channel between central node and edge nodes.

[R28-6] A Control & Management (C&M) channel between the central node transceiver and the edge node shall be supported.

To integrate the Point-to-Multi-Point links into the overall network management, an adapted network level control and management mechanism for the central and edge nodes shall be provided.

[R28-7] Network-level C&M mechanism for the central node transceiver and the edge node transceivers shall be supported.

A Point-to-Multi-Point system consists of a large number of edge nodes connecting to central nodes. In dynamically configured all-optical networks, edge nodes could be reassigned to different central nodes. Also, an expansion of an existing network with additional edge nodes to increase coverage or central nodes to grow overall capacity is expected. Finally, in case of failure of one of the nodes, only this one failed node should be replaced. It is therefore necessary that an individual node can be replaced with a node from the same or a different vendor (in case the original vendor does not offer a suitable replacement). To ensure that such reassignments and upgrade paths are possible, vendor interoperability is required. Therefore, interoperability of edge nodes and central nodes of different vendors shall be guaranteed.

[R28-8] Multi-vendor transceiver interoperability between the central node and the edge nodes shall be guaranteed.

A last requirement relates to securing data in Point-to-Multi-Point infrastructures. To ensure data security, the system shall support securing data meant for one of the edge nodes from being intercepted by another edge node.

[R28-9] The transceivers shall provide a mechanism to secure network traffic meant for one of the edge nodes from being intercepted by another edge node.

Based on the characteristics of an aggregation network, the technical requirements may vary. For an exemplary 5G mid-haul aggregation network, the technical requirements may be specified as follows:

- 16 edge nodes supported per central node.
- 400-Gbits/s total bidirectional throughput of the central node.
- 100-Gbits/s maximum bidirectional throughput of each edge node.
- 25-Gbits/s throughput granularity of each edge node.
- 20-km maximum transmission distance between the central node and an edge node.
- 20-dB minimum loss budget between the central node and an edge node.
- CFP2 form factor for the central node transceiver.
- QSFP-DD form factor for the edge node transceiver.
- Automatic communication between transceivers via the C&M channel.
- Software-defined flexible bandwidth allocation via the overall C&M of the P2MP system.
- Open interfaces that ensure multi-vendor interoperability.

4.25.3 Current related standards

Standardization of related technologies is currently being discussed in multiple standardization bodies. The IOWN forum [i.93] is working towards defining P2MP capabilities in their Open all-phontonic network standards documents. Also, multiple parties have brought contributions to ITU-T, however, the path forward for standardization in ITU-T is still being defined.

Currently, there are no standards related to the high-speed passive P2MP network traffic aggregation use case. There is a Multi-Source Agreement (MSA) working group for P2MP coherent pluggable transceiver technology (XR optics), named the Open XR Forum [i.91]. The Open XR Forum's mission is to "foster collaboration that will advance development of XR optics-enabled products and services, accelerate adoption of intelligent coherent P2P and P2MP network architectures, and drive standardization of networking interfaces to ensure ease of multi-vendor interoperability and an open, multi-source solution ecosystem". The Open XR Forum's focus points are [i.92]:

- To define compatibility requirements with host devices.
- To establish interoperable network and hardware interfaces.
- To enable software-configurable bandwidth.
- To demonstrate interoperability.
- To advance open management interfaces.

- To establish a supply chain ecosystem that provides assurance of supply and serves diverse applications and geographic markets.
- To enable technology licensing programs.

4.25.4 Gap analysis

4.25.4.1 Gap Context

In the present document the gaps refer to existing standards and not to technology in general. Some vendor's products that are not standardized could exist that implement the solutions described in the gaps.

4.25.4.2 Gap Description

Due to the lack of global standards on the high-speed passive P2MP network traffic aggregation use case, the following gaps need to be bridged to enable this use case to be widely supported in F5G networks.

The minimum total bidirectional throughput for P2MP traffic aggregation for the different scenarios such as 5G mid-haul, aggregation, and Data Centre Interconnect (DCI), etc., has not yet been clearly identified.

[Gap28-1] Bidirectional throughput requirements for high-speed passive P2MP network traffic aggregation in the F5G AggN segment, have not been clearly identified.

Lack of the architectural design of coherent Frequency-Division Multiple Access (FDMA) based passive P2MP network traffic aggregation.

[Gap28-2] A standard architecture for high speed P2MP networks is currently not defined.

In mobile xHaul scenarios, a clear definition of maximum throughput for edge nodes is required to support 5G deployments.

[Gap28-3] The maximum throughput for P2MP transceivers connecting 5G antenna sites is currently not defined.

As antenna sites differ in RF bandwidth and number of antennas, granular adaptation of bandwidth is required. The required granularity for P2MP systems needs to be clearly identified.

[Gap28-4] The bandwidth granularity for P2MP transceivers connecting 5G antenna sites is currently not defined.

As antenna sites are placed more sparsely and densely depending on the conditions and capacity requirements in an area, distances vary significantly.

[Gap28-5] The maximum distance that P2MP transceivers connecting 5G antenna sites need to cover is currently not defined.

Coherent P2MP systems face the challenge to align and configure edge nodes to interface with a central node without requiring manual configuration and alignment. The optical functions need to be managed in a way that represents the optical functions in a common way across all segments of the network. This is especially challenging as transceivers of P2MP systems could be pluggable modules that are directly plugged into network equipment like routers and servers.

[Gap28-6] A Control & Management (C&M) channel between the central node transceiver and the edge node is currently not defined.

To integrate P2MP systems in current management systems, modified network level control and management mechanisms are required. While models exist for the access network segment, they need to be adapted and applied to other network segments like the aggregation network.

[Gap28-7] A network-level C&M mechanism for the P2MP systems in the aggregation network is currently not defined.

Multi-vendor interoperability is a key requirement to leverage the benefits of P2MP communications as detailed in the technology requirements clause above.

[Gap28-8] The enabling of multi-vendor interoperability of central node and edge node transceivers is currently not standardized.

To ensure data protection in a P2MP communication system, communication from central to edge nodes needs to be protected against being intercepted by other participants in the P2MP network (e.g. other edge nodes).

[Gap28-9] A mechanism to prevent the interception of data transmitted in the P2MP network is currently not standardized.

4.26 Bandwidth on demand

4.26.1 Use Case briefing

Bandwidth on demand enables the user to request the operator for a specific required bandwidth. The request can be for an instant change of bandwidth or could also be a scheduled change. Users of services such as Online gaming, UHD videos and periodic data backups can benefit from such a feature. Users of said services are probably not inclined to upgrade their existing subscription permanently, because the moments they require more bandwidth are sporadic. However, they might be interested in temporarily boosting their bandwidth, if the underlying PON system allows for it. To realize this use case, operators should have the ability to manage bandwidth in the network dynamically.

4.26.2 Technology Requirements

4.26.2.1 General introduction

The main motivation behind bandwidth on demand is to cater the needs of users who often have highly varying and sometimes even bursty bandwidth requirements. While users are traditionally allocated a constant bandwidth, their needs can result in requirement of high bandwidth for a short period of time while a low bandwidth could suffice during other periods. The on-demand allocation of bandwidth can be done either based upon user's request or based on intelligence in the network.

A key point is that bandwidth on demand is about a temporary change in addition to possibly guaranteed bandwidth allocation to a user.

4.26.2.2 Relation to scenario-based broadband

At first glance there is an overlap between the bandwidth on demand use case and the scenario-based broadband use case. Both scenario-based broadband and bandwidth on demand use cases provide means to optimize the network bandwidth, and both use cases describe AI to do this.

There are however significant differences, and both use cases are complementary with respect to each other.

Overall, the Bandwidth on demand use case is user-centric, whereas the scenario-based broadband use case is application centric. Specifically, in case of bandwidth on demand, a user can explicitly request for an increase or decrease of bandwidth which is not possible in scenario-based broadband.

Artificial Intelligence (AI) is used to identify the applications in scenario-based broadband while it may be used in the bandwidth on demand use case to predict the behaviour of users' bandwidth consumption.

The bandwidth on demand use case focuses on utilizing available resources at the time of request whereas in scenario-based broadband there are guarantees for different types of scenarios and applications.

Furthermore, the scope of bandwidth on demand is limited to network bandwidth (bitrate) and the on-premises network domain is out of scope. Scenario based broadband covers a broader range of network aspects including latency and includes the on-premises network domain.

An important effect of the overall difference (user centric vs application centric) is that privacy requires more attention in bandwidth on demand. In scenario-based broadband, as long as individual applications cannot be traced back to users, privacy can be preserved.

4.26.2.3 User-based Bandwidth change requests

A user can send a request to the network for a temporary increase or decrease in bandwidth. For cases such as periodic backups, online gaming, download of large files/software updates, the user can specify the time slot in which a short-term increase in bandwidth is required. Users may also request a decrease in bandwidth while the usage is predicted to be low or when they are not at home.

[R30-1] The F5G network should support temporary bandwidth user change requests.

4.26.2.4 Network-based Bandwidth change requests

An intelligent network which assesses the behaviour and requirements of user and subsequently allocates bandwidth changes intelligently and autonomously, could be an alternative to the user-initiated allocations mentioned in previous clauses. This assessment can be done in various ways, for instance, it can be based on traffic patterns of the user or source and destination of the traffic. For the latter example, the user may select the services for which bandwidth on demand is enabled.

In scenarios, where a user needs a high amount of bandwidth instantly for a short time slot (e.g. downloading a file), a boost in bandwidth can be provided by the network without user's intervention. This would avoid the complexity for the user to perform the request and receive the desired bandwidth. Additionally, it would enhance the user's experience. For instance, if the user wants to download and use software, the network can autonomously request and allocate a high bandwidth (if available) for a short period of time (e.g. a couple of seconds) during this download.

[R30-2] The F5G network should support temporary bandwidth change requests initiated by an intelligent entity within the network or from the management plane.

4.26.2.5 Allocation of bandwidth changes

The network should also monitor available resources and traffic of other users sharing the same access network. It should prioritize and allocate the optimum amount of bandwidth to avoid unintended consequences to other users.

[R30-3] The F5G network shall support bandwidth allocation based on F5G network resources availability and priority.

4.26.2.6 Privacy

To act autonomously, the network will have to understand and predict the user's behaviour. To reach such an understanding would involve looking at the user's traffic and patterns to predict required bandwidth. This gives rise to various privacy challenges.

Overall, the network should allow to preserve the user's privacy while it is assessing the behaviour to allocate bandwidth. Therefore, techniques such as data anonymization, data masking should be employed so that users are not individually identifiable and traceable. The network should only use the metadata of the traffic generated by user to make its decisions. It should still be possible for the network to distinguish between the users to allocate bandwidth accurately.

[R30-4] The F5G network function that assesses user traffic/ behaviour should only use metadata of F5G network traffic. In addition the F5G network shall not be enabled to individually identify and trace users.

4.26.3 Current related standard specifications

4.26.3.1 ITU-T

Recommendation ITU-T Q.3715 [i.128] (produced by ITU-T Question of Study Group 11) provides an architectural recommendation including signalling requirements to implement dynamic bandwidth adjustment (increase/decrease) based on user's demand with the help of Software Defined Networking (SDN). The proposed architecture consists of a service platform, a controller and network gateway. The controller is connected to operational support system and a billing system. The subscriber directly requests the service platform to adjust his/her bandwidth. The controller receives this request from service platform, assesses if such a request can be fulfilled and acts accordingly.

4.26.3.2 BBF

BBF TR-144 [i.129] by broadband forum provides a set of requirements that an architecture shall comply with in order to support bandwidth on demand. The requirements are: Bandwidth on demand should be supported based on requests from user as well as the application of the user. Bandwidth on demand should also be fulfilled in near real time and should coordinate with resource admission control.

4.26.3.3 ETSI

ETSI TR 182 022 [i.131] presents an overall analysis of architectural requirements for QoS reporting and resource monitoring and describes a service that could fulfil the user's need of higher bandwidth for a limited period upon explicit request. Such a service provides user with options to boost bandwidth in both unidirectional and bidirectional ways. The request by user can be for a specific type of content (e.g. a video boost) or for a specific period of time or a service.

4.26.3.4 Artificial Intelligence

Refer to clause 5.6 about current status of AI.

4.26.4 Gap analysis

4.26.4.1 Gap Context

In the present document the gaps refer to existing standards and not to technology in general. Some vendor's products that are not standardized could exist that implement the solutions described in the gaps.

4.26.4.2 User-based Bandwidth change requests

The current standards mentioned in the previous clauses support dynamic bandwidth allocation and propose architectures to support such a system. Users can explicitly request increase in bandwidth with various options such as type of content, duration, for a particular time slot. While Broadband forum and ITU-T consider the billing of such a system in their architecture, ETSI leaves it out of their scope.

[Gap30-1] None.

4.26.4.3 Network-based Bandwidth change requests

The systems proposed in current standards work only upon explicit user's request. Such requests can be additionally supported by network acting autonomously. Existing standards focus on user-initiated bandwidth change requests whereas network-initiated requests are missing.

[Gap30-2] In the F5G network intelligent functionality to autonomously allocate user bandwidth is currently not defined.

4.26.4.4 Allocation of bandwidth changes

Allocation of bandwidth in the existing standards consider the existing resources of the network.

[Gap30-3] Same as [Gap10-10].

4.26.4.5 Privacy

Existing standards do not address the need for privacy of users. This can be an important aspect, for instance if a user requests to lower the bandwidth for the weekend since they are not at home, the compromise of such an information shall lead to problems to the user.

The intelligent network might also realize that the user is starting to stream a high-quality video and would increase the bandwidth temporarily. However, such an information about the user should be anonymized.

[Gap30-4] Privacy of the user is not considered in the design and architecture of existing standards.

4.27 Intelligent Optical Cable Management

4.27.1 Use case briefing

In ETSI GR F5G 008 [i.75], problems of current optical cable management system are introduced by use case #31:

1) Optical cable route information is managed and maintained manually, which makes it difficult to ensure its accuracy. For example, errors may occur during manual input of cable Shared Risk Link Group (SRLG) information, which may cause the problem that the working fibre and protection fibre are collocated in the same cable.

2) Optical cable routes are not currently associated with Geographic Information System (GIS) information. So as a result, optical cable faults cannot be located accurately.

3) Optical cable quality is monitored manually: Therefore, optical cable degradation cannot be predicted and detected in a timely manner, leading to reactive maintenance, after the fault occurs, being the usual response.

In summary, the current optical cable management accuracy and troubleshooting efficiency is low, which increases the risk to service operation and may have a significant impact on service availability.

4.27.2 Technology Requirements

4.27.2.1 Automatic identification of shared-route

An optical network connection (e.g. an Optical Data Unit (ODU) connection or a wavelength connection) goes through one or multiple fibres in the physical layer. To ensure that the physical fibre routes of each pair of working and protection connections are separated from each other, additional technical mechanisms need to be introduced to automatically detect the physical co-route information (e.g. same cable, same trench or same duct), and to generate the SRLG information.

[R31-1] The F5G Optical Transport Controller shall support collecting the physical fibre SRLG information.

Once the SRLG information is updated in the Optical Transport Controller, it can analyse if there are any fibre pairs of working and protection connections which share the same physical route. If yes, it may trigger the optimization process to reroute the working and/or protection connection to avoid physical co-route, according to the operator's policies.

[R31-2] The Optical Transport Controller shall support optimizing the working and protection connection routes based on the updated SRLG information.

4.27.2.2 GIS-based optical cable management

To enable the fault localization to street level, the Optical Transport Controller needs to get the Geographic Information System (GIS) information of the optical cables.

[R31-3] The Optical Transport Controller shall support obtaining the GIS information of the optical cables.

4.27.2.3 Real-time fibre quality monitoring and health prediction

The fibre quality needs to be monitored in real time by the optical Network Elements (NEs), and the health status of the fibre needs to be evaluated. In this way, potential fibre degradation can be predicted before a fibre fault occurs, and therefore proactive operation and maintenance is enabled.

[R31-4] The Optical Transport Controller shall support evaluating the health status of the fibres.

Once fibre degradation is determined, and a possible fibre failure and failure time is predicted, the Optical Transport Controller may report an advance warning to the F5G E2E Orchestrator, and the orchestrator may automatically reroute the optical connections, which go through the degraded fibre, according to operator's policies.

[R31-5] The Optical Transport Controller should support reporting advance warning to the F5G E2E Orchestrator, to indicate the predicted fibre failure.

[R31-6] The Optical Transport Controller should support rerouting the optical connection which goes through a degrading fibre.

4.27.3 Current related standard specifications

4.27.3.1 Overview

Currently there are no related standards specifying how the physical route information and GIS information of the optical cables are intelligently collected and managed. There are also no related standards specifying how to predict fibre health status.

However, once it is decided to reroute an existing optical connection because of the co-route issue or fibre health status, the existing IETF standardized reroute procedures (see note) can still be applied.

NOTE: The Optical Transport Controller can act as a stateful PCE, and use the extended PCEP to maintain the route information of each pair of working and protection connections, and to update the routes of the working and/or protection connections to avoid physical co-route. See clause 4.27.3.2.

4.27.3.2 IETF

IETF RFC 8231 [i.101] describes the functions of the stateful Path Computation Element (PCE), and defines the protocol extensions to the Path Computation Element communication Protocol (PCEP) to support stateful PCE. With the extended PCEP, A stateful PCE can learn the status information of the connections in the network. Furthermore, a created connection can be delegated to a stateful PCE, so that the stateful PCE has the right to update the connection attributes such as bandwidth and route, via the extended PCEP.

4.27.4 Gap analysis

4.27.4.1 Gap Context

In the present document the gaps refer to existing standards and not to technology in general. Some vendor's products that are not standardized could exist that implement the solutions described in the gaps.

4.27.4.2 Automatic identification of shared-route

Currently there are no standards mechanisms on how the physical co-route information is detected and how the SRLG information of the fibres is generated, because currently these are vendor/operator specific, and do not need to be standardized.

[Gap31-1] None.

Once there is a pair of working and protection connections sharing the same physical route, the Optical Transport Controller, which acts as a stateful PCE, may trigger the rerouting of the working and/or protection connections using the extended PCEP.

[Gap31-2] None.

NOTE: How the Optical Transport Controller analyses the co-route connections and calculates the routes optimization are internal functions of the Optical Transport Controller, and do not need to be standardized.

4.27.4.3 GIS-based optical cable management

Normally manual operation is needed when discovering the GIS information of the optical cable routes. Specific tools may be used to ease the assist operators to discover the GIS information. The discovery mechanism assistance is vendor/operator specific and do not need to be standardized.

[Gap31-3] None.

4.27.4.4 Real-time fibre quality monitoring and health prediction

Currently there are no standards introducing how the health status of the fibre is predicted and evaluated by the optical NEs and/or the Optical Transport Controller, because it depends on vendor-specific algorithms, and does not need to be standardized.

[Gap31-4] None.

IETF is working on the YANG data models for the North Bound Interface (NBI) of a generic Traffic Engineering (TE) network controller, for the management and control of the TE network, including the optical network.

Currently the developed and being developed NBI YANG data models in IETF are mainly for the support of topology discovery, connection control, service provisioning and network slice management. The YANG data model for reporting the predicted optical failure information has not been considered by IETF.

[Gap31-5] Currently there is no standard YANG data models for reporting the predicted optical failure information by an Optical Transport Controller.

As described in clause 4.27.3.1 of the present document, the Optical Transport Controller can act as a stateful PCE, to modify the route of an optical connection which goes through a degrading fibre, using the extended PCEP.

[Gap31-6] None.

4.28 AI-based PON optical path diagnosis

4.28.1 Use case briefing

The occurrence of PON path fault leads to the interruption of network service, mainly appearing as weak optical signal in the F5G PON Access Network (due to low transmission power, large ODN insertion loss, etc.). A number of fault incidents could occur, such as frequent association and disassociation of the ONU, an unstable connection with high bit error rate, which significantly affects the service experience for the user.

The optical path fault is not easy to locate and demarcate. The traditional method uses the Element Management System (EMS) to collect the optical power information from the connected ONUs in the F5G PON Access Network. The fault is then manually located and network recovery determination is made. Due to poor ODN topology information in the EMS, the problem identification requires additional on-site examination to locate the fault. An experienced technician may not resolve the cause of the fault completely, leading to further problem in the future.

By using comprehensive data collection in the F5G PON Access Network and applying AI-based algorithm analysis, the faults can be fully classified and modelled, leading to automatic fault prediction and real-time fault diagnostics.

4.28.2 Technical requirements

4.28.2.1 General introduction

AI-based diagnostic technology identifies the root cause of the path fault, analyses the impact of the weak optical signal, generates a rectification list, and automatically creates the historical connection status of the F5G PON Access Network. In addition, the AI-based diagnostic technology support further analysis of the fault, including feature extraction, fault identification, fault repairing recommendation, etc. By using this technology, it is expected that the efficiency of fault diagnostics will significantly improve and the accuracy of the AI-based technology fault diagnostics can be verified and tracked.

4.28.2.2 Visualization of optical power in the PON network

The visualization of optical power in a PON network is a basic function. Figure 19 shows an example of continuous collection over 48 hours of optical signal power in a PON network with a single optical slitting point. As can be seen in Figure 19, the power trend needs frequent data collection and the power distribution of different users could be very different.

[R32-1] The AI-based diagnostic technology shall support the optical power visualization in the F5G PON Access Network.

[R32-2] The AI-based diagnostic technology shall support the recognition of optical signal fluctuating regulation and initiate an alarm.

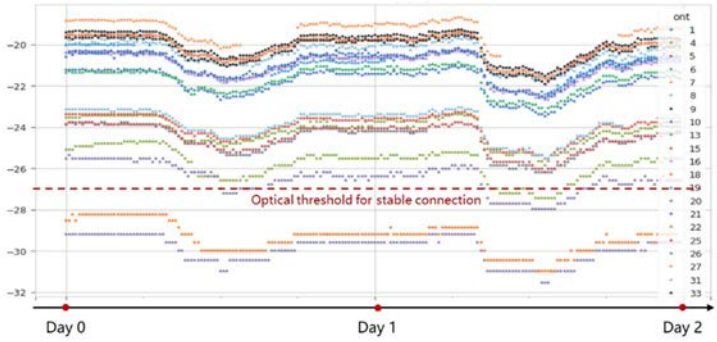


Figure 19: The visualization of the optical power in PON network

4.28.2.3 Data collection

The AI based model training and fault determination system requires a large volume of data. In addition, the real-time data collection helps to diagnose the fault quickly and trigger the appropriate action to resolve all the problems that were found. The AI-based diagnostic technology needs to be capable of data collection within a 15 minutes time period, in order to accurately capture the network problem. In addition, the AI-based diagnostic technology needs to be capable of running fault identification on an hourly basis in the F5G PON Access network.

[R32-3] The AI-based diagnostic technology shall support data collection within a 15 minutes time period.

[R32-4] The AI-based diagnostic technology shall support fault identification on an hourly basis in the F5G PON Access network.

4.28.2.4 Path fault identification and strategy generation

The AI-based diagnostic technology should be capable of identifying the fault type based on the optical signal status in the F5G ODN network (such as feeder, branch, or drop fibre) and power level in the transceiver of both the OLT and the ONU. The AI-based diagnostic system shall recommend solutions for the engineer to maintain or repair the F5G PON Access network.

[R032-5] The AI-based diagnostic technology shall support fault localization in the F5G PON Access network.

[R032-6] The AI-based diagnostic technology shall support the generation of fault recovery solution, with step-by-step repair procedure and the corresponding impact analysis on the network services.

[R032-7] The AI-based diagnostic technology shall support the generation of an optimized action list based on the deployed service priorities and the number of affected users.

4.28.3 Current related standard specifications

4.28.3.1 Broadband Forum (BBF)

The Broadband Forum (BBF) specifies the application layer protocol in BBF TR-069 [i.22] and BBF TR-369 [i.22] specifies the remote management and provisioning of Customer Premises Equipment (CPE) network. The corresponding data model is defined in BBF TR-181 [i.23]. BBF TR-181 [i.23] defines a software object "Device.Optical." to model the optical interface technology, and the reporting of optical based attributes, such as total downstream optical signal level (OpticalSignalLevel), mean optical launch power (TransmitOpticalLevel), etc.

Moreover, BBF TR-369 [i.24] User Service Platform (USP) is a standardized protocol for managing, monitoring, upgrading, and controlling connected devices. It allows service providers and consumer electronics manufacturers to develop applications that gather the telemetry necessary for large scale data processing, AI, and machine learning. USP represents the natural evolution of the Broadband Forum's CPE WAN Management Protocol (CWMP), commonly known as BBF TR-069 [i.22].

4.28.3.2 ITU-T framework standards

ITU-T SG15 Q2 Recommendation G.988 [i.29] (ONU Management and Control Interface (OMCI) specification) has defined the data collection interface between OLT and ONU in the F5G PON Access Network. The OMCI specification addresses ONU configuration, fault management and performance management for optical access system operation, and for several services. Specifically, the Access Network Interface (ANI) includes the management of each physical PON interface, which provides the quantitative read-or-write parameters for optical signalling in the F5G PON ODN, such as optical signal level, lower optical threshold, transmit optical level, etc. In addition, the OMCI message is encapsulated and transmitted in the Transmission Convergence (TC) layer. The data collection of the ONU could be done in real-time by leveraging the PON access link.

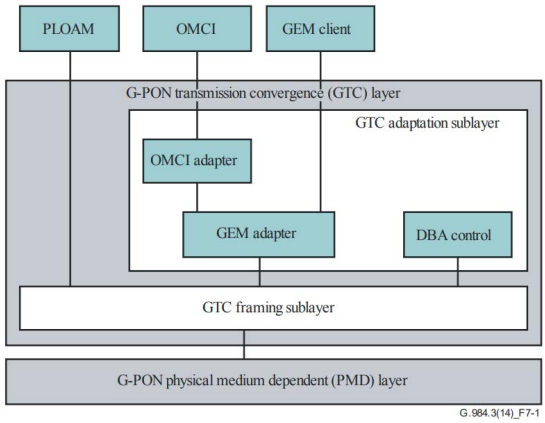


Figure 20: PON protocol framework
(Source: Recommendation ITU-T G.984.3 [i.94])

A number of ITU-T focus groups has initiated research into the introduction of AI and Machine Learning (ML) to optimize network operations and increase energy and cost efficiency. A number of framework recommendation are published, such as Recommendation ITU-T Y.3172 [i.3] (an architectural framework to integrate ML into 5G and future networks), Recommendation ITU-T Y.3174 [i.4] (a framework for data handling in support of ML), etc. The algorithms implemented in the network are usually vendor specific.

4.28.3.3 ISO/IEC JTC1 SC42

ISO/IEC JTC1/SC 42 [i.178] is working on the standard area for AI, serving as the focus and proponent for JTC1's standardization program on Artificial Intelligence and providing guidance to JTC1, IEC, and ISO committees developing Artificial Intelligence applications. More than ten standards have been published, focusing on the fundamental concept of AI architecture and functions.

4.28.3.4 ETSI

ETSI ISG F5G has published ETSI GS F5G 011 [i.179] to define the F5G Telemetry Framework and Requirements for the F5G Access Network. Another project ETSI GS F5G 016 [i.180] Telemetry Models is under development. This study intends to define data models of telemetry for F5G Access Network.

4.28.4 Gap analysis

4.28.4.1 Gap Context

In the present document the gaps refer to existing standards and not to technology in general. Some vendor's products that are not standardized could exist that implement the solutions described in the gaps.

4.28.4.2 General

The AI-based diagnostic technology uses AI capabilities to improve fault diagnostic of the F5G PON Access Network. The data collection protocol should support the requirements mentioned above while the AI algorithm for modelling and determination is vendor specific. The operation of AI function typically is located in the network management system of a cloud platform.

4.28.4.3 Visualization of optical power in the PON network

The visualization of optical power in the F5G PON Access Network needs the support of telemetry data models for the F5G access network. The current protocols support different ways to obtain transient optical power characteristics in the PON network. The recognition of the optical signal fluctuation and corresponding alarm based on AI is in the network management system needs to be supported.

[Gap32-1] None.

[Gap32-2] The recognition of the optical signal fluctuation and corresponding alarm generation based on AI is currently not supported in the network management system standards.

4.28.4.4 Data collection

There are many protocols that could support data collection from OLT and corresponding ONU in the order of tens of minutes. However, AI functions and relevant requirements are not specified yet.

[Gap32-3] None.

[Gap32-4] The periodic fault identification capability based on AI is currently not supported in the network management system standards.

4.28.4.5 Path fault identification and strategy generation

Accurate localization of fault and the creation of recovery solution reflects the intellectualization of the network management system. AI technology needs to provide E2E solution to enable fault detection, localization and recovery.

[Gap32-5] The fault localization function based on AI analysis is not currently supported in the network management system standards.

[Gap32-6] The generation of fault recovery solution based on AI analysis is currently not supported in the network management system standards.

[Gap32-7] The generation of an optimized action list based on AI analysis is currently not supported in the network management system standards.

5 Status Quo of Major Related Technologies

5.1 Wi-Fi® 6 (802.11ax)

From 2014, the IEEE 802.11 working group began to solve the problem of low efficiency of the entire Wi-Fi® network caused by access of more terminals, and they are expected to release IEEE 802.11ax [i.52] in 2020. One of the goals of IEEE 802.11ax [i.52] is to increase the average user throughput by at least four times and increase the number of concurrent users by more than three times in the dense-user environment compared with IEEE 802.11ac [i.61]. Wi-Fi® 6 is short for the IEEE 802.11ax [i.52] standard.

Wi-Fi® 6 inherits all the advanced MIMO features of Wi-Fi® 5 and introduces many new features for high-density deployment scenarios. The following are the new core features of Wi-Fi® 6:

- OFDMA technology.
- DL/UL MU-MIMO technology.

- Higher-order modulation technology (1 024-QAM).
- Spatial Reuse (SR).
- Basic Service Set (BSS) colouring mechanism.
- Extended Range (ER).

Wi-Fi® 6 represents the high speed of WLANs. This high speed is determined by the following factors:

Calculation formula:

Speed = Number of spatial streams x 1/(Symbol + GI) x Encoding scheme x Bit rate x Number of valid subcarriers

1) The maximum number of spatial stream of Wi-Fi® 6 can reach up to 8.
2) Wi-Fi® 6 symbol length is 12,8 µs. Wi-Fi® 6 supports 0,8 µs, 1,6 µs and 3,2 µs GIs.
3) Wi-Fi® 6 supports the higher-order coding 1 024-QAM.
4) Compared with the Wi-Fi® 5, bit rates supported by Wi-Fi® 6 added two more:
   - 3/4 for MCS10; and
   - 5/6 for MCS11.
5) The minimum subcarrier of Wi-Fi® 6 is 78,125 KHz. And different frequency bandwidth has different number of valid subcarriers, 234, 468, 980 and 2 × 980 for 20 MHz, 40 MHz, 80 MHz and 160 MHz, respectively.
6) Different bandwidth and spatial streams provide different throughput rates, as shown in Table 26.

Table 26: Throughput Rates

Bandwidth (MHz)	Spatial Stream	1/(Symbol + GI)	Number of Bits in a Symbol	Bit Rate	Number of Valid Subcarriers	Rate
80	1	1/(12,8 µs + 0,8 µs)	10	5/6	980	600 Mbps
	2				980	1,2 Gbps
	4				980	2,4 Gbps
	8				980	4,8 Gbps
160	1				2 × 980	1,2 Gbps
	2				2 × 980	2,4 Gbps
	4				2 × 980	4,8 Gbps
	8				2 × 980	9,6 Gbps

5.2 Ten gigabit passive optical network: XG(S)-PON

Ten gigabit passive optical networks (XG-PON) technologies have been under development in ITU-T Study Group 15 Question 2. The work on XG-PON (which is 10 G down and 2,5 G upstream) occurred from 2007 to 2010, and resulted in the G.987 series of recommendations. This system was intended as the follow-on to the very successful gigabit (G-PON) system (Recommendation G.984 series [i.27]), and it used a wavelength plan and loss budget that allowed coexistence of XG-PON and G-PON on the same fibres. XG-PON also used the same ONU management and configuration interface (the OMCI, defined in Recommendation ITU-T G.988 [i.29]). Fundamentally XG-PON was simply a speed-up version of G-PON. The primary service scenario for both G-PON and XG-PON was residential access services, and it was this reason that caused the selection of the asymmetric system for cost reasons.

Later in 2015 to 2016, the symmetric XGS-PON was developed into the Recommendation ITU-T G.9807.1 [3]. This second development was driven by two factors. First, the bandwidth demands on PON systems were increasing because they were being used to handle a wider set of use cases (such as FTTbusiness and FTTwireless). Second, the cost of 10 G optics has decreased greatly over the intervening years, making them far more affordable. This system shared the same wavelength plan as XG-PON, therefore inheriting its coexistence capabilities. The downstream signals of both systems and the upstream Media Access Control (MAC) were identical for XG-PON and XGS-PON, and this allowed TDMA coexistence between them, where a hybrid XG- and XGS-PON Optical Line Terminal (OLT) could drive a PON that supported both XG-PON ONUs and XGS-PON ONUs. Thus, triple coexistence between G-PON, XG-PON, and XGS-PON was possible, as illustrated in Figure 21.

All of these systems share a common traffic model that is described in their Transmission Convergence (TC) layer recommendations. User traffic flows are assigned Port-IDs, and these have a one-to-one connectivity through the PON. Port-ID are contained within traffic containers (T-CONTs). The preferred arrangement is to have four T-CONTs per ONU, and these represent the different priorities of traffic. The ONU classifies the incoming user data into the appropriate Ports-IDs and T-CONTs. The OLT collects traffic reports from all the ONUs on the amount of traffic waiting in each T-CONT buffer. The OLT then uses an algorithm to fairly assign bandwidth to all the T-CONTs. In this way, the QoS for the user traffic can be ensured.

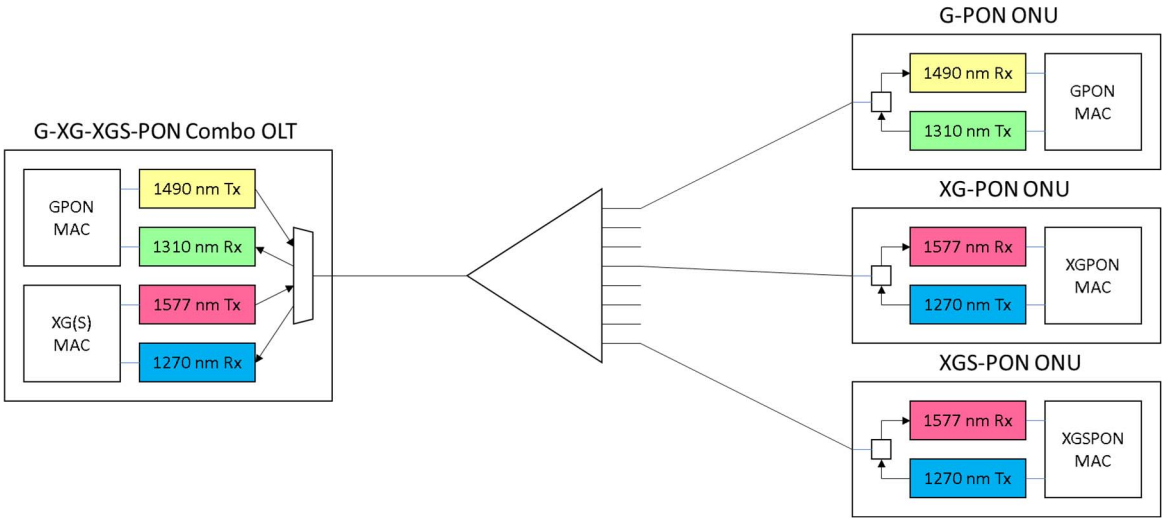


Figure 21: Triple coexistence in the ITU-T PON framework

As the PON network extends over a wide area and is accessible to many actors, the issue of security is important. There are two major parts to this: data transmission security and equipment authentication security. Transmission security is necessary because the PON is a broadcast system, and all traffic arrives at every ONU. The user data is encrypted using the Advanced Encryption Standard (AES), and there is a protocol to rapidly exchange keys between the ONUs and OLT. Equipment security is accomplished by executing a three-way authentication between the OLT and ONU. Once completed, both sides can be sure of the identity of the other. Additionally, the control messages on the PON are authenticated to avoid spoofing.

There are several other features of note for ITU-T PON systems. PONs can support network protection with a couple of architectures. Type B protection duplicates the OLT and feeder fibres, connecting them to a 2:N splitter. Only one OLT should be activated at any one time. Type C protection duplicates the entire PON: two OLTs, two Optical Distribution Networks (ODNs), and dual interfaces on the ONUs. This scheme allows for double capacity during normal operation, then falling back to a single capacity during a failure. The PON protocol can support power saving for the various components of the ONU. The ONU can shut down its UNIs if they are not being used, if enabled by the OLT. The ONU can also put its ANI to sleep under the control of the OLT. Either side can reactivate the ANI when traffic arrives.

The standards that define XG(S)-PON describe the fibre interfaces of the system; however, there is a lot more to an access system than these interfaces. The OLT equipment can come in several forms. A chassis based OLT typically supports 16 line cards (each line card can support 16 PON ports), and is placed in the central office. Smaller OLTs might support as little as two line cards, and is typically located in a remote site (e.g. a cabinet). The most extreme case is a small fixed OLT that is designed for outdoor installation. Regardless of the form factor, the OLT performs a central role as the aggregator of all the access traffic, typically using layer 2 techniques of Ethernet bridging and virtual LANs. Aggregation is important to reduce the number of data interfaces presented to the core network. The OLT also manages all of its subtending Optical Network Units (ONUs), using the OMCI protocol. There can be a variety of PON types supported by the OLT, and some equipment is capable of supporting several PON types on a single port. Resource slicing is also an important feature to allow the allocation of the OLT's capabilities into multiple groups, such that disparate requirements can be met, and independent control can be implemented.

Similarly, the ONU supports a wide range of variations. Simple residential ONUs might have just a single Ethernet UNI port. More elaborate ones typically have multiple data and telephone UNIs, and sometimes even a video UNI. For multiple dwelling unit applications, ONUs are typically a much larger rack-mounted equipment that have multiple UNIs. Most ONUs are designed to operate inside the customer's premise, and resemble consumer electronic devices; however, some ONUs shall be ruggedized to operate in the outdoor environment. All modern ONUs are typically powered locally from the customer's AC power. Since this power is not 100 % reliable, many ONUs are fitted with power back-up equipment (i.e. batteries). All ONUs shall support the OMCI management system for lower layer functions (Access Network Interface (ANI) and User Network Interface (UNI) management, and layer 2 connectivity). Higher layer functions (like telephony services, layer 3 routing) can be managed either using the OMCI or using an "over the top" mechanism, such as BBF TR-069 [i.22]. Interoperability between OLTs and ONUs of multiple types and from multiple vendors is a very important feature. The BBF has promoted interoperability through the development of BBF TR-156 [i.54] and BBF TR-167 [i.55] that describe the compliance requirements for ONUs, BBF TR-247 [i.53] which defines the test plan to confirm ONU compliance, and BBF TR-255 [i.66] that describes the interoperability test plan for PON systems.

5.3 Optical Transport Network (OTN)

Optical Transport Network (OTN) is defined by ITU-T as a set of optical network elements connected by optical fibre links, capable of providing functionalities such as transport, multiplexing, switching, management, supervision, and survivability of optical channels carrying client signals. OTN wraps each client signal transparently into a container for transport across optical networks, preserving the client's native structure, timing information, and management information.

OTN supports Wavelength-Division Multiplexing (WDM) of optical channels with various line rates. Recommendation ITU-T G.709 [i.67] has standardized Optical Transport Unit (OTU) ranging from 2,66 Gbits/s (OTU1) to 112 Gbits/s (OTU4)) and n × 105 Gbits/s (OTUCn). The client signals are wrapped into optical data units (ODUs) whose nominal data rates include 1,25 Gbits/s (ODU0), 2,5 Gbits/s (ODU1), 10 Gbits/s (ODU2), 40 Gbits/s (ODU3), 100 Gbits/s (ODU4)), and any-rate ≥ 1,25 Gbits/s ODUflex. These ODUs are transported over ODU links with 1,25 Gbits/s or 5,24 Gbits/s tributary slots. The OTUCn are carried over Flexible OTN (FlexO G.709.1) interfaces that provide bonding capabilities. The major benefits provided by OTN include universal container supporting multiple service types and enhanced Operation, Administration and Maintenance (OAM) for wavelength channels.

OTN-based core and aggregation networks offer advantages over traditional WDM transponder-based networks, by providing enhanced OAM features such as embedded communication channel, performance monitoring, fault detection, forward error correction, and multiplexing of lower rate client signals into higher speed payloads. The IP-over-OTN architecture also offers reduced hops, better management and monitoring, and increased protection of services.

In the scope of F5G, OTN plays an important role in traffic aggregation and transport. To address the need for aggregating a diverse set of services, an Optical Service Unit (OSU) is under specification by ITU-T to reduce the bandwidth granularity from 1,25 Gbits/s down to 2 Mbits/s. To transport the ever-increasing network traffic, OTN is evolving to support beyond 400 Gbits/s per wavelength channel, achieving an aggregated per-fibre transmission capacity of over 40 Tbits/s when wider bandwidth optical amplifiers are used. To reduce the transport latency and energy consumption, Optical Cross Connect (OXC) with multi-degree Reconfigurable Optical Add/Drop Multiplexer (ROADM) are also expected to find more applications in F5G.

5.4 Slicing technologies

5.4.1 Slicing in Access Networks

Slicing is not a new concept even in Access Network. [i.16] was targeting a business case of sharing an Access Network by multiple Virtual Network Operators (VNOs), where Access Network is sliced by Infrastructure Provider (InP) and operated by multiple VNOs. [i.17] further defines a management interface to support the Access Network between VNOs and InP. [i.18] addresses a preliminary virtual Dynamic Bandwidth Allocation (vDBA) concept for PON tree slicing.

In FANS series TRs, the target is Access Network wholesale and sharing, InP is the resource owner and manager, while VNOs need to negotiate with InP for resource allocation, management and coordination. For example, vAN (virtual Access Node) was introduced to describe a logical Access Node allocated to a certain VNO, ports on physical Access Node are mapped to virtual port on the vAN. Such mapping is managed by a Port Mapper of InP. BBF TR-386 [i.17] is a specification to define general requirements about management and control interfaces between InP and VNOs.

As stated by BBF TR-370 [i.16], Access Nodes rely on VLANs, MPLS LSPs or VxLAN to separate traffic for each VNO. For example, the Operator-VLAN concept was introduced to identify and carry all traffic for a certain VNO. This not only introduces extra overhead and reduced efficiency, but also is difficult to guarantee resource and transport performance for each VNO.

For SDN-based FANS, BBF TR-370 [i.16] addressed a high level framework that Access Network Manager & Controller shall provide modules to manage and control slices for each VNO, but did not provide further specification about data plane implementation for resource guarantees.

The FANS series are limited to the Access Network including handover to Aggregation Networks of multiple operators (VNOs), but it did not address CPN or E2E slicing.

In XGS-PON, Recommendation ITU-T G.9807.1 [3], the Dynamic Bandwidth Assignment is the process by which the OLT distributes upstream PON capacity between the traffic-bearing entities within ONUs, based on dynamic indication of their traffic activity and their configured traffic contracts. This addresses upstream traffic management and different implementations are possible.

5.4.2 Packet-based Aggregation Network

There are several packet-based technologies used today including IP, Ethernet, and MPLS. Each has its own mechanism to separate traffic and achieve a certain degree of isolation. Note that the detailed packet forwarding behaviour is typically implementation specific, so depending on the characteristics of slice different behaviour in the implementation of networking nodes are required.

In Ethernet, the Virtual LAN standard IEEE 802.1Q [i.56] defines VLAN Tags, which are basically virtual networks and the forwarding behaviour can depend on the VLAN tag. A VLAN can be regarded as a slice. With the QinQ feature also several layers of VLANs are possible.

In IP, IETF RFC 2474 [i.57] defines a Differentiated Service Field in the IP protocol header of IPv4 and IPv6. This allows for classifying traffic into different classes, where each class can have a different forwarding behaviour in the routers and with this can implement slicing on a per traffic class bases.

In Multiprotocol Label Switching (MPLS) based networks IETF RFC 3031 [i.58], different mechanisms are defined for slicing. First, the traffic class field is similar to differentiated service, which defines the forwarding behaviour of packets based on their class, which is a coarse-grain traffic management method. With specific extension in the signalling and management of MPLS, per-session forwarding behaviour and traffic management can be achieved. MPLS is used for implementing a variety of virtualization technologies including point-to-point pseudo-wire, virtual private LAN, and virtual private routed networks. Each of them is a certain level of slicing.

VxLAN, IETF RFC 7348 [i.59], is a layer 2 overlay network running over a layer 3 network. It features, point-to-point tunnels and an overlay network, when the underlay supports it. In the underlay, care needs to be taken with regard to avoiding underlay packet fragmentation. Basically, layer 2 packets are encapsulated into UDP packets running over IP to the other end-point of the tunnel. Slicing in VxLAN allows for separating traffic through the proper configuration of VxLAN tunnel end-points. Since the traffic is tunnelled, Ethernet address spaces are isolated from each other. VxLAN itself does not provide features for resource isolation and traffic management that is left to the underlying Layer 3 network. The degree of freedom in VxLAN is to choose the virtual tunnel end-points according to some traffic management policies of the VxLAN management system. Note that VxLAN adds some per packet overhead for VxLAN packet header, UDP packet header, and underlay IP packet overhead, which is not an issue in local data centres, for which this technology was originally designed.

Segment Routing (SR), IETF RFC 8402 [i.60], can be applied to IPv6 and MPLS. The approach leverages the source routing paradigm. It allows the source node of a communication link to give a set of segments, the packet is required to be routed through. SR can be centrally controlled operation, where a controller allocates the segments and initiates the segments with particular SR policies. Or SR can operate decentralized using routing protocols to distribute segment information in the network. Different path protection schemes are available, basically allowing traffic to use different lists of segments. SR allows to steer traffic in the IP network, which allows to control the network and its congestion through traffic management. However hard isolation of traffic and of resources are not available, and need to be implemented through other means, as some of the mechanisms above support. Also in order to have resiliency and traffic management through traffic steering, several paths need to be available in the network. This makes resource management and resiliency of SR dependent on the network topology of the aggregation network deployed.

5.4.3 OTN based Aggregation Network

OTN like PDH and SDH is channelized and as such has the inherent capability of separating user traffic. It delivers user traffic End-to-End with timing transparency. So OTN can be considered a sliced network, however the network slicing has evolved and now requires service layer slicing.

OTN frames are comprised of higher and lower order ODU, which are basically containers of varying rates. Via mapping, ODUs are capable of carrying all known protocols not just SDH and Ethernet. Currently defined in Recommendation ITU-T G.709 [i.67] the minimum granularity is 1 Gbits/s, which is known as an ODU0 designed specifically to support Gigabit Ethernet. What is also supported is an ODUflex which can have any rate from 1 Gbits/s to the rate of the higher order frame. Today ODUs support all standard Ethernet rates from 1 GE to 400 GE, however any rate can be supported from 1 Gbits/s up to 400 Gbits/s by use of ODUflex. All Ethernet frames are carried transparently End-to-End.

Work is progressing in ITU-T Study Group 15 Question 11 and management in Question 12 to support sub-1 Gbits/s, so legacy traffic like 1 Mbits/s-10 Mbits100 Mbits/s as well as SDH and PDH traffic are being discussed.

So OTN can isolate traffic not just user traffic but user services, which via a managed network can generate multiple service path layers or service network slices End-to-End totally separated from one another. Another important aspect of network slicing is hard versus soft isolation. OTN supports hard isolation, so the services can be carried End-to-End without the possibility of being disruption by other service types. Once the path is established the End-to-End latency is fully deterministic. So services can be reliably, consistently, with low latency be delivered End-to-End, and the services can be teared down when no longer required.

5.4.4 Wi-Fi® for CPN

Slicing for Wi-Fi® is also a new concept. Wi-Fi® slicing is a service, works automatically and autonomously, that can guarantee the applications work perfectly. In traditional Wi-Fi® (IEEE 802.11ac [i.61] and previous version) system, APs and STAs are contented for access of the wireless channel resource. This multiplexing mechanism make the QoS of service hard to guarantee.

For Wi-Fi® 6, DL/UL OFDMA technologies are introduced, and the AP can allocate the downlink and uplink resource unit to several STAs simultaneously. These features enhance the ability to partition resources for users and/or slices within Wi-Fi® networks.

IETF RFC 3580 [i.62] specifies how the tunnel attributes defined in IETF RFC 2868 [i.63] can be used to allocate the authenticated Wi-Fi® user into a particular VLAN. The use of dynamic VLAN assignment enables the slice selection to be based on network policy. Such capabilities are widely used within the Wi-Fi® industry and are used within enterprise deployments.

IETF RFC 5176 [i.64] specified dynamic authorization mechanism, which can be used to move a particular Wi-Fi® client from one "network slice" to another and to remove a Wi-Fi® client from the network.

The combination of multiple BSSIDs over the 802.11 interface, coupled with network based VLAN allocation, can be used to provide the traffic isolation between different network slices over a common Wi-Fi® architecture, or even isolation between traffic from different Wi-Fi® devices in the same slice.

In 3GPP, the exact details of the RAN scheduling algorithms are not defined, enabling RAN vendors to differentiate their offerings. The same approach is used by the Wi-Fi® community, with resource allocation being implemented using vendor proprietary capabilities.

In Release 12, 3GPP has defined an approach to enable trusted WLANs to access EPC based services that are based on PDN connectivity concepts that include APNs. The Wireless LAN Control Plane (WLCP) protocol specified in ETSI TS 124 244 [i.65] enables the signalling of such information, together with distinct destination MAC addresses that are used by a Wi-Fi® device to identify multiple flows over an 802.11 based Access Network.

5.5 F5G Network Management and Control

5.5.1 General

The F5G network architecture is comprised of 3 planes, the Underlay Plane, the Service Plane and the Management, Control & Analytics Plane (MCA Plane). Automatic management and control of the networks is a common requirement for various use cases of F5G networks, which can improve the operators' experience of the intelligent operation and maintenance of their networks, and improve the users' experience of the on-demand service provisioning.

There are multiple SDOs defining standards which are relevant to network and service management and control. These standards can be referred to for the design of the management and control of F5G networks.

5.5.2 F5G network automation and autonomy

The Autonomous Networks (AN) Project in TM Forum aims to define fully automated zero wait, zero touch, zero trouble innovative network/ICT services for vertical industries' users and consumers, supporting self-configuration, self-healing, self-optimizing and self-evolving telecom network infrastructures for telecom internal users: planning, service/marketing, operations and management. The Autonomous Networks incorporate a simplified network architecture, autonomous domains and automated intelligent business/network operations for the closed-loop control of digital business, offering the best-possible user experience, full lifecycle operations automation/autonomy and maximum resource utilization. The AN Project is working on the standardization of:

- Levels of Autonomous Networks.
- Autonomous domain definition and multi-domain collaboration.
- Intent-driven Interaction.
- AN Control loop mechanism.
- Intelligent Network Infrastructure.

On the other hand, the ISG Zero touch network and Service Management (ZSM) in ETSI is working on the definition of a new, future-proof, horizontal and vertical end-to-end operable framework and solutions to enable agile, efficient and qualitative management and automation of emerging and future networks and services. Horizontal end-to-end framework refers to cross-domain, cross-technology aspects. Vertical end-to-end framework refers to cross-layer aspects, from the resource-oriented up to the customer-oriented layers. The goal is to have all operational processes and tasks (e.g. delivery, deployment, configuration, assurance, and optimization) executed automatically, ideally with 100 % automation.

The technologies of Autonomous Networks and end-to-end network and service management specified in TM Forum and ETSI ISG ZSM can be applied in F5G networks. This requires the standardization of the end-to-end framework and solutions of F5G autonomous network.

5.5.3 Modelling language and protocols

YANG language, the syntax and semantics of which are defined by IETF NETMOD WG, is a data modelling language used to model configuration data, state data, Remote Procedure Calls, and notifications for network management protocols.

The NETCONF protocol, defined by the IETF NETCONF WG, provides mechanisms to install, manipulate, and delete the configuration of network devices. The NETCONF WG also defines a protocol based on HTTP called "RESTCONF". The RESTCONF protocol provides a programmatic interface for accessing data defined in YANG language. It defines configuration datastores and a set of Create, Read, Update, Delete (CRUD) operations that can be used to access these datastores.

For F5G, the YANG language can be used to model the F5G networks, and the NETCONF/RESTCONF can be used as the protocol of the interfaces from the MCA Plane to Service Plane and Underlay Plane of F5G.

5.5.4 Modelling language and protocols

ITU-T SG15 Q12 and Q14 are working together to define the management and control of the Optical Transport Network, including Automatically Switched Optical Networks (ASON) and Software Defined Networking (SDN). Q12 focuses on the Optical Transport Network architecture including the operational aspects of networks, while Q14 focuses on the management and control of Optical Transport systems and equipment.

And in IETF, the ACTN (Abstraction and Control of Traffic Engineering (TE) Networks) is defined by IETF RFC 8453 [i.26] in the TEAS WG. The ACTN framework includes a set of management and control functions used to operate one or more TE networks, to construct virtual networks that can be presented to customers and that are built from abstractions of the underlying networks.

The ACTN uses a hierarchical controller architecture, and defines three layers of controllers including the CNC (Customer Network Controller), the Multi-Domain Service Coordinator (MDSC) and the Provisioning Network Controller (PNC). A set of YANG data models is also defined in IETF, which can be used for both the MDSC-PNC Interface (MPI) and the CNC-MDSC Interface (CMI) interfaces in the ACTN architecture.

The ACTN can be used as the basic architecture for the control and management of the Optical Transport Network in F5G. Further extensions are needed to support control and management of new features of Optical Transport Network brought by F5G.

5.5.5 Management and control of Optical Transport Network

Cloud Central Office (CloudCO) Project Stream (PS) in the BBF SDN and NFV Work Area is developing the Central Office (CO) System, which re-architects the broadband network using Software Defined Networking (SDN) and Network Functions Virtualization (NFV) technologies running on a cloud-like infrastructure deployed at the Central Offices.

The reference architectural framework of the CloudCO is defined in BBF TR-384 [i.68]. It includes the functional modules and the interfaces interconnecting in between in an interoperable manner. This allows the consumption of the CloudCO functionality through the Northbound Application Programming Interface (API).

The CloudCO can be used as the basic architecture for control and management of the Optical Access Network. Further extensions are needed to support the control and management of new features of Optical Access Network brought by F5G.

5.6 Artificial Intelligence

5.6.1 Introduction

Artificial Intelligence (AI) refers to the broad discipline of incorporating intelligence into machines so they can think and accomplish tasks at the human intelligence level without any human intervention. AI is sometimes referred to interchangeably as Machine Learning (ML) or Deep Learning (DL); however, there are clear differences among them. ML is a subset of AI algorithms that use various statistical tools to develop systems that learn from data and improve from experiences to accomplish a particular task. DL is a subset of ML methods based on Artificial Neural Networks (ANN) that itself is inspired by the way human brain processes information. The term deep in the terminology refers to the use of multiple hidden layers in the architecture of the ANN. In our context, AI should be considered as the overarching terminology referring to a series of algorithms that learn from data with the aim to model particular patterns and behaviours of the environment from which the data is collected to achieve a predefined goal. It should be highlighted that "data" is the key ingredient for the development of any AI based algorithm.

There are various types of AI algorithms; however, they can be generally classified in three different categories:

1) Supervised learning, which requires labelled training data to be available.

2) Unsupervised learning, which learns patterns or behaviours from unlabelled data.

3) Reinforcement learning, which does not require training data to be available, instead it learns the model by formulating the problem as an interactive environment where reward and punishment mechanisms guide the convergences of the model.

AI is one of the key pillars in F5G, which can be employed in different planes (i.e. underlay, service, and management, control & analysis) of the envisioned architecture and impact the identified technical characteristics of F5G (i.e. eFBB, FFC, and GRE).

AI/ML is already being considered in other SDOs and the consensus among them is that there should be cooperation among different SDOs on the topic of AI/ML so the developments do not diverge. The F5G relevant developments should consider the already taken actions from other SDOs while incorporating the topic into the envisioned architecture. Most of the activities of others SDOs, including ETSI ZSM, are formulated within the context of network automation in which AI/ML is one of the technology pillars. However, only a few of them have thus far released architecture or technical details on the incorporation of the AI algorithms. The key developments of these SDOs, which include TM Forum, ITU-T, and O-RAN alliance, are summarized below.

5.6.2 TM Forum

There are different activities going on in TM Forum. In the AI Data Training Repository Project, they intend to develop a set of dataset repositories for training AI models within the TM Forum such that it supports its members in the development and the management of their AI-based solutions. They released a document [i.1] in which they describe the vision of the project and a set of technical recommendations for the establishment of the envisioned data repositories. In addition, they recommend a series of tools that enable proper storage, access, and management of the envisioned data repositories.

In addition, in another document [i.2], they provide a dedicated clause on the role of AI in their technical architecture. They identify two modes of AI operation in telecom ecosystems:

1) Development mode (or sandbox), which refers to offline model development using the data assets already available.

2) Running mode (or production) to which the development mode provides the AI mode for real-time inference and operation.

Moreover, they introduce a layered AI structure targeting three hierarchical layers for AI deployment:

1) AI in cloud layer, which is supposed to host the development mode defined before.

2) AI in management layer, which mainly hosts the running mode for inference purpose in the management layer such as domain managers.

3) AI in network elements, which targets the real-time and rapid inference mode required at the edge of the network.

In addition to this architectural categorization, they propose an overall closed loop process for AI model development that encompasses all of them. The proposed process comprises four main stages:

1) Data service.

2) Model training.

3) Marketplace.

4) Inference framework.

All of these identified recommendations and strategies are relevant to F5G network fabrics and should be closely monitored. In this regard, in the SDO landscape of [i.2], they provide a holistic view of the developments from different SDOs in which they refer to F5G as one of the SDOs that will eventually contribute to the overall vision of autonomous networks incorporating AI.

5.6.3 ITU-T

The ITU-T Focus Group of Machine Learning (ML) for Future Networking develops a unified logical architecture and relevant recommendations to incorporate ML in a technology-agnostic way into the architecture of 5G networks. This SDO focuses mainly on mobile networks and does not target fixed network scenarios. They claim that their technology-agnostic recommendations can become specific when adapted by technology-specific SDOs like 3GPP, MEC, or EdgeX. In the Recommendation ITU-T Y.3172 [i.3], they released their architectural framework for machine learning, which encompasses a management subsystem, a ML sandbox subsystem, a ML pipeline subsystem, and the ML underlay networks. The released specifications, primarily with respect to the ML pipeline architecture, is very relevant to F5G when it comes to the development of data pipeline and AI lifecycle management. In the Recommendation ITU-T Y.3174 [i.4], they release a framework for data handling for the realization of machine learning enabled solutions that is quite relevant to F5G when a telemetry streaming and data pipeline architecture is to be incorporated into the F5G network architecture.

5.6.4 ETSI

5.6.4.1 General description

Artificial Intelligence (AI) is one of the key technology pillars considered across several ISGs of ETSI. In June 2020, ETSI released a white paper [i.5] that summarizes the AI-related activities within ETSI and discusses its future directions in the community. According to [i.5], the following directions and needs have been identified to improve the SDOs', including ETSI, footprint on AI:

1) To guarantee interoperability, coherency in terminology, concepts, and semantics.

2) To identify interchangeable formats and structures for ML data models and algorithms.

3) To allow adaptive and agile governance of AI-based systems to foster piloting and testing.

4) To provide trustworthy AI frameworks for a "certification of AI".

AI systems are being addressed in several ETSI network specifications in ISG Network Function Virtualization (NFV), Technical Committee (TC) Core Network and Interoperability Testing (INT), ISG Zero-touch network and Service Management (ZSM), and ISG Experiential Networked Intelligence (ENI). Within ISG NFV, AI is considered to become a part of the Management and Orchestration (MANO) stack, primarily when it comes to feeding data to or collecting actions from AI modules. One of the significant achievements is an AI Model Life Cycle Management Process, proposed by TC INT in the ETSI GANA Model [i.6]. The proposal addresses the development, training, testing, certification, and deployment of AI systems considering three main associated stakeholders:

- AI regulator/auditor;
- 3rd party AI model tester; and
- AI model dependent certifier.

While the mentioned developments are quite relevant to F5G, the scope of the activities in ISG ZSM and ISG ENI are wider and should be considered while incorporating AI in the F5G network fabric. The following clauses provide a summary of the relevant developments.

5.6.4.2 ISG ZSM

ZSM defines requirements and architecture for end-to-end network and service management to enable fast and dynamic service delivery while ensuring the economic sustainability for the services offered by the service provider [i.7]. The end-to-end architecture is purposefully designed for closed-loop automation (e.g. based on the Observe, Orient, Decide, Act model) and optimized for data-driven Machine Learning (ML)/AI algorithms. The developed architecture is modular, flexible, scalable, extensible and service-based that supports open interfaces as well as model-driven service and resource abstraction (ETSI GS ZSM 002 [i.8]).

ML/AI is one of the means of automation considered for the end-to-end automation in ZSM. In ETSI GR ZSM 005 [i.9], two flavours of ML that are considered as being significant and valuable for zero-touch network automation are introduced:

1) reinforcement learning; and

2) transfer learning.

An extensive problem formulation is provided in ETSI GR ZSM 005 [i.9] on how these two approaches can be used within ZSM framework. Both approaches are relevant to the activities in F5G and can be utilized in some of the use cases, for instance use case #11 of F5G entitled enhanced traffic monitoring and network control in intelligent Access Network.

When it comes to the orchestration of intelligence, ZSM also provides recommendations. The management domains that are responsible for administrative tasks and realize "separation of concern" are key modules of the reference architecture. Within the management domains, "domain intelligence" services are responsible for carrying out intelligent closed-loop automation. This domain intelligence provides several management services of relevance, including:

1) AI model management service;

2) deployed AI model assessment service;

3) AI training data management service;

4) knowledge base service; and

5) health issue reporting service.

These services are certainly relevant to F5G and could be considered in the design of a potential AI services orchestrator in the management, control, and analysis plane.

Moreover, ZSM dedicates efforts to security threats identification that could affect the ZSM framework due to its openness. In this regard, ZSM tries to consider, and wherever possible, to incorporate the country/region/industry security laws and regulations, including those related to AI, since they will eventually become an obligation for ZSM service providers and their suppliers [i.7]. Particularly speaking, ZSM has published ETSI GR ZSM 010 [i.10] in which one of the objectives is to identify security risks of ML/AI models and develop methods to protect the models when integrated in the ZSM framework. They provide a threat and risk analysis for ML/AI related developments in ZSM, which can be utilized for F5G also.

Furthermore, ZSM provides specific solutions for their identified close-loop automation use cases and scenarios in a working document ETSI GS ZSM 009-2 [i.11] in which a scenario specific to ML/AI is introduced called "Maintaining AI Model in Analytics." This scenario is defined based on the assumptions that a trained model may degrade over time as the target environment changes necessitating ML/AI model improvement. Therefore, continuous monitoring of the AI model after their deployment is also a topic of concern within ZSM. This item is also certainly relevant to F5G, as any envisioned architecture incorporating AI should provide the means to monitor the performance degradation of the deployed models such that it enables model update and retraining during the lifecycle of the service.

In addition to the above-mentioned topics, ZSM works on areas such as trustworthiness and explainability of AI, management of AI components and lifecycle orchestration, dataset requirements and quality assurance, and eventually KPIs to evaluate AI-based systems. In the ETSI White Paper No. #34 [i.5], there is a concise but preliminary mapping between AI standardization activities within ETSI and the involvement level of ZSM and ENI in both of them. Even though it is a simple mapping, it provides an overall view on the position of ZSM and ENI with respect to AI activities in ETSI. The comparison is provided in Table 27. The topics listed in Table 27 are certainly among the most important aspects when it comes to the incorporation of AI into the F5G architecture. Therefore, their details have to be studied in depth while developing the AI modules of the F5G architecture.

5.6.4.3 ISG ENI

The main objective of this ISG is to define a set of standards that specify how an ENI System operates and how to interact with it. In a broader perspective, the ISG ENI targets the improvement of the operator experience by adding closed-loop AI mechanisms exploiting context-awareness and metadata-driven policies that recognize and incorporate new knowledge for making actionable decisions more quickly [i.12] and ETSI GS ENI 005 [i.13].

According to [i.12], ENI has advanced the state-of-the-art for standardization in the following key aspects that can be considered as initial seeds for the development of the F5G architecture while incorporating ML/AI. The following bullet points are directly quoted from ETSI GS ENI 005 [i.13]:

1) "*A multi-level closed control loop functional architecture, where the outer loop adjusts for context and situation changes, and the inner loop optimizes business goals when the outer loop is stable.*

2) *A model-driven architecture, which enables the behaviour of the system to be dynamically managed at runtime.*

3) *The definition of how AI mechanisms can be used to improve the operator experience.*

4) *The use of a novel policy information model that represents imperative, declarative, and intent policies using the same model, thereby facilitating their use and interaction.*

5) *The use of context and situational awareness to adapt the goals, and hence the recommendations and commands, produced by ENI to ensure that changing user needs, business goals, and environmental conditions are met.*"

In the rest of the clause, some of the technical details relevant to F5G are reviewed. ENI focuses on two different aspects:

1) Network technology evolution, which results into network intelligence.

2) Network mgmt. and operation evolution, which results into orchestration and operation intelligence.

In this regard, ENI identified seven categories of use cases for which AI can be beneficial:

1) infrastructure management;

2) network assurance;

3) network operations;

4) service orchestration and management;

5) network security;

6) infrastructure optimization; and

7) use of capabilities.

The key difference between these categories rely on how and where to use AI in the network, what data to collect for that purpose, and eventually what actions to provide. Considering these use case categories, an extensive requirements analysis is reported in which three groups of requirements are identified; service and network requirements, functional requirements, and non-functional requirements. The functional requirements are the most relevant ones for F5G that include requirements on:

1) data collection and analysis;
2) policy management;
3) data learning;
4) interworking with other systems;
5) mode of operations (i.e. recommendation mode or management mode);
6) model training and iterative optimization; and
7) API requirements.

Based on these requirements, an ENI System Architecture is specified to deliver the envisioned promises. The architecture is composed of a set of functional blocks that together form the ENI System, which interoperate using internal and external Reference Points (RPs) and will support several protocols and APIs. The environment that the ENI System is providing recommendations and/or management commands to is called the "Assisted System" (ETSI GS ENI 005 [i.13]). ENI uses an API broker to moderate the interactions between the ENI System and the Assisted System. Three categories of Assisted System are identified depending on the AI involvement level in the process:

1) Class 1: an assisted system that has no AI-based capabilities.
2) Class 2: an assisted system with AI that is not in the control loop.
3) Class 3: an assisted system with AI capabilities in its control loop.

When it comes to the data and AI algorithms, ENI has introduced the following mechanisms to be of value for the envisioned premises (ETSI GS ENI 005 [i.13]). The data mechanisms in ENI are addressed in two main contexts: network telemetry and data storage. Network telemetry focuses on:

1) data sources for generation and publishing of data;
2) data subscription, data exporting; and
3) data storage, query, and analysis.

Data storage focuses specifically on how data should be stored at different stages of AI lifecycle, which include:

1) raw data;
2) feature data;
3) training data;
4) model data;
5) deploying data.

These categories have resource implications in terms of storage and in terms of communicating them around in the network. Finally, ENI focuses on a particular set of AI mechanisms, which include:

1) supervised learning;
2) semi-supervised learning;
3) unsupervised learning;
4) reinforcement learning;
5) feature learning;

6) rule-based learning;

7) explanation-based learning; and

8) federated learning.

These mechanisms can be formulated in two different model training modes; online model training and offline model training. Moreover, there are discussions on protecting the models against biases and the consideration of ethical decision making. In addition, ENI provides AI modelling and training model requirements for the functional processing of the architecture.

The recommendations and specifications released by ENI are general-purpose and technology-neutral, such that they can be applied in fixed and/or mobile networks of telco ecosystems. The interfaces and APIs do not limit the application of the outcomes of ENI. In fact, all interactions with external entities use a specific External RPs and inputs are circulated via the API broker, making its integration with external systems, such as the architecture of other ETSI groups, simplified. This makes it possible to integrate the ENI architecture with the F5G architecture at later stages of development.

Table 27: Comparison of AI related activities within ETSI ISG ENI and ISG ZSM

Standardization activities	ISG ENI	ISG ZSM
Terminology	Strong	Strong
Use cases	Strong	Strong
Trustworthiness and explainability	-	Considering
Security/privacy	Considering	Strong
Architecture and reference points	Strong	Strong
Management of AI components	Considering	Strong
Dataset requirements and quality	Strong	Considering
Interoperability	Strong	Strong
Test methodology and systems	Considering	-
KPIs and conformance	Considering	-
System maturity and assessment	Considering	-
NOTE: The terms "strong" and "considering" represent the level of involvement of ISG ENI and ISG ZSM in the listed standardization activities.		

6 Technology Landscape Summary

Table 28 is a collection of requirements and gaps addressed in clause 4 of the present document, and are organized per use cases. Detailed context of these requirements and gaps can be found in clause 4. In case there is no gap for a certain requirement, the gap is "None". In case multiple requirements are mapped to one gap, the following numbered gap is marked as "Same as [Gapyy-xx]", where yy represents the use case number and xx represents the gap number within that use case. The same is true for requirement numbering [Ryy-xx].

Table 28: Summary of Requirements and Gaps

Technology requirements	Gaps
UC#1: Cloud Virtual Reality	
[R01-1] The F5G network shall support configurations that satisfies the network performance requirements of the corresponding Cloud VR phases in Table 1	[Gap01-1] None
[R01-2] To meet the Cloud VR phases 3 and 4 the terminal shall support Wi-Fi® 6 with advanced antenna configuration	[Gap01-2] None
[R01-3] To meet the Cloud VR phases 3 and 4 Wi-Fi® 6 slicing shall be supported	[Gap01-3] None
[R01-4] The F5G Access Network shall support XG(S) PON, ensuring the Cloud VR phases 3 and 4 are satisfied	[Gap01-4] None
[R01-5] The F5G Access Network XG(S) PON shall support a split ratio of less than 1:16, ensuring Cloud VR phases 3 and 4 are satisfied	[Gap01-5] None

Technology requirements	Gaps
[R01-6] The F5G Access Network shall support a low latency scheduling algorithms	[Gap01-6] None
[R01-7] The F5G OLT should support OTN	[Gap01-7] Currently OTN is not supported on the OLT
[R01-8] The F5G OTN Aggregation Network shall support variable size containers to match the Cloud VR bit rate from 40 Mbits/s to 770 Mbits/s	[Gap01-8] OTN container with flexible and sub1G granularity to efficiently support Cloud VR traffic rates are currently not supported
[R01-9] The F5G Aggregation network shall deploy OTN	[Gap01-9] None
[R01-10] The F5G network shall support higher scheduling priority for Cloud VR service compared to other Internet services	[Gap01-10] OTN support for mixed traffic of ODUs and OSUs is currently not defined
[R01-11] The F5G Access Network shall support high quality independent channels for the Cloud VR phases 3 and 4 services	[Gap01-11] The coordination of network slicing between home network, Access Network and Aggregation Network to form an end-to-end slice to meet end-to-end latency requirement is currently not supported
[R01-12] The F5G network shall automatically increase or decrease the bandwidth utilization for VR services to accurately meet the Cloud VR service bandwidth requirements	[Gap01-12] The automatic bandwidth increase or decrease to accurately meet the bandwidth requirements of Cloud VR services in a seamlessly manner, is currently not supported
[R01-13] The F5G network shall support dynamic set up and release of the high-quality network connection for Cloud VR service	[Gap01-13] Currently the F5G network does not support a coordinated management mechanism to setup or release a connection for Cloud VR services
[R01-14] The F5G independent management systems should support a mechanism that dynamically sets up and releases the End-to-End connections	[Gap01-14] The independent management systems do not currently coordinate together to support a mechanism that dynamically sets up the End-to-End connections
[R01-15] The F5G network shall support a mechanism for dynamic bandwidth changes with minimal interaction with the management layer	[Gap01-15] A simple mechanism for dynamic bandwidth changes with minimal need for coordinated management interaction is currently not supported
[R01-16] The F5G network shall support dedicated slices for Cloud VR traffic transport	[Gap01-16] E2E service isolation via slicing is currently not supported
[R01-17] F5G slice shall match the Cloud VR bandwidth requirements	[Gap01-17] Currently OTN container bandwidth matching Cloud VR rates is currently not supported
[R01-18] The F5G management shall support coordinated E2E slice management	[Gap01-18] A simplified E2E slice management system is currently not supported
UC#2: High Quality Private Line	
[R02-1] The F5G network should provide flexible bandwidth allocation	[Gap02-1] Currently sub-1G bandwidth granularity containers are not supported in OTN
[R02-2] The F5G network should provide an end-to-end connection, which is isolated from other traffic	[Gap02-2] Service-level slicing is currently not supported
[R02-3] The F5G network should provide an efficient on-demand connection provisioning and configuration system	[Gap02-3] The on-demand ordering capability for both the CPE and Edge node is not currently supported
[R02-4] The F5G network should support availability greater than 99,999 %	[Gap02-4] None
[R02-5] The F5G network should support deterministic low latency	[Gap02-5] None
[R02-6] The F5G network should support low latency independent of traffic load	[Gap02-6] None
[R02-7] The F5G network should support dedicated access to the users private Data Centres	[Gap02-7] None
[R02-8] The F5G network should support dedicated access to Cloud services	[Gap02-8] None
[R02-9] The F5G network should support configurable connectivity to match the user's current and future needs	[Gap02-9] Currently OTN does not support finer OTN granularity below 1,25 Gbits/s
[R02-10] The F5G network should support efficient on-demand expansion or contraction of the provided connections	[Gap02-10] Current CPE do not support higher speed interfaces
UC#3: High Quality Low Cost private lines for SMEs	
[R03-1] The Wi-Fi® APs shall support plug-and-play setup and seamless roaming between APs	[Gap03-1] Improvement of EasyMesh™ technology for supporting better roaming performance is currently unavailable
[R03-2] The Wi-Fi® APs shall support multi-user MIMO	[Gap03-2] The slicing and quality guaranteed services for multi-AP scenarios are currently not standardized
[R03-3] The SME CPN shall support network slicing	[Gap03-3] Slicing in the CPN to meet the high quality requirements of SMEs is currently not defined
[R03-4] Hardware slicing of the Wi-Fi®, CPE, and PON shall be supported	[Gap03-4] Hard slicing of Wi-Fi®, CPE, and PON is currently not supported

Technology requirements	Gaps
[R03-5] E2E slicing shall be supported isolating different users	[Gap03-5] AI based traffic identification support to distinguish private line service from other users as well as to identify different applications of a private line service is currently not supported
[R03-6] E2E slicing shall be supported isolating different applications	[Gap03-6] E2E slicing mechanism including management standards for fixed network are currently not defined
[R03-7] The SME private line network shall support high quality communication to cloud platforms of different providers	[Gap03-7] None
[R03-8] The interface between the network service provider and the cloud provider shall be open and interoperable	[Gap03-8] The interface between the F5G network and the cloud network for guaranteed services, specifically in cases where the cloud provider and the network operator are in different administrative domains is currently not specified
[R03-9] SME private line services should be supported on the same infrastructure as residential services	[Gap03-9] None
[R03-10] The SME private line management system should support time-of-day based SLAs	[Gap03-10] Time-of-day based SLA management interface and data models are currently not supported to the required level
[R03-11] The F5G Network should support protection to achieve network availability of 99,99 %	[Gap03-11] None
[R03-12] The F5G network shall support fast provisioning of SME private line service, which includes private line CPE and multi-APs systems plug-and-play	[Gap03-12] Fast provisioning of private line services including private line CPE and multi-APs systems plug-and-play are currently not defined
[R03-13] The F5G network shall support automatic fault detection, demarcation, isolation and correction	[Gap03-13] Automatic fast fault detection, demarcation, isolation, and correction are currently not defined
[R03-14] The F5G network management system should support the visualization of network operation SLA indicators to SMEs and operators	[Gap03-14] Visualized SLA indicators for network operation are currently not supported
UC# 4 Fibre on-premises networking: Fibre-to-The-Room (FTTR)	
[R04-1] The fibre-based on-premises network shall support multiple profiles (in terms of data rate) for different types of network device	[Gap04-1] A variety of data rate profiles for fibre-based on-premises network in terms of modulation bandwidth, high modulation scheme, etc., are not currently available
[R04-2] The fibre-based on-premises network shall support up to 10 Gbps date rate	[Gap04-2] None
[R04-3] The fibre-based on-premises Residential network shall support a split ratio of 1:16	[Gap04-3] The optical link budget from 0 ~ 23 dB is currently not specified for Residential networking
[R04-4] The fibre-based on-premises apartment building or SME network shall support a split ratio up to 1:32	[Gap04-4] None
[R04-5] The fibre-based on-premises network shall support a dedicated high-priority channel for exchanging signalling messages	[Gap04-5] The high-priority channel for roaming is currently not supported
[R04-6] The fibre-based on-premises network should support a mechanism, to provide a guaranteed intercommunication channel for APs	[Gap04-6] The mechanism to recognize network signalling and protocols is currently not supported
[R04-7] In order to avoid any potential message contention in the fibre backhaul link between P-ONU and E-ONU and wireless fronthaul link between ONU and STA, The fibre-based on-premises network shall define a coordinated mechanism for different nodes in the network	[Gap04-7] The fibre and wireless coordination mechanism is currently not supported
[R04-8] The transceiver profile shall be optimized to match the fibre deployment.(including fibre topology, fibre and connector types)	[Gap04-8] Optimized transceivers parameters (such as transmission power, receiver sensitivity, dispersion, etc.) for single mode fibre and new parameters of P2MP transceivers for multi-mode fibre and plastic fibre are currently not supported
[R04-9] The on-premises network should support authentication of all new devices connecting to the network	[Gap04-9] Simplified authentication process is currently not supported
[R04-10] The on-premises network should support data encryption	[Gap04-10] None
[R04-11] Fibre with pre-connectorized optical cable should be used in the on-premises network	[Gap04-11] Small size connectors with good protection is currently not standardized
[R04-12] The on-premises network shall be P2MP topology	[Gap04-12] None
[R04-13] The on-premises network should support the use of uneven optical power splitter should in multi-floor buildings	[Gap04-13] None

Technology requirements	Gaps
[R04-14] The on-premises network should support the use of optical and electrical hybrid cable for Wi-Fi® AP devices	[Gap04-14] Small size optical and electrical hybrid cable with appropriate bend radius as well as the connectors are currently not defined
[R04-15] The fibre-based on-premises network shall support a low power mode for IoT applications	[Gap04-15] None
[R04-16] The fibre-based on-premises network shall enable the IoT hub to manage the coordination between the IoT hub and the residential gateway in low power mode	[Gap04-16] A mechanism for IoT hub to manage the coordination between the IoT hub and the RG in low power mode is currently not defined
[R04-17] The fibre-based on-premises network shall define a QoS related transmission mechanism	[Gap04-17] The transmission QoS mechanism that allows for multi-dimension network parameters, such as data rate, round trip delay, packet error rate, etc. is currently not standardized
[R04-18] The fibre-based on-premises network shall support East-to-West data communication	[Gap04-18] A direct node-to-node communication method on layer 2 for fibre-based on-premises network is currently not defined
[R04-19] The fibre-based on-premises network shall support symmetric transmission data rate between P-ONU and E-ONU	[Gap04-19] Symmetric transmission data rate is not supported in 2,5 Gbps data rate profile
UC#5: Passive optical LAN	
[R05-1] POL technology shall support network slicing functionality	[Gap05-1] Slicing standards are not currently defined for the POL scenarios
[R05-2] The POL slicing functionality should support the multiple granularities as defined in Table 7	[Gap05-2] The granularities and requirements of network slicing for POL are currently not supported
[R05-3] POL technology should support data encryption in L2 layer	[Gap05-3] None
[R05-4] POL technology should support PON protection Type B and Type C as defined in Recommendation ITU-T G.984.1 [i.97]	[Gap05-4] None
[R05-5] The POL OLT should support a centralized control function for the Wi-Fi® access in the POL network	[Gap05-5] The functionality requirements and technologies of centralized access control are currently not specified for POL
[R05-6] The ONU should support "Fit AP" mode, controlled by the access controller	[Gap05-6] The "Fit AP" functional requirements of the corresponding ONU are currently not specified for POL
[R05-7] The POL ONU should support PoE/PoE+/PoE++ functionality	[Gap05-7] None
UC#6: PON for Industrial Manufacturing	
[R06-1] The industrial PON system shall support network slicing functionality	[Gap06-1] Industrial slicing scenarios, including granularity of the network slice, the management and control function requirements, and the network resource allocations are currently not standardized
[R06-2] The industrial PON system shall support different deployment scenarios, with scenario-dependent latency, jitter and bandwidth requirements	[Gap06-2] The PON system optimization to support TSN features is currently not supported
[R06-3] The industrial PON system should support interworking functions between the industrial PON system and TSN	[Gap06-3] The interworking of PON and TSN is currently not supported
[R06-4] The industrial PON system should support carrying industrial protocols and satisfy the performance requirements of these protocols	[Gap06-4] Industrial PON ONU with industrial interfaces and protocol interpreting functions are currently not available
[R06-5] The industrial PON ONU should support built-in industrial physical interfaces	[Gap06-5] Same as [Gap06-4]
[R06-6] The industrial PON system shall support protection schemes that cover the OLT, the ODN and the ONU	[Gap06-6] None
[R06-7] The industrial PON system shall support ONU authentication	[Gap06-7] None
[R06-8] The industrial PON system shall support AES data encryption functionality	[Gap06-8] None
[R06-9] The industrial PON system should support standard management protocols and data models	[Gap06-9] Industrial PON telemetry, automatic network resource allocation and configuration enabled by AI based functions within the PON system is not currently defined
[R06-10] The industrial PON system shall support a GUI-based user-friendly network management system	[Gap06-10] None
[R06-11] The industrial PON ONU shall meet the environmental requirements of the corresponding deployment scenarios	[Gap06-11] None

Technology requirements	Gaps
[R06-12] The industrial PON OLT should support embedded edge computing	[Gap06-12] The definition of compute power for edge computing platforms in Industrial PON is currently not defined
[R06-13] The edge computing module should support 3rd party applications	[Gap06-13] None
UC#8: Multiple Access Aggregation over PON (MAAP)	
[R08-1] The F5G Access Network shall support OMCC bandwidth allocation and inter-gap allocation optimization	[Gap08-1] Increase in PON throughput via new technologies such as high-order modulation and wavelength-division multiplexing is currently unavailable
[R08-2] The F5G Access Network PON infrastructure shall support high capacity solutions as defined in table 10 for MAAP	[Gap08-2] Same as [Gap08-1]
[R08-3] The F5G Access Network PON technologies shall support a seamless upgrade and integration with the existing deployed PON ecosystem	[Gap08-3] None
[R08-4] The F5G Access Network PON technologies shall support multiple services (B2B, B2C and mobile xHaul) over the same PON infrastructure	[Gap08-4] None
[R08-5] The F5G Access network PON infrastructure shall support protection mechanisms for MAAP between two distinct OLT, using single or dual ONU	[Gap08-5] None
[R08-6] The F5G Access network PON infrastructure shall support automatic protection switching for MAAP	[Gap08-6] Automatic protection switch with delay compensation between the working path and the protection path to avoid service interruption is currently unavailable
[R08-7] The F5G Access network PON infrastructure shall support distinct service types based on different latency, jitter and bandwidth requirements	[Gap08-7] Improved DBA to support low-latency upstream transmission with latency below 100 µs is currently unavailable
[R08-8] The F5G Access network PON infrastructure shall support 5G end-to-end time accuracy and synchronization requirements for MAAP	[Gap08-8] Enhanced timing & synchronization for future PON systems to ensure end-to-end requirements are met is currently unavailable
[R08-9] The F5G Access network PON infrastructure shall support network slices for different mobile and fixed service levels in the MAAP solution	[Gap08-9] Slicing in PON with suitable mapping of the vDBA and/or VxLAN to the service slice type and traffic isolation processes is currently not supported
[R08-10] The F5G Access network PON infrastructure shall support protocol transparency for MAAP	[Gap08-10] Protocol transparency in PON throughput via new technologies such as Ethernet Private Lines (EPL) and Ethernet Virtual Private Lines (EVPL) is currently not supported
UC#10: Scenario Based Broadband	
[R10-1] The F5G network shall support application type (video, file transfer, Internet browsing, etc.) identification	[Gap10-1] An application type identification mechanism is currently not supported
[R10-2] The F5G network should support AI based application type identification	[Gap10-2] Use of AI for application identification in a F5G network is currently not supported
[R10-3] The application feature database for AI should be established and updated in real-time or periodically	[Gap10-3] The dynamic creation and updates of application feature database entries using Big Data and Machine Learning mechanisms is currently not supported
[R10-4] The F5G network shall support slicing with different service characteristics	[Gap10-4] Mechanisms for F5G End-to-End slicing with consistent SLA on multiple network segments with different physical technologies is currently not supported
[R10-5] The F5G network shall support measurement mechanisms for QoS evaluation	[Gap10-5] None
[R10-6] The F5G network should support measurement mechanisms for QoE evaluation	[Gap10-6] Evaluation schemes for QoE of specific applications are not currently supported
[R10-7] The F5G network should support identification of application network usage, which potentially have acceleration requirements	[Gap10-7] None
[R10-8] The F5G network should support the allocation of available resources	[Gap10-8] Mechanisms to identify application network usage, which potentially have acceleration requirements are currently not supported
[R10-9] The F5G network should avoid links to individual user usage of applications unless this service is explicitly included in the user's SLA. Otherwise, linking should be restricted to an anonymized group of users	[Gap10-9] Same as [Gap30-4]
[R10-10] The F5G network shall support the monitoring of network resource utilization and health status	[Gap10-10] Mechanisms for near real-time monitoring of F5G network resource utilization and health status are currently not supported

Technology requirements	Gaps
UC#11: Telemetry based Enhanced Performance Monitoring in Intelligent Access Network	
[R11-1] The F5G Access Network shall support telemetry-based network performance monitoring techniques	[Gap11-1] Specification for a lightweight Telemetry technology, such as UDP based telemetry, for the F5G Access Network telemetry is currently not supported
[R11-2] The F5G Access Network should define data models for configuration and data collection	[Gap11-2] Development and specification of a dedicate data model for performance monitoring and data collection for the F5G Access Network are not currently available
UC#13: Remote Attestation	
[R13-1] F5G network elements should support the generation of security measurement data, store it securely and securely report its integrity status	[Gap13-1] An appropriate method for security measurement data generation is currently not supported
[R13-2] F5G network elements should prove its trusted status to the challenger, which should be suitable for its own hardware architecture	[Gap13-2] None
[R13-3] F5G network elements should support the function to prove the evidence of its trusted boot	[Gap13-3] An appropriate method for remote attestation support in F5G network elements while running is currently not supported
[R13-4] F5G network elements should support providing the status of its trustworthiness during run-time	[Gap13-4] Same as [Gap13-3]
UC#14: Digitalized ODN/FTTX	
[R14-1] The F5G Access Network shall support the digitization of the physical ODN labels of the various components	[Gap14-1] The digitalized ODN management system as part of the F5G Access Network controller, is currently not standardized
[R14-2] The F5G Access Network Controller shall support the construction and maintenance process, by automatically capturing the ODN information, and visualizing the ODN networks	[Gap14-2] Same as [Gap14-1]
[R14-3] The F5G Access Network Controller shall support troubleshooting by remotely accessing the F5G ODN database by technicians	[Gap14-3] Same as [Gap14-1]
[R14-4] Pre-connecterisation shall be supported for different types of F5G ODN connectors and boxes (including outdoor adapters) and in various environments (indoor, outdoor, simple and complex)	[Gap14-4] Special designs required for connection nodes are currently not standardized
[R14-5] The F5G ODN connectors and boxes (including outdoor adapters) shall meet the appropriate Ingress Protection (IP) level depending on the deployment scenario (such as ingress protection rating IP68 and IP65 [1])	[Gap14-5] Same as [Gap14-4]
[R14-6] The connectors shall support low insertion loss to meet the link loss requirements of the F5G ODN	[Gap14-6] Same as [Gap14-4]
[R14-7] The digitized ODN connection and installation process shall meet the long-term reliability test requirements and mechanical test requirements during onsite construction and deployment	[Gap14-7] Same as [Gap14-4]
UC#15: Virtual Presence	
[R15-1] The F5G network shall meet the corresponding network performance requirements of a given Virtual Presence Phase	[Gap15-1] None
[R15-2] The F5G network shall support the enabling of applications to discover what service level(s) the network can provide	[Gap15-2] A Standard for explicitly discovering application-oriented service levels provided by the network is currently not defined
[R15-3] The F5G network shall support traffic slicing for specified network parameters	[Gap15-3] Explicit slicing mechanism for slicing networks according to a combination of bandwidth, latency, packet jitter, packet loss, is currently not supported
[R15-4] The F5G network shall support multiple parallel slices that each support specific requirements of a specific application	[Gap15-4] The F5G network capability to support a practically unbounded number of parallel slices is currently not supported
[R15-5] The F5G network shall support a control interface with the application layer	[Gap15-5] None
[R15-6] The F5G network shall support on-demand application and service requests, to dynamically setup, release and adapt F5G network slices	[Gap15-6] API and system architecture to allow applications to dynamically request and release network slices are currently not supported
[R15-7] The F5G network shall support the bi-directional exchange of real-time QoE metrics with the applications and services	[Gap15-7] Mechanisms for clients to exchange application-related QoE metrics with the network are currently not supported

Technology requirements	Gaps
[R15-8] The F5G network shall support authentication and authorization specific to VP applications and/or VP systems for a configurable set of services	[Gap15-8] None
[R15-9] The F5G network shall support authentication and authorization to specific VP applications and/or VP systems for a configurable set of allocated network slices	[Gap15-9] None
[R15-10] The F5G network should support dynamic adjustment of slice parameters	[Gap15-10] Same as [Gap15-6]
[R15-11] The F5G network should support edge computing functionality integrated with the OLT	[Gap15-11] Same as [Gap15-12]
[R15-12] The F5G network shall support edge computing services	[Gap15-12] A Standard for edge computing integrated within optical F5G networks is not currently defined
[R15-13] The F5G network should support slices with different QoS/priority levels	[Gap15-13] Prioritization of slices is not currently supported
[R15-14] The F5G network shall support encryption of user data traffic flows	[Gap15-14] None
[R15-15] The F5G network shall prevent side-channel attacks on the encrypted user traffic itself	[Gap15-15] Same as [Gap30-4]
[R15-16] The F5G network should prevent applications from allocating excessive proportion of F5G network resources	[Gap15-16] None
[R15-17] The F5G network should prevent applications from failing to release F5G network resources	[Gap15-17] Mechanisms to prevent the requesting and use of more F5G network resources than required by applications are not supported currently
UC#16: Enterprise private line connectivity to multiple Clouds	
[R16-1] The F5G OTN edge nodes shall support P2MP and MP2MP connectivity to cloud services	[Gap16-1] The mechanism to automatically learn the cloud-side and enterprise-side service address information in the OTN edge node is not currently supported
[R16-2] The F5G OTN edge nodes shall support recognizing the cloud service request and its SLA requirements	[Gap16-2] Standardized YANG data models for the cloud service requests and their SLA requirements are not currently supported
[R16-3] The F5G OTN edge nodes shall support on-demand OTN connection creation, modification and deletion based on the cloud service requirements	[Gap16-3] None
[R16-4] The F5G network shall support OTN container that match the bandwidth requirements of the various enterprise cloud services	[Gap16-4] Same as [Gap23-1]
[R16-5] The F5G OTN shall support dynamic bandwidth adjustment of an OTN connection	[Gap16-5] The dynamic bandwidth adjustment for sub-1 Gbps OTN connections is currently not supported
[R16-6] Same as [R23-2]	[Gap16-6] Same as [Gap23-2]
[R16-7] The F5G E2E OTN shall support network slicing	[Gap16-7] None
[R16-8] The F5G E2E OTN shall support the management and control of network slices	[Gap16-8] The YANG data models for the management and control of the OTN slice are currently not standardized
[R16-9] The F5G E2E OTN should provide scalable connection control to match the increasing number of connections	[Gap16-9] There is a short fall in the current OTN signalling protocol performance when controlling a large number of OTN connections
[R16-10] The F5G E2E OTN should support protection mechanisms to resolve network failures to the Cloud DCs	[Gap16-10] Current OTN protection mechanisms do not support the case where the destination node of the OTN protection path is different from that of the working path
[R16-11] The F5G E2E OTN connection protection mechanisms should resolve single or multiple network failures	[Gap16-11] None
[R16-12] The F5G E2E OTN should support connection restoration mechanisms to resolve single or multiple network failures in OTN, with deterministic restoration performance	[Gap16-12] Same as [Gap16-9]
UC#17: Premium home broadband connectivity to multiple Clouds	
[R17-1] Same as [R16-1]	[Gap17-1] The mechanism to learn the cloud-side and user-side service address information and automatically build the mapping table in the OTN edge nodes, are not currently supported
[R17-2] The OLT shall support the coordination of service request with OTN through the Access Network Controller	[Gap17-2] The mechanism to automatically generate the mapping table from service addresses to OTN connections is not currently supported

Technology requirements	Gaps
[R17-3] The OLT shall support triggering the OTN edge node, to create OTN service based connections	[Gap17-3] Same as [Gap16-2]
[R17-4] The F5G OTN edge nodes shall support on-demand OTN connection creation, modification and deletion based on the cloud service requirements	[Gap17-4] A standardized interaction process between the OLT and the edge OTN node for the cloud service requests and their SLA requirements is currently not defined
[R17-5] The OLT shall support triggering the automatic bandwidth adjustment of the OTN connection	[Gap17-5] Same as [Gap16-9]
[R17-6] Same as [R16-4]	[Gap17-6] Same as [Gap23-1].
[R17-7] Same as [R16-5]	[Gap17-7] Same as [Gap16-5].
[R17-8] Same as [R23-2]	[Gap17-8] Same as [Gap23-2]
[R17-9] The F5G network shall support PON slicing, for premium home broadband services	[Gap17-9] Same as [Gap08-9]
[R17-10] Same as [R16-7]	[Gap17-10] None
[R17-11] Same as [R16-8]	[Gap17-11] Same as [Gap16-8]
[R17-12] Same as [R16-9]	[Gap17-12] Same as [Gap16-9]
[R17-13] Same as [R16-10]	[Gap17-13] Same as [Gap16-10]
[R17-14] F5G network protection mechanisms should resolve network failure between the OLT and OTN	[Gap17-14] Current OTN protection mechanisms do not support the source node of the OTN protection path being different from that of the working path
[R17-15] Same as [R16-11]	[Gap17-15] None
[R17-16] Same as [R16-12]	[Gap17-16] Same as [Gap16-9]
UC#18: Virtual Music	
[R18-1] The F5G network should support constant/deterministic low latency	[Gap18-1] None
[R18-2] The F5G network shall meet the latency requirements in Table 19 between any pair of musicians or participants	[Gap18-2] None
[R18-3] The F5G network shall support dynamic set up and release of the high-quality end-to-end network channel for virtual music audio sessions between multiple musicians	[Gap18-3] Currently each F5G network segment does not support the coordinated management mechanism to dynamically set up and release of a high-quality end-to-end network channel for audio
[R18-4] The F5G network should guarantee a bandwidth of 20 Mbps for the audio channel	[Gap18-4] None
[R18-5] The F5G network should support dynamic (re)allocation of a central server ensuring optimized End-to-End latency	[Gap18-5] On demand allocation of a central server based on an overall End-to-End latency optimization is currently not standardized
[R18-6] The edge server should support 3rd party applications	[Gap18-6] None
UC#19: Next Generation Digital Twin	
[R19-1] The F5G network should support connectivity between TSN ports on-premises and in data centre(s) in such a way that TSN functionality is preserved	[Gap19-1] None
[R19-2] The F5G network shall provide latency information of the F5G connection between TSN switches connected through an F5G network to the TSN control plane	[Gap19-2] Support of gPTP and IEEE 1588-2019 [i.79] in PON to exchange latency information to Ethernet/TSN switches interconnected via PON is missing
[R19-3] The F5G network shall support a gateway function between the F5G network and TSN network for interpreting TSN traffic in optical (terminating) equipment in F5G networks	[Gap19-3] Same as [Gap04-17]
[R19-4] The F5G network shall support Ethernet and TSN traffic stream filtering and policing	[Gap19-4] Same as [Gap04-17]
[R19-5] The F5G network shall support the mapping of Ethernet and TSN traffic streams to F5G-specific QoS flows	[Gap19-5] TSN gateway or translator function on OLT or ONU may be needed to support specific TSN features e.g. for time synchronization via IEEE 802.1AS [i.34] /gPTP or topology discovery of logical ports/bridges (IEEE 802.1Qcc [i.96])
[R19-6] The F5G network shall support a mix of traffic, both deterministic latency traffic following a time-aware schedule and lower priority traffic	[Gap19-6] None
[R19-7] The F5G network shall support time-aware scheduling with guaranteed maximum latency of 100 µs over 5 hops	[Gap19-7] The F5G PON access network support for time-aware scheduling is not sufficient to support this use case
[R19-8] The F5G PON access network shall support network protection mechanisms	[Gap19-8] None

Technology requirements	Gaps
[R19-9] The F5G network shall support TSN element clock synchronization as defined in IEEE 802.1AS	[Gap19-9] An update of Recommendation ITU-T G.987.1 [i.28] is needed to support gPTP (IEEE 802.1AS [i.34]) and IEEE 1588-2019 [i.79] in ONU and OLT in PON networks
[R19-10] The F5G network shall support clock synchronization of network elements to a main clock with an accuracy better than 1µs	[Gap19-10] None
[R19-11] The F5G network shall support timing redundancy	[Gap19-11] None
UC#20: Media transport	
[R20-1] OTN for media transport shall support the interfaces (SD-SDI, HD-SDI, 3G-SDI, 12G-SDI) to transport the uncompressed raw video signal	[Gap20-1] None
[R20-2] OTN for media transport shall support the interfaces (GE, 10GE, 25GE) to transport the shallow compressed video signal	[Gap20-2] None
[R20-3] OTN for media transport shall support the interfaces (DVB-ASI, GE) to transport the deeply compressed video signal	[Gap20-3] None
[R20-4] OTN for media transport shall support L0 network slicing by applying wavelength-based hard isolation technologies to provide >100 Gbps data rate	[Gap20-4] None
[R20-5] OTN for media transport shall support L1 network slicing by using ODUk/OSU-based hard isolation technologies to enable flexible data rate up to 100 Gbps	[Gap20-5] The standardization of L1 network slice OSU (Optical Service Unit) in not currently defined
[R20-6] OTN for media network transport shall support deterministic and low transmission latency with load-independent, satisfying the particular video signal type requirements	[Gap20-6] None
[R20-7] OTN for media transport shall support $<10^{-5}$ packet loss rate for 4K video transmission	[Gap20-7] None
[R20-8] OTN for media transport shall support $<10^{-6}$ packet loss rate for 8K video transmission	[Gap20-8] None
[R20-9] OTN for media transport shall support ODU/OTU level encryption	[Gap20-9] The ODU/OTU level encryption is not currently standardized
[R20-10] OTN for media transport shall provide service-level 1+1/1:1 protection in dual-path scenarios.	[Gap20-10] None
[R20-11] OTN for media transport shall support protection switching time <50ms	[Gap20-11] None
[R20-12] OTN for media transport shall support fast multi-route protection and restoration capabilities based on ASON	[Gap20-12] None
UC#21: Edge/Cloud-based visual inspection for automatic quality assessment in production	
[R21-1] The F5G network should support functionality and performance requirements for industrial automation	[Gap21-1] TSN features of the industrial automation profile IEC/IEEE 60802 [i.76] or similar/equivalent features are currently not fully supported
[R21-2] Same as [R19-1]	Gap21-2] None
[R21-3] The F5G network shall support cyclic communication with configurable cycle time boundaries in the range of 2 ms - 10 ms	[Gap21-3] Time-aware scheduling with absolute cycle time boundaries is currently not supported
[R21-4] Same as [R19-7]	[Gap21-4] Same as [Gap19-7]
[R21-5] The F5G network should support GiGE Vision® and USB3 Vision™ time synchronization	[Gap21-5] None
[R21-6] The F5G network should support transport of industrial Ethernet protocols	[Gap21-6] Native support for transport of industrial Ethernet protocols is currently not available
[R21-7] The F5G networks should support the performance requirements of industrial Ethernet protocols	[Gap21-7] Performance requirements of these protocols is currently not fully supported
[R21-8] The F5G network should support GiGE Vision® Streaming Protocol (GVSP)	[Gap21-8] None
[R21-9] The F5G network should support upstream bandwidth ≥ 20 Gbits/s per vision inspection station	[Gap21-9] Upstream bandwidth in excess of 50 Gbits/s is not yet standardized for PON
[R21-10] Same as [R19-9]	[Gap21-10] Same as [Gap19-9]
[R21-11] The F5G network shall provide AES link protection	[Gap21-11] AES link protection is currently not standardized for OTN

Technology requirements	Gaps
[R21-12] Same as [R06-11]	[Gap21-12] None
UC#22: Edge/Cloud-based control of automated guided vehicles (AGV)	
[R22-1] The F5G network should support interworking with 5G campus networks	[Gap22-1] None
[R22-2] The F5G network should support interworking with Wi-Fi® 7 access networks	[Gap22-2] Interworking with next-generation Wi-Fi® 7 is currently not supported
[R22-3] The F5G network should support interworking with LiFi access networks	[Gap22-3] None
[R22-4] Same as [R21-1]	[Gap22-4] Same as [Gap22-1]
[R22-5] Same as [R19-1]	[Gap22-5] None
[R22-6] Same as [R21-3]	[Gap22-6] Same as [Gap21-3]
[R22-7] Same as [R19-7]	[Gap22-7] Same as [Gap19-7]
[R22-8] The F5G network availability between AGV and data centre should be > 99,9999 %	[Gap22-8] None
[R22-9] Same as [R21-9]	[Gap22-9] Same as [Gap19-9]
[R22-10] Same as [R21-11]	[Gap22-10] Same as [Gap21-11]
UC#23: Cloudification of Medical Imaging	
[R23-1] The F5G network shall support OTN containers that match the bandwidth requirements of the various medical image formats and sizes	[Gap23-1] The support for sub 1 Gbits/s bandwidth granularity OTN containers is not currently supported by OTN
[R23-2] The F5G network shall support non service affecting bandwidth adjustment	[Gap23-2] The support for non-service-affecting bandwidth adjustment below 1 Gbits/s is not currently supported by OTN
[R23-3] The F5G network should support lossless bandwidth adjustment from 2 Mbits/s to 100 Gbits/s	[Gap23-3] The support for lossless bandwidth adjustment from 2 Mbits/s to 100 Gbits/s is not currently supported by OTN
[R23-4] The F5G network shall support hard isolation on end-to-end service flows	[Gap23-4] The support of hard service flow isolation is not currently supported by OTN
[R23-5] The F5G network management system shall support on demand configuring and provisioning of private line services	[Gap23-5] The support of on-demand private line provisioning for customer network equipment and edge nodes is not currently supported
[R23-6] The F5G network management system should support user applications for non-intrusively monitoring of their SLA parameters indicators	[Gap23-6] The F5G network management support of user applications for non-intrusively monitoring their SLA parameters is not currently supported
[R23-7] The F5G network shall support 99,999 % reliability	[Gap23-7] None
[R23-8] The F5G network shall support the agreed SLA latency	[Gap23-8] None
[R23-9] The F5G network latency should be independent of traffic load	[Gap23-9] None
[R23-10] The F5G network shall provide dedicated connections to the user's private Data Centre	[Gap23-10] None
[R23-11] The F5G network shall provide dedicated connections to access Cloud service	[Gap23-11] None
UC#24: F5G for Intelligent Mining	
[R24-1] The F5G mining network shall support Type-C dual-homing protection	[Gap24-1] None
[R24-2] F5G mining network shall support switching to the standby link within 30 ms	[Gap24-2] The F5G mining network support for switching times better than 30 ms and with Type-C dual-homing protection is currently not defined
[R24-3] The F5G mining network shall meet IP65 protection requirements	[Gap24-3] None
[R24-4] The F5G mining network shall be installed in explosion-proof box or intrinsic safety box	[Gap24-4] None
[R24-5] The F5G mining network shall support fully functional operation in an environment of temperature ranging from -40 °C to 70 °C and a relative humidity of 95 % (non-condensing)	[Gap24-5] None
[R24-6] The F5G mining network fibre connection shall meet IP65 ingress protection	[Gap24-6] None
[R24-7] The F5G mining network shall use pre-connectorised fibre segments for optical fibre deployment	[Gap24-7] The support for more reliable and faster fibre connection technologies for the mining industrial is currently not defined
[R24-8] The F5G Network Management System (NMS) should support visualization and management of the optical fibre network infrastructure	[Gap24-8] None
[R24-9] The F5G mining network should support a digitalized intelligent ODN management system	[Gap24-9] None

Technology requirements	Gaps
UC#25: Enhanced optical transport network for Data Centre Interconnections	
[R25-1] The data rate for intra-city DCI shall support 800 Gbits/s per channel, with range up to 100 km	[Gap25-1] The intra-city DCI support for 800 Gbits/s per channel standard for up to 100 km is currently not supported
[R25-2] The data rate for inter-city DCI shall support 400 Gbits/s per channel, with range from 100 km to 1 500 km	[Gap25-2] The inter-city DCI support 400 Gbits/s per channel standard for up to 1 500 km is currently not supported
[R25-3] DCI equipment shall support Extend C-band and L-band to support up to 120 × 50 GHz-spaced channels	[Gap25-3] The DCI support for extend C-band and L-band to support up to 120 × 50 GHz-spaced channels in each band is currently not supported
[R25-4] The DCI should support bidirectional transmission over two fibres or single fibre	[Gap25-4] The standard for bidirectional transmission over two fibres or single fibre for data rate up to 800 Gbits/s is currently not defined
[R25-5] Inter-city DCI shall support an all optical transparent connection for distances up to1 500 km	[Gap25-5] Standard for 400 Gbits/s per channel standard for all optical transparent connection up to 1 500 km is currently not defined
[R25-6] DCI shall support optical layer wavelength grooming	[Gap25-6] Standard for function model of integrated photonic cross-connecting with higher integration, smaller size, lower power, zero manual fibre connection is currently not defined
[R25-7] DCI network elements shall support protection and automatic recovery functions	[Gap25-7] None
[R25-8] DCI should support dynamic allocation of bandwidth, route and traffic profile	[Gap25-8] None
[R25-9] DCI should support online delay measurement and visualization, and traffic allocation based on that measurement	[Gap25-9] Standards to specify online delay measurement and visualization, and traffic allocation based on the measurement are currently not defined
UC#26: Use case Enhanced Point to Point optical access	
[R26-1] The F5G Access network shall support Bi-directional P2P fibre technologies	[Gap26-1] None
[R26-2] The F5G P2P Access Network test and diagnostics technologies shall not be service affecting	[Gap26-2] None
[R26-3] The F5G P2P Access Network RSSI (Received Signal Strength Indication) resolution, accuracy, repeatability and response time shall be appropriate for high-performance supervision algorithms	[Gap26-3] Exporting F5G P2P Access Network metrics to a controller is currently not standardized
[R26-4] The F5G P2P Access Network monitoring and optical medium health check should differentiate optical medium failures from transport system failures	[Gap26-4] None
[R26-5] The F5G P2P Access Network key performance indicators shall be provided by the F5G Access network controller to the E2E F5G orchestrator in an abstract way	[Gap26-5] The interface and data model is currently not standardized
[R26-6] The F5G P2P Access network technology shall support up to 10 km for highly dense areas	[Gap26-6] None
[R26-7] The F5G P2P Access network technology shall support up to 20 km for moderately dense areas	[Gap26-7] None
[R26-8] The F5G P2P Access network technology shall support up to 60 km for low density areas	[Gap26-8] None
[R26-9] The F5G P2P Access network technology shall support P2P bidirectional bit rates up to 100 Gbits/s	[Gap26-9] P2P bidirectional 100 Gbits/s is under study and needs to be specified
[R26-10] The F5G P2P Access network technology shall support energy saving mechanisms	[Gap26-10] None
UC#28: High speed passive P2MP network traffic aggregation	
[R28-1] The total bidirectional throughput of the central node shall be sufficient for the deployment scenario	[Gap28-1] Bidirectional throughput requirements for high-speed passive P2MP network traffic aggregation in the F5G AggN segment, have not been clearly identified
[R28-2] The total number of edge nodes supported shall be sufficient for the deployment scenario	[Gap28-2] A standard architecture for high speed P2MP networks is currently not defined.

Technology requirements	Gaps
[R28-3] The maximum throughput of each edge node shall be sufficient for the deployment scenario	[Gap28-3] The maximum throughput for P2MP transceivers connecting 5G antenna sites is currently not defined
[R28-4] The bandwidth granularity of each edge node shall be sufficient for the deployment scenario	[Gap28-4] The bandwidth granularity for P2MP transceivers connecting 5G antenna sites is currently not defined
[R28-5] The maximum transmission distance between the central node and an edge node shall be sufficient for the deployment scenario	[Gap28-5] The maximum distance that P2MP transceivers connecting 5G antenna sites need to cover is currently not defined
[R28-6] A Control & Management (C&M) channel between the central node transceiver and the edge node shall be supported	[Gap28-6] A Control & Management (C&M) channel between the central node transceiver and the edge node is currently not defined
[R28-7] Network-level C&M mechanism for the central node transceiver and the edge node transceivers shall be supported	[Gap28-7] A network-level C&M mechanism for the P2MP systems in the aggregation network is currently not defined
[R28-8] Multi-vendor transceiver interoperability between the central node and the edge nodes shall be guaranteed	[Gap28-8] The enabling of multi-vendor interoperability of central node and edge node transceivers is currently not standardized
[R28-9] The transceivers shall provide a mechanism to secure network traffic meant for one of the edge nodes from being intercepted by another edge node	[Gap28-9] A mechanism to prevent the interception of data transmitted in the P2MP network is currently not standardized
UC#30: Bandwidth on demand	
[R30-1] The F5G network should support temporary bandwidth user change requests	[Gap30-1] None
[R30-2] The F5G network should support temporary bandwidth change requests initiated by an intelligent entity within the network or from the management plane	[Gap30-2] In the F5G network intelligent functionality to autonomously allocate user bandwidth is currently not defined
[R30-3] The F5G network shall support bandwidth allocation based on F5G network resources availability and priority	[Gap30-3] Same as [Gap10-10]
[R30-4] The F5G network function that assesses user traffic/ behaviour should only use metadata of F5G network traffic. In addition the F5G network shall not be enabled to individually identify and trace users	[Gap30-4] Privacy of the user is not considered in the design and architecture of existing standards
UC#31: Intelligent Optical Cable Management	
[R31-1] The F5G Optical Transport Controller shall support collecting the physical fibre SRLG information	[Gap31-1] None
[R31-2] The Optical Transport Controller shall support optimizing the working and protection connection routes based on the updated SRLG information	[Gap31-2] None
[R31-3] The Optical Transport Controller shall support obtaining the GIS information of the optical cables	[Gap31-3] None
[R31-4] The Optical Transport Controller shall support obtaining the GIS information of the optical cables	[Gap31-4] None
[R31-5] The Optical Transport Controller should support reporting advance warning to the F5G E2E Orchestrator, to indicate the predicted fibre failure	[Gap31-5] Currently there is no standard YANG data models for reporting the predicted optical failure information by an Optical Transport Controller
[R31-6] The Optical Transport Controller should support rerouting the optical connection which goes through a degrading fibre	[Gap31-6] None
UC#32 AI-based PON optical path diagnosis	
[R32-1] The AI-based diagnostic technology shall support the optical power visualization in the F5G PON Access Network	[Gap32-1] None
[R32-2] The AI-based diagnostic technology shall support the recognition of optical signal fluctuating regulation and initiate an alarm	[Gap32-2] The recognition of the optical signal fluctuation and corresponding alarm generation based on AI is currently not supported in the network management system standards
[R32-3] The AI-based diagnostic technology shall support data collection within a 15 minutes time period	[Gap32-3] None
[R32-4] The AI-based diagnostic technology shall support fault identification on an hourly basis in the F5G PON Access network	[Gap32-4] The periodic fault identification capability based on AI is currently not supported in the network management system standards
R32-5] The AI-based diagnostic technology shall support fault localization in the F5G PON Access network	[Gap32-5] The fault localization function based on AI analysis is not currently supported in the network management system standards

Technology requirements	Gaps
[R32-6] The AI-based diagnostic technology shall support the generation of fault recovery solution, with step-by-step repair procedure and the corresponding impact analysis on the network services	[Gap32-6] The generation of fault recovery solution based on AI analysis is currently not supported in the network management system standards
[R32-7] The AI-based diagnostic technology shall support the generation of an optimized action list based on the deployed service priorities and the number of affected users	[Gap32-7] The generation of an optimized action list based on AI analysis is currently not supported in the network management system standards

Table 29 is a list of suggested actions to gaps found in the present document. Suggested actions for other organization or groups shall be carried out by members in corresponding organizations and groups, though a liaison shall be issued from ISG F5G. For actions assigned to ISG F5G, ISG F5G may address them in proper work items under ETSI directives.

Table 29: Suggested actions for identified gaps

SDO/Group	Suggested actions	Relevant gaps
ETSI ISG F5G	Define a high quality slicing mechanism.	Gap03-3, Gap15-3, Gap15-13
	Define the mechanisms for a large number of different parallel slices.	Gap15-4
	Define hard slicing for Wi-Fi®, CPE and PON.	Gap03-4
	Define AI based traffic and application type identification.	Gap03-5, Gap10-2
	Define E2E slicing management including management and control function requirements and network resource allocation.	Gap03-6, Gap01-11, Gap01-18
	Define slice management APIs for applications to request and release network slices.	Gap15-6, Gap15-10
	Define interface between telco network and cloud network for guaranteed services.	Gap03-8
	Define Time-of-day based SLA management interface and data models for commercial customers.	Gap03-10
	Define mechanism of fast provisioning of private line service.	Gap03-12, Gap23-5
	Define management interfaces to coordinate end-to-end path setup and release.	Gap18-3
	Define mechanism of automatic and fast fault detection, localization, demarcation, isolation and correction/recovery.	Gap03-13, Gap32-4, Gap32-5, Gap32-6
	Specify management tools and action lists of fault and service degradation issues.	Gap32-7
	Define visualized network operation SLA indicators.	Gap03-14
	Define service level slicing for OTN.	Gap02-2
	Specify on-demand ordering capability for CPE and Edge node.	Gap02-3
	Define E2E slicing mechanism with consistent SLA on multiple network segments with different physical technologies, including slice granularity.	Gap06-1, Gap10-4, Gap01-16
	Specify interworking of PON and TSN.	Gap06-3
	Specify Industrial PON ONU with industrial interfaces and protocol interpreting functions.	Gap06-4, Gap06-5
	Specify PON telemetry requirements.	Gap06-9
	Define automatic network resource allocation and configuration enabled by AI based functions within the PON system.	Gap06-9, Gap30-2, Gap30-3
	Define support for F5G network protection switching times better than 30 ms (e.g. dual-homing with Type-C in PON).	Gap24-2
	Define standards for edge/cloud computing integrated with optical F5G networks.	Gap15-11, Gap15-12
	Define a mechanism for on-demand allocation of compute resources for optimized multi-party latency optimization.	Gap18-5
	Define Industrial PON system with computing power metric for edge computing platforms.	Gap06-12
	Define application type identification mechanism.	Gap10-1
	Specify method of dynamic establishment and updates of application feature database using Big Data and Machine Learning mechanisms.	Gap10-3
	Define mechanisms to identify network usage of applications, which have potential acceleration demands.	Gap10-8
	Define mechanisms for near real-time non-intrusive monitoring of F5G network resource utilization, delay, and health status.	Gap10-10, Gap23-6, Gap25-9, Gap30-3
	Specify a light-weight Telemetry technology for Access Network.	Gap11-1

SDO/Group	Suggested actions	Relevant gaps
	Develop and specify a dedicate data model for performance monitoring and data collection for Access Network.	Gap11-2, Gap26-3, Gap26-5, Gap32-2
	Define OLT device with OTN capabilities.	Gap01-7
	Define a mechanism for transport network resource allocation and adjustment for services like Cloud VR.	Gap01-12, Gap01-13, Gap 01-14, Gap01-17
	Define a simple mechanism for bandwidth demand changing.	Gap01-15
	Specify interfaces for applications to detect service capabilities supported by the F5G network.	Gap15-2
	Define mechanisms and APIs to exchange QoE related metrics between application and network.	Gap15-7
	Specify access management mechanisms to prevent over-requesting resources from the F5G network, which are not used by the application.	Gap15-17
	Define a mechanism to learn the client and cloud side of the F5G networks addressing and building up the mapping tables (in the SMP) automatically.	Gap16-1, Gap17-1, Gap17-2
	Specify YANG models for the request for network connectivity to the cloud.	Gap16-2, Gap17-3
	Specify YANG models for OTN slice management.	Gap16-8, Gap17-11
	Specify YANG models for optical predicted and real failure information reporting.	Gap31-5
	Specify OTN signalling protocols for large scale OTN connections (plenty of OTN connections).	Gap16-9, Gap16-12, Gap17-5, Gap17-16, Gap17-12
	Define a Ethernet/TSN translation and mapping function to run on ONUs and OLTs.	Gap19-5
	Specify TSN-like features for industrial automation.	Gap21-1, Gap22-4
	Specify support of native industrial Ethernet protocols (functional and performance).	Gap21-6, Gap21-7
	Specify functional model for photonic automatic cross-connects.	Gap25-6
	Specify the P2MP aggregation network architecture.	Gap28-2
	Specify the P2MP aggregation network control and management interface and mechanisms.	Gap28-6, Gap28-7
	Specify privacy conserving mechanisms for the F5G network.	Gap30-4, GAP10-9, Gap15-15
	Define evaluation schemes for QoE of specific applications.	Gap10-6
ETSI TC Cyber	Define an appropriate method for remote attestation support in F5G network devices running period.	Gap13-3, Gap13-4
ETSI TC ATTM	Define a new approach of a digitalized ODN management system, which helps to solve the challenges in traditional ODN construction and maintenance, needs to be standardized including system architecture and its interfaces, labels for the components, and the terminals used by the workforce to capture installation data, access ODN network information, and visualize the ODN network.	Gap14-1, Gap14-2, Gap14-3
ITU-T SG15/Q6	Specify DCI range up to 100 km supporting 800 Gbits/s per channel.	Gap25-1
	Specify DCI range up to1 500 km supporting 400 Gbits/s per channel.	Gap25-2
	Specify extended C- and L-bands for the support of 120 channels with 50GHz spacing.	Gap25-3
	Specify all-optical transparent connections up to 1 500 km with 800 Gbits/s per channel.	Gap25-5
	Specify bidirectional high-speed P2MP traffic aggregation.	Gap28-1
	Specify maximum throughput for P2MP aggregation network transceivers.	Gap28-3
	Specify the bandwidth granularity of P2MP aggregation network connections.	Gap28-4
	Specify the maximum range of P2MP aggregation network connections.	Gap28-5
	Guarantee vendor interoperability the P2MP aggregation network.	Gap28-8
	Specify privacy protection mechanisms for P2MP aggregation network connections.	Gap28-9

SDO/Group	Suggested actions	Relevant gaps
ITU-T SG15/Q11	Specify finer granularity OTN. Define OTN container with flexible and/or sub 1 Gbits/s granularity.	Gap02-1, Gap02-9, Gap01-8, Gap16-4, Gap16-5, Gap17-6, Gap17-7, Gap23-1
	OTN Higher speed CPE needed.	Gap02-10
	Standardize mechanisms for non-service-affecting bandwidth adjustment below 1 Gbits/s.	Gap16-6, Gap23-2, Gap17-8
	Specify a mechanism for lossless OTN bandwidth adjustments	Gap23-3
	Optimize OTN to support mixed traffic of ODUs and OSUs.	Gap01-10
	Standardize Layer1 OSU slicing.	Gap20-5
	Specify OTN protection mechanisms such that the destination or source OTN node or port are different.	Gap16-10, Gap17-13, Gap17-14
	Specify ODU/OTU encryption.	Gap20-9, Gap21-11,Gap22-10
	Specify hard isolation of service flows.	Gap23-4
ITU-T SG15/Q2	Supporting TSN features on PON system.	Gap06-2, Gap19-2
	Increase in PON throughput via new technologies such as high-order modulation and wavelength-division multiplexing.	Gap08-1, Gap08-2
	Automatic protection switch for PON with delay compensation between the working path and the protection path to avoid service interruption.	Gap08-6
	Improve DBA to support low-latency upstream transmission with latency below 100 µs.	Gap08-7
	Enhance timing & synchronization in future PON systems to ensure end-to-end requirements are met.	Gap08-8
	Specify PON slicing. Suitable mapping of the vDBA and/or VxLAN to the service slice type and traffic isolation processes shall be considered.	Gap08-9, Gap17-9
	Realize protocol transparency in PON throughput via new technologies such as Ethernet Private Lines (EPL) and Ethernet Virtual Private Lines (EVPL).	Gap08-10
	Specify time-aware scheduling in the F5G PON access network.	Gap19-7, Gap21-3, Gap21-4, Gap22-6, Gap22-7
	Define update of ITU-T G.987.1 to support gPTP (IEEE 802.1AS [i.34]) and IEEE 1588-2019 [i.79] in ONU and OLT in PON networks	Gap19-9, Gap21-10, Gap22-9
	Specify PON upstream bandwidth in excess of 50 Gbits/s.	Gap21-9
	Specify P2P bidirectional 100 Gbits/s transmission.	Gap26-9
ITU-T SG15/Q3	Define data rate profiles for fibre-based on-premises network.	Gap04-1
	Specify low optical link budget for home networking and small building.	Gap04-3
	Specify a high priority channel for signalling in fibre networks.	Gap04-5
	Define a mechanism to recognize network signalling and protocols.	Gap04-6
	Specify proper interfaces for a fibre and wireless coordination mechanism.	Gap04-7
	Define optimized parameters transceivers for single mode fibre and new parameters of P2MP transceivers for multi-mode fibre and plastic fibre.	Gap04-8
	Define simplified authentication process.	Gap04-9
	Define a mechanism for IoT Hub to manage the coordination in low power mode between the IoT Hub and the RG.	Gap04-16
	Define a transmission QoS mechanism allowing for multi-dimension network parameters.	Gap04-17, Gap19-3, Gap19-4
	Define a direct node-to-node communication method on layer 2 for fibre-based on-premises network.	Gap04-18
	Specify symmetric data transmission data rates of 2,5 Gbits/s.	Gap04-19
	Define slicing for the FTTR/POL segment of the F5G network with slicing granularity as defined in Table 7.	Gap05-1, Gap05-2
	Specify centralized Wi-Fi® access control for FTTR/POL.	Gap05-5
	Define ONUs with low effort APs ("fit APs").	Gap05-6
IETF RATS	Define an appropriate method for secured measurement data generating.	Gap13-1
WFA	Improve EasyMesh™ to support plug-and-play setup and seamless roaming between APs.	Gap03-1
	Define slicing with quality guarantee for multi-AP.	Gap03-2

SDO/Group	Suggested actions	Relevant gaps
IEC	Define small size connectors with good protection for pre-connectorized fibres.	Gap04-11, Gap24-7
	Define small size optical and electrical hybrid cable with appropriate bend radius as well as the connectors.	Gap04-14
	Define special designs and standards for connection nodes (optical cable connectors and adapters of boxes and box products) of pre-connected ODN products to ensure appropriate link budgets, IP protection level, and service life. The criteria shall be defined for different ODN deployment scenarios.	Gap14-4, Gap14-5, Gap14-6, Gap14-7
IEEE	Specify interworking between PON networks and Wi-Fi®7.	Gap22-2
	Specify bidirectional 800 Gbits/s transmission over single or dual fibre.	Gap25-4
	No action needed.	Gaps with None

NOTE: In Table 29, there are several suggested actions related to slicing. Considering slicing may have potential impact to Cloud CO, BBF is a related organization. Similarly, 3GPP is also a reference organization for slicing related topics, when connected to mobile networks.

Annex A (informative): Bibliography

- K. Christodoulopoulos, S. Bidkar, W. Lautenschlaeger, T. Pfeiffer and R. Bonk: "Demonstration of Industrial-grade Passive Optical Network", 2022 Optical Fiber Communications Conference and Exhibition (OFC), 2022, pp. 01-03.

History

Document history		
V1.1.1	April 2023	Publication