ETSI GS F5G 003 V1.1.1 (2021-09)

GROUP SPECIFICATION

Fifth Generation Fixed Network (F5G); F5G Technology Landscape

Disclaimer

Reference

DGS/F5G-003_Techno_Landscape

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

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, explore 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) (August 2019): "Zero-touch network and Service Management (ZSM); Reference Architecture".

[i.9] ETSI GR ZSM 005 (V1.1.1) (May 2020): "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 (V2.0.30) (July 2021): "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.17] BBF TR-402: "Functional Model for PON Abstraction Interface", October 2018.

[i.19] ETSI TR 103 775: "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] ITU-T G.Sup51: "Passive optical network protection considerations".

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

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

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

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

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

[i.36] Draft-ietf-rats-architecture-07: "Remote Attestation Procedures 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] 3GPPP TR 38.801: "Study on new radio access technology: Radio access architecture and interfaces".

[i.40] IEEE 1588v2™: "Precision Time Protocol".

[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 Conformanc".

[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".

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

PIN: type of Photodiode with P-I-N structure

3.2 Symbols

Void.

3.3 Abbreviations

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

AC	Alternating Current
AES	Advance Encyption Standard
AI	Artificial Intelligence
AIM	Automated and Intelligent Management
ANN	Artificial Neural Network
AP	Access Point
APD	Avalanche PhotoDiode
API	Application Programming Interface
AR	Augment Reality
BBU	Base Band Unit
BW	BandWidth
CAN	Controller Area Network
CMI	CNC-MDSC Interface
COAP	Constrained Application Protocol
CPE	Customer Premises Equipment
CPN	Customer Premises Network
CU	Central Unit
DC	Datacentre

DL	Deep Learning
DL/UL	DownLink/UpLink
DML	Directly Modulated Laser
DU	Distributed Unit
EMC	Electric Magnetic Compatibility
EML	Electro-absorption Modulated Laser
ENI	Experiential Networked Intelligence
EPC	Enhanced Packet Core
EPON	Ethernet Passive Optical Network
EVC	Ethernet Virtual Circuit
EVPL	Ethernet Virtual Private Line
FANS	Fixed Access Network Sharing
FDD	Frequency Division Diplexing
FEC	Feed-forward Error Correction
FFC	Full Fibre Connection
FP	Fabry-Perot laser diode
FSAN	Full Services Access Network organization
FTTH	Fibre-To-The-Home
FTTR	Fibre-To-The-Room
FWA	Fixed Wireless Access
GANA	Generic Autonomic Network Architecture
GI	Guard Interval
GPON	Gigabit Passive Optical Network
GRE	Guaranteed Reliable Experience
GSMA	Global System for Mobile Communication Association
HD	High Definition
HDTV	High Definition TV
HQ	Headquarters
HTTP	HyperText Transfer Protocol
ICT	Information & Communication Technology
INT	Interoperability Testing
IOAM	In-situ Operations, Administration, and Maintenance
IP	Internet Protocol
IPFIX	Internet Protocol Flow Information Export
ISG	Industry Specification Group
KPI	Key Performance Index
LAN	Local Area Network
LC	Little Connector
LTE-A	Long Term Evolution - Advanced
MAC	Media Access Control
MANO	Management and Orchestration
MEC	Mobile Edge Computing
MEF	Metro Ethernet Forum
ML	Machine Learning
MPLS	Multiprotocol Label Switching
MQTT	Message Queuing Telemetry Transport
MU-MIMO	Multi User Multiple Input Multiple Output
NBI	North Bound Interface
NFV	Network Function Virtualization
NR	New Radio
ODN	Optical Distribution Network
ODU	Optical Data Unit
OFDMA	Orthogonal Frequency Division mMultiple access
OLT	Optical Line Terminal
OMCC	OMCI Communications Channel
OMCI	ONU Management and Control Interface
ONU	Optical Network Unit
OPEX	OPeration EXpenditure
OSI	Open Systems Interconnection
OSS	Operating Support System
OTDR	Optical Time Domain Reflectometer
OTN	Optical Transport Network

OTT	Over the Top
OTU	Optical Transport Unit
P2MP	Point-to-Multi-Points
PDH	Plesiochronous Digital Hierarchy
PDN	Public Data Network
PMD	Physical Media Dependent
POL	Passive Optical LAN
PON	Passive Optical Network
PTP	Precision Time Protocol
QAM	Quadrature Amplitude Modulation
QoE	Quality of Experience
QoS	Quality of Service
RAM	Ramdom Access Memory
RAN	Radio Access Network
RFC	Requests for Comments
RG	Residential Gateway
RJ	Registered Jack
RP	Reference Point
RPC	Remote Procedure Call
RS	Reed Solomon
RTT	Round Trip Time
SC	Square Connector
SDH	Synchronous Digital Hierarchy
SDN	Software Defined Networking
SDO	Standard Organisation
SLA	Service Level Agreement
SME	Small and Medium Enterprises
SNMP	Signalling Network Management Protocol
TC	Technical Committee
T-CONT	Traffic Container
TDD	Time Division Duplexing
TDM	Time Division Multiplexing
TDMA	Time Division Multiple Access
TEAS	Traffic Engineering Architecture and Signaling
TEE	Trusted Execution Environment
TSN	Time-Sensitive Networking
UDP	User Data Protocol
UHDTV	Ultra High Definition TeleVision
UNI	User Network Interface
URLLC	Ultra Reliable Low Latency Communication
VCSEL	Vertical-Cavity Surface-Emitting Laser
vDBA	virtual Dynamic Bandwidth Assignment
VLAN	Virtual LAN
VNO	Virtual Network Operator
VR	Virtual Reality
VxLAN	Virtual Extensible LAN
WAN	Wide Area Network
WDM	Wavelength-Division Multiplexing
WG	Working Group
WT	Working Text
XGS-PON	10-Gigabit-capable Symmetric Passive Optical Network
YANG	Yet Another Next Generation data modelling language
ZSM	Zero-touch network and Service Management

4 Technology requirements and landscape

4.1 Executive summary

This clause is reliant on the use cases as defined in [i.14] and specifies per use case the technology requirements, the current available related standards, and describes the gaps in technology 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 handled, refer to [i.14] for a detailed description of the use case. In the following, only brief use case titles are given for reference.

- Use case PON on-premises & Passive Optical LAN
- Use case High Quality Low Cost private lines for SMEs
- Use case High Quality Private Line
- Use case PON for Industrial Manufacturing
- Use case Remote Attestation
- Use case Digitalized ODN/FTTX
- Use case Scenario Based Broadband
- Use case Multiple Access Aggregation over PON (MAAP)
- Use case Telemetry-based Enhanced Performance Monitoring in Intelligent Access Network
- Use case Cloud Virtual Reality

4.2 Use case PON on-premises & Passive Optical LAN

4.2.1 Use case briefing

PON has been accepted and deployed in the market as a major solution for optical Access Network. Because of the mass deployment, the cost of PON system and optics has reduced significantly. This brings the possibility to develop an optical system like PON for on-premises networking. For example, a 10G-PON system could be leveraged as a reference technology to achieve "fibre to everything or everywhere" in F5G.

One application is FTTR (Fibre-To-The-Room). A PON like system could be used for home networks, connecting end devices (like HDTV, HD surveillance cameras and VR/AR helmets), as well as for Wi-Fi backhauling. In comparison to the current on-premises networking technologies, such as Ethernet, Wi-Fi mesh, and so on, such a system could potentially provide higher data rate, better coordination, and controlled latency.

The other application 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 PON like system would have several advantages, i.e. simple fibre deployment, wider coverage, immunity to EMI (Electro-Magnetic Interference), low power, and long life cycle.

4.2.2 Technical requirements

4.2.2.1 General

In the short term, a PON system can be directly used for on-premises LAN applications. However, the on-premises applications are quite different from that in an Access Network, leading to distinct technical requirements for network topology, optical components parameters, physical and data link layer protocol, network configuration and management should all be addressed for the fibre-based on-premises network.

4.2.2.2 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. 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.

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

[R-2] The fibre-based on-premises network shall support the coexistence of multiple generations of fibre-based on-premises technologies on the same LAN network.

[R-3] The fibre-based on-premises network shall support up to 10 Gbps date rate to deliver VR/AR service.

4.2.2.3 Lower optical link budget

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

For PON on-premises, 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 1:8 is considered to be sufficient and lower than that in the Access PON Network, which means the optical link budget can be much lower than that of a typical PON in the Access Network.

For an apartment building or SME LAN, using PON technology, the split ratio could be 1:16 or 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.

[R-4] For home networking, a split ratio of 1:8 for fibre-based on-premises network shall be supported.

[R-5] For an apartment building or SME LAN, the fibre-based on-premises network shall support a split ratio up to 1:32.

4.2.2.4 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 handover 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.

[R-6] The fibre-based on-premises network shall support a dedicated high-priority channel for exchanging handover messages in order to minimize the transmission latency over the fibre-based backhauling network.

[R-7] The fibre-based on-premises network should define a mechanism to recognize network signalling and protocols, e.g. EasyMesh™, in order to provide a high performance channel for them.

[R-8] In order to avoid any potential message contention, the optical LAN network shall define a well-coordinated mechanism for different nodes in the network.

4.2.2.5 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.

[R-9] The transceiver profile shall be optimized according to dedicated fibre deployment (including fibre topology, fibre and connector types, etc.).

4.2.2.6 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. The following are minimum requirements that an on-premises network should comply with in terms of security.

[R-10] Authentication of new devices should be supported to ensure that all devices in the network are known and safe.

[R-11] Data encryption should be supported.

4.2.2.7 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 now become common use, could 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 is defined as follows. It contains at least a PON 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 at least two branches are unequal to each other, usually the trunk branch has a higher split ratio than an ONU branch's split ratio.

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

[R-12] Fibre with pre-connectorized optical cable should be used to simplify the on-premises fibre deployment.

[R-13] A P2MP architecture should be supported.

[R-14] The uneven optical power splitter should be used for multi-floor buildings.

[R-15] Optical and electrical hybrid cable should be used for Wi-Fi AP devices.

4.2.2.8 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, which may also be battery powered, acting as a gateway between the IoT network and the residential gateway. 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. Also since the triggering of some IoT events is coming from the sensor, the IoT hub shall be able to control the low power modes.

[R-16] The fibre-based on-premises network shall support a low power mode for IoT relevant applications.

[R-17] The fibre-based on-premises network shall give permission for the IoT hub to manage the coordination in low power mode between the IoT hub and the residential gateway.

4.2.2.9 Support of network QoS

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

[R-18] The fibre-based on-premises network shall define a QoS related transmission mechanism to guarantee service quality.

4.2.2.10 Support of East-to-West data streaming

LAN network allows communication to be established between the connected devices, which represents East-to-West data communication. For example, data storage requires East-to-West transmission since data is normally transferred from a device to the data storage location.

[R-19] The fibre-based on-premises network shall support East-to-West data communication.

4.2.3 Current related standard specifications

4.2.3.1 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 1 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 1: 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 fibers	1						–
Nominal downstream line rate	10.3125						GBd
Nominal upstream line rate	1.25	10.3125	1.25	10.3125	1.25	10.3125	GBd
Nominal downstream wavelength	1577						nm
Downstream wave-length tolerance	–2, +3						nm
Nominal upstream wavelength	1310	1270	1310	1270	1310	1270	nm
Upstream wavelength tolerance	±50	±10	±50	±10	±50	±10	nm
Maximum reach[a]	≥10		≥20		≥20		km
Maximum channel insertion loss	20		24		29		dB
Minimum channel insertion loss	5		10		15		dB

4.2.3.2 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.x. GPON has a downstream capacity of 2,488 Gb/s and an upstream capacity of 1,244 Gb/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 Gb/s downstream and 2,5 Gb/s upstream (nominal line rate of 9,95328 Gb/s downstream and 2,48832 Gb/s upstream).Symmetric 10G-PON is also proposed as XG-PON2 with 10 Gb/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 2: 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, and management (OAM) information in an ITU-T PON system is carried in three ways: embedded OAM, physical layer operations, 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 Q16/SG15 has been working on Recommendation ITU-T L.109, 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. The next step for the group is to specify the system architecture of FTTR technology before defining the protocols.

4.2.3.3 Broadband Forum (BBF)

The Broadband Forum (BBF) specifies the application layer protocol 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 1 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 TR-181 [i.23]. This protocol could be extended to manage the fibre-based on-premises network.

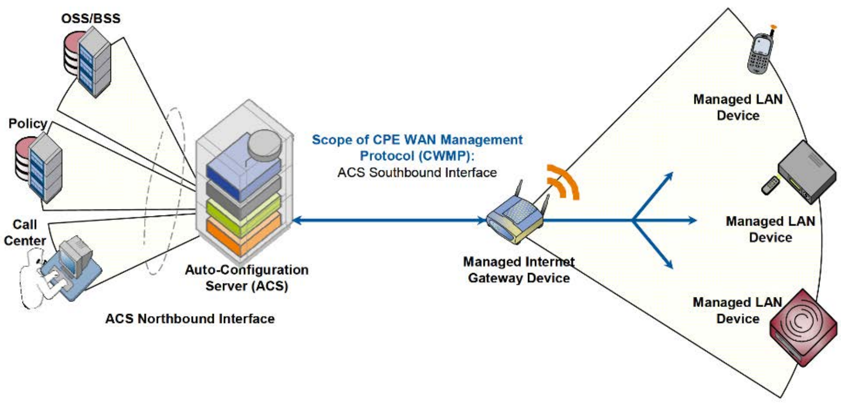


Figure 1: CWMP remote management in E2E architecture

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.

4.2.3.4 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.

4.2.4 Gap analysis

4.2.4.1 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.

4.2.4.2 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.

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

[Gap-2] None.

[Gap-3] None.

4.2.4.3 Lower optical link budget

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

[Gap-4] The optical link budget from 0~14 dB needs to be specified to support home networking.

[Gap-5] The optical link budget from 6~21 dB should be specified for small building and the link budget classes of current PON system can be used for the scenarios with high link budget.

4.2.4.4 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 support 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 bond to the transmission technology itself. Obviously, this is not optimized for the protocol.

[Gap-6] The high-priority channel for roaming does not exist in the present document.

[Gap-7] The mechanism to recognize network signalling and protocols needs to be specified.

[Gap-8] None.

4.2.4.5 Diversified transceiver and fibre types

Since different fibre deployments will lead to distinct requirements for transceiver design. Of course, to re-use the current optical components in the new design need 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 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 industry supply chain, future evolution ability and so on.

[Gap-9] Optimized parameters of transceivers (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 needs to be defined.

4.2.4.6 Network security

For traditional PON system, 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 home area or business building, the users may not be knowledgeable of the detailed security configuration.

[Gap-10] Simplified authentication process should be defined.

[Gap-11] None.

4.2.4.7 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.

[Gap-12] Small size connectors with good protection needs to be standardized.

[Gap-13] None.

[Gap-14] None.

[Gap-15] Small size optical and electrical hybrid cable with appropriate bend radius as well as the connectors need to be defined.

4.2.4.8 Power saving and management

Many of the wireline communication technologies have defined power saving mode in the specification. 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 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.

[Gap-16] None.

[Gap-17] A mechanism for IoT hub to manage the coordination in low power mode between the IoT hub and the RG needs to be defined.

4.2.4.9 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 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.

[Gap-18] The transmission QoS mechanism should allow for multi-dimension network parameters, such as data rate, round trip delay, packet error rate, etc. needs to be standardized.

4.2.4.10 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.

[Gap-19] A direct node-to-node communication method on layer 2 is not defined in the current fibre-based on-premises network.

4.3 Use case High Quality Low Cost private lines for SMEs

4.3.1 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 is proposed for these SMEs.

4.3.2 Technology Requirements

4.3.2.1 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.

4.3.2.2 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.

[R-20] The Wi-Fi APs shall support plug-and-play setup and seamless roaming between APs.

[R-21] The Wi-Fi APs shall support multi-user MIMO.

[R-22] The SME CPN shall support network slicing.

4.3.2.3 Quality assurance (bandwidth, latency, reliability)

SME users have higher requirements on bandwidth 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 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.

[R-23] Hardware slicing of the Wi-Fi, CPE, and PON shall be supported.

[R-24] E2E slicing shall be supported to isolate private line service from other users such as home broadband users and other SMEs for quality assurance.

[R-25] E2E slicing shall be supported to isolate different applications of a private line service for application quality assurance.

4.3.2.4 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.

[R-26] The SME private line network shall support high quality communication to cloud platforms of different providers.

[R-27] The interface between the network service provider and the cloud provider shall be open and interoperable.

4.3.2.5 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 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.

[R-28] A private line service should be able to be deployed on the same infrastructure as residential customers to reduce cost.

[R-29] The private line management system should enable time-of-day based SLAs, to take advantage of the different traffic profiles of business and residential customers.

4.3.2.6 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 %.

[R-30] Network should support protection to achieve network availability of 99,99 %.

4.3.2.7 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 Northbound 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 service 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.

[R-31] Fast provisioning of private line service shall be supported, which includes private line CPE and multi-APs systems plug-and-play.

[R-32] The network shall support automatic and fast fault detection, demarcation, isolation and correction.

[R-33] The network management system should be able to visualize network operation SLA indicators to end-users and operators.

4.3.3 Current related standard specifications

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

Please 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 providers 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.

4.3.4 Gap analysis

4.3.4.1 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 has defined multi-user MIMO, which supports up to 128 devices concurrently.

[Gap-20] Improvement of EasyMesh™ technology is needed for supporting better roaming performance.

[Gap-21] The slicing and quality guaranteed services are not standardized for multi-AP scenarios yet.

[Gap-22] Slicing in the CPN to meet the high quality requirements of SMEs is not defined.

4.3.4.2 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.

[Gap-23] Hard slicing of Wi-Fi, CPE, and PON is typically not supported.

[Gap-24] AI based traffic identification shall be supported to distinguish private line service from other users as well as to identify different applications of a private line service.

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.

[Gap-25] E2E slicing mechanism including management standards for fixed network needs to be defined.

4.3.4.3 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.

[Gap-26] None.

[Gap-27] Interface between telecommunication network and cloud network for guaranteed services is not specified, specifically in cases where the cloud provider and the network operator are in different administrative domains.

4.3.4.4 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.

[Gap-28] None.

[Gap-29] Time-of-day based SLA management interface and data models do not exist to the required level.

4.3.4.5 High availability and reliability

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

[Gap-30] None.

4.3.4.6 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.

[Gap-31] Fast provisioning of private line services shall be defined, which includes private line CPE and multi-APs systems plug-and-play.

[Gap-32] There are alarming and fault detection methods, but automatic and fast fault detection, demarcation, isolation, and correction need to be studied.

[Gap-33] So far there are no visualized SLA indicators for network operation.

4.4 Use case High Quality Private Line

4.4.1 Use Case briefing

High quality Private Line means 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.

4.4.2 Technology Requirements

4.4.2.1 General introduction

High quality Private Line means 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.

4.4.2.2 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 2. 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.

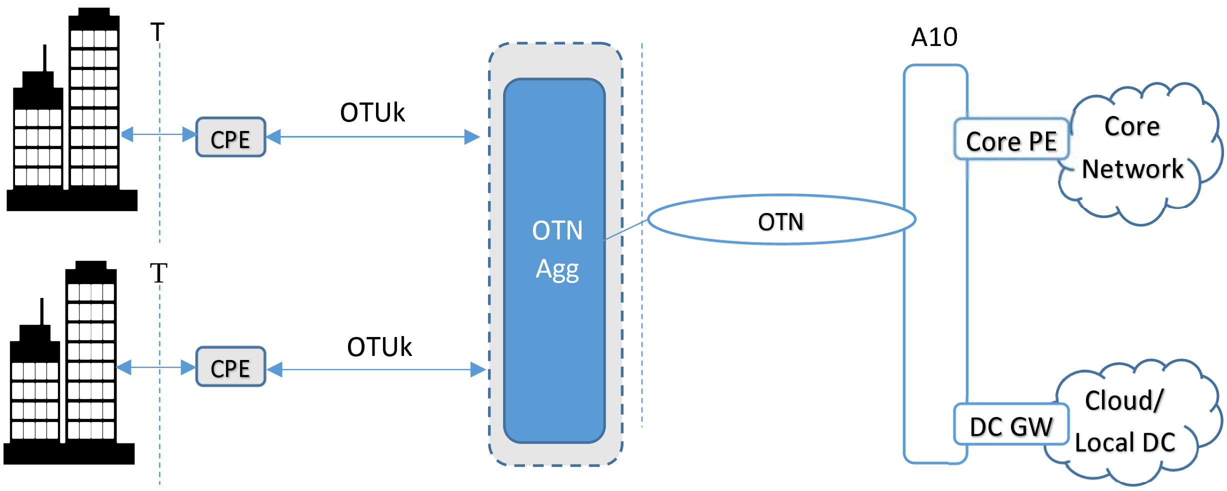


Figure 2: OTN Aggregation Equipment in the CO

4.4.2.3 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.

[R-34] The network should provide flexible bandwidth allocation.

4.4.2.4 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.

[R-35] The network should provide an end-to-end path, which is isolated from other traffic.

4.4.2.5 On Demand Ordering

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

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

[R-36] The network should provide an efficient on-demand connection provisioning and configuration system.

4.4.2.6 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 %.

[R-37] The network should provide availability of higher than 99,999 %.

4.4.2.7 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

[R-38] The network should provide deterministic low latency.

[R-39] The network should provide low latency independent of traffic load.

4.4.2.8 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.

[R-40] The network should provide dedicated access to the private Data Centres of the users.

[R-41] The network should provide dedicated access to Cloud services.

4.4.2.9 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.

[R-42] The network should provide configurable connectivity to match the user's current and future needs.

[R-43] The network should provide efficient on-demand expansion or contraction of the provided connections.

4.4.3 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:

- **G.709** Interfaces for Optical transport networks
- **G.709.1** Flexible OTN short-reach interfaces
- **G.709.2** OTU4 long-reach interface
- **G.709.3** Flexible OTN long-reach interfaces
- **G.709.4** OTU25 and OTU50 short-reach interfaces

4.4.4 Gap analysis

4.4.4.1 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 standard rate.

There is a need for a more flexible bandwidth allocation. Current OTN containers are based on ODUk and ODUCn nominal rates such as of 1,2 G, 2,5 G, 10 G, 25 G, 40 G, 50 G, 100 G, and any rate ≥ 1,25 G. 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.

[Gap-34] Finer bandwidth granularity is needed.

4.4.4.2 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 recognise 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.

[Gap-35] Service-level slicing is needed.

4.4.4.3 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.

[Gap-36] The CPE and Edge node need to support the on-demand ordering capability.

4.4.4.4 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.

[Gap-37] OTN CPE redundant connection is needed.

4.4.4.5 Low Latency

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

[Gap-38] None.

[Gap-39] None.

4.4.4.6 Private DC and Cloud access

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

[Gap-40] None.

[Gap-41] None.

4.4.4.7 Scalability

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

The current OTN is a scalable network anywhere from 1,2 G to 400 G and beyond. The legacy services such as 100 Mb/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 Gb/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.

[Gap-42] Finer OTN granularity is needed.

[Gap-43] Higher speed CPE is needed.

4.5 Use case PON for Industrial Manufacturing

4.5.1 Use Cases briefing

PON (Passive Optical Network) 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 issues 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 office network along with industrial manufacturing networks, and the data flows between these two sub-networks are very busy. It is much more cost efficient 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 PoE (Power over Ethernet) 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.

4.5.2 Technology Requirements

4.5.2.1 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 VLANs, 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 3.

Table 3: 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

[R-44] The industrial PON system shall support network slicing functionality.

4.5.2.2 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 in the IEEE 802.1 TSN (Time Sensitive Network) standards.

PON systems can provide similar features as TSN without supporting native TSN, in the case PON is 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 4.

Table 4: 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

[R-45] The industrial PON system shall support different deployment scenarios, with scenario-dependent latency, jitter and bandwidth requirements.

[R-46] Interworking functions should be supported between the industrial PON system and TSN.

4.5.2.3 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, and 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.

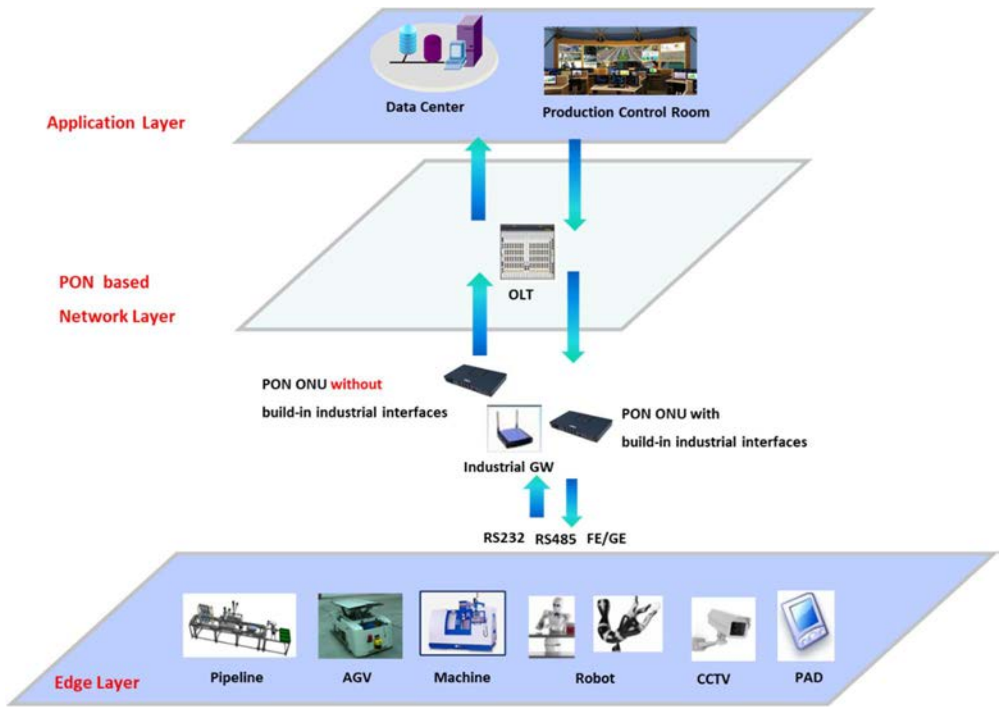


Figure 3: The architecture of the industrial interfaces and protocols carried by a PON system

[R-47] The industrial PON system should support carrying industrial protocols as well as satisfying the performance requirements of these protocols.

[R-48] The industrial PON ONU should support UNI physical interfaces other than RJ-45, including but not limited to RS-232, RS-485, and CAN.

4.5.2.4 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.

[R-49] The industrial PON system shall support protection schemes that cover OLT, ODN and ONU.

4.5.2.5 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.

[R-50] The industrial PON system shall support ONU authentication.

[R-51] The industrial PON system shall support AES data encryption functionality.

4.5.2.6 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.

For example, Netconf/YANG is nowadays the dominant solution for the smart management system, supported by typical industrial PON solution providers and major PON vendors.

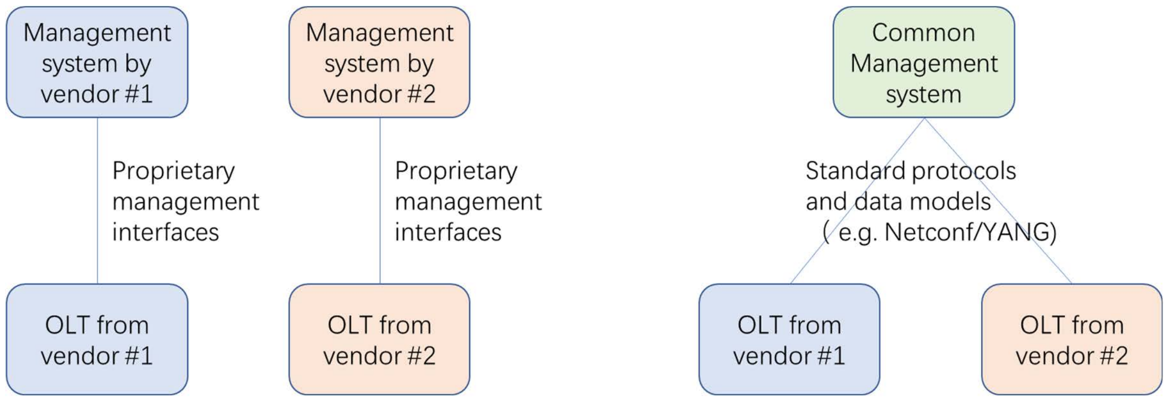


Figure 4: The comparison of vendor-specific management system and standard protocols based management system

[R-52] The industrial PON system should support standard management protocols and data models.

[R-53] The industrial PON system shall provide a GUI-based user-friendly network management system to the end users.

4.5.2.7 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.

[R-54] The industrial PON ONU shall meet the environmental adaptation requirements of the corresponding deployment scenarios.

4.5.2.8 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, to integrate 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.

[R-55] The industrial PON OLT should support embedded edge computing.

[R-56] The edge computing module should be capable of running 3rd party applications.

4.5.3 Current related standards

4.5.3.1 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.

4.5.3.2 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 ITU-T G.Sup51 [i.30] (06/2017).

4.5.3.3 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.

4.5.3.4 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.

4.5.4 Gap analysis

4.5.4.1 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 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.

[Gap-44] Slicing standards are missing for Industrial scenarios, including granularity of the network slice, the management and control function requirements, and the network resource allocations.

4.5.4.2 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.

[Gap-45] PON system needs to be optimized to support TSN features.

[Gap-46] The interworking of PON and TSN should be studied.

4.5.4.3 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.

[Gap-47] Industrial PON ONU with industrial interfaces and protocol interpreting functions is not available.

[Gap-48] Same as [Gap-47].

4.5.4.4 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.

[Gap-49] None.

4.5.4.5 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.

[Gap-50] None.

[Gap-51] None.

4.5.4.6 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.

[Gap-52] Standards are missing for PON telemetry, automatic network resource allocation and configuration enabled by AI based functions within the PON system.

[Gap-53] None.

4.5.4.7 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.

[Gap-54] None.

4.5.4.8 Edge computing

Edge computing in industrial scenarios do not emphasize NFV or SDN based functionality, but 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.

[Gap-55] There is no standard to define computing power metric for edge computing platforms on Industrial PON.

[Gap-56] None.

4.6 Use case Remote Attestation

4.6.1 Use Cases briefing

The trustworthiness of network devices (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 devices 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 devices. 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.

4.6.2 Technology Requirements

4.6.2.1 General introduction

In recent years, attacking techniques are evolving dramatically. Telecommunication network devices, 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 devices. 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 devices (attestator) that constitute the F5G network.

4.6.2.2 Secure measurement data generating, storing and reporting

A telecommunication network consists of a large number of different network devices. It is necessary for a challenger to obtain the status of trustworthiness of these devices. 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.

[R-57] An F5G network device should be able to generate measurement data, store it securely and report its integrity status in a secured manner.

4.6.2.3 Remote attestation support for device with multiple hardware architectures

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

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

In a multi-slots device, each blade contains independent hardware running its own operating system. Thus the trustworthiness of the device depends on the evidence provided by all the blades it contains. Among these blades, only a 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 device.

In a multi-chassis device, a main chassis and 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 device cluster.

[R-58] An F5G network device should be able to prove its trusted status in a proper manner, which should be suitable for its own hardware architecture.

4.6.2.4 Remote attestation support for device booting and running

Attacks can occur at every stage during a network device'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 device. Secured boot can be helpful to frustrate 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 attacking 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 device 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).

[R-59] An F5G network device should be able to prove the evidence of its trusted booting;

[R-60] An F5G network device should be able to provide the status of its trustworthiness during run-time.

4.6.3 Current related standards

4.6.3.1 IETF

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

Table 5: IETF RATS draft briefing

Documents	Summary
Draft-ietf-rats-architecture-07 Remote Attestation Procedures Architecture	This document defines a flexible architecture consisting of attestation roles and their interactions via conceptual messages.
Draft-ietf-rats-eat-04 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-modles-01 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-05 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-03 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-05]

4.6.3.2 Global Platform

GlobalPlatform 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 6: Trusted Execution Environment specifications briefing

Documents	Summary
TEE System Architecture v2.1	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	This document defines the communication between applications running in a rich operating environment and the applications residing in the TEE.

4.6.4 Gap analysis

4.6.4.1 Secured measurement data generating, storing and reporting

Recently, IETF Remote ATtestation ProcedureS (RATS) working group has published Draft-ietf-rats-reference-interaction-modles-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). GlobalPlatform™ TEE 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.

[Gap-57] An appropriate method for secured measurement data generation is requested to be studied and IETF RATS WG is considered as the suitable place to take over this task.

4.6.4.2 Remote attestation support for devices with multiple hardware architectures

Draft-ietf-rats-architecture-07 [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 device. The guidance depicted in this draft can be applied to F5G network devices.

[Gap-58] None.

4.6.4.3 Remote attestation support for device booting and running

Currently, most existing remote attestation solutions focus on the integrity of the firmware during boot time. However, carrier-level network devices 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 device 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 device.

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 devices shall be periodically challenged by the challenger to form the up-to-date status of the devices.

[Gap-59] An appropriate method for remote attestation support in F5G network devices running period is requested to be studied and ETSI TC Cyber is considered as the suitable place to take over this task.

[Gap-60] Same as [Gap-59].

4.7 Use case Digitalized ODN/FTTX

4.7.1 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.

4.7.2 Technology Requirements

4.7.2.1 General description

FTTx has been recognized by the majority of fixed network operators worldwide as a strategic approach for the deployment of broadband access. 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.

4.7.2.2 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:

[R-61] The physical labels for the various components of the ODN shall be digitized.

[R-62] The ODN intelligent management system shall support the construction and maintenance process, by automatically capturing the information about the ODN, and visualizing the networks.

[R-63] The ODN intelligent management system shall support troubleshooting by remotely accessing the ODN database by technicians.

4.7.2.3 ODN quick construction based on pre-connection

To support ODN quick construction, there are some requirements for pre-connection:

[R-64] The pre-connection shall be applicable to different types of ODN connectors and boxes (including outdoor adapters) and to various environments (indoor, outdoor, simple and complex).

[R-65] The connection shall meet the appropriate Ingress Protection (IP) level depending on the scenario (such as ingress protection rating IP68 and IP65 [1]).

[R-66] The connectors shall ensure low insertion loss in order to meet the link loss requirements of the ODN.

[R-67] The quick connection and installation process shall meet the long-term reliability test requirements (for example, 2 000-hour, dual 85-hour test for closures) and mechanical test requirements (for example, optical cable tension and strain requirements) during onsite construction and deployment.

4.7.3 Current related standards

4.7.3.1 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.

4.7.3.2 ITU-T

Recommendation ITU-T L.100 to L.199 are standards for optical fibre cables, including cable structure and characteristics, cable evaluation, guidance and installation technique; L.200 to L.299 are optical infrastructure standards, focusing on infrastructure including node elements (except cables), general aspects and network design. L.300 to L.399 are maintenance and operation standards that include optical fibre cable maintenance, infrastructure maintenance, operation support and infrastructure management and disaster management.
Recommendation ITU-T L.400 - L.429 focuses on passive optical devices standards.

In conclusion, similar to IEC, the ITU standardizes the single-point product solution and corresponding test requirements for optical fibres, cables, and node boxes. The OTDR (Optical Time Domain Reflectometer) and reflector detection solutions are used in traditional ODN network construction and maintenance.

4.7.3.3 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.

4.7.4 Gap analysis

4.7.4.1 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.

4.7.4.2 ODN digital management

[Gap-61] 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.

[Gap-62] Same as [Gap-61].

[Gap-63] Same as [Gap-61].

4.7.4.3 ODN quick 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.

[Gap-64] 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.

[Gap-65] Same as [Gap-64].

[Gap-66] Same as [Gap-64].

[Gap-67] Same as [Gap-64].

4.8 Use case Scenario Based Broadband

4.8.1 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 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 game 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.

4.8.2 Technology Requirements

4.8.2.1 General

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.

4.8.2.2 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 DPI (Deep Packet Inspection). 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.

[R-68] The network shall support application type (video, file transfer, Internet browsing, etc.) identification.

[R-69] The network should support AI based application type identification.

4.8.2.3 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 network actions for experience guarantee. 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.

[R-70] The application feature database for AI should be established and updated in real-time or periodically.

4.8.2.4 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.

[R-71] The network shall support slicing with different service characteristics.

4.8.2.5 QoE evaluation

The network shall be able to evaluate current QoE performance and verify if 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.

[R-72] The network shall support QoS evaluation.

[R-73] The network should support QoE evaluation.

4.8.2.6 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.

[R-74] The network should be able to identify network usage of applications, which potentially have acceleration demands. The network usage of such applications may be linked to a specific user, only if this is explicitly within the scope of the user's service level agreement. Otherwise, linking should be restricted to an anonymized group of users.

4.8.2.7 The network capacity monitoring and expansion prediction

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

[R-75] The network shall be able to monitor network resource utilization and their health status.

4.8.3 Current related standards

4.8.3.1 ITU

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.

4.8.3.2 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.

4.8.3.3 ETSI

ETSI TC MEC works on:

1) Increasing the accessibility and adoption of MEC specifications by exposing OpenAPI™ (aka 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.

4.8.3.4 Artificial Intelligence

Please refer to clause 5.6 about current status of AI.

4.8.4 Gap analysis

4.8.4.1 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" network. 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 DPI (Deep Packet Inspection) used to identify the traffic of different services. This kind of mechanism may distinguish different types of service 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 App when mass samples are used to train the AI data model. The more times 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.

[Gap-68] Define application type identification mechanism.

[Gap-69] Application of AI architecture for identification of applications in a F5G network.

4.8.4.2 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 Layer2 or Layer3 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.

[Gap-70] The dynamic creation and updates of application feature database entries using Big Data and Machine Learning mechanisms need to be defined.

4.8.4.3 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 QoE (Quality of Experience) 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.

[Gap-71] Mechanisms for F5G end to end slicing with consistent SLA on multiple network segments with different physical technologies are needed.

4.8.4.4 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.

[Gap-72] None.

[Gap-73] Evaluation schemes for QoE of specific applications are needed.

4.8.4.5 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.

[Gap-74] Mechanisms to identify network usage of applications, which potentially have acceleration demands.

4.8.4.6 Network status monitoring

In past networks before 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.

[Gap-75] Mechanisms for near real-time monitoring of F5G network resource utilization and health status.

4.9 Use case Multiple Access Aggregation over PON (MAAP)

4.9.1 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 3GPPP 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 brings additional possibilities and complexity when analysed from a PON perspective being addressed in a specific use case.

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.

4.9.2 Technology requirements

4.9.2.1 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 more.

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 interface 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.

4.9.2.2 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.

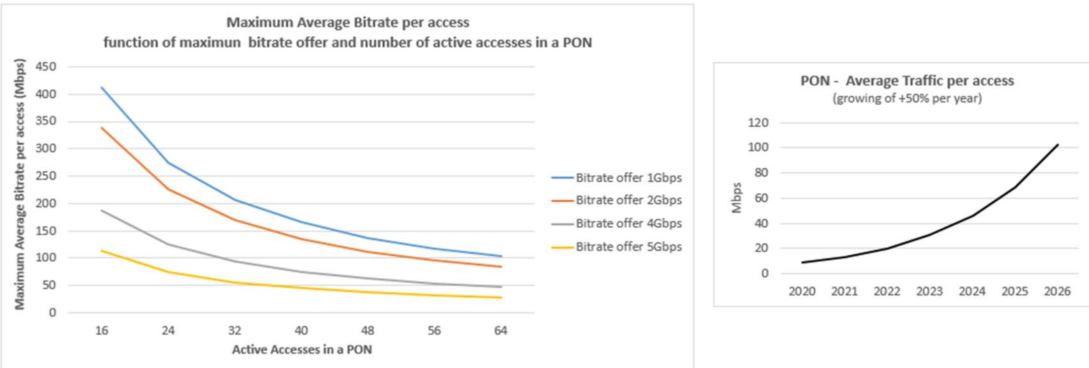
With current GPON, and even with new XGS-PON implementations, some improvements can be made in order to enhance the OMCC bandwidth allocation and inter-gap allocations (guard band, preamble and delimiter), without detriment of ONU's inband management and bandwidth map assignments, freeing up PON upstream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

Table 7: 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 B2C clients due to the FTTH market massification 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 in the next 3 years.



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

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

If in addition to 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 8: 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 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 2 or 3 years from now it will start to show its bandwidth limitations.

Due to the complexity (In Side 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.

[R-76] For GPON, XGS-PON and future generation PON systems the OMCC bandwidth allocation and inter-gap allocations shall be revised in order to reduce fixed bandwidth reserved for the OMCC channels.

[R-77] For Multiple Access Aggregation over PON higher capacity solutions are required.

[R-78] The new PON technologies shall allow a seamless integration with existing PON ecosystem.

[R-79] The new PON technologies shall support multiple services (B2B, B2C and mobile xhaul) in the same PON.

4.9.2.3 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-localized or not.

If PONs are in the same OLT, the features associated with PON switching can be applicable in a monolithic or 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.

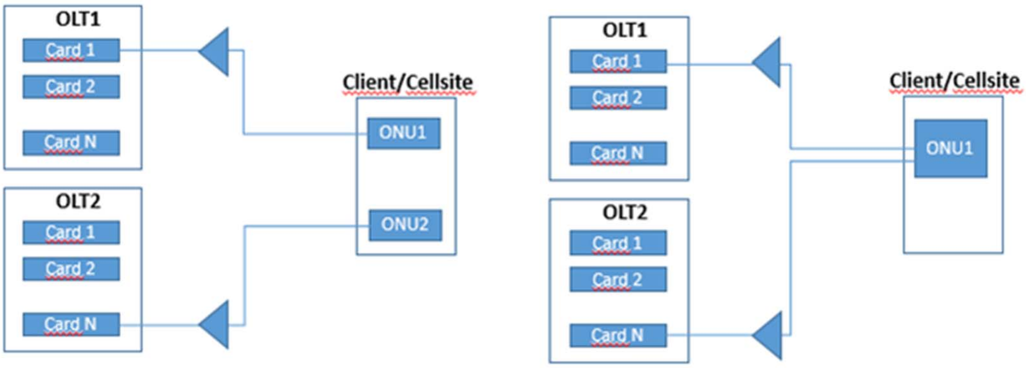


Figure 6: Protection schemes

[R-80] For Multiple Access Aggregation over PON a protection solution between two distinct OLT, using single or dual ONU, shall be available.

[R-81] For Multiple Access Aggregation over PON the automatic protection switching solution shall be based on performance degradation statistics.

4.9.2.4 Latency

Ultra-low latency and low jitter communication is becoming an important requirement for future Access Networks, mainly for URLLC and mMTC services. PONs are known to be a resource efficient and low cost technology for 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 9: 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 service the other for uRLLC service.
- 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, 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 10: 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

[R-82] PON shall support distinct type of services based on different latency, jitter and bandwidth requirements.

4.9.2.5 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 1588v2/PTP for network time synchronization.

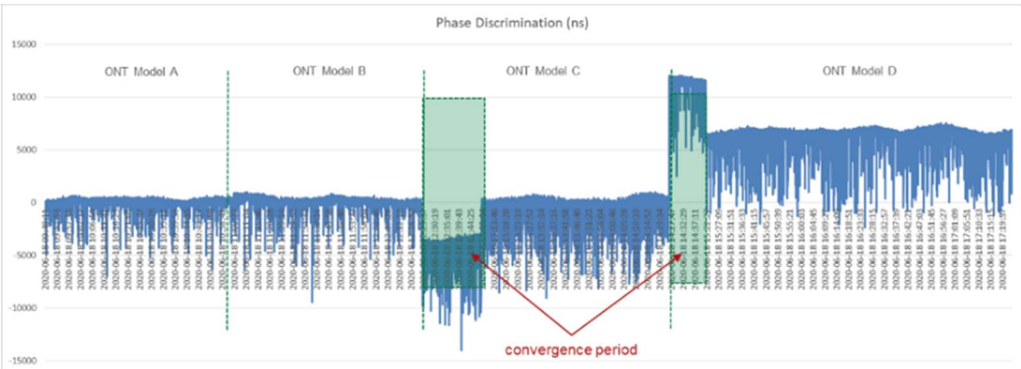


Figure 7: Example of phase discrimination measured in a GPON solution

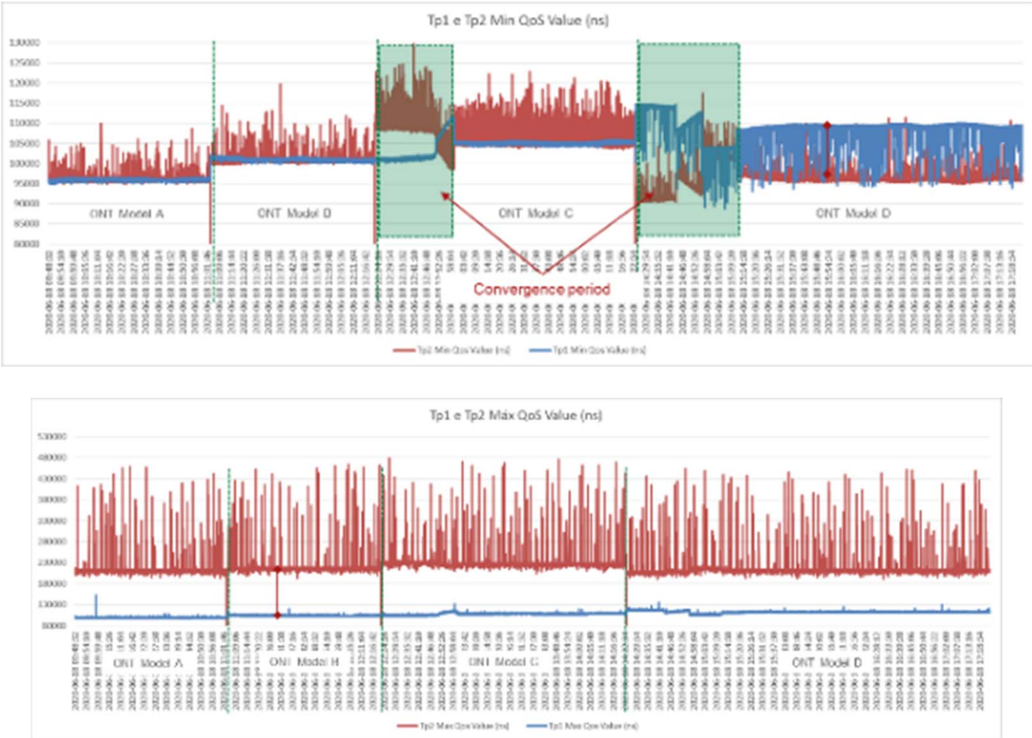


Figure 8: Example of PDV for downlink (Tp1) and uplink (Tp2) measured in a GPON solution

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.

[R-83] For Multiple Access Aggregation over PON, PON systems shall support specific and tight synchronization requirements set for the end-to-end time accuracy in 5G networks.

4.9.2.6 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 also 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 steering 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.

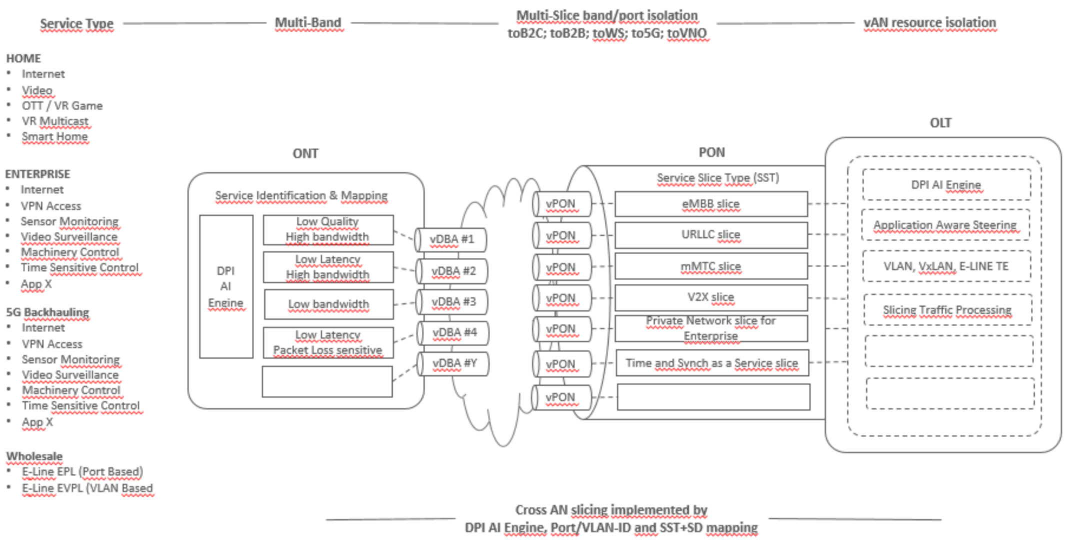


Figure 9: Example of an Access Network slicing model

[R-84] For Multiple Access Aggregation over PON, slices for different mobile and fixed service levels shall be supported

4.9.2.7 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 V-ID or Port based mappings, they are not completely fully transparent, meaning that some protocol's frame are still going to CPU.

Future Access Networks 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.

[R-85] For Multiple Access Aggregation over PON, PON systems shall ensure protocol transparency.

4.9.3 Current related standard specifications

4.9.3.1 ITU-T

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

Its evolution, XG-PON standards are published in the G.987.x series Recommendations [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 Recommendations G.987 [i.28].

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

ITU-T also defined PON system protection schemes as ITU-T G.Sup51 (06/2017).

In 2018, ITU-T established the high-speed passive optical network (HSP) project to define the next generation PON. 50-Gb/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, 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.
- ITU-T G.hsp.50GPMD, describing the Physical Media Dependent (PMD) layer specifications based on 50-Gb/s time-division multiplexing PON (TDM PON).
- ITU-T G.hsp.TWDMPMD, describing the PMD layer specifications of time-and-wavelength-division multiplexing PON (TWDM-PON) with per-channel data rate at up to 50 Gb/s. This standard is under development.
- ITU-T G.hsp.comTC, 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.
- ITU-T G.WDMPON, describing Point-to-Point (P2P) wavelength-division multiplexing PON (WDM-PON) with over 40 total wavelength channels for both directions at up to 25-Gb/s per wavelength channel. This standard is still under development.

Also, ITU has been making G.989 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 (ORAN) alliance is working on the specification of the cooperative transport interface, while the G.989 Amendments provide all the protocol elements needed to communicate with the OLT. Moreover, ITU is working on G.sup.66 for 5G applications in a PON context, and specifying the needed interfaces such as the F1 and Fx interfaces in the ORAN terminology.

4.9.3.2 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.

4.9.3.3 IEEE

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

4.9.3.4 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.

4.9.3.5 MEF

MEF 6.3 [i.46**]** defines several Subscriber Ethernet Service Types that are used to create Point-to-Point, Multipoint-to-Multipoint, and Rooted-Multipoint 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.

4.9.3.6 BBF

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

4.9.4 Gap analysis

4.9.4.1 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.

4.9.4.2 Bandwidth

Based on Table 2, 5G xHaul requires backhaul and midhaul interface bit rates of 4 Gb/s. When a PON system is used to aggregate 16, 32 and 64 such interfaces, the required net data rates are 64 Gb/s, 128 Gb/s and 256 Gb/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.

[Gap-76] Increase in PON throughput via new technologies such as high-order modulation and wavelength-division multiplexing.

[Gap-77] Same as [Gap-55].

[Gap-78] None.

[Gap-79] None.

[Gap-80] None.

4.9.4.3 Protection

Based on Figure 4, 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, i.e. cause no interruption of the mission critical services. This would require the delay compensation between the working path and the protection path. This has not been done in current PON systems.

[Gap-81] Automatic protection switch with delay compensation between the working path and the protection path to avoid service interruption.

4.9.4.4 Latency

Based on Table 3, 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.

[Gap-82] Improved DBA to support low-latency upstream transmission with latency below 100 µs.

4.9.4.5 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.

[Gap-83] Enhanced timing & synchronization in future PON systems to ensure end-to-end requirements are met.

4.9.4.6 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.

[Gap-84] Introduce slicing in PON with suitable mapping of the vDBA and/or VxLAN to the service slice type and traffic isolation processes.

4.9.4.7 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.

[Gap-85] Realize protocol transparency in PON throughput via new technologies such as Ethernet Private Lines (EPL) and Ethernet Virtual Private Lines (EVPL).

4.10 Use case 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 Network.

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 technics, which can provide a lower resource utilisation 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.

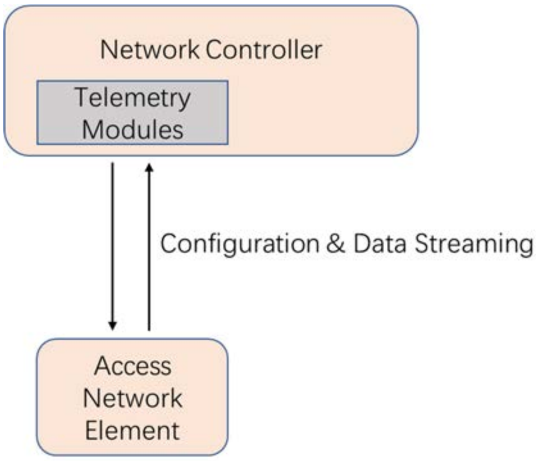


Figure 11: Telemetry based network monitoring scheme

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.

[R-86] The Access Network shall support telemetry-based network performance monitoring technics in order to provide better service experiences.

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.

[R-87] Data models regarding configuration and data collection should be defined for the Access Network to realize telemetry.

4.10.3 Current related standards

4.10.3.1 BBF

BBF defines the Access Network YANG models, such as TR-383 [i.48] and 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 TR-436 [i.50] and WT-477 [i.51]. 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.

WT-477 [i.51] has started discussion of telemetry, which is specific mapping of 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 11 and 12 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 11: Telemetry related RFC

Related RFCs	Description
IETF RFC 8641 (was draft-ietf-netconf-yang-push)	Subscription to YANG Notifications for Datastore Updates

Table 12: Telemetry related IETF working drafts

Related IETF working drafts	Description
draft-song-opsawg-ntf-06	Network Telemetry Framework
draft-ietf-netconf-udp-pub-channel-03	UDP based Publication Channel for Streaming Telemetry
draft-openconfig-rtgwg-gnmi-spec-01	gRPC Network Management Interface (gNMI)
draft-song-opsawg-ifit-framework-14	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 Network.

4.10.4 Gap analysis

4.10.4.1 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 Network 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 grows. Novel lightweight telemetry technology such as UDP-based telemetry should be further studied and deployed.

[Gap-86] Specify a lightweight Telemetry technology, such as UDP based telemetry, for Access Network telemetry.

4.10.4.2 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.

[Gap-87] Develop and specify a dedicate data model for performance monitoring and data collection for Access Network.

4.11 Use case Cloud Virtual Reality

4.11.1 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. Ethernet) and do not need further discussion.

4.11.2 Technical requirements

4.11.2.1 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, and ultimate-experience phases. The network requirements of Cloud VR for each phase are shown in Table 13.

NOTE 1: There are other sources mention similar network requirements e.g. https://www.gsma.com/futurenetworks/wiki/cloud-ar-vr-whitepaper/. 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 13 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	≥ 6 5Mbps	≥ 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.

[R-88] For each phase of Cloud VR the network shall meet the corresponding network performance requirements.

4.11.2.2 High performance channel requirements

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, the bandwidth requirements are 540 Mbps and 1,5 Gbps. The theoretical data rate of Wi-Fi 6 standard are shown in Table 14, and due to interference in 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-Fi6 can meet the bandwidth requirements of Cloud VR services and Wi-Fi slicing technology can provide lower latency.

Table 14: Data rate of Wi-Fi standards depending on the antenna configuration

IEEE Protocol	Frequency	Theoretical Data Rate
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 14, latency and jitter are not mentioned as it is assumed they do not change for different antenna capabilities.

[R-89] To meet Cloud VR ideal or ultimate experience, the terminal shall have advanced antenna configuration.

[R-90] To meet Cloud VR ideal or ultimate experience, Wi-Fi 6 slicing shall be supported.

Access network performance

In ideal and ultimate experience phases, the average bit rate of a single channel of Cloud VR is 270 Mbps and 770 Mbps respectively. It can be seen in Table 15, 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 15 that XG PON should have a split ratio less than 1:16 to meet ultimate experience phase. In addition, a low latency scheduling algorithm shall be used to reduce the latency and delay jitter of the Access Network part.

Table 15: 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

[R-91] To meet Cloud VR ideal and ultimate experience phases XG PON shall be used.

[R-92] To meet Cloud VR ultimate experience phase, the split ratio of XG PON shall be less than 1:16.

[R-93] To achieve low latency and delay jitter a low latency scheduling algorithm shall be used in the Access Network.

OLT Enhancement

Current OLT are Ethernet based and all traffic is switched via a layer 2 switch, which is responsible for routing 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 allocate 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 requires 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 Mb/s to 770 Mb/s. Current ODUj (j = 0, 1, 2, 3, 4, flex) nominal minimum bit rate is 1,25 Gb/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 Mb/s to 770 Mb/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 as Optical Service Unit (OSU), which will support client rates from 2 Mb/s to 1 GB/s, which is an efficient mechanism to transport Cloud VR traffic from the OLT to the Cloud VR data centre.

[R-94] In the case that OTN is used, the OLT should support OTN capabilities.

[R-95] OTN shall support variable size containers to match the Cloud VR bit rate from 40 Mb/s to 770 Mb/s.

Metro network performance

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

Table 16: Metro network rate requirements

User Number	VR User Penetration Rate	Peak Concurrency Rate	Bit Rate (Mbps)	Data Rate Requirement (Gbps)
20 000	50 %	20 %	280 (Idea 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 need 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 isolated the traffic from existing internet services traffic. To implement this, an ONU identifies Cloud VR traffic and directs it to the independent channel provided. 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 singularity case 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 singularity case however if other uses remain on the service then the slice bandwidth needs to seamlessly decrease without interference with the other users.

[R-96] Taking the capacity, reach and high quality needs into account, OTN shall be deployed in the metro network.

[R-97] For fair experience phases, the Cloud VR service shall have higher scheduling priority compared with other Internet services.

[R-98] For comfortable, ideal and ultimate experience phases, the Cloud VR service requires lower latency and delay jitter in the network, so a high quality independent channel shall be used.

[R-99] When a Cloud VR service is established or released, the link bandwidth of the Cloud VR transport network shall automatically increase or decrease the bandwidth to accurately meet the bandwidth requirements of the Cloud VR service in a seamlessly manner.

4.11.2.3 Dynamic channel requirements

When the Cloud VR service is transported via 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, metro network and data centre parts. The data plane and management plane of each part is independent from each other. Hence, the channel setup mechanism of each part is also different and independent. To improve the efficiency of the network, these four parts 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.

[R-100] The network shall support dynamic set up and release of the high-quality network channel for Cloud VR service to guarantee the performance of Cloud VR service and increase the transmission efficiency of the network.

[R-101] The independent management systems should support a mechanism that dynamically sets up the end to end channel.

[R-102] To support bandwidth demand changes a simple mechanism is required with minimal interaction with the management layer.

4.11.2.4 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 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 13, the four levels of VR experiences, require channel data rates from 40 Mbit/s to 770 Mb/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.

[R-103] Cloud VR traffic shall be transported on a dedicated slice on the chosen network.

[R-104] The slice shall match the Cloud VR bandwidth requirements in an efficient manner.

[R-105] The slice shall have E2E coordinated management support.

4.11.3 Current related standard specifications

For the current related standard specifications refer to in clause 5.

4.11.4 Gap analysis

4.11.4.1 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 13. The following clauses elaborate on the potential gaps to meet these performance parameters.

[Gap-88] None.

4.11.4.2 High performance channel requirements

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.

[Gap-89] 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.

[Gap-90] None.

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.

[Gap-91] None.

[Gap-92] None.

[Gap-93] None.

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 Mb/s to 770 Mb/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 GB/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 %.

[Gap-94] The OLT should support OTN capabilities.

[Gap-95] OTN container with flexible and small granularity to efficiently support Cloud VR traffic is missing.

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.

[Gap-96] 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 metro network then there is no gap in technology deployment. The only available OTN container is nominally 1,25 G, 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 400G, by using muxing of ODU4 into ODUC4, up to 320 channels can be obtained, which is a very inefficient use of the metro core network bandwidth, assuming all the traffic is of Cloud VR type. But metro core shall support a variety of traffic bandwidth including 400GE. However if for example the Cloud VR bit rate of 40 Mb/s is considered and using OSU then an OTU4 could carry around 2 380, and ODU0 (nominal rate 1,25 Gb/s) can carry 30 channels.

[Gap-97] OTN support for mixed traffic of ODUs and OSUs need to be defined.

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

[Gap-98] Need coordination of network slicing between home network, Access Network and metro network to form an end-to-end slice to meet end-to-end latency requirement.

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.

[Gap-99] When a Cloud VR session is established or released, the link bandwidth of the Cloud VR transport network should automatically increase or decrease to accurately meet the bandwidth requirements of the online Cloud VR service in a seamlessly manner, such a method is missing.

4.11.4.3 Dynamic channel setup and release

The management plane for the home network, Access Network, metro 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 E2E on demand request are difficult to coordinate. A simple handshake mechanism with minimal need for inter management coordination is missing.

[Gap-100] Each part of the network channel needs to support the coordinated management plane to setup or release a channel for Cloud VR service.

[Gap-101] Same as [Gap-79].

[Gap-102] A simple mechanism for dynamic bandwidth changes with minimal need for inter management coordination is missing.

4.11.4.4 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.

[Gap-103] E2E service isolation via slicing is missing.

[Gap-104] Bandwidth matching is missing.

[Gap-105] Simplified E2E slice management is missing.

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 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 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 us. 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 x 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 17.

Table 17: 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 x 980	1,2 Gbps
	2				2 x 980	2,4 Gbps
	4				2 x 980	4,8 Gbps
	8				2 x 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 (G.984 series), 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 12.

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.

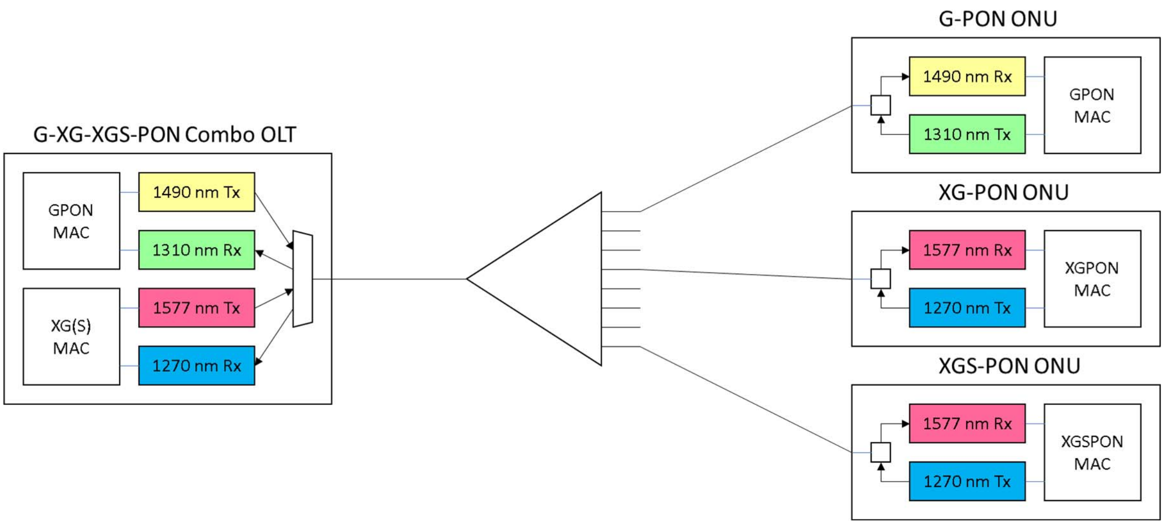


Figure 12: Triple coexistence in the ITU PON framework

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 Broadband Forum (BBF) TR-69. 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 TR-156 [i.54] and TR-167 [i.55] that describe the compliance requirements for ONUs, TR-247 [i.53] which defines the test plan to confirm ONU compliance, and 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 units (OTU) ranging from 2,66 Gb/s (OTU1) to 112 Gb/s (OTU4)) and n × 105 Gb/s (OTUCn). The client signals are wrapped into optical data units (ODUs) whose nominal data rates include 1,25Gb/s (ODU0), 2,5 Gb/s (ODU1), 10 Gb/s (ODU2), 40 Gb/s (ODU3), 100 Gb/s (ODU4)), and any-rate ≥ 1 25 Gb/s ODUflex. These ODUs are transported over ODU links with 1,25 Gb/s or 5,24 Gbit/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 metro 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 Gb/s down to 2 Mb/s. To transport the ever-increasing network traffic, OTN is evolving to support beyond 400 Gb/s per wavelength channel, achieving an aggregated per-fibre transmission capacity of over 40 Tb/s when wider bandwidth optical amplifiers are used. To reduce the transport latency and energy consumption, optical cross connects (OXC) with multi-degree Reconfigurable Optical Add/Drop Multiplexers (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 Gb/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 1Gb/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 Gb/s up to 400 G by use of ODUflex. All Ethernet frames are carried transparently end to end.

Work is progressing in ITU Study Group 15 Question 11 and management in Question 12 to support sub-1Gbs, so legacy traffic like 1 Mb/s-10 Mb/s-100 Mb/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 & Analysis 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 Management and control of Optical Transport Network

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 Access 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 section 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 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 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 [i.8].

ML/AI is one of the means of automation considered for the end-to-end automation in ZSM. In [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 White Paper [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 18. The topics listed in Table 18 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 [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" [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 [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 18: 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 19 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 [Gap-xx]".

Table 19: Summary of Requirements and Gaps

Use Case		Technology requirements	Gaps
#04	Use case PON on-premises & Passive Optical LAN	[R-1] The fibre-based on-premises network shall support multiple profiles (in terms of data rate) for different types of network device. [R-2] The fibre-based on-premises network shall support the co-existence of multiple generations of fibre-based on-premises technologies on the same LAN network. [R-3] The fibre-based on-premises network shall support up to 10 Gbps date rate to deliver VR/AR service. [R-4] For home networking, a split ratio of 1:8 for fibre-based on-premises network shall be supported. [R-5] For an apartment building or SME LAN, the fibre-based on-premises network shall support a split ratio up to 1:32. [R-6] The fibre-based on-premises network shall support a dedicated high-priority channel for exchanging handover messages in order to minimize the transmission latency over the fibre-based backhauling network. [R-7] The fibre-based on-premises network should define a mechanism to recognize network signalling and protocols, e.g. EasyMesh™, in order to provide a high performance channel for them. [R-8] In order to avoid any potential message contention, the optical LAN network shall define a well-coordinated mechanism for different nodes in the network. [R-9] Transceiver profile shall be optimized according to dedicated fibre deployment (including fibre topology, fibre and connector types, etc.).	[Gap-1] Variety of data rate profiles for fibre-based on-premises network in terms of modulation bandwidth, high modulation scheme, etc. are not available in the current standard. [Gap-2] None. [Gap-3] None. [Gap-4] The optical link budget from 0~14 dB needs to be specified to support home networking. [Gap-5] The optical link budget from 6~21 dB should be specified for small building and the link budget classes of current PON system can be used for the scenarios with high link budget. [Gap-6] The high-priority channel for roaming does not exist in the current standard. [Gap-7] The mechanism to recognize network signalling and protocols needs to be specified. [Gap-8] None. [Gap-9] Optimized parameters of transceivers (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 needs to be defined. [Gap-10] Simplified authentication process should be defined. [Gap-11] None. [Gap-12] Small size connectors with good protection needs to be standardized. [Gap-13] None. [Gap-14] None.

Use Case		Technology requirements	Gaps
		[R-10] Authentication of new devices should be supported to ensure that all devices in the network are known and safe. [R-11] Data encryption should be supported. [R-12] Fibre with pre-connectorized optical cable should be used to simplify the on-premises fibre deployment. [R-13] A P2MP architecture should be supported. [R-14] The uneven optical power splitter should be used for multi-floor buildings. [R-15] Optical and electrical hybrid cable should be used for Wi-Fi AP devices. [R-16] The fibre-based on-premises network shall support a low power mode for IoT relevant applications. [R-17] The fibre-based on-premises network shall give permission for the IoT Hub to manage the coordination in low power mode between the IoT Hub and the residential gateway. [R-18] The fibre-based on-premises network shall define a QoS related transmission mechanism to guarantee service quality. [R-19] The fibre-based on-premises network shall support East-to-West data communication.	[Gap-15] Small size optical and electrical hybrid cable with appropriate bend radius as well as the connectors need to be defined. [Gap-16] None. [Gap-17] A mechanism for IoT Hub to manage the coordination in low power mode between the IoT Hub and the RG needs to be defined. [Gap-18] The transmission QoS mechanism should allow for multi-dimension network parameters, such as data rate, round trip delay, packet error rate, etc. needs to be standardized. [Gap-19] A direct node-to-node communication method on layer 2 is not defined in the current fibre-based on-premises network.
#3	Use case High Quality Low Cost private lines for SMEs	[R-20] The Wi-Fi APs shall support plug-and-play setup and seamless roaming between APs. [R-21] The Wi-Fi APs shall support multi-user MIMO. [R-22] The SME CPN shall support network slicing. [R-23] Hardware slicing of the Wi-Fi, CPE, and PON shall be supported. [R-24] E2E slicing shall be supported to isolate private line service from other users such as home broadband users and other SMEs for quality assurance. [R-25] E2E slicing shall be supported to isolate different application types of a private line service for application quality assurance. [R-26] The SME private line network shall support high quality communication to cloud platforms of different providers. [R-27] The interface between the network service provider and the cloud provider shall be open and interoperable. [R-28] A private line service should be able to be deployed on the same infrastructure as residential customers to reduce cost. [R-29] The private line management system should enable time-of-day based SLAs to take advantage of the different traffic profiles of business and residential customers. [R-30] Network should support protection to achieve network availability of 99,99 %. [R-31] Fast provisioning of private line service shall be supported, which includes private line CPE and multi-APs systems plug-and-play. [R-32] The network shall support automatic and fast fault detection, demarcation, isolation and correction.	[Gap-20] Improvement of EasyMesh™ technology is needed for supporting better roaming performance. [Gap-21] The slicing and quality guaranteed services are not standardized for multi-AP scenarios yet. [Gap-22] Slicing in the CPN to meet the high quality requirements of SMEs is not defined. [Gap-23] Hard slicing of Wi-Fi, CPE, and PON is typically not supported. [Gap-24] AI based traffic identification shall be supported to distinguish private line service from other users as well as to identify different application types of a private line service. [Gap-25] E2E slicing mechanism including management standards for fixed network needs to be defined. [Gap-26] None. [Gap-27] Interface between telecommunication network and cloud network for guaranteed services is not specified, specifically in cases where the cloud provider and the network operator are in different administrative domains. [Gap-28] None. [Gap-29] Time-of-day based SLA management interface and data models do not exist to the required level. [Gap-30] None. [Gap-31] Fast provisioning of private line services shall be defined, which includes private line CPE and multi-APs systems plug-and-play. [Gap-32] There are alarming and fault detection methods, but automatic and fast fault detection, demarcation, isolation and correction need to be studied. [Gap-33] So far there are no visualized SLA indicators for network operation.

Use Case		Technology requirements	Gaps
		[R-33] The network management system should be able to visualize network operation SLA indicators to end-users and operators.	
#2	Use case High Quality Private Line (see note)	[R-34] The network should provide flexible bandwidth allocation. [R-35] The network should provide an end-to-end path, which is isolated from other traffic. [R-36] The network should provide an efficient on-demand connection provisioning and configuration system. [R-37] The network should provide an availability of higher than 99,999 %. [R-38] The network should provide deterministic low latency. [R-39] The network should provide low latency independent of traffic load. [R-40] The network should provide dedicated access to the private Data Centres of the users. [R-41] The network should provide dedicated access to Cloud services. [R-42] The network should provide configurable connectivity to match the user's current and future needs. [R-43] The network should provide efficient on demand expansion or contraction of the provided connections.	[Gap-34] Finer bandwidth granularity is needed. [Gap-35] Service level slicing is needed. [Gap-36] The CPE and Edge node need to support the on-demand ordering capability. [Gap-37] OTN CPE redundant connection is needed. [Gap-38] None. [Gap-39] None. [Gap-40] None. [Gap-41] None. [Gap-42] Finer OTN granularity is needed. [Gap-43] Higher speed CPE is needed.
#6	Use case PON for Industrial Manufacturing	[R-44] The industrial PON system shall support network slicing functionality. [R-45] The industrial PON system shall support different deployment scenarios, with scenario-dependent latency, jitter and bandwidth requirements. [R-46] Interworking functions should be supported between the industrial PON system and TSN. [R-47] The industrial PON system should support carrying industrial protocols as well as satisfying performance requirements of these protocols. [R-48] The industrial PON ONU should support other UNI physical interfaces other than RJ-45, including but not limited to RS-232, RS-485, and CAN. [R-49] The industrial PON system shall support protection schemes that cover OLT, ODN and ONU. [R-50] The industrial PON system shall support ONU authentication. [R-51] The industrial PON system shall support AES data encryption functionality. [R-52] The industrial PON system should support standard management protocols and data models. [R-53] The industrial PON system shall provide a GUI-based user-friendly network management interface to the end users. [R-54] The industrial PON ONU shall meet the environmental adaptation requirements of the corresponding deployment scenarios. [R-55] The industrial PON OLT should support embedded edge computing. [R-56] The edge computing module should be capable of running 3rd party applications.	[Gap-44] Slicing standards are missing for Industrial scenarios, including granularity of the network slice, the management and control function requirements, and the network resource allocations. [[Gap-45] PON system needs to be optimized to support TSN features. [Gap-46] The interworking of PON and TSN should be studied. [Gap-47] Industrial PON ONU with industrial interfaces and protocol interpreting functions is not available [Gap-48] Same as [Gap-47]. [Gap-49] None. [Gap-50] None. [Gap-51] None. [Gap-52] Standards are missing for PON telemetry, automatic network resource allocation and configuration enabled by AI based functions within the PON system. [Gap-53] None. [Gap-54] None. [Gap-55] There is no standard to define computing power metric for edge computing platforms on Industrial PON. [Gap-56] None.

Use Case		Technology requirements	Gaps
#13	Use case Remote Attestation	[R-57] An F5G network device should be able to generate measurement data, store it securely and report its integrity status in a secured manner. [R-58] An F5G network device should be able to prove its trusted status in a proper manner, which should be suitable for its own hardware architecture. [R-59] An F5G network device should be able to prove the evidence of its trusted booting; [R-60] An F5G network device should be able to provide the status of its trustworthiness during run time.	[Gap-57] An appropriate method for secured measurement data generation is requested to be studied and IETF RATS WG is considered as the suitable place to take over this task. [Gap-58] None. [Gap-59] An appropriate method for remote attestation support in F5G network devices running period is requested to be studied and ETSI TC Cyber is considered as the suitable place to take over this task. [Gap-60] Same as [Gap-59].
#14	Digitalized ODN/FTTX	[R-61] The physical labels for the various components of the ODN shall be digitized. [R-62] The ODN intelligent management system shall support the construction and maintenance process, by automatically capturing the information about the ODN, and visualizing the networks. [R-63] The ODN intelligent management system shall support troubleshooting by remotely accessing the ODN database by technicians. [R-64] The pre-connection shall be applicable to different types of ODN connectors and boxes (including outdoor adapters) and to various environments (indoor, outdoor, simple and complex). [R-65] The connection shall meet the appropriate Ingress Protection (IP) level depending on the scenario (such as ingress protection rating IP68 and IP65 [1]). [R-66] The connectors shall ensure low insertion loss in order to meet the link loss requirements of the ODN. [R-67] The quick connection and installation process shall meet the long-term reliability test requirements (for example, 2000-hour, dual 85-hour test for closures) and mechanical test requirements (for example, optical cable tension and strain requirements) during onsite construction and deployment.	[Gap-61] 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. [Gap-62] Same as [Gap-61]. [Gap-63] Same as [Gap-61]. [Gap-64] 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. [Gap-65] Same as [Gap-64]. [Gap-66] Same as [Gap-64]. [Gap-67] Same as [Gap-64].
#10	Scenario Based Broadband	[R-68] The network shall support application type (video, file transfer, Internet browsing, etc.) identification. [R-69] The network should support AI based application type identification. [R-70] The application feature database for AI should be established and updated in real-time or periodically. [R-71] The network shall support slicing with different service characteristics. [R-72] The network shall support QoS evaluation. [R-73] The network should support QoE evaluation. [R-74] The network should be able to identify network usage of applications, which potentially have acceleration demands. The network usage of such applications may be linked to a specific user, only if this is explicitly within the scope of the user's service level agreement. Otherwise, linking	[Gap-68] Define application type identification mechanism. [Gap-69] Application of AI architecture for identification of application types in a F5G network. [Gap-70] The dynamic creation and updates of application feature database entries using Big Data and Machine Learning mechanisms need to be defined. [Gap-71] Mechanisms for F5G end to end slicing with consistent SLA on multiple network segments with different physical technologies are needed. [Gap-72] None. [Gap-73] Evaluation schemes for QoE of specific applications are needed. [Gap-74] Mechanisms to identify network usage of applications, which potentially have acceleration demands. [Gap-75] Mechanisms for near real-time monitoring of F5G network resource utilization and health status.

Use Case		Technology requirements	Gaps
		should be restricted to an anonymized group of users. [R-75] The network shall be able to monitor network resource utilization and health status.	
#08	Multiple Access Aggregation over PON	[R-76] For GPON, XGS-PON and future generation PON systems the OMCC bandwidth allocation and inter-gap allocations shall be revised in order to reduce fixed bandwidth reserved for the OMCC channels. [R-77] For Multiple Access Aggregation over PON higher capacity solutions are required. [R-78] The new PON technologies shall allow a seamless integration with existing PON ecosystem. [R-79] The new PON technologies shall support multiple services (B2B, B2C and mobile xhaul) in the same PON. [R-80] For Multiple Access Aggregation over PON a protection solution between two distinct OLT, using single or dual ONU, shall be available. [R-81] For Multiple Access Aggregation over PON the automatic protection switching solution shall be based on performance degradation statistics. [R-82] PON shall support distinct type of services based on different latency, jitter and bandwidth requirements. [R-83] For Multiple Access Aggregation over PON, PON systems shall support specific and tight synchronization requirements set for the end-to-end time accuracy in 5G networks [R-84] For Multiple Access Aggregation over PON, slices for different mobile and fixed service levels shall be supported [R-85] For Multiple Access Aggregation over PON, PON systems shall ensure protocol transparency	[Gap-76] Increase in PON throughput via new technologies such as high-order modulation and wavelength-division multiplexing. [Gap-77] Same as [Gap-76]. [Gap-78] None. [Gap-79] None. [Gap-80] None. [Gap-81] Automatic protection switch with delay compensation between the working path and the protection path to avoid service interruption. [Gap-82] Improved DBA to support low-latency upstream transmission with latency below 100 µs. [Gap-83] Enhanced timing & synchronization in future PON systems to ensure end-to-end requirements are met. [Gap-84] Introduce slicing in PON with suitable mapping of the vDBA and/or VxLAN to the service slice type and traffic isolation processes. [Gap-85] Realize protocol transparency in PON throughput via new technologies such as Ethernet Private Lines (EPL) and Ethernet Virtual Private Lines (EVPL).
#11	Telemetry-based Enhanced Performance Monitoring in Intelligent Access Network	[R-86] The Access Network shall support telemetry-based network performance monitoring technics in order to provide better service experiences. [R-87] Data models regarding configuration and data collection should be defined for the Access Network to realize telemetry.	[Gap-86] Specify a light-weight Telemetry technology, such as UDP based telemetry, for Access Network telemetry. [Gap-87] Develop and specify a dedicate data model for performance monitoring and data collection for Access Network.
#01	Cloud Virtual Reality	[R-88] For each phase of Cloud VR the network shall meet the corresponding network performance requirements. [R-89] To meet Cloud VR ideal or ultimate experience, the terminal shall have advanced antenna configuration. [R-90] To meet Cloud VR ideal or ultimate experience, Wi-Fi 6 slicing shall be supported. [R-91] To meet Cloud VR ideal and ultimate experience phases XG PON shall be used. [R-92] To meet Cloud VR ultimate experience phase, the split ratio of XG PON shall be less than 1:16. [R-93] To achieve low latency and delay jitter a low latency scheduling algorithm shall be used in the Access Network. [R-94] In the case that OTN is used, the OLT should support OTN capabilities.	[Gap-88] None. [Gap-89] None. [Gap-90] None. [Gap-91] None. [Gap-92] None. [Gap-93] None. [Gap-94] The OLT should support OTN capabilities. [Gap-95] OTN container with flexible and small granularity to efficiently support Cloud VR traffic is missing. [Gap-96] None. [Gap-97] OTN support for mixed traffic of ODUs and OSUs need to be defined. [Gap-98] Need coordination of network slicing between home network, Access Network and metro network to form an end-to-end slice to meet end-to-end latency requirement.

Use Case		Technology requirements	Gaps
		[R-95] OTN shall support variable size containers to match the Cloud VR bit rate from 40Mb/s to 770Mb/s. [R-96] Taking the capacity, reach and high quality needs into account, OTN shall be deployed in the metro network. [R-97] For fair experience phases, the Cloud VR service shall have higher scheduling priority compared with other Internet services. [R-98] For comfortable, ideal and ultimate experience phases, the Cloud VR service requires lower latency and delay jitter in the network, so a high quality independent channel shall be used. [R-99] When a Cloud VR service is established or released, the link bandwidth of the Cloud VR transport network shall automatically increase or decrease the bandwidth to accurately meet the bandwidth requirements of the Cloud VR service in a seamlessly manner. [R-100] The network shall support dynamic set up and release of the high-quality network channel for Cloud VR service to guarantee the performance of Cloud VR service and increase the transmission efficiency of the network. [R-101] The independent management systems should support a mechanism that dynamically sets up the end to end channel. [R-102] To support bandwidth demand changes a simple mechanism is required with minimal interaction with the management layer. [R-103] Cloud VR traffic shall be transported on a dedicated slice on the chosen network. [R-104] The slice shall match the Cloud VR bandwidth requirements in an efficient manner. [R-105] The slice shall have E2E coordinated management support.	[Gap-99] When a Cloud VR session is established or released, the link bandwidth of the Cloud VR transport network should automatically increase or decrease to accurately meet the bandwidth requirements of the online Cloud VR service in a seamlessly manner, such a method is missing. [Gap-100] Each part of the network channel needs to support the coordinated management plane to setup or release a channel for Cloud VR service. [Gap-101] Same as [Gap-100]. [Gap-102] A simple mechanism for dynamic bandwidth changes with minimal need for inter management coordination is missing. [Gap-103] E2E service isolation via slicing is missing. [Gap-104] Bandwidth matching is missing. [Gap-105] Simplified E2E slice management is missing.
NOTE: Gaps section sequence shall be adjusted to match with requirements section.			

Table 20 is a list of suggested actions to gaps found in this 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 20: Suggested actions for identified gaps

SDO/Group	Action number	Suggested actions	Relevant gaps
ITU-T SG15/Q18	1	Define data rate profiles for fibre-based on-premises network.	Gap-1
	2	Specify low optical link budget for home networking and small building.	Gap-4, Gap-5
	3	Specify a high priority channel for signalling in fibre networks.	Gap-6
	4	Define a mechanism to recognize network signalling and protocols.	Gap-7
	5	Define optimized parameters transceivers for single mode fibre and new parameters of P2MP transceivers for multi-mode fibre and plastic fibre.	Gap-9
	6	Define simplified authentication process.	Gap-10

SDO/Group	Action number	Suggested actions	Relevant gaps
	7	Define a mechanism for IoT Hub to manage the coordination in low power mode between the IoT Hub and the RG.	Gap-17
	8	Define a transmission QoS mechanism allowing for multi-dimension network parameters.	Gap-18
	9	Define a direct node-to-node communication method on layer 2 for fibre-based on-premises network.	Gap-19
IEC	10	Define small size connectors with good protection.	Gap-12
	11	Define small size optical and electrical hybrid cable with appropriate bend radius as well as the connectors.	Gap-15
WFA	12	Improve EasyMesh™ to support plug-and-play setup and seamless roaming between APs.	Gap-20
	13	Define slicing with quality guarantee for multi-AP.	Gap-21
ETSI ISG F5G	14	Define high quality slicing mechanism of CPN for SME.	Gap-22
	15	Define hard slicing for Wi-Fi, CPE and PON. For PON, suitable mapping of the vDBA and/or VxLAN to the service slice type and traffic isolation processes shall be considered.	Gap-23, Gap-84
	16	Define AI based traffic and application type identification.	Gap-24, Gap-69
	17	Define E2E slicing management including management and control function requirements and network resource allocation.	Gap-25, Gap-98, Gap-105
	18	Define interface between telco network and cloud network for guaranteed services.	Gap-27
	19	Define Time-of-day based SLA management interface and data models for commercial customers.	Gap-29
	20	Define mechanism of fast provisioning of private line service.	Gap-31
	21	Define mechanism of automatic and fast fault detection, demarcation, isolation and correction.	Gap-32
	22	Define visualized network operation SLA indicators.	Gap-33
	23	Define service level slicing for OTN.	Gap-35
	24	Specify on-demand ordering capability for CPE and Edge node.	Gap-36
	25	Include OTN CPE redundancy connection in architecture.	Gap-37
	26	Define E2E slicing mechanism with consistent SLA on multiple network segments with different physical technologies, including slice granularity.	Gap-44, Gap-71, Gap-103
	27	Specify interworking of PON and TSN.	Gap-46
	28	Specify Industrial PON ONU with industrial interfaces and protocol interpreting functions.	Gap-47, Gap-48
	29	Specify PON telemetry requirements.	Gap-52
	30	Define automatic network resource allocation and configuration enabled by AI based functions within the PON system.	Gap-52
	31	Define Industrial PON system with computing power metric for edge computing platforms.	Gap-55
	32	Define application type identification mechanism.	Gap-68
	33	Specify method of dynamic establishment and updates of application feature database using Big Data and Machine Learning mechanisms.	Gap-70
	34	Define mechanisms to identify network usage of applications, which have potential acceleration demands.	Gap-74
	35	Define mechanisms for near real-time monitoring of F5G network resource utilization and health status.	Gap-75
	36	Specify a light-weight Telemetry technology for Access Network.	Gap-86
	37	Develop and specify a dedicate data model for performance monitoring and data collection for Access Network.	Gap-87
	38	Define OLT device with OTN capabilities.	Gap-94
	39	Define a mechanism for transport network resource allocation and adjustment for services like Cloud VR.	Gap-99, Gap-100, Gap-101, Gap-104
	40	Define a simple mechanism for bandwidth demand changing.	Gap-102
BBF	41	Define evaluation schemes for QoE of specific applications.	Gap-73
ITU-T SG15/Q11	42	specify finer granularity OTN.	Gap-34, Gap-42
	43	OTN Higher speed CPE needed.	Gap-43
	44	Define OTN container with flexible and small granularity.	Gap-95
	45	Optimize OTN to support mixed traffic of ODUs and OSUs.	Gap-97

SDO/Group	Action number	Suggested actions	Relevant gaps
ITU-T SG15/Q2	46	Supporting TSN features on PON system.	Gap-45
	47	Increase in PON throughput via new technologies such as high-order modulation and wavelength-division multiplexing.	Gap-76, Gap-77
	48	Automatic protection switch for PON with delay compensation between the working path and the protection path to avoid service interruption.	Gap-81
	49	Improved DBA to support low-latency upstream transmission with latency below 100 µs.	Gap-82
	50	Enhanced timing & synchronization in future PON systems to ensure end-to-end requirements are met.	Gap-83
	51	Realize protocol transparency in PON throughput via new technologies such as Ethernet Private Lines (EPL) and Ethernet Virtual Private Lines (EVPL).	Gap-85
IETF RATS	52	Define an appropriate method for secured measurement data generating.	Gap-57
ETSI TC Cyber	53	Define an appropriate method for remote attestation support in F5G network devices running period.	Gap-59, Gap-60
ETSI TC ATTM	54	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.	Gap-61, Gap-62, Gap-63
IEC TC86	55	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.	Gap-64, Gap-65, Gap-66, Gap-67
		No action needed.	Gaps with None

NOTE 1: In Table 20, 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.

NOTE 2: For action point #37, BBF is considered to be the reference organization.

History

Document history		
V1.1.1	September 2021	Publication