ETSI GR F5G 008 V1.1.1 (2022-06)

GROUP REPORT

Fifth Generation Fixed Network (F5G); F5G Use Cases Release #2

Disclaimer

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

Reference

DGR/F5G-008 use casesR2

Keywords

customer premises, cyber security, F5G, fibre, industry, smart city, use case, X-Haul

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

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

If you find a security vulnerability in the present document, please report it through our Coordinated Vulnerability Disclosure Program:
https://www.etsi.org/standards/coordinated-vulnerability-disclosure

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.
The content of the PDF version shall not be modified without the written authorization of ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2022.
All rights reserved.

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

Modal verbs terminology

In the present document "**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 present document describes the use cases to be enabled by the Fifth Generation Fixed Network (F5G). These use cases include services to residential, business and vertical industry customers as well as functionalities to optimize the management and performance of F5G. These use cases will be used as input to a gap analysis and a technology landscape study, aiming to extract the technical requirements needed for their implementations. The use cases are identified based on their influence on the fixed network architecture and requirements. The context and description of each use case are presented in the present document.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

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] ETSI GR F5G 001: "Fifth Generation Fixed Network (F5G); F5G Generation Definition Release #1".

[i.2] 3GPPP TR 38.801: "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Study on new radio access technology: Radio access architecture and interfaces (Release 14)".

[i.3] Recommendation ITU-T G.987: "10-Gigabit-capable passive optical network (XG-PON) systems: Definitions, abbreviations and acronyms".

[i.4] AIA Global Association for Vision Information: "GiGE Vision 2.1".

[i.5] AIA Global Association for Vision Information: "USB3 Vision 1.1".

[i.6] IEEE 1588™: "Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems".

[i.7] IEEE 802.1™: "Time-Sensitive Networking (TSN) Task Group".

NOTE: Available at https://1.ieee802.org/tsn/ [accessed Feb. 2018].

[i.8] IEEE Std 802.1AS™: "IEEE Standard for Local and Metropolitan Area Networks - Timing and Synchronization for Time-Sensitive Applications", January 2020.

[i.9] IEC/IEEE 60802: "TSN Profile for Industrial Automation", Draft D1.2, June 2020.

[i.10] PROFIBUS Nutzerorganisation e. V.: "PROFINET System Description: Technology and Application," Version November 2018, Order Number 4.132.

[i.11] PROFIBUS Nutzerorganisation e.V.: "PROFINET over TSN Guideline", Version 1.21, June 2020.

[i.12] IEC 62541: "OPC unified architecture".

[i.13] IEC 61131-3: "Programmable controllers - Part 3 : Programming languages".

[i.14] OPC Foundation, PROFIBUS Nutzerorganisation e.V.: "OPC UA for PROFINET", Version 1.00, January 2020.

[i.15] Recommendation ITU-T G.697: "Optical monitoring for dense wavelength division multiplexing systems".

[i.16] IETF RAW: "Reliable and Available Wireless Technologies", Internet Draft, February 2021.

[i.17] IETF RAW: "RAW use cases," Internet Draft, February 2021.

[i.18] IETF RAW: "Requirements for Reliable Wireless Industrial Services", Internet Draft, March 2021.

[i.19] 3GPP: "Study on Communication for Automation in Vertical Domains", Technical Specification (TS) 22.804, section 5.3.7, version 16.3.0, July 2020.

[i.20] 5G ACIA: "Key 5G Use Cases and Requirements From the Viewpoint of Operational Technology Providers", White Paper, May 2020.

[i.21] K. Löser: "Wi-Fi 6 in the Industry", White Paper, Siemens AG, 2020.

[i.22] E. Khorov, I. Levitsky, I. F. Akyildiz: "Current Status and Directions of IEEE 802.11be, the Future Wi-Fi 7," IEEE Access, vol. 8, pp. 88664-88688, May 2020.

[i.23] K. L. Bober, S. M. Mana, M. Hinrichs, S. M. Kouhini, C. Kottke, D. Schulz, C. Schmidt, R. Freund, V. Jungnickel: "Distributed Multiuser MIMO for LiFi in Industrial Wireless Applications", Journal of Lightwave Technology, early access, March 2021.

[i.24] IEEE 802.11-18/1109r5: "LC Usage Document", July 2018.

[i.25] Y. Le, H. Zeng, X. Zhou, N. Deng, S. Megeed, A. Shen, Z. Dong, Z. Feng, T. Chang and X. Liu: "Real-Time Demonstration of an Integrated Metro-Access Network Carrying Live VR Traffic Based on Multi-Carrier Modulation and Simplified Sub-band Coherent Detection", in Optical Fibre Communication Conference (OFC) 2019, paper Th3F.3 (2019).

[i.26] D. F. Welch: "Disruption Cycles for Optical Networks: How Point to Multi-Point Coherent Optics can Transform the Cost and Complexity of the Optical Network", in European Conference on Optical Communications 2020, Invited Talk Tu1C-1 (2020).

[i.27] Optical Internetworking Forum (OIF): "Implementation agreement 400ZR", March 2020.

[i.28] 5G-ACIA White Paper (2021): "Integration of 5G with Time-Sensitive Networking for Industrial Communications", published by 5G-ACIA.

[i.29] Boschert, S., Heinrich, C., Rosen, R. (2018): "Next Generation Digital Twin", Proceedings of TMCE 2018.

[i.30] Qiuchen Lu, Ajith Kumar Parlikad, Philip Woodall, Gishan Don Ranasinghe, Xiang Xie, Zhenglin Liang, Eirini Konstantinou, James Heaton and Jennifer Schooling (2020): "Developing a dynamic digital twin at building and city levels: A case study of the West Cambridge campus", Journal of Management in Engineering, 36(3).

[i.31] ETSI GS F5G 003: "Fifth Generation Fixed Network (F5G); F5G Technology Landscape".

[i.32] ETSI GS F5G 004: "Fifth Generation Fixed Network (F5G); F5G Network Architecture".

[i.33] IEEE 802.3br-2016™: "IEEE Standard for Ethernet Amendment 5: Specification and Management Parameters for Interspersing Express Traffic".

[i.34] IEEE Std 802.1CB-2017™: "IEEE Standard for Local and Metropolitan Area Networks - Frame Replication and Elimination for Reliability".

NOTE: Available at https://ieeexplore.ieee.org/servlet/opac?punumber=8091137.

[i.35] IEEE Std 802.1Qbv-2015™: "IEEE Standard for Local and Metropolitan Area Networks - Bridges and Bridged Networks - Amendment 25: Enhancements for Scheduled Traffic".

NOTE: Available at https://standards.ieee.org/findstds/standard/802.1Qbv-2015.html.

[i.36] IEEE Std 802.1Qbu-2016™: "IEEE Standard for Local and Metropolitan Area Networks - Bridges and Bridged Networks - Amendment 26: Frame Preemption".

NOTE: Available at https://standards.ieee.org/findstds/standard/802.1Qbu-2016.html.

[i.37] IEEE Std 802.1AB-2016™: "Station and Media Access Control Connectivity Discovery (specifies the Link Layer Discovery Protocol (LLDP))".

NOTE: Available at https://ieeexplore.ieee.org/servlet/opac?punumber=7433913.

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

AI annotation: task of labelling data with metadata in preparation for training a machine learning model

rendering: process of generating a photorealistic or non-photorealistic image from a 2D or 3D model by means of a computer program

3.2 Symbols

Void.

3.3 Abbreviations

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

6DoF	Six Degrees of Freedom
AC	Access Controller
ACIA	Alliance for Connected Industries and Automation
AggN	Aggregation Network
AGV	Automated Guided Vehicle
AI	Artificial Intelligence
AN	Access Network
AP	Access Point
API	Application Programming Interface
AR	Augmented Reality
ASI	Asynchronous Serial Interface
ATM	Automatic Teller Machine
AZ	Availability Zone
B2B	Business to Business
B2C	Business to Customer
BBU	Base Band Unit
BIP	Bit-Interleaved Parity
BNG	Broadband Network Gateway
CAPEX	CAPital EXpenditure
CCTV	Closed Circuit TeleVision
CDN	Content Delivery Network
CE	Customer Equipment
CFP	C Form-factor Pluggable
CO	Central Office
CoS	Class of Service

CPE	Customer Premise Equipment
CPN	Customer Premises Network
CR	Computed Radiography
CR	Core Router
CSP	Communication Service Provider
CT	Communication Technology/Computed Tomography
CU	Central Unit
CWDM	Coarse Wavelength Division Multiplexing
DBA	Dynamic Bandwidth Allocation
DC	Data Centre
DC-GW	Data Center Gateway
DCI	Data Centre Interconnect
DHCP	Dynamic Host Control Protocol
DICOM	(Digital Imaging and Communications in Medicine
DIM	Dynamic Integrity Measurement
DR	Digital Radiography
DSA	Digital Subtraction Angiography
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
DT	Digital Twin
DU	Distributed Unit
DWDM	Dense Wavelength Division Multiplexing
E2E	End to End
EAU	Electrical Aggregation Unit
EG	Enterprise Gateway
eMBB	Enhanced Mobile Broadband
EMI	Electro-Magnetic Interference
EMS	Element Management System
ERP	Enterprise Resource Planning
EU	European Union
F5G	Fifth Generation Fixed Network
FAT	Fibre Access Terminal
FDMA	Frequency-Division Multiple Access
FEC	Forward Error Correction
FFC	Full-Fibre Connection
FGW	Fibre GateWay
FIN	Fibre in-premises Network
FPS	First Person Shooter
FTTB	Fibre To The Building
FTTB/C	Fibre To The Building/Curb
FTTC	Fibre To The Curb
FTTH	Fibre To The Home
FTTR	Fibre To The Room
FWL	Fixed Wireless Link
GE	Gigabit Ethernet
GiGE Vision®	GiGabit Ethernet Vision
GIS	Geographic Information System
GPON	Gigabit-capable Passive Optical Network
GPS	Global Positioning System
GPU	Graphics Processing Unit
GRE	Guaranteed Reliable Experience
GVCP	GiGE Vision Control Protocol
GVSP	GiGE Vision Stream Protocol
HD	High Definition
HDR	High Dynamic Range
HDTV	High Definition TeleVision
HGW	Home Gateway
HIS	Hospital Information System
HMD	Head-Mounted-Display
HMI	Human Machine Interface
HQ	Head Quarter
HSI	High Speed Internet

HW	HardWare
IBC	International Broadcasting Centre
ICT	Information and Communication Technology
IIoT	Industrial Internet of Things
IOR	Industrial Optical Ring
IP	Internet Protocol
IPTV	Internet Protocol TeleVision
ISP	Internet Service Provider
IT	Information Technology
LAN	Local Area Network
LiFi	Light Fidelity
LoS	Line of Sight
MAC	Media Access Control
MDU	Multiple Dwelling Unit
MES	Manufacturing Execution System
ML	Machine Learning
mMTC	Massive Machine Type Communication
MOBA	Multiplayer Online Battle Arena
MOOC	Massive Open Online Course
MPEG	Moving Picture Experts Group
MPLS	Multiprotocol Label Switching
MR	Mixed Reality
MRI	Magnetic Resource Imaging
MSA	Multi-Source Agreement
MSCO	Multi-Service Connectivity Orchestrator
MWDM	Metro Wavelength Division Multiplexing
NFV	Network Functions Virtualisation
NMS	Network Management System
OA	Office Automation
OAM	Operation And Maintenance
ODN	Optical Distribution Network
ODTR	Optical Time Domain Reflectometer
OEHC	Optical Electric Hybrid Cable
OLO	Optical Local Oscillator
OLT	Optical Line Termination
OMCI	ONU Management and Control Interface
ONU	Optical Network Unit
OPC UA	Open Platform Communications Unified Architecture
OPC	Open Platform Communications
OPEX	OPerational Expenses
ORE	Optical Ring End
ORH	Optical Ring Head
ORP	Optical Ring Passive
OS	Operating System
OSS	Operation Support System
OT	Operational Technology
OTDR	Optical Time Domain Reflectometer
OTN	Optical Transport Network
OXC	Optical Cross-Connect
P2MP	Point-to-MultiPoint
P2P	Point to Point
PACS	Picture Archiving and Communication Systems
PC	Personal Computer
PCC	Point Cloud Compression
PDM	Polarization-Division Multiplexed
PE	Provider Edge
PET-CT	Positron Emission Tomography-Computed Tomography
PLC	Programmable Logical Controller
PM	Post Meridiem
PoD	Point of Delivery
PoE	Power over Ethernet
POL	Passive Optical LAN

PON	Passive Optical Network
PoP	Point of Presence
PTP	Precise Time Protocol
QSFP	Quad (4-channel) Small Form-factor Pluggable
RA	Remote Attestation
RAC	Real Application Cluster
RAN	Radio Access Network
RAW	Reliable and Available Wireless
RF	Radio Frequency
RFS	Resource Facing Services
RGBD	Red Green Blue Depth
RIS	Radiology Information System
RN	Remote Node
RRH	Radio Remote Head
RSSI	Received Signal Strength Indication
RTT	Round Trip Time
RTU	Remote Terminal Unit
RU	Radio Unit
SA	StandAlone
SCADA	Supervisory Control and Data Acquisition
SD	Standard Definition
SDI	Serial Digital Interface
SDN	Software-Defined Network
SD-WAN	Software-Defined Wide Area Network
SFP	Small Form-factor Pluggable
SLA	Service-Level Agreement
SME	Small and Medium Enterprises
SNI	Service Node Interface
SRLG	Shared Risk Link Group
STP	Shielded Twisted Pair
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Address
TPM	Trusted Platform Module
TSN	Time-Sensitive Networking
TTM	Time To Market
TV	TeleVision
TWT	Target Wake Time
UA	Unified Architecture
UAC	User Application Client
UAS	User Application Server
UDP	User Datagram Protocol
UHD	Ultra-High Definition
UPF	User Plane Function
URLLC	Ultra-Reliable and Low Latency Communications
UTP	Unshielded Twisted Pair
VAS	Value Added Services
VLAN	Virtual Local Area Network
VM	Virtual Machine
VoIP	Voice over Internet Protocol
VPC	Virtual Private Cloud
V-PCC	Video codec based Point Cloud Compression
vPLC	virtual Programmable Logic Controller
VPN	Virtual Private Network
VR	Virtual Reality
VR/AR	Virtual Reality/Augmented Reality
VTM	Video Teller Machine
VXLAN	Virtual eXtensible Local Area Network
WDM	Wavelength Division Multiplexing
Wi-Fi®	Wireless Fidelity
WLAN	Wireless Local Area Network
XFP	Gigabit Small Form-factor Pluggable
XG-PON	10-Gigabit-capable Passive Optical Network

XGS-PON 10-Gigabit-capable Symmetric Passive Optical Network

4 Overview

As described in ETSI GR F5G 001 [i.1], the main business requirements identified by F5G are outlined in Figure 1. They improve various dimensions over previous generations of fixed networks.

Networks	Services	Operations
a) Speed and Capacity (Bandwidth)	e) Reliability	h) Operational Efficiency
b) Coverage (Connectivity)	f) Availability	i) Energy Efficiency
c) Responsivity (Latency)	g) Security	j) Spectral Efficiency
d) Density (Connection)		

Figure 1: Business requirements for F5G in the categories of Network, Service and Operation

In the present document, 32 use cases are described. Fourteen use cases were presented in Release 1 and 18 use cases were added to the present Release 2, taking advantage of the key technical characteristics defined for F5G. Each use case may demand a different subset of the 10 requirements depicted in Figure 1. With further research, subsequent use cases may be specified in future releases of the present document.

5 Categorization of use cases

5.1 Driving the characteristics of F5G

The use cases as described in the present document are driving the three dimensions of characteristics that are specified in ETSI GR F5G 001 [i.1] on generation definitions, namely eFBB (enhanced Fixed Broadband), FFC (Full-Fibre Connection), and GRE (Guaranteed Reliable Experience). Figure 2 shows that:

- Depending on the use case, one or more dimensions are particularly important.
- All dimensions of the F5G system architecture are implemented by the following use cases.

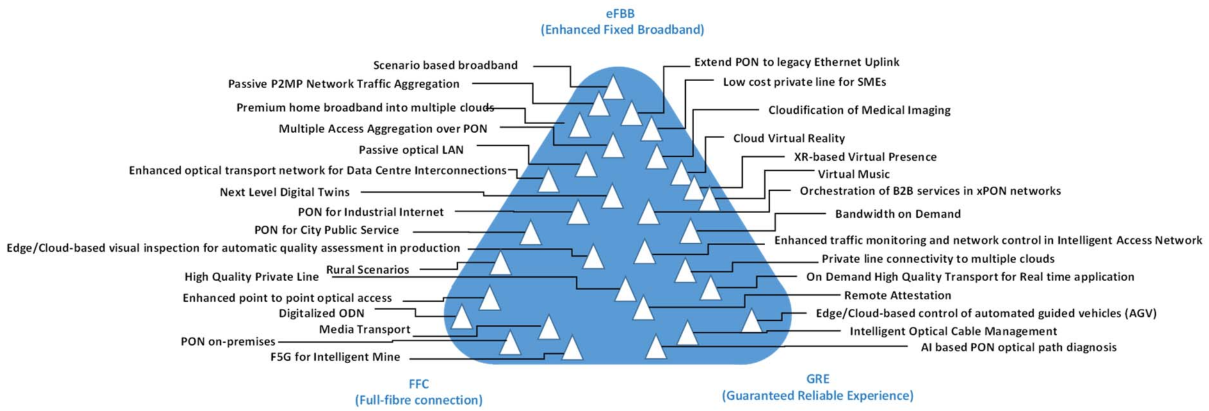


Figure 2: F5G use cases (illustrative)

5.2 Paving the Way for Fibre to Everywhere

F5G is leveraging technologies of fibre optical networks to benefit multiple segments including residential applications, business applications, network internal topics such as network optimizations plus the use of F5G for mobile xHaul, and finally vertical industries oriented use cases.

Figure 3 shows the different segments where fibre to everywhere is applicable. The larger circle named network features focus on optimization of the networking technologies.

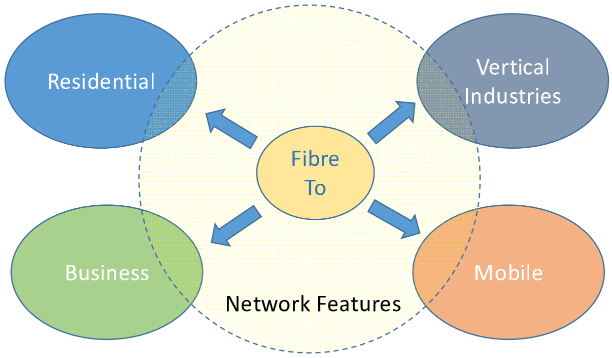


Figure 3: High-level Segment Perspective

As a quick reference, Table 1 summarizes the different use cases from three different perspectives:

a) Key F5G dimensions requirements.

b) Key segment and business area addressed.

c) Key focus of the use case - new or enhanced services, network infrastructure and services features or in network management and optimization.

Table 1: Use cases with key dimensions, segments and focus

USE CASES	Key F5G Dimensions	Key Segment					Key Focus			Clause
		Residential	Business	Mobile	Vertical - Industry	Network features	Service	Network	Management	
Use case #1: Cloud Virtual Reality	GRE	x	x		x		x			6.1
Use case #2: High Quality Private Line	GRE		x				x			6.2
Use case #3: High quality low cost private line for small and medium enterprises	eFBB		x				x			6.3
Use case #4: Fibre on-premises networking: Fibre-to-The-Room (FTTR)	eFBB,FFC	x	x					x		6.4
Use case #5: Passive optical LAN	eFBB, FFC		x					x		6.5
Use case #6: PON for Industrial Manufacturing	GRE, eFBB, FFC				x			x		6.6
Use case #7: Using PON for City Public Service	FFC				x			x		6.7
Use case #8: Multiple Access Aggregation over PON	eFBB,FFC			x		x		x		6.8
Use case #9: Extend PON to legacy Ethernet Uplink	eFBB,FFC					x		x		6.9
Use case #10: Scenario based broadband	eFBB,FFC					x		x		6.10
Use case #11: Enhanced traffic monitoring and network control in Intelligent Access Network	GRE,FFC					x		x		6.11
Use case #12: On Demand High Quality Transport for Real time applications	GRE					x			x	6.12
Use case #13: Remote Attestation for Secured Network Elements	GRE					x			x	6.13
Use case #14: Digitalized ODN/FTTX	eFBB					x			x	6.14
Use case #15: XR-based Virtual Presence	eFBB, GRE	x	x				x			7.1
Use case #16: Enterprise private line connectivity to multiple clouds	GRE		x				x			7.2
Use case #17: Premium home broadband connectivity to multiple clouds	GRE, FFC	x					x			7.3
Use case #18: Virtual Music	eFBB, GRE	x	x				x			7.4
Use case #19: Next Generation Digital Twins	eFBB, GRE				x		x			7.5
Use case #20: Media Transport	eFBB, GRE	x	x		x	x	x			7.6
Use case #21: Edge/Cloud-based visual inspection for automatic quality assessment in production	GRE, FFC				x		x			7.7
Use case #22: Edge/Cloud-based control of automated guided vehicles (AGV)	GRE				x		x			7.8
Use case #23: Cloudification of Medical Imaging	eFBB, GRE		x				x			7.9
Use case #24: F5G for Intelligent Mine	GRE, FFC				x		x			7.10
Use case #25: Enhanced optical transport network for Data Centre Interconnections	eFBB, GRE					x		x		7.11
Use case #26: Enhanced point to point optical access	FFC			x		x		x		7.12
Use case #27: Rural Scenarios	FFC, eFBB					x		x		7.13
Use case #28: High-speed Passive P2MP Network Traffic Aggregation	eFBB, FFC			x		x		x		7.14
Use case #29: Orchestration of B2B services in xPON networks	GRE, eFBB					x			x	7.15
Use case #30: Bandwidth on Demand	GRE	x	x		x				x	7.16
Use case #31: Intelligent Optical Cable Management	GRE, FFC					x			x	7.17
Use case #32: AI-based PON optical path diagnosis	GRE					x			x	7.18

5.3 Application Area Perspective

F5G use cases leverage the technologies of the fibre optical networks to benefit several segments. It addresses multiple topics that may be applicable in different application areas. Therefore features and solutions needed by one use case may benefit other areas as well.

In this clause, the use cases are evaluated from the application perspective based on the strongest existing affinities. Each of the use cases is then mapped into one or more of the application categories, as shown in Table 2.

Table 2: Mapping use cases into application categories

Application category	Corresponding use cases
Broadband networking	6.3 Use case #3: High quality low cost private line for small and medium enterprises (6.8 Use case #8: Multiple Access Aggregation over PON) (6.9 Use case #9: Extend PON to legacy Ethernet Uplink) (6.10 Use case #10: Scenario based broadband) 7.11 Use case #25: Enhanced optical transport network for Data Centre Interconnections (7.6 Use case #20: Media Transport) 7.9 Use case #23: Cloudification of Medical Imaging 7.12 Use case #26: Enhanced Point to Point optical access 7.16 Use case #30: Bandwidth on Demand (7.13 Use case #27: Rural Scenarios) 7.14 Use case #28: High-speed Passive P2MP Network Traffic Aggregation
Customer premises networking	6.4 Use case #4: Fibre on-premises networking: Fibre-to-The-Room (FTTR) (6.5 Use case #5: Passive optical LAN) (7.9 Use case #23: Cloudification of Medical Imaging) 7.3 Use case #17: Premium home broadband connectivity to multiple Clouds
Physical networking	6.14 Use case #14: Digitalized ODN/FTTX (7.12 Use case #26: Enhanced Point to Point optical access) 7.13 Use case #27: Rural Scenarios 7.17 Use case #31: Intelligent Optical Cable Management (7.18 Use case #32: AI-based PON optical path diagnosis)
Immersive experiences	6.1 Use case #1: Cloud Virtual Reality 7.1 Use case #15: XR-based Virtual Presence 7.4 Use case #18: Virtual Music
Time-sensitive applications	6.12 Use case #12: On Demand High Quality Transport for Real time applications (7.9 Use case #23: Cloudification of Medical Imaging)
Reliable communications	6.2 Use case #2: High Quality Private Line 6.13 Use case #13: Remote Attestation for Secured Network Elements 7.6 Use case #20: Media Transport 7.2 Use case #16: Enterprise private line connectivity to multiple Clouds
High-density endpoints	(6.4 Use case #4: Fibre on-premises networking: Fibre-to-The-Room (FTTR)) (6.5 Use case #5: Passive optical LAN) 6.7 Use case #7: Using PON for City Public Service (6.8 Use case #8: Multiple Access Aggregation over PON) (6.9 Use case #9: Extend PON to legacy Ethernet Uplink)
Industrial ecosystems	6.6 Use case #6: PON for Industrial Manufacturing 7.7 Use case #21: Edge/Cloud-based visual inspection for automatic quality assessment in production 7.8 Use case #22: Edge/Cloud-based control of automated guided vehicles (AGV) 7.10 Use case #24: F5G for Intelligent Mine 7.5 Use case #19: Next Generation Digital Twins
Autonomous networks	(6.10 Use case #10: Scenario based broadband) 6.11 Use case #11: Enhanced traffic monitoring and network control in Intelligent Access Network 7.15 Use case #29: Orchestration of B2B services in xPON networks (7.17 Use case #31: Intelligent Optical Cable Management) (7.18 Use case #32: AI-based PON optical path diagnosis)
NOTE: The use cases mapped into more than one category are identified by brackets.	

The application area subcategories are defined based on the following characteristics:

- Broadband networking is typified by using gigabit connectivity broadband services in areas such as online education, smart home, enterprise cloudification, collaborative work and social networking.
- Customer premises networking are mostly defined by the needs of using gigabit connectivity on the customer premises. Service areas include wireless and wired access, enhanced broadband services and smart home/enterprise.
- Physical networking is mostly defined by the needs of using physical layer services in areas such as very-high point-to-point transport capacities and low-level transport capacities for legacy systems.

- Immersive experiences are mostly defined by the needs of using VR/AR/XR user experiences in human/machine interactive communication environments such as healthcare, cloud gaming and social networking.
- Time-sensitive applications are mostly defined by the needs of ensuring time-critical, low-latency and data processing capacity requirements in areas such as audio and video streaming/processing, industrial automation and healthcare.
- Reliable communications are mostly defined by the needs of stringent quality of service requirements, such as high-availability and data-integrity, in public services areas, healthcare, real-time banking and mission-critical applications.
- High-density endpoints are mostly defined by the needs of increasing PON density in areas such as public venues, data centres, enterprise and residential buildings and outside plant fibre densification.
- Industrial ecosystems are mostly defined by the needs of using analytics and intelligent devices in areas such as smart manufacturing in vertical sectors and industries.
- Autonomous networks are mostly defined by the needs of using Artificial Intelligence and automation techniques in areas such as networking, IoT, edge computing and smart city applications.

The present release of F5G use cases includes a set of services and functionalities enabled by the new generation of fixed network, leveraged on its eFBB (enhanced Fixed Broadband, FFC (Full-Fibre Connection) and GRE (Guaranteed Reliable Experience) characteristics. Future releases will enhance existing use cases and add more use cases.

5.4 Use case structure

Each use case is described following a pre-defined structure that includes:

- The Context, providing a quick overview of the covered application and associated challenges.
- The Description, providing a more detailed information of the use case including:
  a) The use case overview (what is the use case).
  b) The use case motivation (the benefits the use case provides).
  c) The use case precondition (what should be ready before the use case is running).

All use cases already described in Release 1 of the present document are described in clause 6, whereas the new use cases introduced in this Release 2 are described in clause 7.

These use cases will contribute to the definition of the requirements for a new architecture, new devices with new interfaces, new network topologies and a set of advanced management and optimization capabilities that will enhance the fields of applicability and the quality of experience of next generation fibre networks.

6 Description of use cases, Release 1

6.1 Use case #1: Cloud Virtual Reality

6.1.1 Use case context

Based on cloud computing and cloud rendering technologies, Cloud Virtual Reality (VR) applications introduce a large amount of data exchange between the terminal and the cloud server. It will place stringent requirements on the bearer network (e.g. bandwidth, latency, packet jitter, and packet loss), which will require the upgrading of the bearer network technology and architecture. The current network may be able to support early versions of Cloud VR (e.g. 4K VR) with limited user experience, but will not meet the requirements for large scale deployment of Cloud VR with enhanced experience (e.g. Interactive VR applications, cloud games). To support more applications and ensure a high-Quality of Experience, much higher available and guaranteed bandwidth (e.g. > 1 Gbps), lower latency (e.g. < 10 ms) and lower packet jitter (e.g. < 5 ms) are necessary.

This use case gives a brief introduction to Cloud VR applications and the required capabilities of fixed networks.

6.1.2 Description of the use case

6.1.2.1 Overview

Cloud VR offloads computing and VR rendering from local dedicated hardware to a shared cloud infrastructure. Cloud rendered video and audio outputs are encoded, compressed, and transmitted to the user terminals through fast and stable networks. This is in contrast to the current VR applications, where good user experience primarily relies on the end user purchasing expensive high-end PCs for local VR rendering. Cloud VR promotes the popularization of VR services by allowing users to enjoy various VR services where rendering is carried out in the cloud.

Cloud VR service experience is impacted by several factors that can influence the achieved sense of reality, interaction, and immersion, which are related to the network properties (e.g. bandwidth, latency, packet jitter and packet loss).

- The sense of reality requires the network to provide sufficiently high bandwidth.

The sense of reality depends on the audio and video quality. High-quality video transmission needs high network bandwidth.

- The sense of interaction requires the network to provide sufficiently low latency and low packet jitter.

Cloud VR implements computing and rendering in the cloud. Any latency from remote processing compromises the sense of interaction, including latency in loading, switchover, and joystick operations. The main effect of high latency in VR is that the user becoming sea-sick or dizzy. Note that high packet jitter will cause the VR play-out to be less smooth and frames may be distorted or lost.

- The sense of immersion requires high bandwidth, low latency, low packet jitter, and low packet loss.

The sense of enjoyment depends on the smoothness of the VR service. It is strongly related to factors such as frame freezing and artefacts. The network performance indicators, such as bandwidth, latency, and packet loss rate, should meet the requirements to realize a pleasurable experience.

Figure 4 shows an overview of a Cloud VR network architecture.

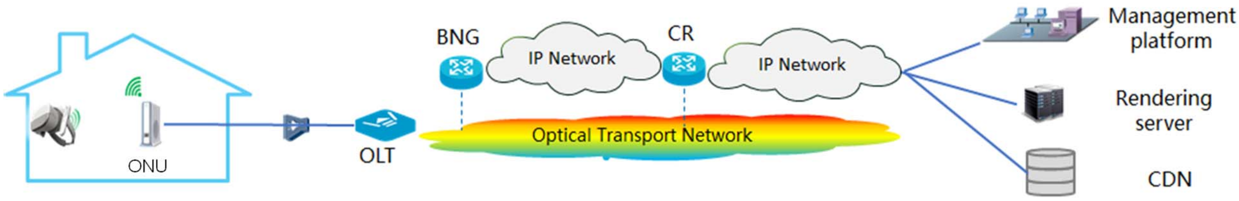


Figure 4: Cloud VR network architecture

As depicted in Figure 4, the Cloud VR bearer network includes the home network, Access Network, Aggregation Network both IP Network, and Optical Transport Network as infrastructure:

- The home network provides Wi-Fi® access and authentication capabilities for Cloud VR headsets.
- The Access Network provides optical fibre infrastructure (ODN), aggregates and processes packets from the home networks through the OLT.
- The Aggregation Network provides the IP forwarding function, and it is connected to the Cloud VR management platform, rendering server and CDN through the backbone network.

Cloud VR places stringent requirements on the network. It can be transported with other Internet services, however these Internet services could affect Cloud VR performance. The VR service experience would be difficult to guarantee due to current IP forwarding limitations. To ensure an excellent VR experience, VR traffic is transported via an independent channel that guarantees the desired performance and is thereby isolated from existing internet services. To implement this, an ONU identifies Cloud VR traffic and directs it to the independent channel provided by an Optical Network. From the server side, Cloud VR traffic is transported via the same independent channel. A general overview is shown in Figure 5.

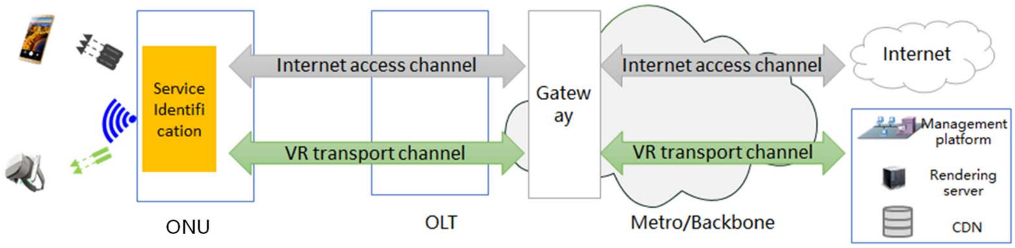


Figure 5: Cloud VR transport in independent channel

6.1.2.2 Motivation

The key features of Cloud VR are Cloud-based rendering and VR content delivery. Powerful cloud computing capabilities can improve the user experience and reduce the cost and energy consumption of terminals, promoting the evolution of VR to Cloud VR, as well as the fast popularization of VR services.

Main advantages and driving forces of Cloud VR development includes:

- Reduction in VR costs for users. Cloud VR requires terminal devices to have only basic functions.
- Protection for VR content copyrights. Precise content management and provisioning can be implemented in the cloud.
- Improvement in user experience. Cloud VR can improve logical computing and image processing capabilities.
- Acceleration of VR commercial take-up. Currently, the high cost per-user, lack of content, impaired mass adoption of VR, results from a poor ecosystem. After VR service is moved to the cloud, user costs are greatly reduced, popularizing VR in more households and enriching people's VR experience. High-quality VR content and VR commercial scenarios will continue to develop.
- Cloud VR could be a new value-added service and business for operators beyond triple play.

6.1.2.3 Pre-conditions

The operational flow of actions in this use case shows the process of a Cloud VR service via an independent channel, with pre-conditions as follows:

- VR services are deployed on the Cloud.
- The bearer network has created independent transport channels for Cloud VR services.
- The subscriber has subscribed to the Cloud VR service and service identification rules have been configured on the ONU.

6.1.2.4 Operational flow of actions

This clause shows an example of the operational flow of actions for enabling high-quality VR games. See Figure 6.

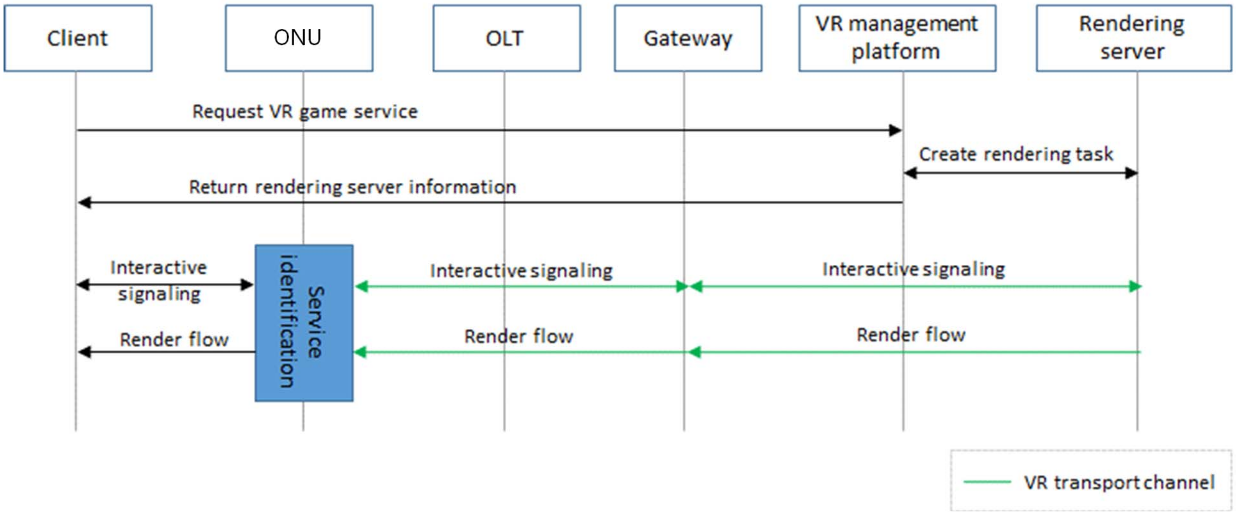


Figure 6: Operational flow of Cloud VR game service

1) When a user starts the game, the client sends a request to a VR management platform for a gaming service. The VR management platform returns the rendering server information after it has created the requested rendering task. Because these are initial signals between client and VR management platform, they can be transported through the best-effort network.

2) With the rendering server information obtained, the client will set up a dedicated connection with the rendering server for interactive signalling. During the interaction, traffic from the client will be identified by the ONU, and will be directed to the VR transport channel for transmission. The access transport channel is terminated on the Gateway functional module. Depending on an operator's network architecture, the Gateway function module can be located in a BNG (Broadband Network Gateway) or inside the OLT.

3) The traffic will then be directed to the Cloud VR transport channel in Aggregation/ Core Network. After receiving these messages, the rendering server gives feedback to the client.

4) When receiving the game operation information from the client, the rendering server will send back the rendered video flow after processing including calculation, rendering and encoding.

6.2 Use case #2: High Quality Private Line

6.2.1 Use case context

High quality private lines are necessary in certain demanding scenarios. High quality private line place strict requirements on bandwidth, delay, availability, security, Cloud accessibility, service provisioning time, as well as operation and maintenance of the bearer network. This use case briefly introduces some applications of this service as well as expected capabilities of the bearer network.

6.2.2 Description of the use case

6.2.2.1 Overview

6.2.2.1.1 General

Government institutions, financial organizations and medical organizations require high quality private lines. Both network components and cloud components are required to be compliant with this high quality demand.

6.2.2.1.2 Network Components

- Government Institutions:

  A government network provides public services and ensures the security of internal offices traffic at the same time. It is therefore divided into the government extranet and the government intranet. The government extranet is physically isolated from the government intranet and logically isolated from the Internet. The government extranet is mainly used to run the public-society-oriented professional services. A government network needs to be secure, reliable and have the necessary bandwidth.

- Financial Organizations:

  Financial organizations include banking and financial services:

  a) Banking: Digital transformation has brought unprecedented challenges to the traditional banking business. It is also putting tremendous pressure on the ICT infrastructures, which require front-end, back-end and the network to have stronger processing and real-time response capabilities.

     The bank's hierarchical Aggregation and Access Network is evolving towards a flattened Access Network, eliminating the Aggregation nodes of its second-level branches. All district-county-level branches and ATMs are directly connected to the provincial-level branches. This means that high-quality private lines are required. The evolution of the banking network architecture is shown in Figure 7.

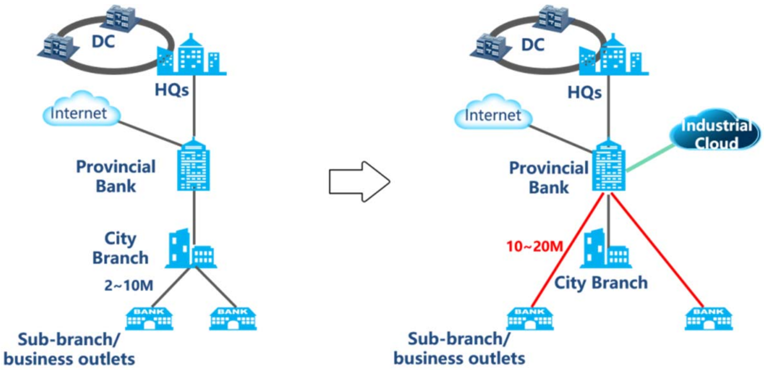


Figure 7: Banking network architecture evolution

     The bank's internal network is divided into an office network and a production network. The office network services include: OA (Office Automation) system, mail system, video conference system, video surveillance system, etc. The production network services include all the various financial and banking services. With the migration of ATM to VTM and the continuous popularization of face recognition and HD video applications, the bandwidth of the connections to a provincial branch are expanding from 2 ~ 10 Mbps to 10 ~ 20 Mbps. Assuming a large number of sub branches connecting to a provincial branch, the total bandwidth of all these high quality private line connections will reach several Gbps.

     The bank's Data Centre is typically geo-redundant. The private lines between these DCs require large bandwidth and low latency.

     The banking services require secure and reliable networks, being physically isolated from other network users.

  b) Financial services generally have headquarters and data processing centres, and geographically distributed branch offices. In order to ensure uninterrupted work during trading hours, each branch office has redundant connections to the headquarters. There are also redundant connections within the headquarters itself. A typical financial services networking architecture is shown in Figure 8.

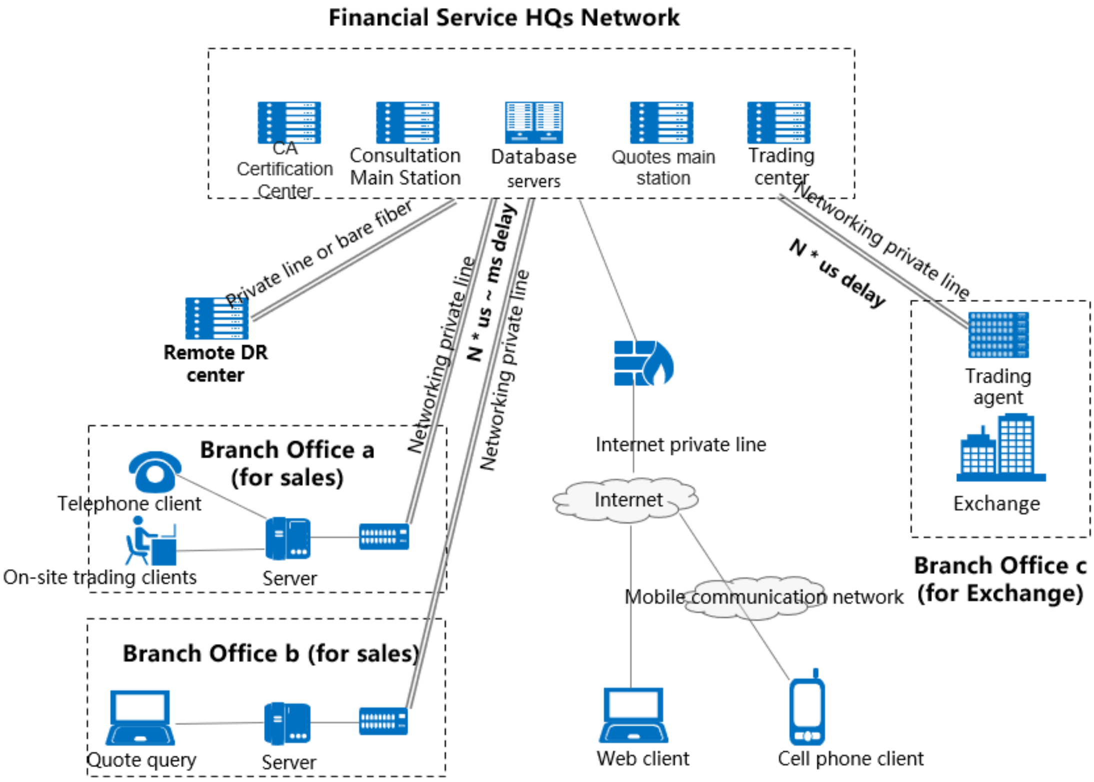


Figure 8: Typical network architecture for financial services

Hub & Spoke is a typical network topology for financial services. All sites are managed by the HQ and processed through the HQ for transaction and market query.

Typically private lines are used for data exchange between branch offices and headquarters, as well as data exchange between the headquarters and the stock exchanges.

The headquarters network is divided into an office network and a production network:

- The office network only supports the non-financial services. Its security level is relatively low. Therefore it can be connected to the Internet.
- The services carried by the production network include: communication between the branch offices and the headquarters; and between the headquarters and the stock exchanges for orders and market inquiries. The security level of the production network is very high. Therefore the production network needs to be isolated from both the office network and the Internet.

Network delay directly affects the speed and efficiency of market query and transaction confidence. Some operators have begun to build financial private networks that perform route selection and latency optimization based on delay indicators. These networks provide very low, stable delays for trading transactions, facilitating faster transaction.

- Medical Organizations:

Various types of medical institutions at all levels need to use the network for services such as remote medical care, online appointments, payment, diagnosis and treatment report query. In addition a medical information sharing service platform including medical images, health records, reports, is needed for sharing and exchanging medical data between hospitals and other medical organizations. A large amount of medical image data needs to be uploaded and downloaded within a certain period of time, for this a stable high-bandwidth private line is required.

6.2.2.1.3 Cloud-based services

With enterprise digitization, enterprises cloud services are further extended from common office processes and document management to core production services, such as time-sensitive services, and cloud-based collection of regulatory data and financial data. This generates higher quality requirements for Cloud private lines. Cloud resources can be exclusively used by organizations to allow for higher security and performance.

For risk reduction and for cost-efficiency, most enterprises use multiple Cloud providers. This allows them to choose the provider based on the application.

- Medical cloud:

  To reduce the on-premises assets, many medical associations are migrating their applications from on-premises Data Centres to the Cloud. The Cloud used by healthcare organizations is industry-specific, and hospital's PACS (Picture Archiving and Communication Systems) and HIS (Hospital Information System) systems are the typical applications preferably deployed on the cloud.

  A large number of medical high-resolution images are uploaded by PACS to the medical Cloud, and doctors download medical images from the cloud for review. The volume of data in medical imaging is very large, which normally needs higher than 1 Gits/s speeds to ensure good experience during upload and download. The images needs to be stored on the Cloud for months or even for years, which requires the medical cloud to support high storage volume and high reliability.

  HIS is used to record the patient's diagnosis and treatment data. This information is highly confidential and requires a dedicated network from the medical institutions to the medical Cloud to support secure transmission, which isolates the medical information from other data.

- Offices with Thin Clients (Cloud Desktop):

  Enterprises use cloud desktop to reduce assets by retaining only thin terminals and displays on-premises, and moving all the computing and storage resources from the office to the cloud. In order to guarantee the quality of experience of on-premises terminal access to the desktop Cloud, it requires that the RTT (Round Trip Time) of the link between office and cloud to be within 30 ms, and a packet loss rate less than 0,1 %. This requires a high quality dedicated network from the Enterprise to the Cloud.

- Financial cloud:

  Financial enterprises require high security and high reliability. They often use private or proprietary Clouds running on their own DCs to meet such requirements. High-security private lines are required between the Enterprise and the Cloud. Financial transaction data is transferred between DCs of different financial enterprises, therefore, the lower the delay, the better the experience. Some financial private lines need a delay of less than 1 ms.

In response to competition from Internet Service Providers (ISPs), carriers use multiple technical methods to implement fast provisioning and efficient O&M of private lines. For this, the intelligent management system needs to synchronize network devices in real time, manage and accurately schedule network-wide resources in a unified manner, and provide users with a series of applications such as network quality monitoring and optimization, and bandwidth adjustment.

According to the requirements of the above scenarios, a high quality private line has the following capabilities:

a) Guaranteed bandwidth: the bandwidth is absolutely guaranteed. Private line bandwidth granularity can be flexibly configured from 2 Mb/s to 100 Gb/s to meet the bandwidth demands of different users.

b) High link availability: end-to-end protection paths are required, such as cross-device dual-homing protection, fibre break protection, etc. The protection switching time need to achieve carrier-class 50 ms, and the link availability needs to achieve 99,999 %.

c) Business security: physical equipment isolation; L1 hard isolation; L2 soft isolation.

d) Low latency: end-to-end deterministic low latency and delay jitter, which are independent of network load.

e) Extensive private line connections: the number of private line connections can be very large between enterprise branches, headquarters, and Clouds. Therefore, the number of connections needs to scale with the size of the networks.

f) One-hop flexible Cloud access: end-to-end hard pipe enables an enterprise to access the industry-specific Cloud/private Cloud with one hop. If the Cloud is not operated by operators, the private line can reach the handover points (i.e. PoP) between the network and the Cloud. Enterprises can flexibly connect to multiple Clouds with high security, high reliability and high bandwidth.

g) Fast provisioning of private lines: the intelligent management system of network equipment provides open northbound APIs to realize the integration of OSS and implement fast provisioning of end-to-end private lines. In addition, the OSS can also provide a private line Portal for users to monitor the provisioning process and operation quality of the private line.

h) Efficient management, operation and maintenance: a high quality private line service can be quickly provisioned in days or even minutes. Therefore, E2E service provisioning and O&M, plug-and-play of private line CPE, and automatic and fast provisioning of combined Cloud-network services are required to simplify the configuration of the CEs of enterprises.

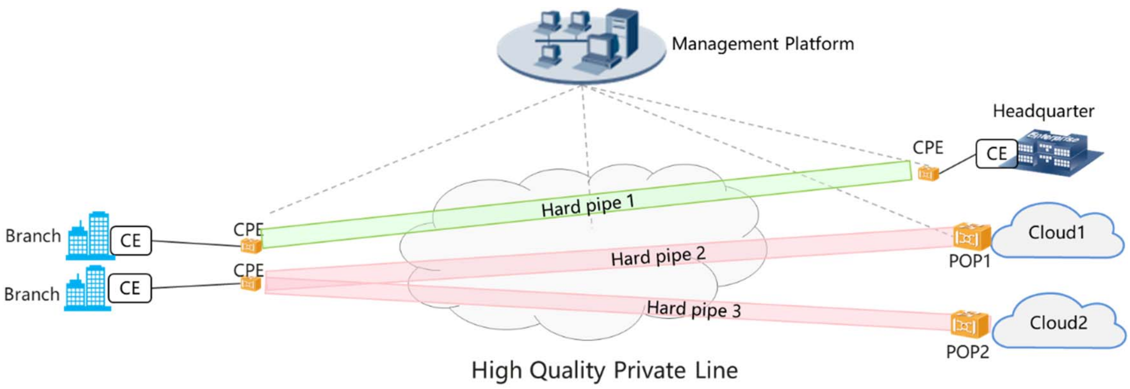


Figure 9: High quality private network

As shown in Figure 9, the high quality private line network includes CPEs, hard pipes and an intelligent management system:

a) CPEs are placed in the enterprise or in the operator's equipment room, and are connected to the enterprise CE for the support of the enterprise's private line services.

b) The high quality private line network provides a hard pipe, connecting branch office CPEs, headquarters CPEs and multiple Clouds.

c) The intelligent management system is used to manage CPEs and the network, to achieve rapid service provisioning and management, and is responsible for the combined configuration of the Cloud and the network.

In order to ensure that multiple private line users do not affect each other, each private line requires a different hard pipe connection to guarantee bandwidth, delay, availability and security. The hard pipes support flexible access to multiple Clouds. When an enterprise is connected to multiple Clouds, each connection uses a different hard pipe. An independent hard pipe is used between an enterprise branch and headquarters.

6.2.2.2 Motivation

The high quality private line provides high security and reliability and is suitable to ensure the end-to-end user experience for government institutions, financial enterprises, medical centres and large enterprises.

The main advantages and driving forces of the high quality private line are as follows:

- High quality private lines provide large bandwidth, low latency, secure and reliable connection.
- Accelerate the development of Cloud services. The high-quality and high-security of the private line connecting to the Cloud can enable enterprises to move more core assets to the Cloud and use low-latency services on the Cloud. Cloud-based deployment helps enterprises substantially reduce asset allocation and improve energy saving, so that enterprises can focus on their major business.

- Reduce operator's CAPEX and OPEX. The end-to-end service provisioning system enables quick provisioning of private line services and fault location and improves user experience.
- Enable operators to develop value-added services by providing enterprise users with latency maps, availability maps, comprehensive SLA reports, customized latency levels, and dynamic bandwidth adjustment packages.

6.2.2.3 Pre-conditions

Before the deployment and enabling the high quality private line service, the following preconditions are required:

- The CE and CPE of the enterprise branches and headquarters have been deployed.
- There are enough computing and storage resources on the Cloud.

6.2.2.4 Operational flow of actions

Flow chart of provisioning a high quality private line is shown in Figure 10.

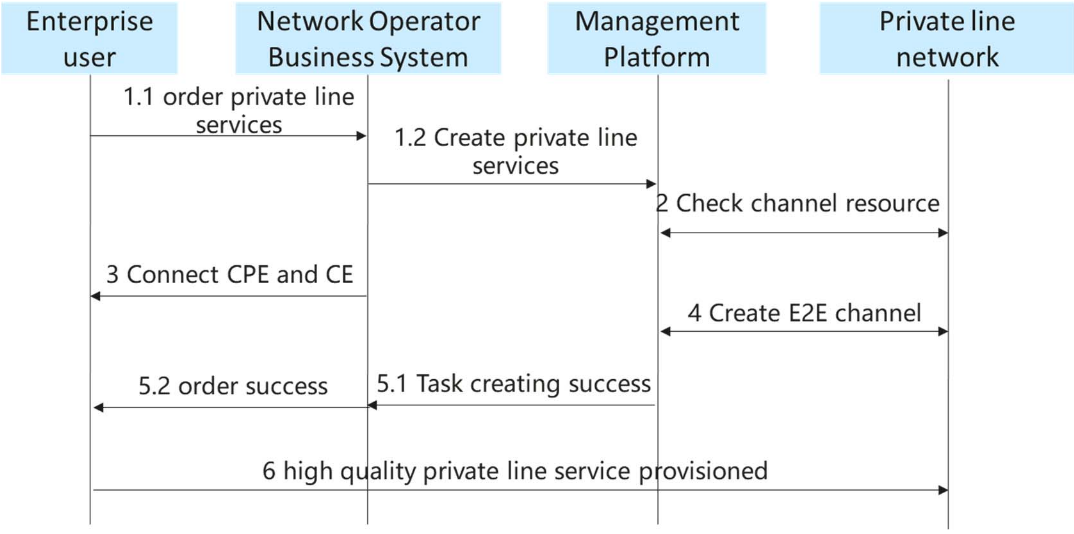


Figure 10: Provisioning process of high quality private line

1) The enterprise orders a high quality private line service (1.1) from the operator, and the operator creates the task of the private line service through the management system (1.2).
2) The operator's management system checks whether there are sufficient channel resources (2).
3) If resources are available, the operator deploys CPEs, connects CPEs to the CEs, and performs necessary configurations.
4) The management system creates an E2E Channel for the private line hard pipe, to automatically configure all network equipment end-to-end (4).
5) After the private line service is successfully established, the management system returns a successful response to the operator and enterprise user (5.1 and 5.2).
6) The high quality private line service is provisioned and can be used (6).

6.3 Use case #3: High quality low cost private line for small and medium enterprises

6.3.1 Use case context

SMEs are increasing demand for networking services, which are not currently met by available solutions, such as better service quality according to an SLA (assured bandwidth, low latency, guaranteed availability, quick provisioning and troubleshooting), improved network capability to support larger number of connected end devices and various types of business services. Traditional private line services can meet these requirements but are too costly for SMEs. By sharing infrastructure with other users such as residential can enable network operators to provide private leased line services in a cost effective manner and give network operator new opportunities for diverse service offerings.

6.3.2 Description of the use case

6.3.2.1 Overview

Small- and Medium-sized Enterprises (SMEs) can be classified into micro-, small-, and medium-sized enterprises. Each type of enterprises has its own requirements on the operators' networks.

Four key services are required by SMEs:

- Internet access: the operator's CPE needs to support from 32 ~ 128 terminal devices. The Internet access bandwidth is assured.
- Cloud service: Micro enterprises need Cloud-based virtual desktop based on the public Cloud, and use Cloud applications such as payment systems, meal ordering systems, and live video streaming. Small and medium enterprises need Cloud-based virtual desktop, cloud storage, and cloud Wi-Fi® management. Low latency communication is necessary for accessing Cloud services.
- VPN service: Some small and medium enterprises have chain stores or branches. Low cost VPN connections among these chain stores and branch offices are needed. The VPN connection needs to be secure and reliable.
- Telephony services: Multiple telephony clients need to be supported.

Based on the above mentioned service requirements, a SME private line service need to have the following capabilities:

- Wide coverage: The network and the SME private line service needs to cover a wide geographical area.
- Low cost: Most SMEs are sensitive to network service costs, and need different service packages (i.e. premium, medium and low cost) to meet the requirement from different types of enterprises.
- Connecting up to 128 terminals (many of which are wireless devices).
- Supporting high network availability and 1 Gbit/s to 10 Gbit/s bandwidth.
- Supporting the four key services mentioned above over a single SME private line service subscription.
- Isolating SME users from residential broadband users, as they may share the network infrastructure with residential customers.
- Fast provisioning.
- Plug-and-play CPE and fast and efficient troubleshooting.

To meet the user requirements for quality of experience, selected high priority traffic needs to be identified and mapped by the CPE to different paths. An example is shown in Figure 11.

- High priority users' service traffic is mapped to the Optical Transport Network with guaranteed bandwidth and low latency capabilities.
- Medium and low priority users' service traffic is carried over the IP network. Network slicing on the IP network can be used for higher-priority service traffic (such as voice and video traffic).

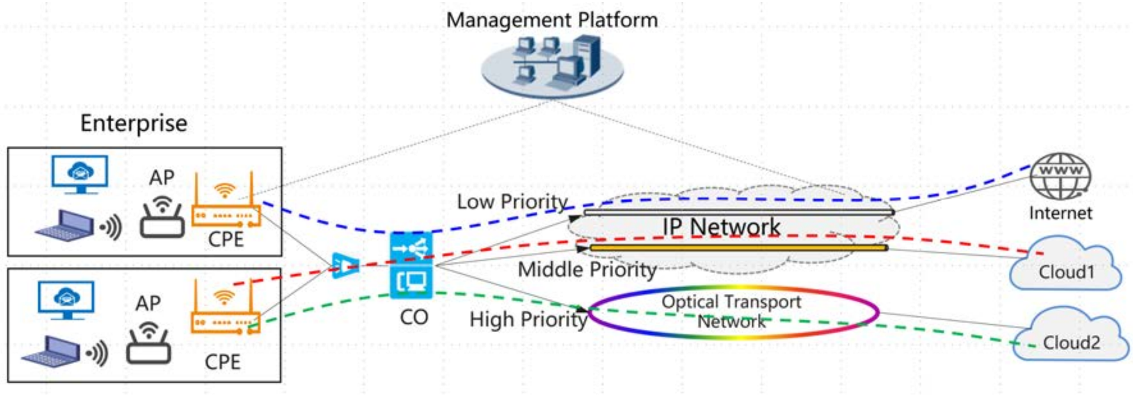


Figure 11: SME private line service identification and distribution of application traffic

6.3.2.2 Motivation

SME private line services provide cost-effective connections for a large number of small or medium enterprises. They are used for Internet access, Cloud access and to build an Enterprise Network connecting remote offices. In addition, SME private line services ensure bandwidth and low latency for high-priority communication and provide differentiated communication for enterprises.

The advantages and driving forces of SME private line services are as follows:

- To provide assured bandwidth, wide coverage, on-demand services, plus secure and reliable assurance for a large number of connections with low cost.
- To support many end users (including data and telephone terminals).
- To accelerate Cloud-based services deployment. Cloud-based deployment helps enterprises to reduce investment in IT assets, save energy, and to focus on their core businesses.
- To reduce operators' deployment and maintenance costs. The E2E service provisioning system enables fast provisioning of SME private line services, fast fault localization, reduced OPEX and improved user experience.
- To help operators to explore new value-added services by providing differentiated SME private line services.

6.3.2.3 Pre-conditions

The following pre-conditions are needed before SME private line services are deployed and services are provided:

- Basic SME-internal hardware infrastructure has been deployed.
- Suitable Cloud infrastructure is available.

6.3.2.4 Operational flow of actions

Flowchart of SME private line service provisioning is illustrated in Figure 12.

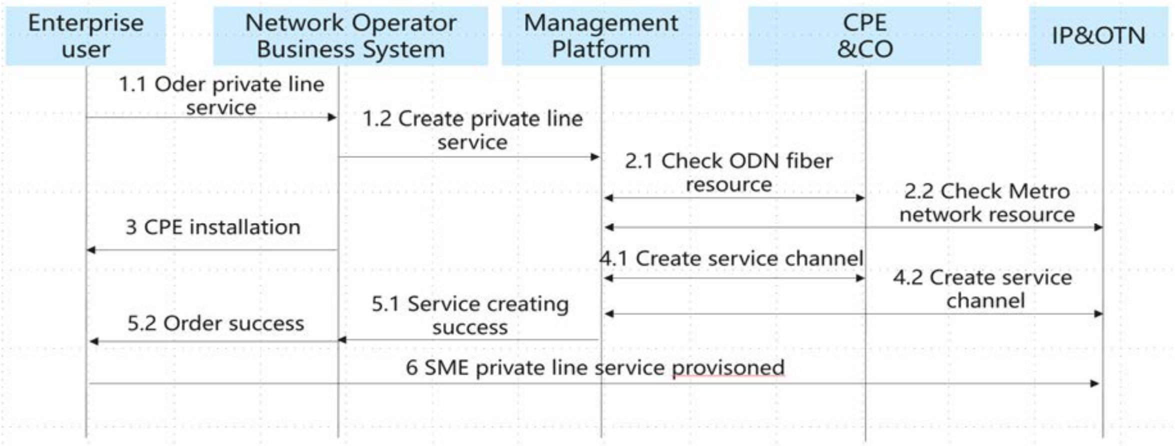


Figure 12: Flowchart of SME private line service provisioning

1) When SMEs need a private line service, they order this service from network operator (1.1), and the operator creates the SME private line services through its management system (1.2).

2) The operator's management system checks whether the Access Network has sufficient ODN optical fibre resources (2.1) and Aggregation Network (AggN) resources (2.2).

3) If the resources are available, the operator installs the CPEs, connects the enterprise's devices to these CPEs and configure service channels for ports and VLANs (3).

4) The management system creates a service channel on the Access Network device to identify the priorities of different services (4.1). Create service channels on the Aggregation Network devices to forward service data traffics with different priorities (4.2).

5) After the Access Network and Aggregation Network service channels are successfully created, the management system acknowledges the success with a response to the operator and enterprise users (5.1 and 5.2).

6) The SME private line service is provisioned and can be used (6).

6.4 Use case #4: Fibre on-premises networking: Fibre-to-The-Room (FTTR)

6.4.1 Use case context

The current connections in the house are mostly copper or wireless based, and they suffer from limited capacity due to the restricted frequency range and limited spectrum resource. In this case, users would like to deploy a new media for the on-premises network. Fibre is a preferred upgrade choice for the on-premises network due to its future proof capabilities. FTTR needs to support up to 1 Gbps bandwidth per room or per fibre end-point. Different FIN (Fiber in-premises Network) technologies can be used and may need to be developed. One potential technology is being defined in the G.fin series work items in progress at ITU-T SG15/Q18 [i.4].

6.4.2 Description of the use case

6.4.2.1 Overview

6.4.2.1.1 General

Fibre on-premises networking can be used in different scenarios. The requirements and system architectures of different scenarios could be different. In the following are three typical scenarios of fibre on-premises network that will be shown as good examples in the context of this use case.

- FTTR for the home area network.

- FTTR as an extension of FTTB/C for apartment buildings and dense residential areas.
- FTTR for SMEs.

6.4.2.1.2 FTTR for the home area network

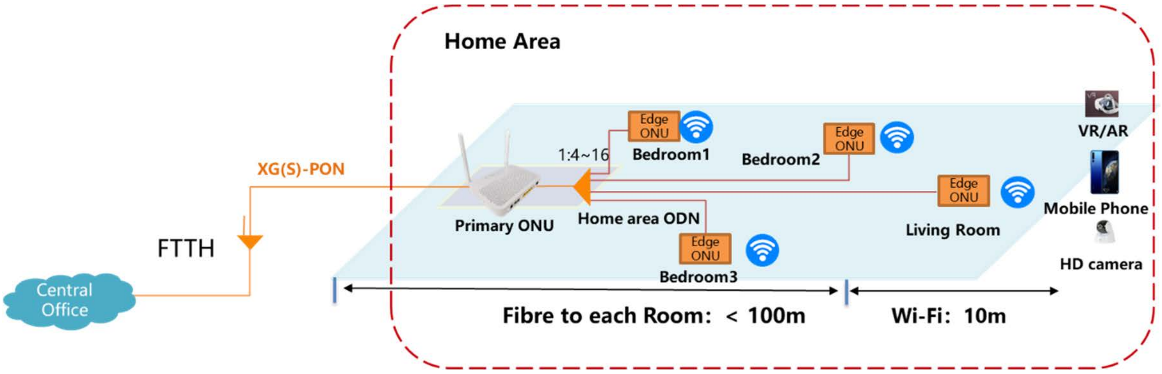


Figure 13: FTTR for home area networks

Wi-Fi® is widely used in home networks due to its convenience. As the frequency increases, the structural attenuation of the wireless signal increases significantly. More Wi-Fi® APs are required to cover the home area, when there are several rooms or floors in the house. Wi-Fi® 6 has been defined and will be widely deployed in the coming years. The maximum data rate for Wi-Fi® 6 is 9,6 Gbps. For the next generation Wi-Fi®, even higher bitrate will be needed.

In-home copper links have limited transmission distance due to their high insertion loss, especially for high frequency signals. If the current copper-based medium can no longer support the requirements of future home network (bandwidth & latency), a new medium is needed. Category 6 Ethernet cable could be a choice. Due to its size, weight and its physical properties, it is not so easy to deploy Category 6 Ethernet cable in the existing ducts (if they are present at all). However, fibre cables are small, light and flexible, so it is easy to deploy fibre in the home area. Figure 13 shows a FIN system for the home area network. From the central office to the primary ONU, there is an XG(S)-PON system (FTTH) that can deliver Gigabit access bandwidth from the network operator. From the primary ONU, Wi-Fi® and FIN is used in the home area network for the connectivity of terminal devices. There are devices such as HDTV, HD surveillance cameras and VR/AR head mounted displays in the home area that needs cable connections for a stable network performance. The FIN system can connect to Wi-Fi® Access Points (Edge ONUs) in several rooms of the home area network. In order to optimize the performance of the Wi-Fi®, coordination of the Wi-Fi® APs (Edge ONUs) is supported by the FIN system.

6.4.2.1.3 FTTR as an extension of FTTB/C for apartment buildings and dense residential areas

Figure 14: FTTR for apartment buildings

In some apartment buildings and dense residential areas, the fibre for the Access Network is deployed to the building or to the curb (FTTB/C). From the access point in the building or curb to each apartment, copper cabling is used. Due to the requirements of high-quality network services such as Cloud VR, on-line education, teleconference and others, the copper-based media may not be able to satisfy the increasing bandwidth and latency requirements. In this case, fibre can be deployed in the building to replace the current copper cable. FTTB/C with XG(S)-PON can be deployed from the central office to the building or curb, and then a FIN system can be deployed from this point onwards inside the building for each individual apartment. FTTR can be further used within each individual apartment. In this way, the operator could reuse the deployed fibre and sites, and the users can enjoy an excellent network experience.

6.4.2.1.4 FTTR for SMEs

The FTTR for SME (Small-Medium Enterprise) overall architecture is shown in Figure 15. This architecture has the following features:

- One single fibre infrastructure for all the services required by the SME.
- The primary ONU is an all-in-one device which integrates ONU, router/switch, voice and AC (Access Controller). All edge ONUs are connected by fibre or OEHC (Optical Electric Hybrid Cable) to provide Wi-Fi® service.
- The primary ONU supports a large number of end-devices (for example, 300 terminals). The edge ONUs enable a large number of end-devices and guaranteed bandwidth (for example, an edge ONU can support a maximum of 64 terminals with guaranteed 5Mbps per terminal).
- Edge ONUs may have Ethernet ports for wired connections in the room.
- Seamless Wi-Fi® roaming is required for mobile office and mobile video/voice meetings.
- OAM support is required.
- Web Management Portal and management APP.

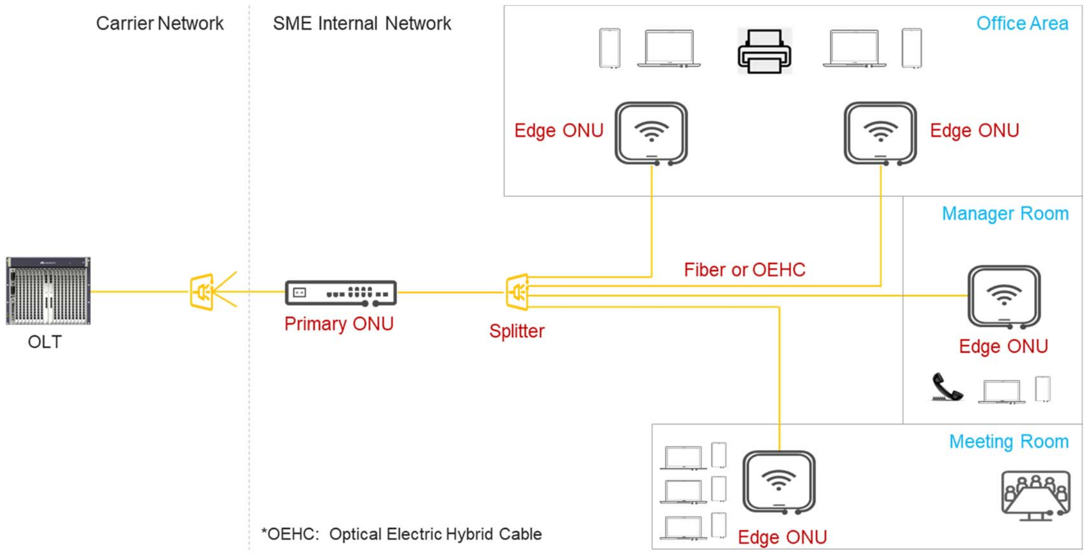


Figure 15: FTTR for SME work space

6.4.2.2 Considerations for on-premise devices

In order to deploy FIN, the primary ONU needs a FIN port, in place of the legacy LAN side Ethernet ports. For example, a typical Home Gateway has 4 Ethernet ports. Once a FIN system is deployed, these 4 Ethernet ports may be replaced by one FIN port when necessary. Therefore, the size of the primary ONU is smaller. The uplink of this Home Gateway/primary ONU is FTTH. The cascaded fibre system could have common management tools and cooperative mechanisms to forward the customers' traffic (i.e. a shared Media Access Control (MAC) function).

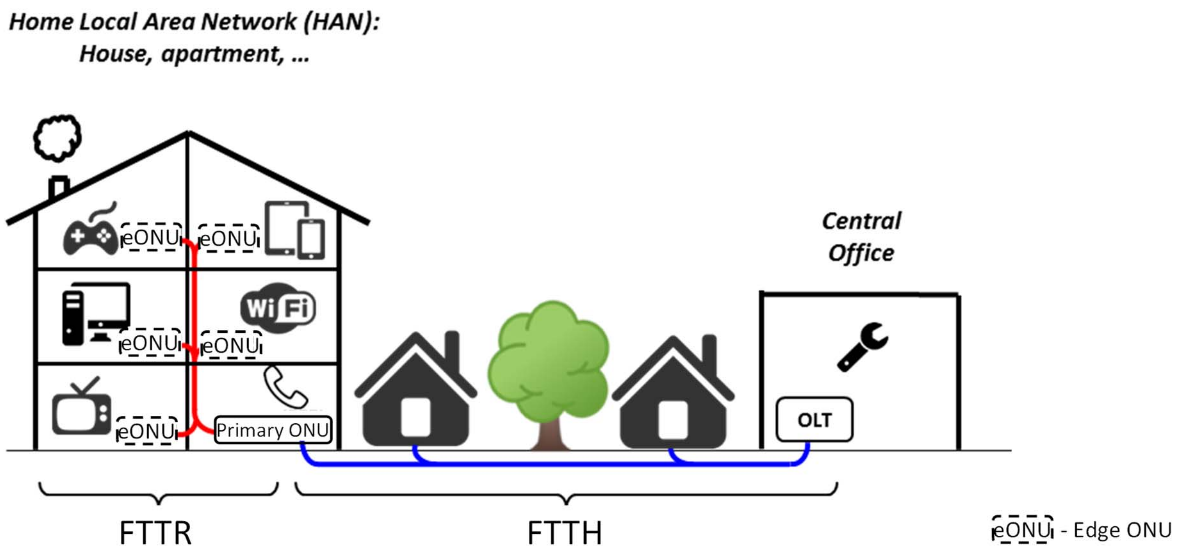


Figure 16: Cascaded fibre system with new on-premises devices

6.4.2.3 Motivation

Using fibre connections within home brings several advantages:

- The bandwidth can be upgraded easily.
- Future proofing the medium.
- Since the insertion loss of fibre is quite low (< 0,3 dB/km), low power consumption in the transmission link is possible.
- Wavelength multiplexing in one fibre could provide separate transmission channels for different services.
- The optical signal in the fibre is immune to Electro-Magnetic Interference (EMI).
- The fibre is lightweight and small in size, leading to easy deployment.
- The lifetime of fibre can be as long as 30 years even in an extreme environment.

6.4.2.4 Pre-conditions

In order to deploy FIN, there are several pre-conditions as follows:

- Fibre or OEHC has been deployed on-premises.
- An efficient and cost-effective FIN solution is available for deployment.

6.5 Use case #5: Passive optical LAN

6.5.1 Use case context

Legacy LAN networks are used in business areas, campus and buildings, to connect end-users and support business services such as voice services, high data bit rate Internet access, Wi-Fi® connectivity, videoconferencing, telepresence, etc. Most traditional LAN networks use Layer 2 switches, Layer 3 routers and connections using Category 5 Ethernet cable. This approach is becoming difficult to satisfy the emerging campus network requirements:

- The bandwidth is insufficient to meet the traffic requirements of new applications.
- Copper wire deployment costs are high and not effective for future network upgrades.

- The power consumption is high and the equipment occupies a large area.

To overcome these challenges, some enterprises use passive optical LAN (POL) solutions, which are based on the Passive Optical Network (PON) technology. POL not only brings great values to customers and causes no change to the service planning and user terminal network connections, but also supports all functions provided by the traditional LAN network.

6.5.2 Description of the use case

6.5.2.1 Overview

6.5.2.1.1 General

From Figure 17, it is clear that the OLT and ONU in the POL solution act as the convergence and access switches in the traditional solution. The OLT is connected upstream to the core switch (not shown in Figure 17). Like switches, the OLT and ONU forward data based on Ethernet or IP addresses. Ethernet interfaces are available on both user and network sides in the POL system.

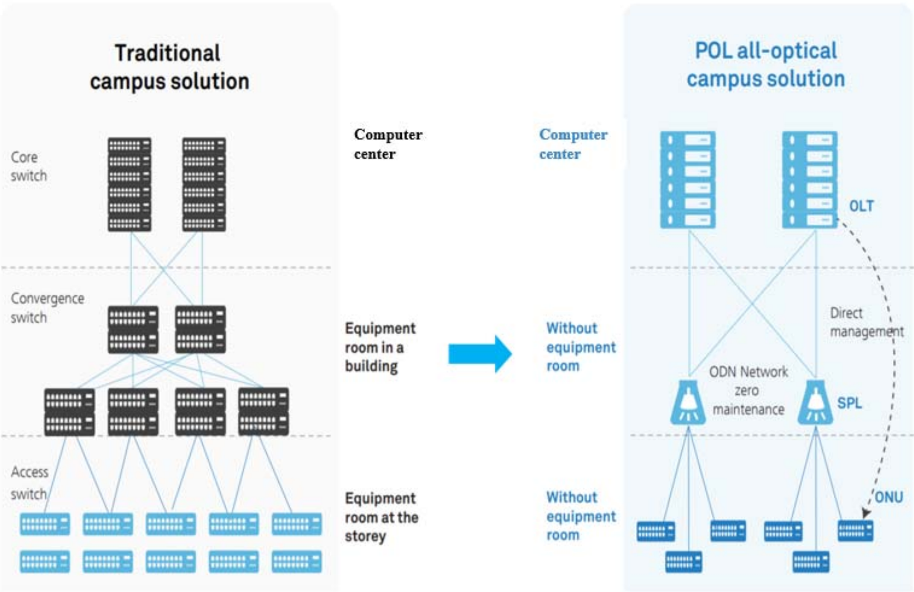


Figure 17: The POL all-optical solution compared with traditional campus solution

- POL can be used in different scenarios. The location of OLT and ONU in different scenarios could be different. The following tables describe three typical POL scenarios:
  - Table 3 - POL in High-rise Building.
  - Table 4 - POL in Multi-storey Building.
  - Table 5 - POL in Flat-Storey or Low-Density Building.

Table 3: POL in High-rise Building

Basic Description	Routing Principle	Application Scenarios	Line Routing
Number of information points at each storey: 50-60.	Optical splitters are placed in the storey management subsystem area.	State-owned office buildings or government buildings.	
Number of information points at each storey: over 100.	Optical splitters are placed in the storey management subsystem area. Each storey has multiple such areas.	High-end hotels.	
Number of information points at each storey: over 100 (their positions in the working area are to be determined).	Optical splitters are placed in the storey management subsystem area.	High-end office buildings.	

Table 4: POL in Multi-storey Building

Basic Description	Routing Principle	Application Scenarios	Line Routing
Number of information points at each storey: 20-30.	Level-1 optical splitters are placed in the fibre distribution subsystem area.	Schools, libraries, community centers, and express inns.	
Information points are centralized in a limited area.	Level-1 optical splitters are placed in the fibre distribution subsystem area.	Students' dormitories and small office buildings.	

Table 5: POL in Flat-Storey or Low-Density Building

Basic Description	Routing Principle	Application Scenarios	Line Routing
A small number of information points are scattered in a large area.	Level-1 optical splitters are managed by partitions.	Large shopping malls, industrial buildings, airport warehouses, and railway station buildings.	In the case of a villa:  Large supermarket: 

POL can also be used in hotels, stadiums, holiday resorts, railways/highways and shopping centres.

6.5.2.1.2 Hotel

In the hotel, the overall architecture is shown in the Figure 18. This architecture has the following features:

- One single fibre infrastructure for all the services required at the hotel.
- One Fibre Gateway (FGW), an ONU with integrated router and Wi-Fi® capabilities, per guestroom providing all the services (internet, Wi-Fi®, Voice, TV and IPTV).
- ONUs are distributed across the hotel providing the backbone infrastructure for Wi-Fi® seamless coverage and CCTV cameras.
- APIs for integration with Hospitality Software to support dynamic guest experience with a variety of real-time applications (in-app messaging, voice, video, personal VPN, etc.), secure point-of-sale, management of connectivity credential, IoT, etc.
- Simplified OAM support.
- One OLT can support all the end points required at the hotel.
- Web Management Portal.
- VoIP Server included.
- IPTV Server/Streamer.

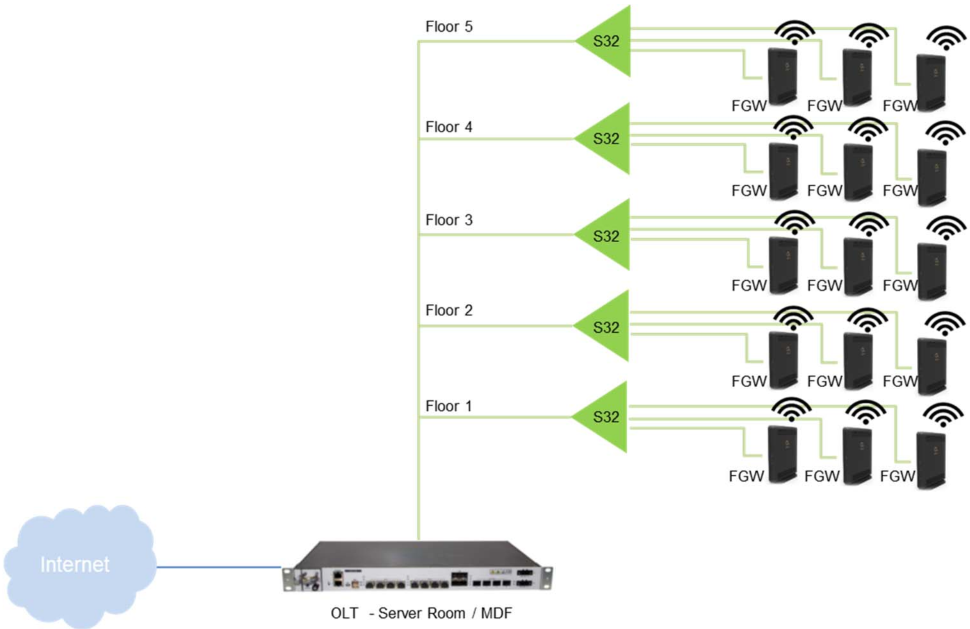


Figure 18: Overall PON architecture in the hotel

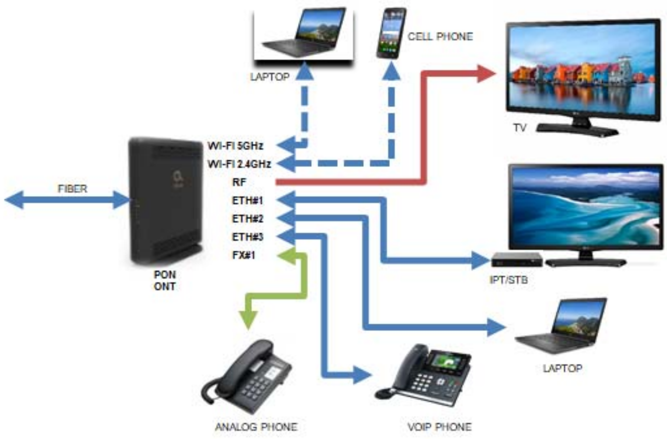


Figure 19: ONU at each guestroom

In the hotel each guestroom uses an ONU, providing HSI, TV, IPTV and phone as shown in Figure 19. There are also ONUs distributed across the hotel, providing additional services such as hot-lines for emergency situations and IP cameras for surveillance as shown in Figure 20. As ONUs can provide both standard Ethernet outlets as well as Wi-Fi® connectivity, this avoids the need to install two devices (ONU and AP) for the common areas (lobby, hallway, stairs, pool, gym, etc.). The ONU supports multiple Wi-Fi® users in the 2,4 GHz and 5 GHz bands. It enables independent data streams. It provides QoS on L2 or L3 as well as Wi-Fi® roaming.

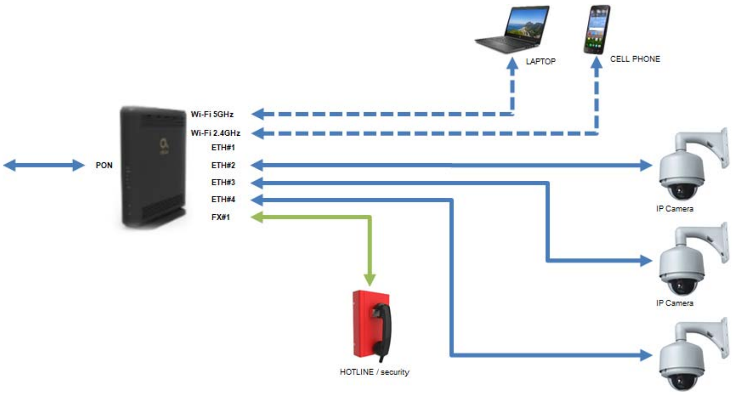


Figure 20: ONUs spread across the hotel for common services

6.5.2.1.3 Stadium

In the stadium, the overall architecture is shown in Figure 21. This architecture has the following features:

- One single fibre infrastructure for all the services required throughout the stadium providing all the services (internet, Wi-Fi®, Voice, TV and IPTV).
- ONUs are distributed across the sports complex providing the backbone infrastructure for Wi-Fi® seamless coverage and CCTV cameras.
- APIs for integration with Security systems as well as Publicity and Digital signing to support dynamic guest experience with a variety of real-time applications (in-app messaging, voice, video, personal VPN, etc.), secure point-of-sale, management of connectivity credential, IoT, etc.
- Simplified OAM support.
- One OLT can support all the end points required at the stadium/arena.

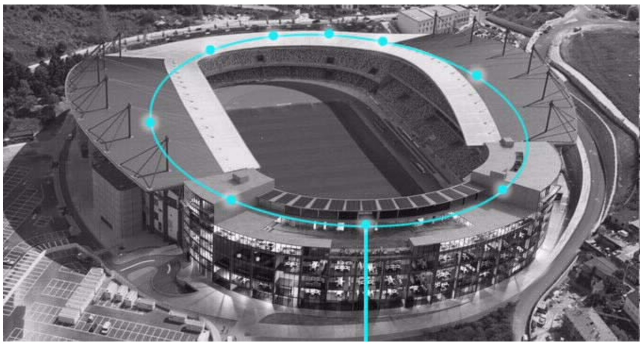


Figure 21: Overall PON architecture in the stadium

6.5.2.1.4 Holiday Resort

In the holiday resort, the overall architecture is shown in Figure 22. This architecture has the following features:

- One single fibre infrastructure for all the services required at the resort.
- One ONU per villa, guestroom, apartment providing all the services (internet, Wi-Fi®, Voice, TV and IPTV).
- ONUs are distributed across the resort providing the backbone infrastructure for Wi-Fi® seamless coverage and CCTV cameras.
- APIs for integration with Hospitality Software to support dynamic guest experience with a variety of real-time applications (in-app messaging, voice, video, personal VPN), secure point-of-sale, management of connectivity credential, IoT, etc.
- Simplified OAM support.
- One OLT can support all the end points required at the resort.

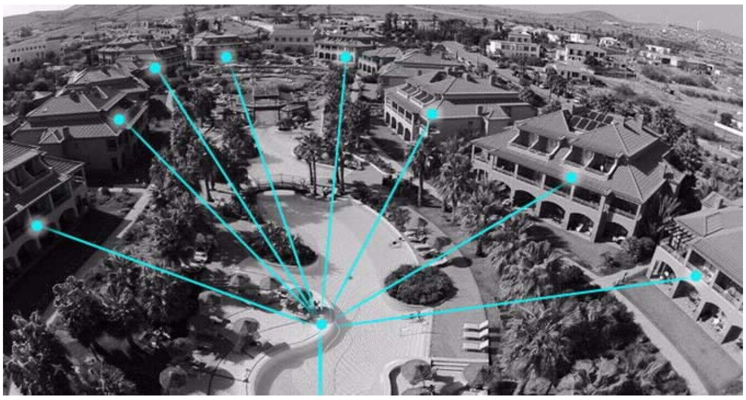


Figure 22: Overall PON architecture in the resort

6.5.2.1.5 Railways/Highways

In the railways/highways case, OLTs with a low number of PON ports are installed along the railway or highway every 60 km. From these OLTs at the 60 km points, ONUs are installed with unbalanced splitters. This network will provide the required secure telecom infrastructure for the railway or highway operator. The network is used to transport data coming from CCTV cameras (High Definition), for telemetry, for road signals and for display panels as well as VoIP (SOS/hotlines).

6.5.2.1.6 Shopping Centre

An OLT could be installed in a central technical room of the shopping centre and from there multiple fibres would reach not just all the stores but also places across the shopping centre where CCTV cameras and Wi-Fi® access points (embedded in the ONU) are installed. All UTP cabling would not be necessary outside the premises of each store. This fibre infrastructure could be Point to Point to the main technical room where the splitters would be installed or splitters could be installed along the shopping centre, depending on the desired split ratio and configuration of the shopping centre. This fibre will be used for all telecom needs of the shopping centre, meaning internet, intranet, CCTV, voice, TV, IPTV and Wi-Fi®. All services would be separated by assigning different VLANs. Each store would receive an ONU with embedded gateway functionality and that would be the demarcation point of the shopping centre infrastructure. The network would allow bitstream services (also supported with a unique VLAN) for each store that requires a specific Service Provider for Internet services. Within the same PON network multiple service providers can coexist.

6.5.2.2 Motivation

Compared with traditional LAN, passive optical devices such as fibre and optical splitter will be introduced into the network, with several advantages:

- It has a wide coverage and can reach more than 20 km. There is less need for the per-floor or intermediate network rooms (with energy and cooling) relative to those needed for a copper infrastructure.
- It is immune to the Electro-Magnetic Interference (EMI).
- Fibre cannot oxidize and has a longer service life. It adopts a point-to-multipoint networking topology which can save a lot of backbone fibre resources.
- The OLT is placed in the central technical room and functions as the LAN infrastructure, which provides a simplified passive optical LAN.

6.5.2.3 Pre-condition

In order to deploy POL, there is a pre-condition as follows:

- Fibre has been deployed on-site.

6.6 Use case #6: PON for Industrial Manufacturing

6.6.1 Use case context

The continued modernization and automation of the manufacturing industry demands more from its network. The basic principles behind the new Industry 4.0: Big Data & Analytics, Autonomous Robots, Simulation, the Industrial Internet of Things (IIoT), Industrial Cloud, Additive Manufacturing and Augmented/Virtual Reality, have a common denominator, connectivity. Higher performance, better stability, reduced maintenance, and easier upgrades are all needed, e.g. in Industry 4.0. Currently deployed industrial networks have a shortfall in these attributes.

Due to the variety of industrial equipment, the diversity of industrial communication protocols, and associated large costs on protocol interpretations, industrial enterprises need flexible and intelligent network solutions to be available.

With the rise of Cloud-based intelligent manufacturing, edge computing, and other emerging technical solutions, the intra-plant communication has new networking requirements. The existing fieldbus-based factory intra-plant network needs to be upgraded to support the new Cloud-based production machine control system. The fundamental feature of an intelligent factory is end-to-end equipment networking, which includes data collection and transport.

PON technology has become a major direction for factories intra-plant network based on advanced passive optical fibre communication technology. When it is combined with factory automation systems, intelligent factory is possible.

PON technology can be used in industry application to effectively solve the following problems:

1) Construction of reliable factory intra-plant network, communication among intelligent factories and digital shop floors.

2) Support for the fundamental network and data services for enterprise cloud connections.

3) Support for a wide range of interfaces used by diversified equipment in many factories and associated real-time data transmission

6.6.2 Description of the use case

6.6.2.1 Overview

The overview of the PON based industrial network solution is illustrated in Figure 23.

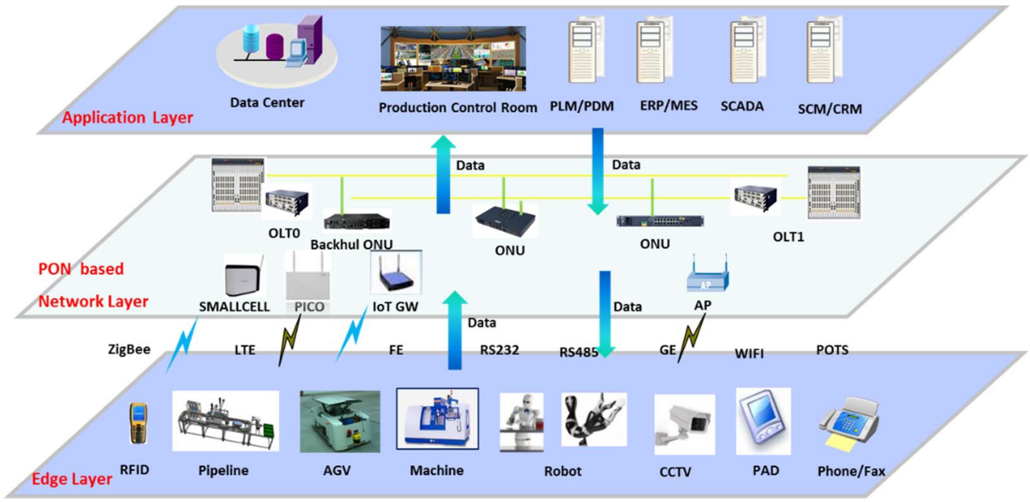


Figure 23: PON based industrial network solution overview

The followings features are expected for PON-based networking in industrial application scenarios:

1) Edge computing capability to realize the convergence of IT (Information Technology), OT (Operational Technology), and CT (Communication Technology), which leads to a universal intranet with capabilities of data collection, transmission and computation.

2) Network Slicing: is realized by a complete multi-service PON system, which can simplify the factory intra-plant network architecture and can reduce the network transmission latency.

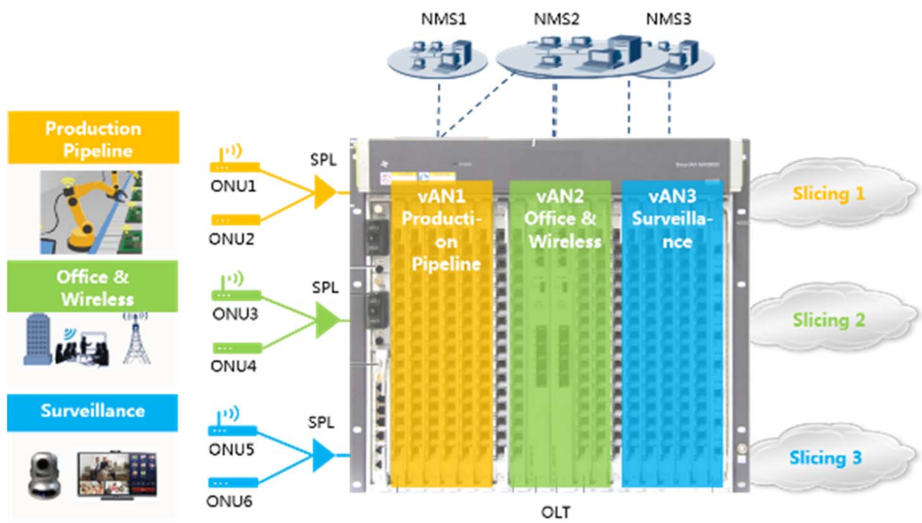


Figure 24: Schematic diagram of PON slice

3) Industrial protocols support: Being able to provide connectivity and QoS in compliance with diverse industrial standards. The industrial control data is always the highest priority for operation and management in the factory. It can be collected and transmitted in real time during industrial producing procedures.

4) Encryption ability: to ensure valuable industrial data security.

5) Low latency: The transmission delay can be controlled to less than 1 ms in some specific applications. Time synchronization functionality is available when necessary. Time Sensitive Networking (TSN) features may need to be supported in the future.

6) Network resilience and availability: using protection switching (restoration time expected to be less than 50 ms), ensures the non-stop operation of industrial workflows. Including multiple network protection schemes (for example type A ~ D introduced in ITU-T PON recommendations).

7) High resilience hardware: Supporting industrial grade ambient temperature capabilities, explosion-proof and dust-proof capabilities, and other harsh environment compatibility.

8) Intelligent operation: Capable of intelligent network diagnosis for early warning of network failures, big-data based network behaviour prediction by introducing new technologies such as SDN and AI.

PON introduces the following into the industrial world:

- Electromagnetic interference immunity using fibre optics only. This guarantees connectivity in a very noisy electromagnetic environment (electric motors, Variable Frequency Drives, Inverters, etc.). Traditional copper based networks prevent this problem by using expensive shielded cables (STP).

- Conventional copper cables require a large amount of duct resources which make future network expansion or scaling difficult. The copper cables also have several problems such that the replacement and updating needs to be planned in the short-term (3 years in some cases) due to the deteriorating characteristics of copper cables (e.g. oxidation). The PON network has the advantage of both lifetime and volume, for example, optical fibre generally has long lifetime around 20 years, which means minimal network change and lower OPEX.

- Extend communications range through a passive network up to 20 km. This ends the 100 meters limitations of traditional structured cabling and switching systems, which do not fit with the industrial dimensions and layouts.

Industrial PON is able to integrate in a single network all the connectivity needs of the industrial environment as shown in Figure 25.

Industrial PON includes three typical scenarios or networks:

- Industrial Process Field Data network.

- Office network.

- Surveillance network.

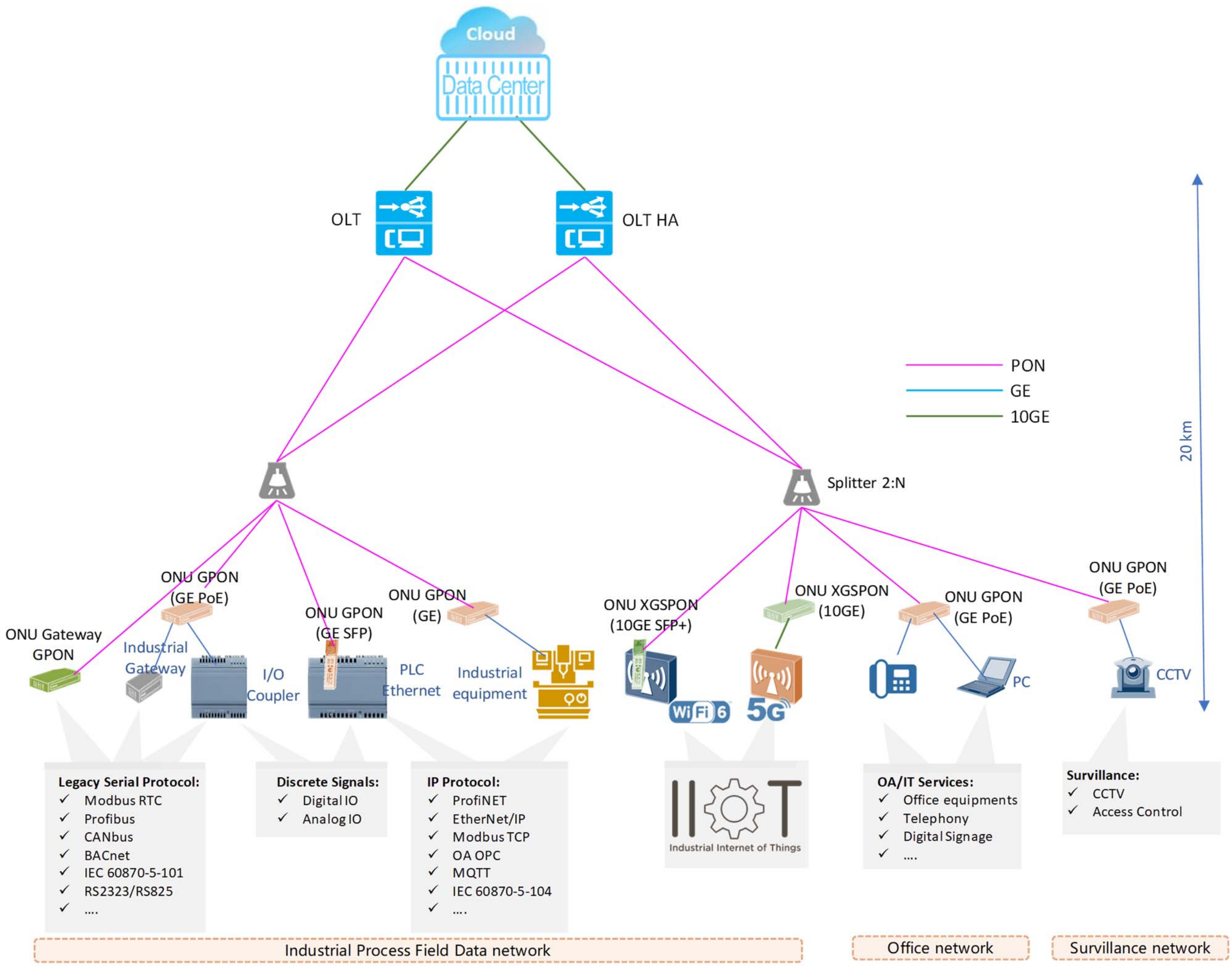


Figure 25: Industrial PON

1) Industrial Process Field Data network

The transport of enterprises factory intra-plant process data files is a major application scenario for industrial PON as shown in Figure 25.

Industrial PON allows through the multilayer capacity of PON networks to simultaneously implement different current and future services (GPON, XG(S)-PON, NG-PON2, etc.), to provide specific connectivity for all industrial data:

- Connectivity services through PON interfaces: The transport of enterprises factory intra-plant fieldbus services is a major application scenario for industrial PON as shown in Figure 25. Gateway ONUs can be designed with multiple industrial physical interfaces and built-in gateway functions, supporting communication among gateway, PLC, production management system, etc. The new type of ONU devices could also support integrated open source or client customized industrial applications. It is used to provide customization of industrial data collection and conversion processes. It also interacts with industrial cloud platforms. This completes the entire interconnection between devices and information systems.
- Connectivity services through GE (Gigabit Ethernet) interfaces:
  - Supporting legacy serial protocols (Modbus RTU™, RS232/RS485, Profibus, etc.) and discrete Analog & Digital I/O Signals, via Industrial Gateways and PLC. As well as distributed I/O Couplers that support the new centralized vPLC (virtual PLC) services in Data Centre.
  - Supporting IP Industrial protocols (ProfiNET®, EtherNet/IP™, Modbus TCP™, etc.) from PLC or other Industrial Equipment.

- IIoT devices: The massive expansion of connectivity in Industry 4.0 will come from these devices and their connectivity will most likely be wireless through Wi-Fi®6 and 5G services. Industrial PON provide xHaul services that allow the deployment of Wi-Fi®6 or 5G networks.

In addition to the above interfaces, Industrial PON also provide QoS mechanisms that guarantee minimum packet delay, packet jitter, packet loss and larger bandwidth. QoS is essential for the compliant transport of industrial protocols such as EtherNet/IP™ or ProfiNET®.

For the integration of these services, industrial grade ONU will be used. They have the mechanical and environmental characteristics necessary for the industrial environment such as degrees of protection (dust, water, etc.) and extended temperature ranges. The following describes the ONU types:

- GPON Gateway ONU with industrial physical interfaces and built-in gateway functions
- GPON ONU with GE (Gigabit Ethernet) interfaces and PoE functionality.
- XG(S)-PON ONU with 10GE interfaces needed for AR/VR applications or 5G/Wi-Fi®6 xHaul.

Likewise, the use of an ONU in SFP/SFP+ format is especially important for Industrial PON, allowing it to be integrated into industrial equipment: PLC, Access Point Wi-Fi®6, etc.

2) Office network

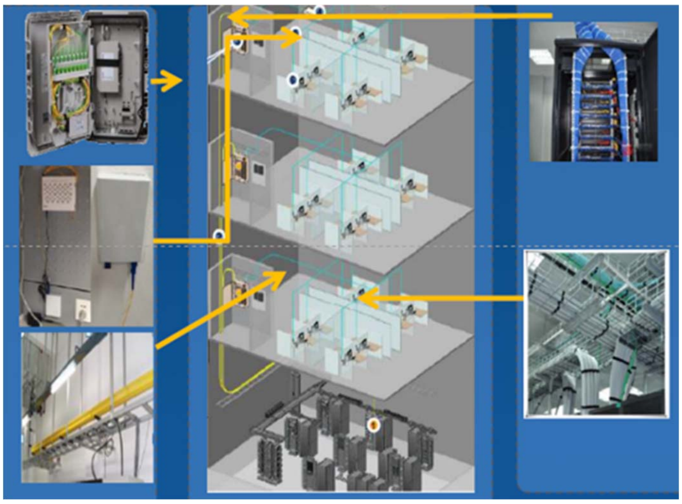


Figure 26: PON for office network, the internal networking in the office park with internet/intranet, telephone, fax services

Industrial PON is capable of transporting OA (Office Automation) traffic, telephony, etc. in the office area as shown in Figure 26. Conventional office networks are typically based on Ethernet switches, which needs to be configured and managed independently, resulting in complex and inefficient services configuration. Ethernet switches lack a mature unified network management system, hence their maintenance, performance monitoring and troubleshooting often causes network operation problems.

However industrial PON, with its unified services configuration and management, can achieve fast troubleshooting.

3) Surveillance network

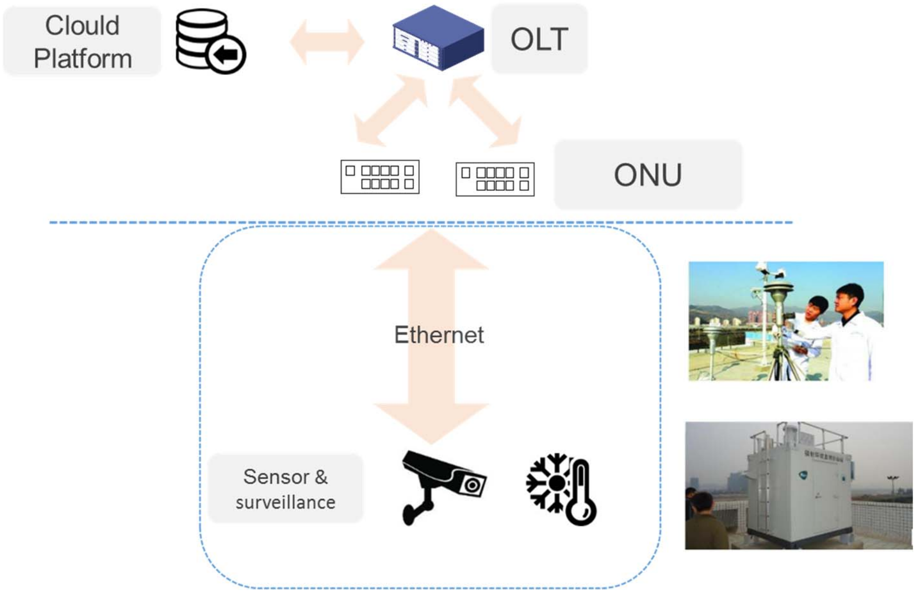


Figure 27: PON for sensor & surveillance network overview

Industrial enterprises have real-time application requirements such as video monitoring and environment sensing. The industrial PON can provide full support for these sensing services as shown in Figure 27. The PON ONU is capable of PoE (Power over Ethernet) function to provide both network connection and electricity supply for remote video monitoring cameras. This enables full scale camera deployment in a flexible and easy way.

Other capabilities such as Wi-Fi® AP is also available in the PON ONU to realize the data collection and transmission for several kinds of sensors.

6.6.2.2 Motivation

There are several advantages of PON being used for industrial application:

- PON technology is widely used worldwide to construct FTTH network for a large number of residential users, which is mature, reliable and cost-effective. Thus, it is believed that PON technology is one of the best choices for industry intra-plant network construction due to its high quality, high reliability, and high security abilities.
- New abilities can easily be built in, to enhance the network capability, such as integrating diversified industrial protocols, and full interconnection of all equipment in the factory. This provides a uniform intra-plant factory network supporting any traffic in the factory.
- Industrial PON can deliver long distance connection, low-density layouts and EMI immunity.
- Industrial PON optimizes the data continuity between shop floor and production management system. This will increase production efficiency and quality, reduce costs, improve production management, and enable intelligent manufacturing.

6.6.2.3 Pre-conditions

To use PON technology in the industrial application, there are several pre-conditions as follows:

- The equipment to be connected through industrial PON in the factory needs to be available.
- The optical distribution network needs to be well designed and deployed.

6.7 Use case #7: Using PON for City Public Service

6.7.1 Use case context

Because of its networking advantages, PON could be a promising network technology in the context of city public service, and a typical scenario could be using PON in a smart city network. F5G technologies used in smart cities enable city officials to interact directly with both the citizens and city infrastructure and to monitor what is happening in the city and how the city is evolving. Therefore, a reliable, easily deployed, maintenance-free bearer network is well suited. A good example in the context of a smart city is a smart light pole system, which supports Wi-Fi® hotspot, monitoring, information broadcasting, advertisement, etc.

6.7.2 Description of the use case

6.7.2.1 Overview

Smart light poles are viewed as a viable solution for building up a smart city communications infrastructure. In fact as light poles are deployed in large numbers, they offer the advantage of easy access to electricity, excellent location, and can support an easy expansion of the smart light pole network. A smart light pole system is known as a composite public infrastructure that integrates various functions, such as intelligent lighting, video acquisition, mobile communication, public broadcasting, road traffic flow and environmental monitoring, meteorological monitoring, radio monitoring, emergency help, public information delivery, etc. offering a comprehensive network into the future. By using the integrated design of a multi-function smart light pole system, different information equipment and accessories are installed with reduced CAPEX.

It is critical to choose the appropriate design solution in terms of positioning and engineering. The following are the fundamental aspects:

- Meet the requirements of urban landscape and environmental constraints.
- The selection of poles needs to meet the objectives of the effective coverage of the target area. The selection process needs to take into account the effective coverage of each installed device, combined with the needs of users and services.
- The poles need to be distributed as evenly as possible.

Ethernet has been used in some areas for the connection of smart light poles. However, based on its system features, PON can provide a more reliable, better space-saving connections with high performance and high energy efficiency. Furthermore, benefiting from the wide scale deployment of PON in Access Network for years, PON systems can be cost effective, and can be extended to other scenarios. Figure 28 shows a practical example of PON use for connecting smart light poles.

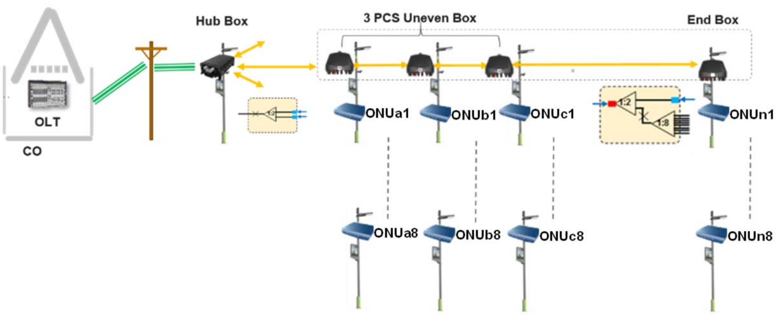


Figure 28: PON based connection for smart light poles

To support a smart light pole system with a XG(S)-PON system, some key points should be considered:

1) The laying of network for a smart light pole system is generally along the roads. This kind of linear topology requires a suitable ODN to assure the needed power budget in covering the required area. A chained split of the ODN can then better meet the requirements, saving fibre resources, and achieving fast and flexible deployment of ODN.

2) As part of a smart city public infrastructure, optical fibre network can be deployed at low cost, and with high efficiency.

3) Fibre resources have to be accurately and automatically operated and managed, for example, with ODN's digitalization and intelligent management.

6.7.2.2 Motivation

Smart light pole systems based on a fibre infrastructure can efficiently and cost-effectively support a smart city.

6.7.2.3 Pre-conditions

- The positioning of smart light poles has been chosen to re-use the existing light poles along the road/street.
- A suitable ODN topology chosen to allow the support of the needed services.
- The deployment of a basic optical network infrastructure.

6.8 Use case #8: Multiple Access Aggregation over PON

6.8.1 Use case context

PON technologies is beneficial for the high density deployment in the residential market. PON technologies are more suitable for this market compared to P2P solutions due to the lower cost per client, lower number of equipment ports, and lower number of CO fibre termination, CO space reduction, and lower power consumption. PON still guarantees a high quality of service and customer experience.

One of the main challenges to be address in 5G implementation is the coverage/density. For the same reasons that PON satisfies the residential market, PON technology can address all services and network requirements for 5G. PON technology is well positioned to be effective in the large scale deployment of 5G.

The GPON technology is not optimized for the requirements imposed by 5G for many aspects, such as architecture, bandwidth, traffic model, slicing, latency, time synchronization and an ultra-high availability. Comparing with P2P solutions, PON offers a lower cost per client/cell site. It could be advantageous to use PON for the support of the 5G high density of radio points and of the geographical coexistence of B2C and B2B markets. The current XG(S)-PON and future PON technologies (25/50G-PON, NG-PON2, etc.) could in fact be adapted to implement the 5G mobile xHaul scenarios.

This use case focuses on the support of mobile xHaul on the same PON network used for B2C and B2B services.

6.8.2 Description of the use case

6.8.2.1 Overview

Figure 29 describes the multiple access aggregation over PON.

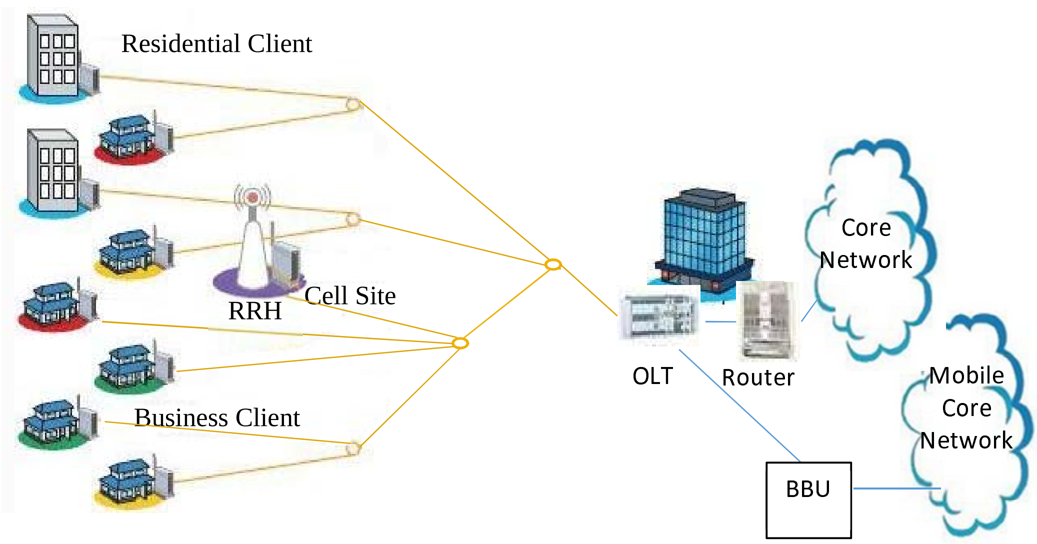


Figure 29: Overview of the multiple access aggregation over PON

The typical distribution of Residential Clients, Business Clients and Cell Sites Clients, driven by the residential market and its geographical mix, shows the advantage of a common fibre optical network. This leads to the technological demand that-PON needs to support a wide variety of Clients and services.

Figure 30 illustrates the three main Access Network goals that F5G will need to address:

- Network QoS;
- Network availability;
- Network densification.

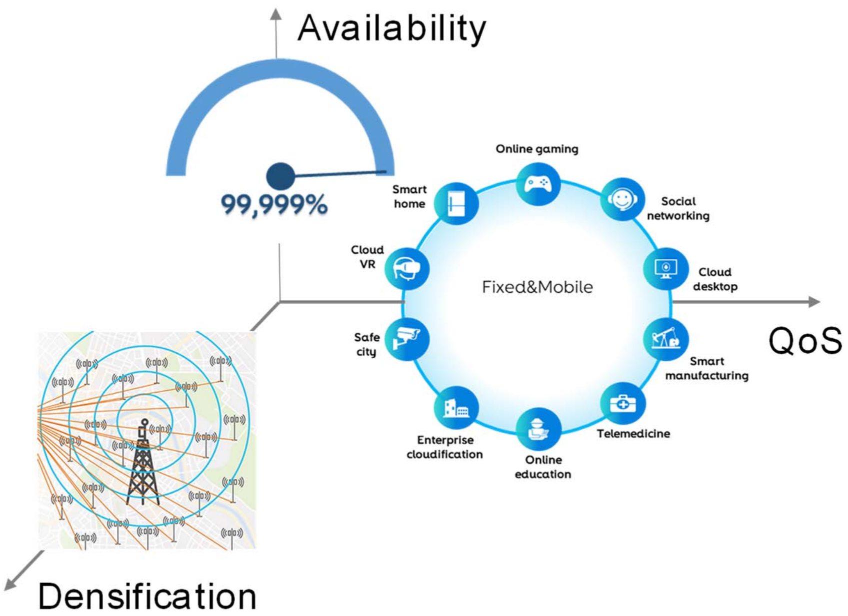


Figure 30: Main features of the multiple access aggregation over PON

1) Network QoS

For QoS, it is essential that as network resource usage increases, there is support-for multiple applications with very diverse requirements (Residential, Enterprise and Mobile Transport). It is necessary to add flexibility and scalability to meet these requirements.

Features such as high data rate, low latency, precise time synchronization and high security are needed as part of the three main 5G classes of service:

- Enhanced Mobile Broadband (eMBB);
- Ultra-Reliable and Low Latency Communications (URLLC); and
- Massive Machine Type Communication (mMTC).

A good example of a QoS challenge is the ultra-high-precision time synchronization, introducing ultra-short frames, carrier aggregation and coordinated multipoint (CoMP) in 5G, to improve time synchronization accuracy by an order of magnitude from ±1,5 µs in 4G to ±130 ns.

2) Network availability

Network availability is related to the level of end to end protection of equipment and paths. For the residential market, protection in the Access Network may not be essential, however, supporting cell sites, or some enterprise services, effective network protection and resilience are mandatory. Auto recovery from failover is mandatory to achieve immediate restoration with 99,999 % availability. Protection may be achieved via a variety of transmission media (e.g. fibre and/or radio). Service protection via PON technology means that OLTs need to support these features in the same or in different equipment, which may imply different paths to the client. This is a good reason for SDN/NFV deployments, as this is the most efficient management of different PON terminations and services requirements on a particular OLT (HW protection/selection) achieving QoS and services assurance independently of the used PON. Protection also means additional fibre connections.

Both Network QoS and Network Availability are features that may be improved by the introduction of SDN/NFV implementations on Fixed Access Networks in the near future. Orchestration will be addressed by a converged view of both Fixed and Mobile. The inclusion of 5G transport in next-generation PON technologies means orchestration will need to be end-to-end in order to support future services and application requirements as shown in Figure 31. Optimized bandwidth and high availability requirements can eventually be achieved by implementing programmable and autonomous channel bonding techniques, enhanced Dynamic Bandwidth Allocation (DBA) and wavelength mobility schemas using SDN and NFV.

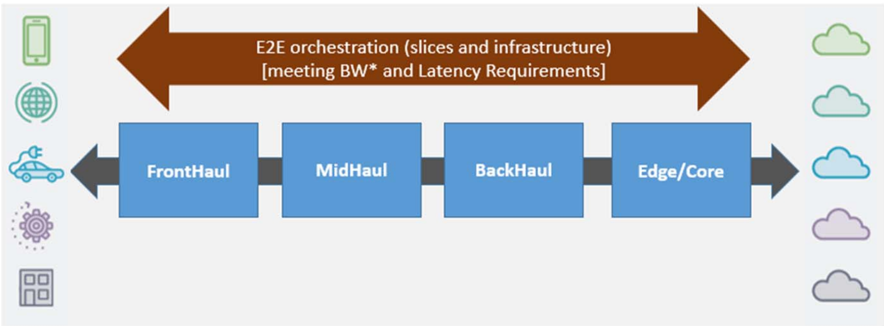


Figure 31: End-to-end Orchestration

3) Network densification

The diverse QoS, availability and large scale Points of Presence needed, affects the way fibre can be deployed. With densification, the PON solution has the advantage to significantly reduce the number of fibre terminations at the Central Office (CO). The higher the splitting ratio is, the smaller is the number of fibres ending at the CO. For example, by using a 1:64 split a reduction of 64 times with respect to the P2P solution is obtained on the number of fibres of the primary cable, the fibre terminations, and in terms of the space occupied and equipment power consumption.

On the other hand, if the data rate is critical, the splitting ratio in a PON solution should not be high (≤ 64). Addressing the densification ratio is a crucial aspect, not only for the data rate, but also the density of ports per equipment and the uplink capacity.

There is no difference between PON and P2P solutions in terms of the transmission delay, 5 µs per km.

The 5G RAN and the expected evolution of the 4G RAN brings additional challenges due to the partitioning of the base station (BBU+RRH) into three parts (CU, DU and RU). These splits simplify the path to RAN virtualization and decrease the fronthaul line's data rates, while meeting latency requirements. A high level representation of this evolution is presented in Figure 32.

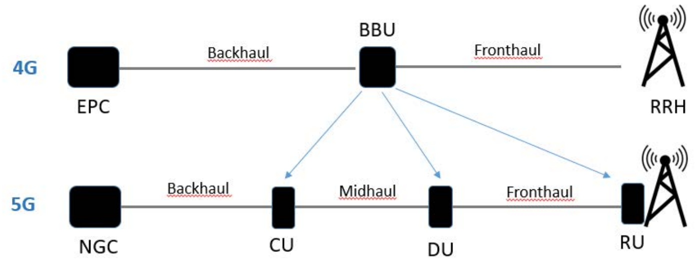


Figure 32: RAN Evolution from 4G to 5G

For this use case, it is crucial to understand the requirements and network architectures of PON networks to support all the B2C and B2B services along with the main 5G transport scenarios, based on different gNB functional splits (defined in 3GPPP TR 38.801 [i.2]):

- Backhaul: connection from the Central Unit (CU) to the Core.
- Midhaul: connection between the Central Unit (CU) and the Distributed Unit (DU).
- Fronthaul: connection from the Distributed Unit (DU) to the Radio Unit (RU).

The different options for gNB modules integration/separation are shown in Figure 33.

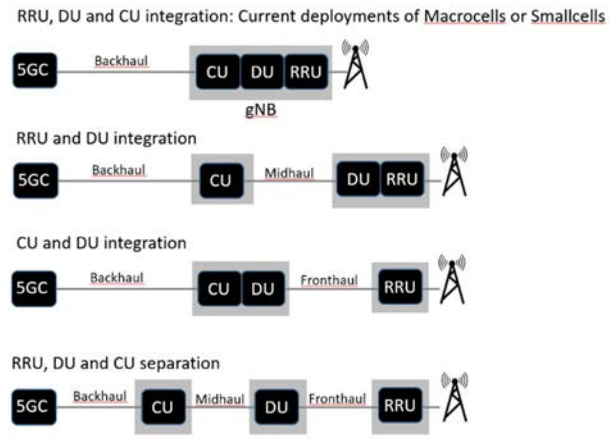


Figure 33: Different options for gNB modules integration/separation

6.8.2.2 Motivation

There are several motivations as follows:

- Fast realization of 5G network construction by reusing the existing ODN.
- Sharing the same ODN between residential clients, business clients and cell sites, reducing the CAPEX.

6.8.2.3 Pre-conditions

In order to define real PON technology requirements, there are several pre-conditions as follows:

- Knowledge of 5G spectrum available per country and per operator.
- Knowledge of 5G roadmap evolution.

6.9 Use case #9: Extend PON to legacy Ethernet Uplink

6.9.1 Use case context

PON has been used in Access Network for many years. There is a move towards deploying PON systems for other scenarios including legacy Ethernet markets, because of its better performance, higher reliability and lower cost. Since different scenarios raise different requirements for a PON system, this use case will give a brief introduction of the extensions of PON to legacy Ethernet markets as well as provide some consideration for new requirements on PON devices.

6.9.2 Description of the use case

6.9.2.1 Overview

6.9.2.1.1 General

PON is now considered a potential candidate for various markets other than typical FTTB/C in the Access area. Compared with legacy solutions in these markets, an optical fibre based passive network introduces benefits such as energy saving, ease of management, multi-service capability, etc. For some of these markets, there is existing equipment, which may have specific and quite simple network requirement. For example, the Ethernet market is now moving to the adoption of optical fibres and PON systems. This may need devices with different requirements compared to those used by the traditional Access markets.

6.9.2.1.2 DSLAMs - Switches - Routers

DSLAM systems are still deployed in the Access Network. With OLT usage increasing in the network, it will be more beneficial to deploy DSLAMs with SFP ONUs. In some outdoor DSLAM applications, there can be a L2 switch to aggregate DSLAMs. DSLAM PON Backhaul solutions enable the use of passive splitters instead of active switches for the aggregation. Usage of passive splitters will reduce power consumptions and will prevent some switch issues such as heat, power cut offs, etc. PON equipment (ONUs, MDUs) and DSLAM backhaul equipment can be separated by using different OLT cards or PON ports. Figure 34 shows the differences between DSLAM Backhaul and current DSLAM.

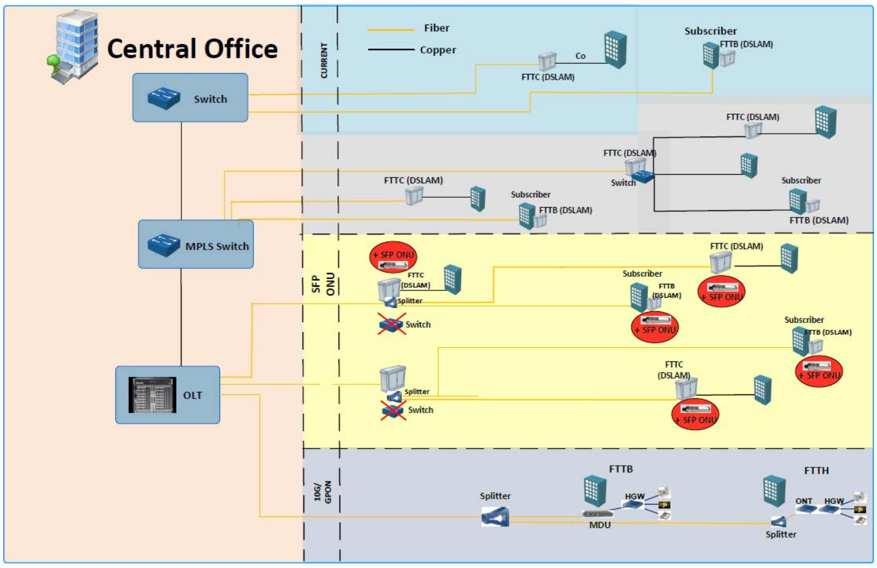


Figure 34: Extend PON to DSLAM Ethernet Uplink

6.9.2.1.3 Wi-Fi® AP backhaul

Wi-Fi® is widely deployed for its network connection convenience. With increasing requirements for network capability, more and more APs will be deployed in premises. Figure 33 shows a multi Wi-Fi® APs backhaul solution migrating from Ethernet switches to PON technology. An OLT will be deployed in the central equipment room to replace the core switch. An embedded ONU with Ethernet interface will be deployed so that existing Wi-Fi® AP devices can still be used. By using PON, the Ethernet switches are replaced by OLTs and optical splitters that will reduce power consumption and cost. In addition all the Wi-Fi® APs are managed and controlled by the OLT as shown in Figure 35.

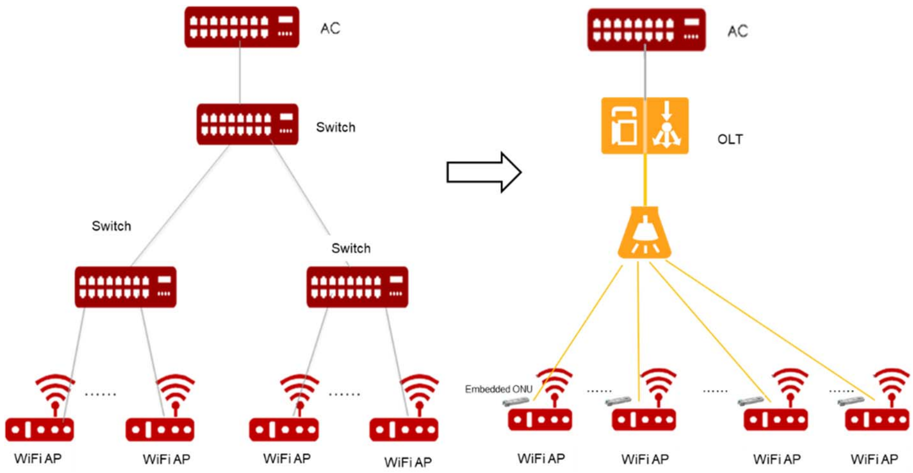


Figure 35: Extend PON to AP Ethernet Uplink

6.9.2.1.4 Video surveillance backhaul

A video surveillance system is used for public security by public and private entities. All video data is aggregated at the surveillance centre. There is a backhaul link from the cameras to the surveillance centre. Currently, the interface from the surveillance camera is Ethernet. In Figure 36, it can be observed that the distance from a camera to the surveillance centre could be greater than 10 km in large cities. The network between the surveillance centre and each camera is a point-to-multi-point topology, which suits PON. In addition, the PON system could support distances of at least 20 km or even up to 40 km. The OLT can support split ratio of 1:128, which is very suitable for deployments involving many cameras. One challenge is that cameras are always installed on top of buildings, poles or roofs, where there is no space for an extra ONU.

Therefore, a modified ONU with more flexibility, smaller size and simpler power supply could be used in this scenario and will not occupy extra space. In addition, an optical/electrical hybrid fibre cable could remotely power the camera and the ONU, wherever a local power supply is unavailable.

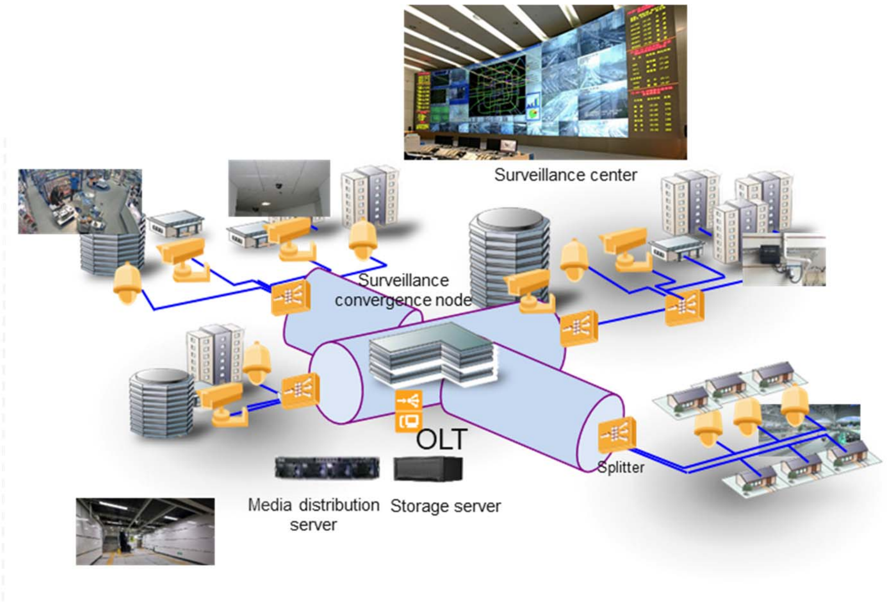


Figure 36: Extend PON to Video surveillance backhaul

6.9.2.1.5 General considerations

For the Access Network, there are several different fibre deployment modes such as FTTH, FTTB and FTTC/Cab, and the types of ONUs are designed and optimized for each different mode. For legacy Ethernet deployments, there are two possibilities when introducing PON:

- Using ONUs to interface Ethernet-based devices to the PON network;
- Using SFP ONUs, when the device has a SFP socket.

Comparatively, Option a) is cheaper but requires more effort to change legacy devices; while Option b) is much more flexible, but is only applicable to devices with SFP socket.

6.9.2.2 Motivation

PON technology is widely used in Access Networks. The technology is mature and the device cost is relatively low. In order to enjoy the benefits of PON technology, a PON system with appropriately modified devices as an Ethernet adaptor is proposed to upgrade the legacy Ethernet deployments.

6.9.2.3 Pre-condition

- Reuse of the existing devices in legacy Ethernet markets

6.10 Use case #10: Scenario based broadband

6.10.1 Use case context

Applications such as on-line gaming, on-line education, and on-line meetings are among the most popular scenarios for residential broadband from the utilization and business opportunity perspective. PON-based Internet leased line for small business subscribers such as small grocery or shops are also considered since they require network capabilities that are similar to those provided to residential high-end broadband users. As illustrated in Figure 37, high value broadband applications are identified by the broadband network equipment to distinguish them from best effort Internet traffic. For those high value applications, dedicated network resources are allocated between the application terminal and the application Cloud to guarantee the optimal user experience. All the network operations are managed by the E2E management plane.

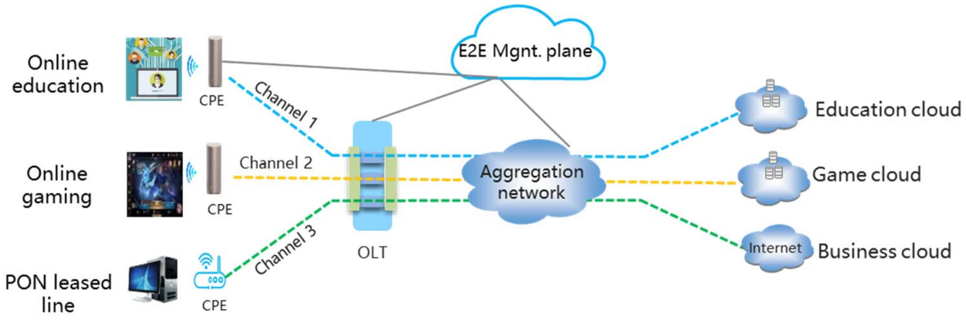


Figure 37: Multiple applications carrying on the network

Broadband network users often experience poor quality service even when the bandwidth is high enough. The bandwidth is only one aspect of a reliable broadband application. Different traffic models generated by different broadband applications and the interaction between the application Cloud and the device have different requirements on the network performance. In order to provide a good quality user experience in addition to high bandwidth, other network characteristics (such as low latency, high reliability) have to be considered and supported. Service quality assurance functions include automatic application identification, application elasticity and adaptation, automatic application quality measurement.

New Internet applications and user devices are frequently connected to the network. The broadband network needs to flexibly and automatically adapt to these changes without manual intervention. The changing user behaviour and the addition of new applications should be detected by the E2E management plane. The E2E management plane needs to take the appropriate actions to guarantee the matching network performance.

In previous network generations, the network behaviour has to be defined and programmed accurately to react to any changes. The accuracy can be managed, but it is not self-managed and not able to handle unpredicted changes. With the technological advancements in Artificial Intelligence, automatic learning capability can be added to the broadband network to implement the automatic network performance adaptation to a variety of broadband application scenarios. That is also the key features of the scenario based broadband use case.

6.10.2 Description of the use case

6.10.2.1 Overview

6.10.2.1.1 General

The scenario based broadband use case is illustrated in Figure 38. The most frequently used broadband applications are education, gaming, media streaming, and best-effort Internet (browsing and Email). Different applications could be identified by the network with its embedded Artificial Intelligence functions so that the application features could be distinguished from each other. The network resources are allocated to the identified high value applications, including the home network segment. To support the flexible changes of the broadband application, the AI learning centre learns the high value applications, which are to be guaranteed.

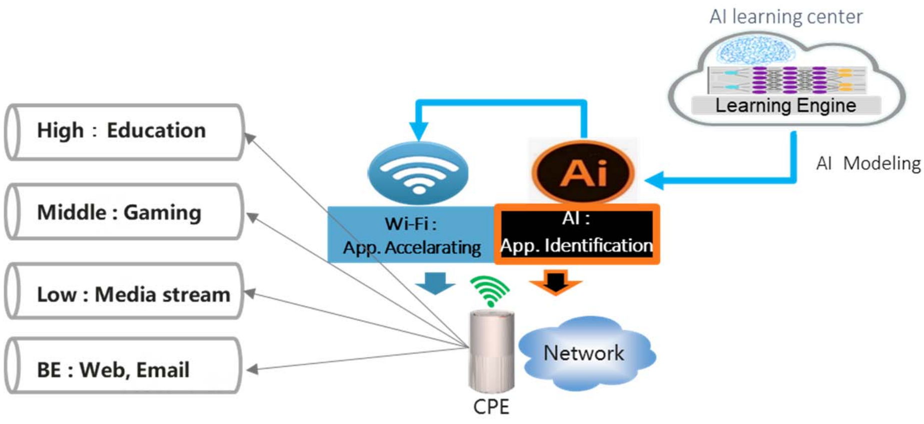


Figure 38: Overview of the scenario based broadband

This use case may be relevant to any possible broadband application when its quality is essential to the end users. Several examples are given here as references.

6.10.2.1.2 Gaming broadband

Gaming is a huge industry with over 2 billion global players. The players are also classified into several types. Around 80 % of them play casual handset games for which the requirements on the network performance is not high. The remaining players can be considered as high-end players. This includes professional players, who rely on high performance PC and network. The live broadcast of the top game is also a popular video service on the Internet. The network architecture for gaming is shown in Figure 39.

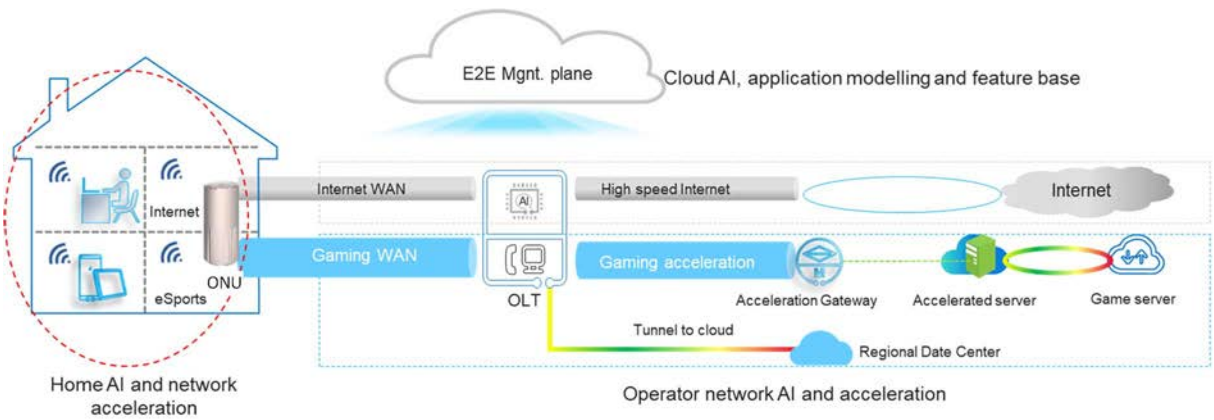


Figure 39: Network architecture for gaming

High-end games need good network performance. Bandwidth is one of the performance factors. The installation software kit of high-end games is usually large and takes in the order of hours to download.

Network latency is even more essential for mobile and PC gaming. The latency impacts to some of the most popular FPS (First-Person Shooters) and MOBA (Multiplayer Online Battle Arena) games are listed in Table 6. Note that the latency numbers listed here refer to the E2E latency from the gaming terminal to the Cloud. For the new generation Cloud games, the latency requirement will be 30 ms or as low as 10 ms E2E.

Table 6: Latency impacts on gaming experience

	Excellent	Good	Medium	Poor
E2E Latency (ms)	0~50	51~90	91~150	> 150
Experience description	Smooth without delay	Normal operation without obvious delay	Capable of playing but with pauses	Frequent pauses, dropping the connection occasionally

Gaming broadband needs the network performance to improve, especially reducing the network latency for guaranteed experience. The traffic model and feature base of popular Internet games are established and are automatically updated by the AI engine embedded in the home network and the operator network and are stored in the operator's E2E management plane. Key network components receive the data policy from the E2E management plane to setup a network slice for the identified gaming traffic to implement acceleration. A dedicated transport channel or an acceleration device could be deployed in the network. The channel or the device's scheduling function is controlled by the E2E management plane. The status of the gaming broadband is visible and managed by the E2E management plane.

6.10.2.1.3 Education broadband

On-line education is another important home broadband service. MOOCs (Massive Open Online Course) are launched by top universities and educational institutes globally. On-line education is also changing from video record to live video, from unidirectional video broadcast to interactive multi-media, from high definition video to 4K UHD video and Virtual Reality. On-line education was considered supplementary to the traditional school education. It is gradually changing into one of the main stream methods similar to classroom education.

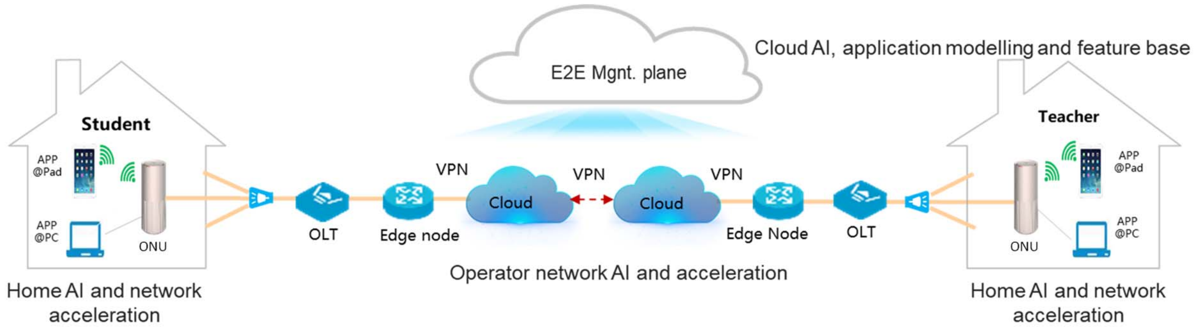


Figure 40: Network architecture of the on-line education

The end to end education broadband network is shown in Figure 40. The teacher may be located quite far away from the student, sometime abroad or even in another continent. The bandwidth requirement of the existing education application is not extremely high, depends on the video resolution it makes use of and will tend to increase in the future. In this case, network latency and packet loss are the critical parameters.

The traffic model and feature base of the popular education applications are established and automatically updated by the AI engine embedded in the home network and the operator network and is stored in the E2E operator's management plane. The key network component receives the data policy from the E2E management plane to setup a network slice for an identified education application to implement acceleration. The status of the education broadband is visible and managed by the E2E management plane.

6.10.2.1.4 Home office broadband

A high quality broadband network provides people with more flexibility to work from home. They may get connection to their Intranet with VPN software, join on-line meeting, share screen or have a white-board discussion with their colleague at the other corner of the world. The home network performance is normally not as good as an office network especially for an employee of a big enterprise. Table 7 shows the performance requirement of a typical on-line meeting software.

Table 7: Performance requirement for online meetings

	Excellent	Good	Poor
Latency (ms)	< 100 ms	< 150 ms	> 200 ms
Jitter (ms)	< 30 ms	< 50 ms	> 50 ms
Packet loss	< 3 %	< 5 %	> 5 %

The home office broadband network is shown in Figure 41. The home office user starts the Intranet VPN or other office software from the PC or other terminals and connects to the business Cloud. The traffic model and feature base of the popular home office applications of enterprise VPN software are established and are automatically updated by the AI engine embedded in the home network and the operator network and stored in the operator's E2E management plane. The key network component receives the data policy from the E2E management plane to setup a network slice for an identified home office application to implement acceleration. The status of the home office broadband is visible and managed by the E2E management plane.

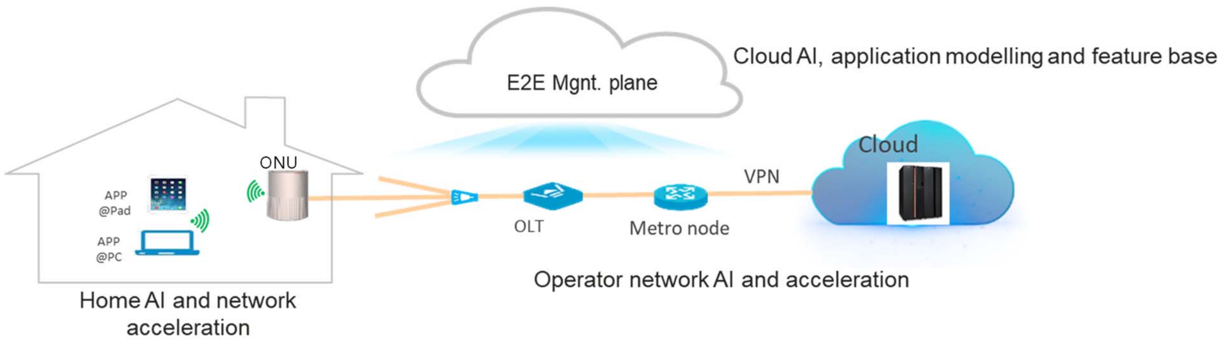


Figure 41: Network architecture of the on-line meeting

6.10.2.1.5 PON leased line

A Business leased line is used by small and medium enterprise customers, such as small shops and branch offices, etc., as shown in Figure 42. There are two kinds of broadband services needed, Internet leased line and business leased line. Normally the business leased line is a higher SLA demanding service in terms of bandwidth, latency, stability and reliability. QoS guaranteed business leased lines are getting more important when more business applications are deployed on the Cloud, including the public Cloud, operators' Cloud and the private enterprise Cloud. The connection SLA is of high concern to the business user, network operators and Cloud service providers. Different connection technologies could be used here for different SLA, including network slicing, VPN, SD-WAN, OTN or direct physical connection. The capability and the reliability of the customer premise network differ a lot from the residential broadband, with large capacity Access, network redundancy, self-management, etc.

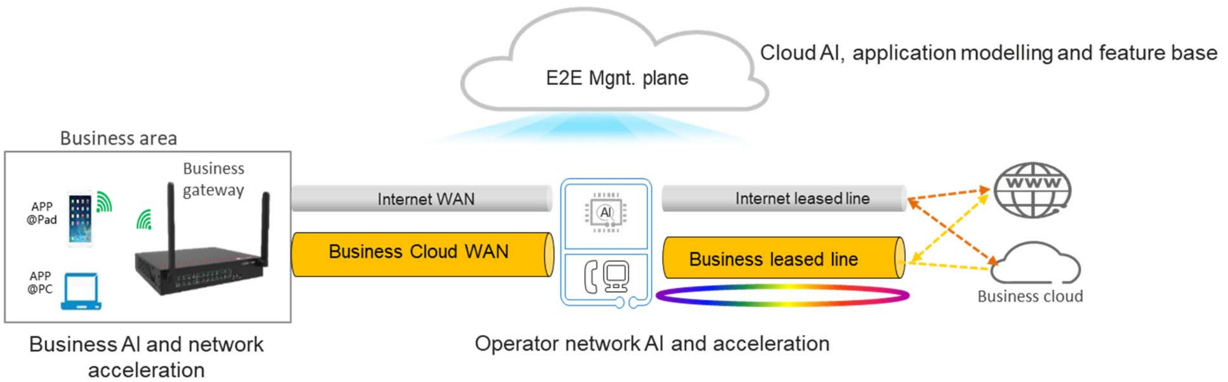


Figure 42: Network architecture of the PON leased line

The traffic model and feature base of the business applications or enterprise VPN software are established and are automatically updated by the AI engine embedded in the customer premise network and the operator network and is stored at the operator's E2E management plane. Key network components receive the data policy from the E2E management plane to setup the leased line to the service Cloud for an identified application to implement acceleration. The status of the PON leased line is visible and managed by the E2E management plane.

6.10.2.2 Motivation

The bandwidth has been increasing over past decades, reaching Gigabits level in F5G. The high bandwidth does not mean good service quality and application experience. It is quite often that the user experience is not satisfied even when the network is lightly loaded. One of the key reasons is that all the Internet applications are in general treated nearly the same as the so called HSI (High Speed Internet) services and transported similarly on the broadband network. It prevents the network operator from improving their service level to broadband users. The applications and user behaviours have to be considered and differentiated to provide the adequate network services and solutions. That leads to the scenario based broadband use case, which supports multiple application scenarios.

New applications, changes in user behaviour and the Internet evolution are the primary reason for this use case. Scenario based broadband needs the network to be a self-managed to keep up with the application development.

6.10.2.3 Pre-conditions

- The network equipment is designed with scenario-based broadband in mind.
- The network resources are sufficient especially for the high demanding application SLA.

6.11 Use case #11: Enhanced traffic monitoring and network control in Intelligent Access Network

6.11.1 Use case context

In traditional Access Networks, network operators normally have traffic monitoring data collection capability in the order of minutes (for example, a typical traffic monitoring data collection cycle is 15 minutes), designed for routine network maintenance. However, it is hard to monitor traffic in the order of seconds to satisfy the operation of new services such as Cloud VR. For instance, when the end user suffers poor service experience due to unexpected traffic congestion of tens of seconds, it is hard for the operator to detect what really happened in its network. This is due to the coarse granularity of the traffic monitoring data collection, which could fail to detect traffic bursts within the monitoring period. It is insufficient to use the estimated traffic status, which will lead to missed traffic anomalies. Figure 43 illustrates actual traffic versus a perceived flattened view due to the coarse granularity monitoring.

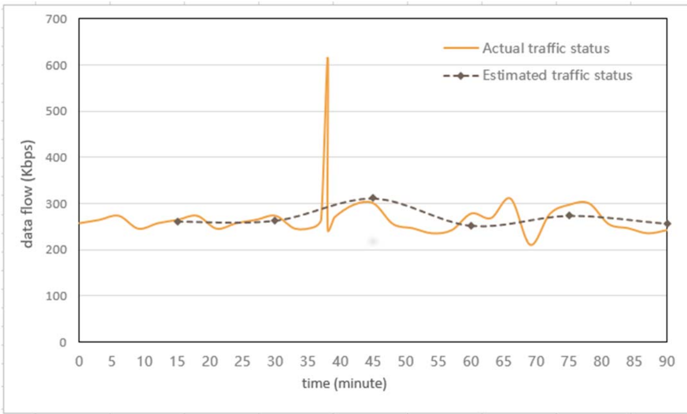


Figure 43: Example diagram of micro traffic burst

Intelligent and services logic-oriented control and management of Access Network should be employed to improve the granularity of network monitoring and simplify network operation.

6.11.2 Description of the use case

6.11.2.1 Overview

Data collection in the order of seconds can improve traffic monitoring capabilities. One example for enhanced traffic monitoring and network control for intelligent Access Network is illustrated in Figure 44. Several functions are included in the management layer, such as Access Network data collection used by the Access Network management system and OLT control.

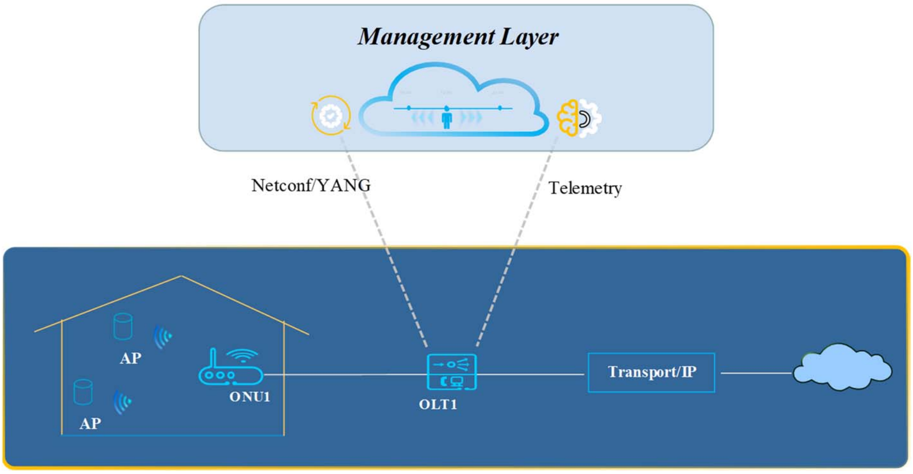


Figure 44: Example of enhanced traffic monitoring and network control for intelligent Access network

In general, an Access Network is deployed for FTTH. It can be extended by cascading the Access Network (tier 1 PON) and the customer premises network (tier 2 PON). Cascaded PON achieves better traffic monitoring, operation, and maintenance capability as shown in Figure 45. The management layer for cascaded PON provides comprehensive support to the tier 2 cascaded PON. One example is the automatic setup of the tier 2 PON. Collected traffic characteristics can help to fine-tune the network parameters. The tier 2 PON ONUs can be configured according to different customer profile. In home networks, for example, traffic flows in the bedroom might need to support video streaming, while the living room ONU might need to offer Cloud gaming VR capabilities. In the case of cascaded PON, end-to-end orchestration enables the control and management of the customer premises network.

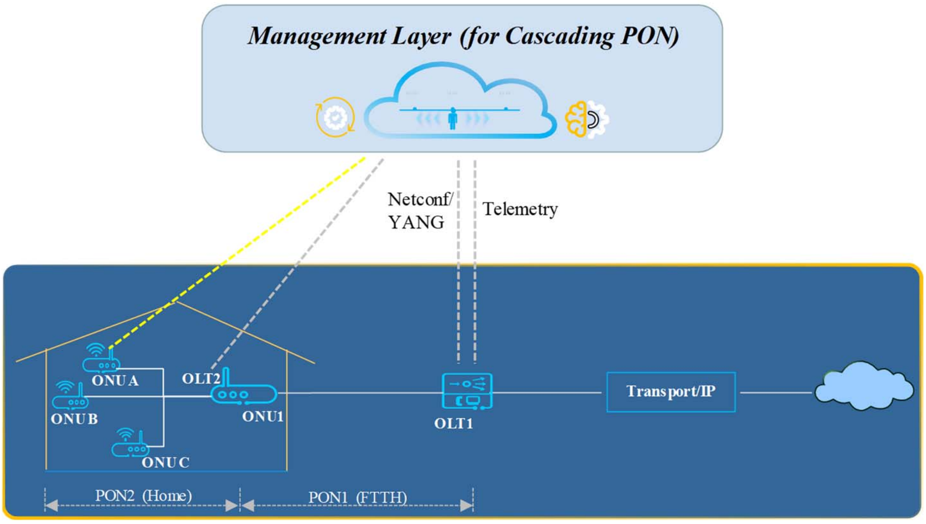


Figure 45: Example of enhanced traffic monitoring and network control for cascading PON

NOTE: Use Case #4 on FTTR is very similar to this scenario, and the monitoring aspects of this use case would also apply.

The expected technical features of the Access Network in this use case are listed below:

1) Telemetry: real-time, end-to-end, and precise traffic monitoring data collection.

2) Big data analytics: traffic monitoring data analysis and processing, with network status visualization.

3) Machine learning: transform the network orchestration from a static encoding to a data-driven dynamic machine learning algorithm, to realize the network automation. This includes analysis, prediction, network configuration, and achieving closed loop control and dynamic resources allocation.

4) Access Network abstraction and automatic network configuration enabled by SDN technologies such as YANG model, Netconf, etc.

6.11.2.2 Motivation

There are several motivations as follows:

- Improve the service experience.
- Improve operation and maintenance, and reduce OPEX.

6.11.2.3 Pre-conditions

There are the following pre-conditions:

- SDN technologies and interfaces need to be supported by the OLT.
- Telemetry interface and model need to be supported by the OLT.

6.11.2.4 Operational flow of actions

Flow chart is shown in Figure 46.

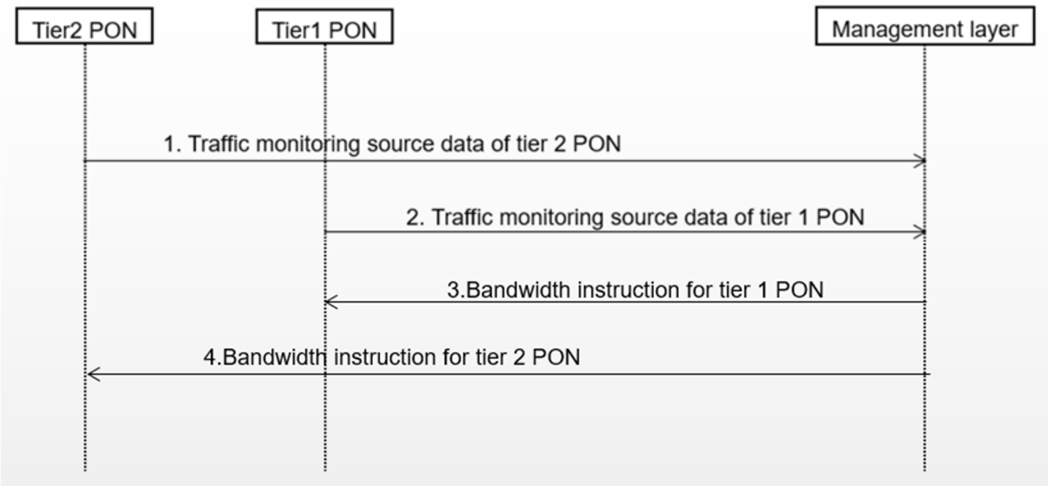


Figure 46: Operational flow of bandwidth dynamic adjustment in Intelligent Access Network

1) The Tier 2 PON reports traffic monitoring source data (e.g. the number of received/transmitted bytes, packets, error packets, etc. corresponding to a given monitoring object such as Wi-Fi® Port or specific VLANs containing high priority services) to Management layer.

2) The Tier 1 PON reports traffic monitoring source data (e.g. the number of received/transmitted bytes, packets, error packets, etc. corresponding to a given monitoring object such as OLT uplink interface, OLT PON Port, or specific VLANs containing high priority services) to Management layer based on telemetry technology.

3) The management layer processes and analyses the source data, and iteratively trains the dynamic bandwidth model by the machine learning algorithm. It updates the configuration of the Tier 1 PON based on the monitored traffic status of both Tier 1 and Tier 2, and provides traffic control strategy for each network.

4) The management layer processes and analyses the source data, and iteratively trains the dynamic bandwidth model by machine learning algorithm. It updates the configuration of the Tier 2 PON based on the monitored traffic status of both Tier 1 and Tier 2, and provides traffic control strategy for each network.

6.12 Use case #12: On Demand High Quality Transport for Real time applications

6.12.1 Use case context

Real-time applications increase network requirements with respect to latency/drop ratios in the network. This performance cannot be deterministically reached on a shared resource, where communication are concurrent. In fact, simultaneous communications will create some packet jitter and unavailability of resource for short periods of time. It will also create a delay in the real-time communication, which will lead to deteriorated consumer experience. The goal of F5G network will be to support these applications.

6.12.2 Description of the use case

6.12.2.1 Overview

This use case describes how an End-user high quality communication is managed. This communication could be used for Cloud VR as an example.

Depending on the application two scenarios can occur as shown in Figure 47:

- In the first scenario, the applications has knowledge of the network performance requirement to deliver the expected quality of experience. The application will inform the network about this network performance requirement, and the network will reserve pro-actively the necessary resources and will implement the appropriate configurations.
- In the second scenario, the application is unaware of the network requirement. The application will detect poor quality during the communication process and will inform the network. The network reacts e.g. by reserving some dedicated communication resources. The application will also have the possibility to inform the network when the quality of the communication has reached the expected level.

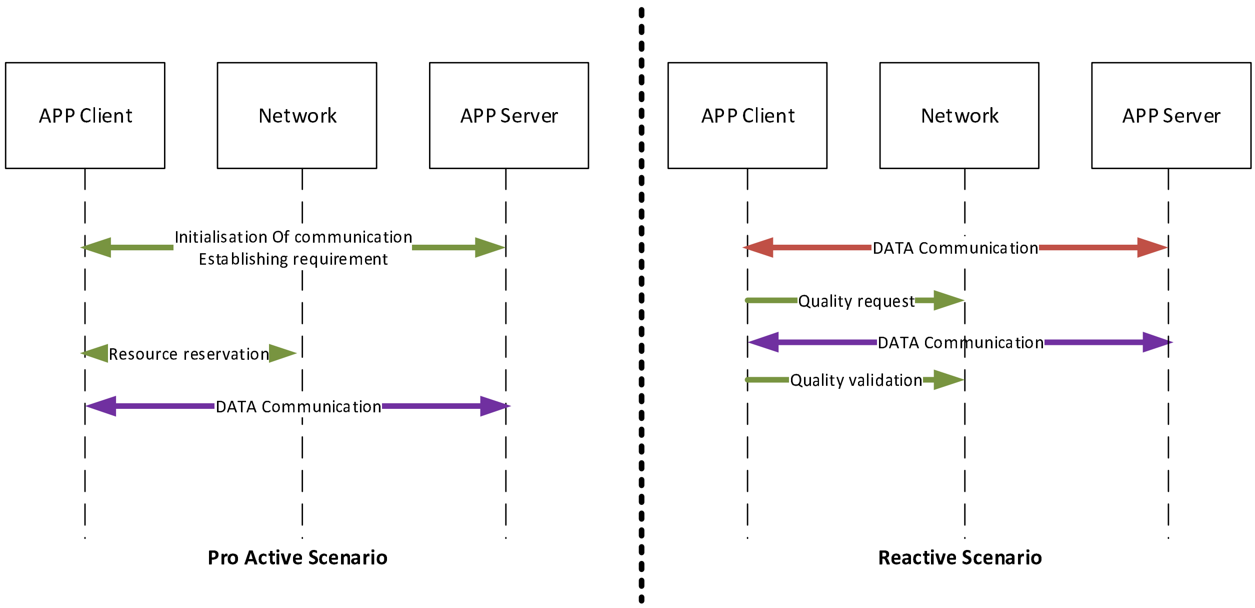


Figure 47: Dedicate Resource scenarios

Figure 48 gives an example based on communication established by Cloud VR Application using pro-active resource allocation mechanisms.

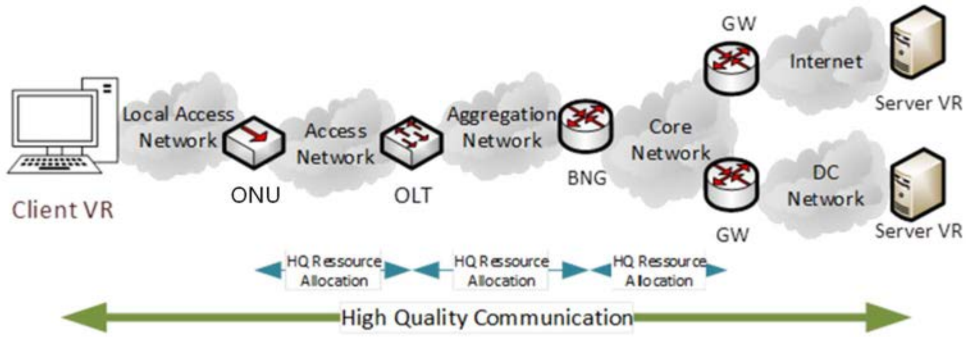


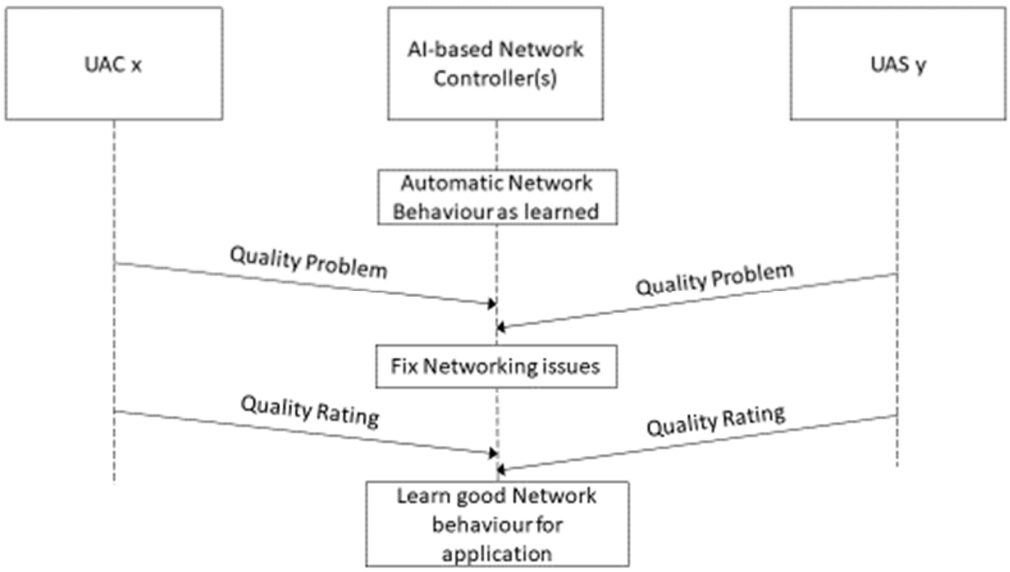
Figure 48: Initialization of dedicated transport channel for Cloud VR

During the initialization of the communication between application server and the application client, the application client will request a high-quality communication. This request will be granted, based on policies and depending on the service agreement, segment by segment in the network. The network will support the requested communication, for example, it will allocate dedicated resources for the data flow of the application and make appropriate routing decisions. Alternatively, the network starts monitoring this flow and reacts to detected performance degradation.

At the end of the communication between the client and the server, the network will clean up and roll-back the changes, for example, dedicated resources will be released.

Regarding security, the network could limit the number of reservations as well as quantity, duration, etc.

Figure 49 gives an example of a reactive scenario using an AI-based network controller and reactive network quality improvements.



NOTE: This is an example of the use of the reactive network controller mechanism based on AI.

Figure 49: Example reactive scenario

This scenario is targeting cases, where the application developers do not exactly know what the network behaviour should be for their applications. This is the case, because it is difficult to have an analytical way of deriving network performance requirements, or because it is subjective to the end-consumers, whether the application performance is perceived as good. In this use case, one or more network controllers based on AI algorithms are considered. These are based on specific knowledge of the application and its protocols, and on past experience and behaviours learned in the model training phase. Basically, the network is operated automatically based on that knowledge.

When the User Application Client (UAC x) or User Application Server (UAS y) detect quality problems at the application layer or through end-user interaction, the network controller is notified. The network controller in turn will perform the needed actions to restore the desired quality. Also, both the client and the server can notify a quality rating, such that the network controller can learn about the particular application performance expectations. The notification can also be sent upon an end-user trigger.

This approach might not be applicable to applications with very high-performance requirements and mission critical applications, since those require deterministic network performance, which are a priori known and managed by the controller.

6.12.2.2 Motivation

This functionality introduces a great improvement compared to the previous generation of networks. The previous generation of services were limited to best effort communication without any possibility to improve the quality of a communication based on its needs. This feature will give the opportunity for over the top applications to use high quality data communication.

6.12.2.3 Pre-conditions

- The network has the capability to change its settings so that the requests for certain level of network performance can be granted.
- The Client/Server application has the capability to communicate its communication requirements to the network controller.
- The Client/Server application has the capability to communicate the poor quality of experience to the network controller.

6.13 Use case #13: Remote Attestation for Secured Network Elements

6.13.1 Use case context

Device security has been very important for previous generations of fixed networks, and is even more important for F5G. One of the essential aspects of F5G network security is to ensure that the network devices deployed in the network are operated with trusted software. An OLT will be used as an example in this description. In this use case, a Remote Attestation (RA) mechanism enables the OLT to prove the integrity of its software to the Network Management System (NMS) on demand. The remote attestation mechanism and two security features based on this mechanism are introduced in this use case.

6.13.2 Description of the use case

6.13.2.1 Overview

A cyber-attack is usually initiated via software tampering. A hacker could tamper with the boot code or hijack a process and modify its binary code or data at runtime. Such malicious modifications will destroy the software integrity of the device and therefore put the whole network at risk. The goal of remote attestation is to allow for a network device to prove its integrity status to the challenger that is concerned with the integrity of this device.

Remote attestation plays a critical role in device integrity measurement. The two best practices for remote attestation are measured boot (verification of boot code at start-up time) and Dynamic Integrity Measurement (DIM, verification of code running).

Figure 50 shows the network architecture and the deployment position of RA client and RA server.

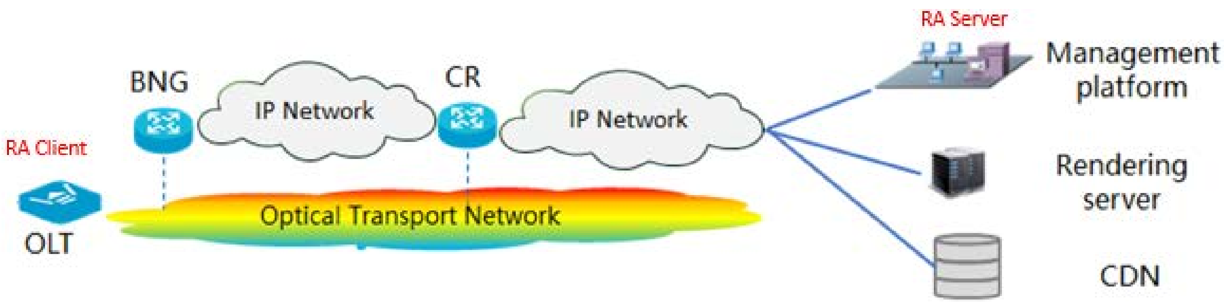


Figure 50: Remote Attestation Network Architecture

Figure 51 introduces the process of measured booting with remote attestation applied.

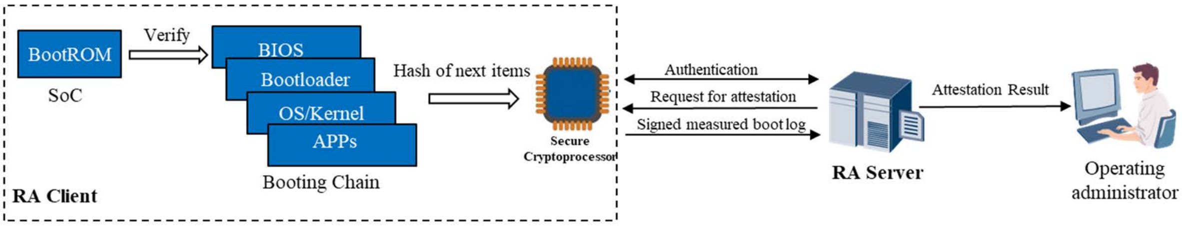


Figure 51: Measured Boot with Remote Attestation

As depicted in Figure 51, in a measured boot attestation the RA client computes and stores the hash value of the boot code at each phase to a secure cryptoprocessor. For instance a Trusted Platform Module (TPM) is designed to carry out cryptographic operations and keep the confidentiality of sensitive data. The stored value as well as boot log is signed and returned to the challenger as a response to the request. After comparing with the baseline, the RA server determines the integrity of the boot code of the device.

DIM (Dynamic Integrity Measurement) is another approach to check the software integrity at device run time. Figure 52 shows the DIM process with remote attestation to determine the integrity of the running programs.

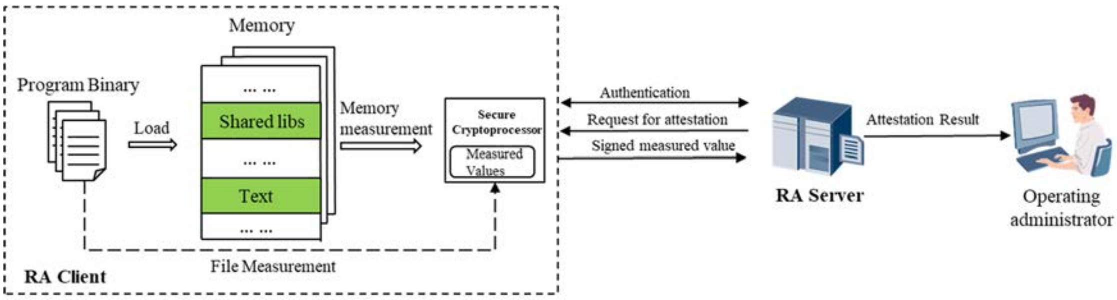


Figure 52: DIM With Remote Attestation

The RA Client audits the program binary files and memory segments for each process and computes and stores the hash values in the secure cryptoprocessor. The result will be returned upon the request from a RA Server. By comparing the baseline values with the hash value received, the RA server can determine whether the programs running on the RA client has been tampered with.

6.13.2.2 Motivation

The implementation of remote attestation benefits the whole network by:

- Maintaining the integrity status of network devices. With measured boot and remote attestation, devices with tampered software can be detected and software recovery or an isolation processes will be triggered.
- With remote attestation, the efficiency of network device management is improved.
- With remote attestation, the network administrator has a better view of the integrity status of each device in the network.

6.13.2.3 Pre-conditions

The secure processing of remote attestation is based on the following pre-conditions:

- The RA client and RA server have been deployed in the network devices.
- Secure cryptoprocessor technology is used on the RA client to keep the confidentiality and integrity of the measured values.
- The system resource baseline value should be calculated and stored on the RA server in advance.

6.13.2.4 Operational flow of actions

Figure 53 introduces the operational flows of remote attestation in the case of a tampered client. The deployment location of RA server and client can be dynamically changed as needed. In this example case, the RA client is deployed on the OLT and the RA server is deployed in the NMS.

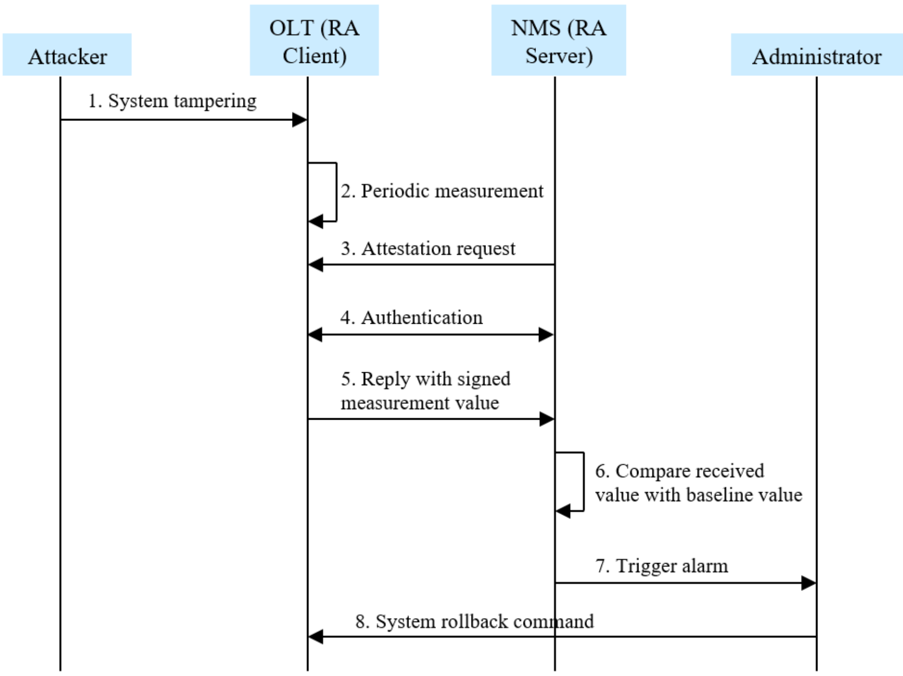


Figure 53: Operational flow of remote attestation

1) At any time, the attacker hacks the OLT and tampers with the system (software, data, file, etc.).
2) The OLT periodically calculate the hash of the system software and stores the encrypted result in the secure cryptoprocessor.
3) The NMS sends the attestation request to the OLT for integrity checking.
4) The OLT and NMS initiate a mutual authentication.
5) Once the mutual authentication passed, the OLT will send the signed measurement value to the NMS.
6) The NMS compares the received signed measurement value with the baseline value.
7) The values will not match, therefore the NMS will alert the administrator that the device might be invaded or tampered with.
8) The administrator can conduct a rollback command to the OLT to recover the system.

6.14 Use case #14: Digitalized ODN/FTTX

6.14.1 Use case context

Traditional ODN deployment has several critical factor, such as the time required, inaccurate port and usage data, inefficient service provisioning. Therefore, in order to deploy fibre to everywhere, the ODN needs to allow for fast deployment and accurate and efficient resource management.

6.14.2 Description of the use case

6.14.2.1 Overview

Currently paper and plastic labels are used on ODN network components. However, they cannot be updated in a timely manner. They are exposed to high temperature and high humidity during their life time, which means they can easily fall off or be damaged. Furthermore, in the ODN deployment phase, a large number of technicians are required to record resource data. Manual asset recording and tracking are inefficient as well as error-prone. Data can neither be verified nor updated in a timely manner, which causes database errors. The ripple effect of inaccurate resources information causes low service provisioning success rate, difficulties in locating faults, etc. In addition, when the subscription is terminated, the Fibre Access Terminal (FAT) will not normally be disconnected after the ONU is removed. For example, as shown in Figure 54, after some users have cancelled their subscription, their in-door fibre stays connected in the FAT. As a consequence, the port usage status is not updated, which might result in unavailable ports due to inaccurate resource records. In the service provisioning phase, it is difficult to find vacant ports, causing multiple site visits and long service provisioning time.

Figure 54: The challenges of paper labels

Ensuring accurate identification and recoding of ODN resources is critical. The digital ODN and intelligent information management makes ODN resources more visible and manageable in the network deployment and service provisioning phase. In this way, ODN resources can be managed more accurately and used more efficiently (see Figure 55).

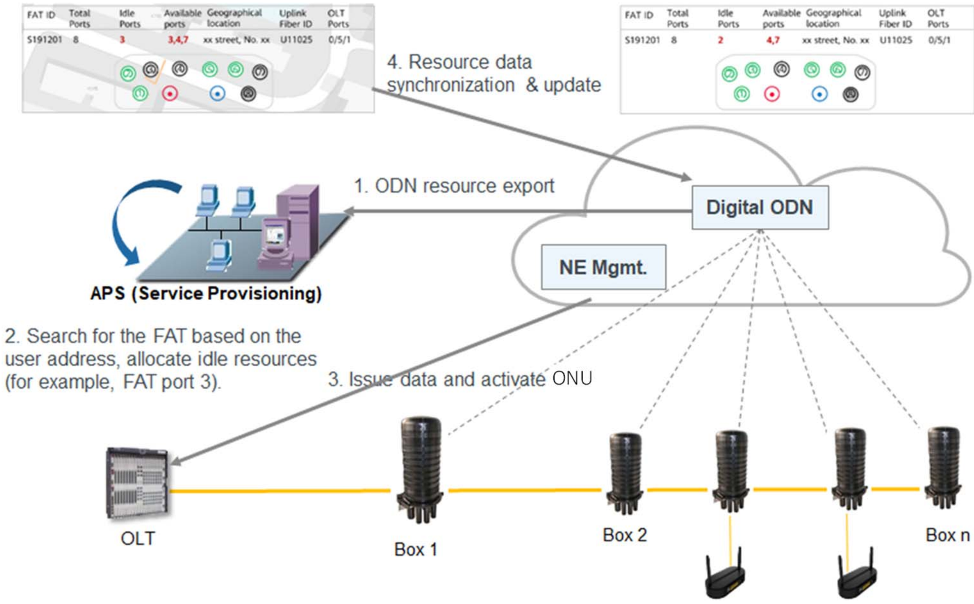


Figure 55: Digitalized ODN enables automatic service provisioning and accurate resource management

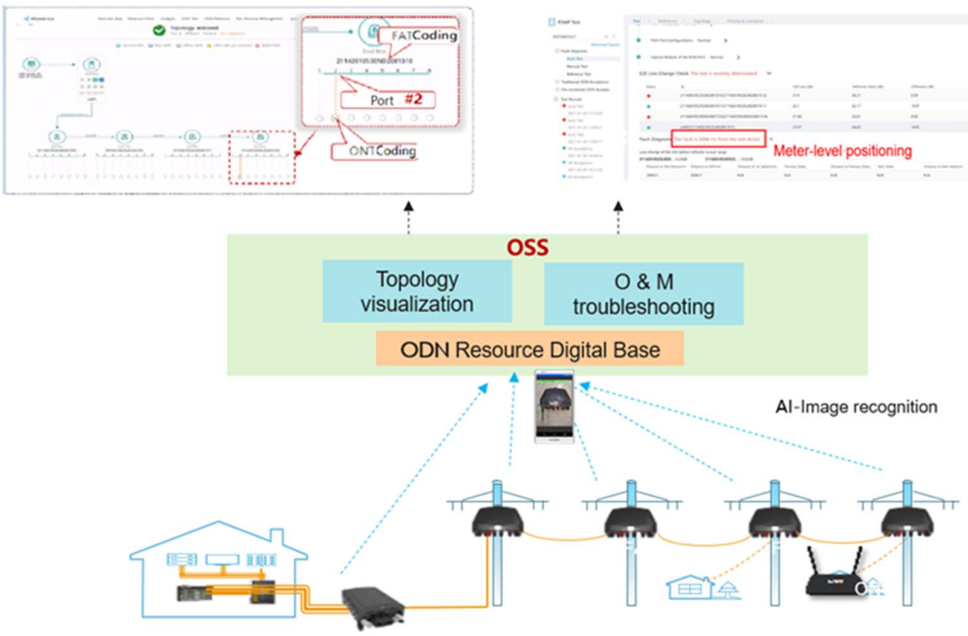


Figure 56: Intelligent Management of ODN

In some cases, such as in smart cities or vertical industries, the fibre resource management (such as resource database entry recording and retrieval) need to be handled by skilful qualified ODN technicians, which are scarce and costly. Digital ODN supports real time resource recording and database update, port status monitoring, automatic resource allocation and automatic service provisioning. Therefore, the efficient utilization and management of the fibre resources and its management can be greatly improved, see Figure 56.

6.14.2.2 Motivation

- Digitalized and intelligent identification of ODN labels, achieving 100 % accurate resource recording and digital management, enable automatic service provision.
- Provides real-time visualization of ODN topology and resource management.

- Digitized ODN deployment provides fast (in the order of minute-level and within meter-level) remote fault localisation and easy maintenance.
- Remote and automatic measurement and analysis of the attenuation, analyses of events, and fault localisation of fibre links can be done at the CO site.

6.14.2.3 Pre-conditions

- Digital labels of ODN components, including the optical cable, FAT, connectors, etc. are inserted in the factory (including the FATs of optical splitter digital labels).
- The technician carry an intelligent portable device with the positioning function (e.g. GPS).
- The operator has complete network planning and user information.

6.14.2.4 ODN deployment operation flow

1) O&M personnel use optical cables and appropriate components with digital labels to quickly complete the network infrastructure deployment based on the network plan.
2) O&M personnel after the installation is complete, scan the digital label on site to identify the product and upload the location information.
3) The Network Management System automatically identifies and displays the ODN topology based on the uploaded location information.
4) The Network Management System provisions services and displays fibre resource usage.
5) The Network Management System perform automatic verification based on the automatically identified topology information and the planned information.

7 Description of use cases, Release 2

7.1 Use case #15: XR-based Virtual Presence

7.1.1 Use case context

Virtual presence can be defined as a virtual media application that provides the experience of someone being present. Telephony is in that sense a rudimentary form of virtual presence. Here extended Reality (XR) based virtual presence will be discussed, a more immersive method for implementing virtual presence, as another step towards further removing the barriers of distance.

XR is comprised of Virtual, Augmented, and Mixed Reality. In all cases, users wear some type of Head-Mounted-Display (HMD) which provides the user with a surround view of some virtual elements. In Virtual Reality, the entire environment is virtual, whereas in AR and MR, parts of the environment may correspond to the (local) real world.

Recent developments in XR rendering technology, such as, spatial tracking and video conferencing have inspired the field of social XR. In current market applications (such as VRChat™, AltspaceVR™, BigRoomVR™, Facebook Spaces™ and Mozilla Hubs™), users are placed in virtual rooms with other users, where they can interact and share experiences. The added immersion provided by XR allows users to experience a greater degree of freedom and feeling of being together. This use case considers virtual presence, an effort to optimize the feeling of being together in the same virtual space.

In the aforementioned systems, users are typically represented as 3D avatars (with varying degrees of closeness to reality). However, an improved virtual presence can be achieved by using photorealistic representations of users instead. Given the developments in the capturing, compression and transmission of point-clouds and other 3D representation formats this is starting to become technically feasible. However, similar to the Cloud VR rendering use case, the streaming of photorealistic avatars for virtual presence places high demands on the network performance.

This use case provides a brief introduction to Virtual Presence applications and the required capabilities for the F5G networks.

7.1.2 Description of the use case

7.1.2.1 Overview

With virtual presence, users are consuming immersive content while also simultaneously producing immersive content of their own. For instance, in photo-realistic social XR, users are captured by a number of depth-enabled cameras (such as the Microsoft Azure Kinect™ or Intel RealSense models™). Depending on the capabilities of the end-user devices, the captured content is further processed and prepared for streaming in the mobile edge, in the network or in the cloud, as shown in Figure 57.

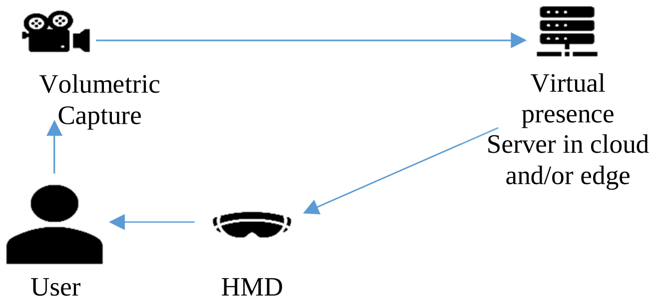


Figure 57: Schematic high level overview of components from one of the end users to virtual presence server

In the ideal case, users receive photorealistic representations of each other in a timely fashion, allowing for realistic communication and a high degree of immersion and presence. More elaborate scenarios involve streaming low-latency haptic and locomotion (body motion) inputs and feedback for remote operation of devices.

A lot of computation and optimization are required to implement high-end virtual presence services. To avoid the use of specialized and/or expensive hardware in the user equipment, some computation and hardware can be implemented in a central location, where this can be used more efficiently by sharing it among several users.

Furthermore, a centralized architecture allows the optimization of bandwidth by forwarding streams (e.g. a selective forwarding unit) or by assembling and compressing multiple inputs (a Multipoint control unit). Moreover, the latter enables more efficient use of client-side decoder hardware. Such architectures place requirements on both the uplink as well as the downlink (see Figure 58).

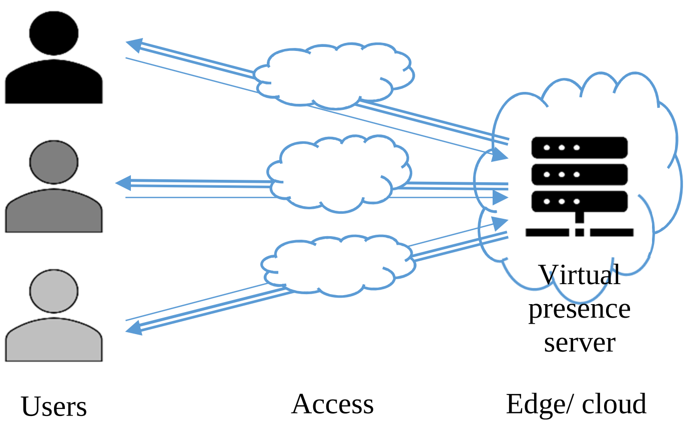


Figure 58: Schematic high level overview of the bi-directional nature of virtual presence services

In general, rendering on a HMD is performed at 90 Hz for high-end devices and 60 Hz for low-end devices. This entails refresh rates of ~11 ms and ~16 ms respectively. From the rendering side, these rates determine the maximum time available for generating a frame, given that other motion-to-photon latency compensation measures are in place on the client-side.

Contemporary volumetric media formats are comprised of meshes and point clouds, and in the future lightfields may become more commonplace for Six Degrees of Freedom (6DoF) content. Volumetric media formats typically require more data to be transmitted compared to regular video. For instance, the current figures for MPEG's point cloud encoding, such as Video codec based Point Cloud Compression (V-PCC), are in the ballpark of 15 Mbit/s-40 Mbit/s. Figures for Red Green Blue Depth (RGBD) compression are in a similar order of magnitude with rates up to 60 Mbit/s.

A multi-user setup will require bitrates of multiples of the values indicated above. Note that these bitrates may be asymmetric for the up-/downlink depending on the ability of the clients and the server to make use of the available bandwidth to increase quality and/or reduce compression latency. Moreover, the server may be able to enhance compression by combining inputs into a single compressed output stream.

Current encoding techniques typically allow some fine-tuning that enables a trade-off between lower latency and compression efficiency. However, these techniques currently do not yet achieve the desired motion-to-photon latency. On the other hand, not applying compression at all requires multiple Gbit/s per depth camera stream.

NOTE: Depth cameras are able to provide a depth map, which provides the distance information between points on an object's surface and the camera. Some cameras are also able to provide a synchronized RGB image along with a depth map.

At the time of writing, the bandwidth and latency constraints in the current Access Networks are input to the requirements of newly developed media codecs. By improving the network characteristics F5G is an enabler for virtual presence technology.

For general social interaction, volumetric video delays can be similar to video conferencing (<150 ms). However, for increased immersiveness, much lower latencies are required in the order of <10 ms. For example, lower latency is needed to enable a natural experience in a virtual shared environment either by manipulating objects (such as handing over a virtual pencil) or high-fiving other users. The XR user experience depends on receiving an appropriate haptic feedback.

7.1.2.2 Motivation

Tools and platforms that enable remote communication and collaboration provide a strong contribution to societal challenges. Virtual meetings and conferencing, in particular, can help to reduce commutes and to lower our ecological footprint. In case physical presence is not feasible or desirable, then a virtual meeting can offer a possible solution.

Studies show that current remote collaboration tools have their limitations. With video calling apps, most of the body language is lost and the word "zoom fatigue" has entered daily language. Social XR aims to solve these issues and, in addition, offer a true feeling of being together. This promises to be useful in a variety of applications such as remote collaboration, online meetings, hybrid meetings, and social interaction in a private or professional context.

By addressing bitrate and latency requirements posed by virtual presence platforms, F5G networks can accelerate the development of mature and widespread virtual presence applications.

Video-conferencing businesses can be upgraded to the next level by integrating XR components and photo-realistic streaming into their systems. Telecom operators can provide either the virtual presence business with their service platforms or they can offer network bandwidth and latencies required for virtual presence to end-users and B2B clients.

7.2 Use case #16: Enterprise private line connectivity to multiple Clouds

7.2.1 Use case context

Enterprise customers have stringent requirements on the performance of their private line connectivity to the Cloud, such as high security, high bandwidth, low latency, and high availability. The enterprise migration to the Cloud is accelerating, and enterprises require multiple Cloud services to meet different service requirements. Disaster recovery and backup is essential to ensure high service availability. This use case describes the application scenario of high quality enterprise private line access to multiple Clouds. In the following diagrams, the carrier network can be considered as an Enterprise Access and/or Aggregation Network and/or Core network depending on the deployment scenario.

7.2.2 Description of the use case

7.2.2.1 Overview

7.2.2.1.1 General

The interconnection model for enterprise access to multiple Cloud destinations can be classified as:

a) Single-point access to multiple Clouds: this is the scenario where enterprise branches access the Cloud Networks through the enterprise headquarters, as illustrated in Figure 59.

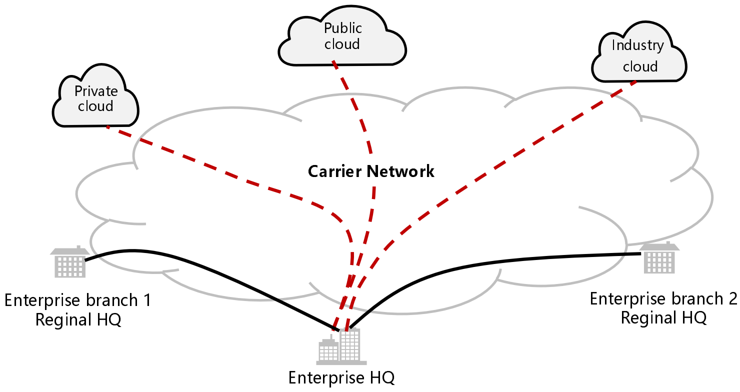


Figure 59: Single-point access to multiple Clouds

b) Multi-point access to multiple Clouds: this is the scenario where enterprise headquarters and its branches (maybe regional HQs) are each directly connected to multiple Cloud Networks, as illustrated in Figure 60.

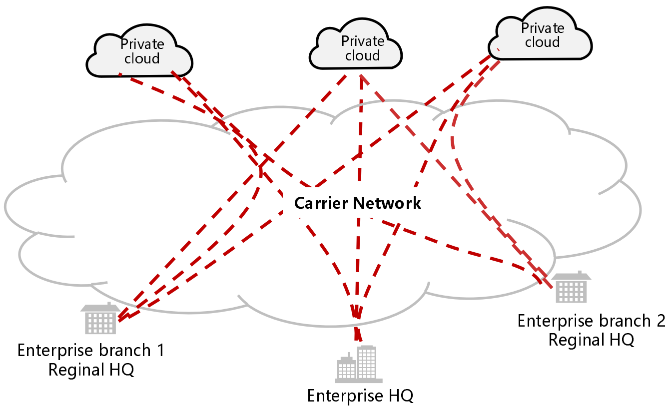


Figure 60: Multipoint access to multiple Clouds

7.2.2.1.2 IP address Management

If an enterprise has multiple Cloud connections, the question arises whether to isolate and decouple the IP address planning of the enterprise and Cloud hosted functional elements. This includes both IPv4 and IPv6 addresses. This can be divided into the following scenarios:

a) The first scenario is where the IP addresses of enterprise CEs and Cloud DC gateways are in the same network segment. The Transport network provides Layer 2 transparent transmission. The Enterprise IT department manages the IP addresses of PCs, terminals, and VPCs on the enterprise side. The enterprise CEs need to have a coordinated IP address planning with the Cloud DC gateway, as illustrated in Figure 61.

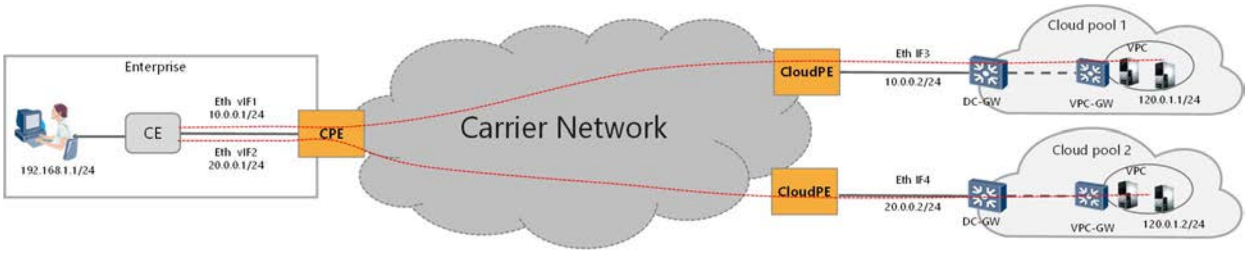


Figure 61: Enterprise CEs and Cloud DC gateways IP addresses are in the same network segment

b) The second scenario is where the IP addresses of enterprise CEs and Cloud DC gateways are in different network segments. The Transport network provides cross-network segment interworking capability. The Enterprise IT department manages the IP addresses of PCs, terminals, and VPCs on the enterprise side. Enterprise CEs need to negotiate IP address planning with carriers. This case is illustrated in Figure 62.

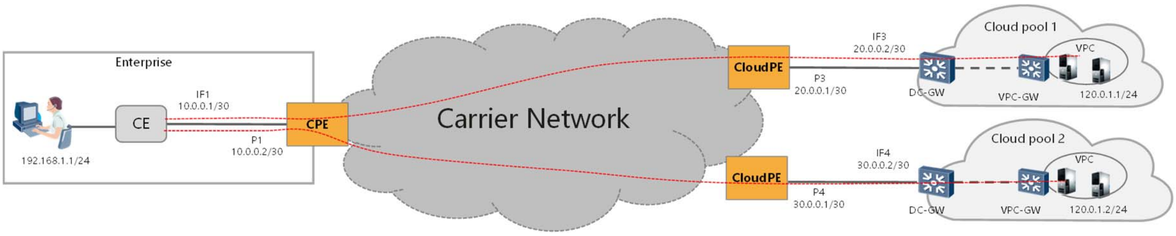


Figure 62: Enterprise CEs and Cloud DC gateways IP addresses are in different network segments

7.2.2.1.3 Cloud Access

To access multiple Clouds, an enterprise requires the Transport network to provide point-to-multipoint and multipoint-to-multipoint interconnection capabilities.

a) On traditional Transport networks, enterprise IT leases multiple point-to-point private lines (L2 E-Line/MPLS PWs) from the carriers to implement single-point to multiple Clouds and multi-point to multiple Clouds access.

b) The Transport network could provide private lines or a private network to implement point-to-multipoint or multipoint-to-multipoint interconnection. In this way enterprises only need to purchase these private lines or private network to access multiple Clouds. When access points or Cloud pools need to be added, it is only necessary to add access points and bandwidth to the purchased private lines or private network.

7.2.2.1.4 Slicing

Enterprises need to ensure that their private data is securely separated from other enterprises on the multiple Clouds Transport network. Such separation usually requires hard or soft slicing or connection isolation. The service data of different enterprises needs to be transmitted with equivalent quality. Therefore, the service data of different enterprises needs to be separated and quality assurance mechanisms need to be provided. Additionally, the private IP addresses of the different enterprises are maintained and planned independently. The Transport network needs to be able to support the same private IP addresses for different enterprises. Therefore, a private IP address isolation mechanism needs to be supported for enterprise data transfer, as illustrated in Figure 63.

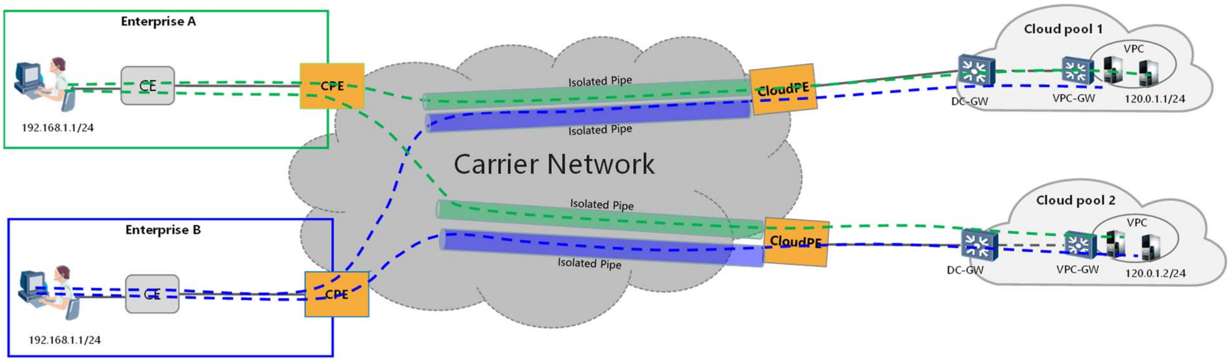


Figure 63: The carrier network provides hard slicing isolation for different enterprises

7.2.2.1.5 Network Provisioning

Enterprises need automatic provisioning of Cloud services, Cloud resources, and network connectivity to the Cloud. When Cloud PEs (Cloud Provider Edges) or Cloud pools need to be added, automatic remote provisioning is necessary. Hence there is no necessity for on-site O&M personnel to manually configure the services.

7.2.2.1.6 Redundancy and Protection

The Cloud PEs on the Transport network connected to the Cloud gateway should support cross-node dual-homing protection to ensure that services can be protected and restored when and if a Cloud PE fails. The DC-GW interconnection with the dual-homed active and standby Cloud PEs need to use separate links. The Cloud PEs need to be physically separated from each other to prevent simultaneous failures. The active and standby service routes from the CPE to the dual-homed active and standby Cloud PEs need to use alternate paths to prevent simultaneous failures. This case is illustrated in Figure 64.

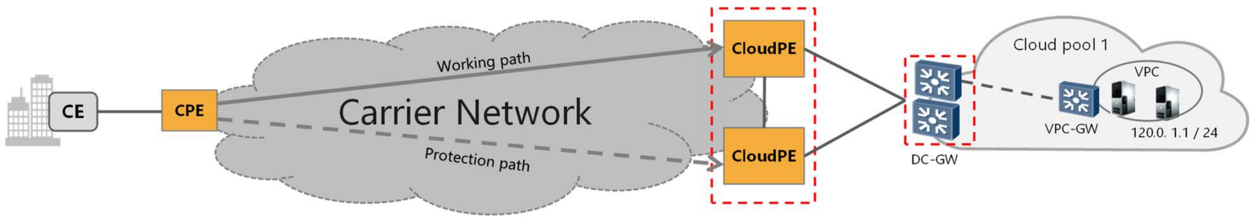


Figure 64: Dual-homing protection for Cloud interconnection

The mesh networking on the Transport network needs to support protection and restoration of services in the event of multiple fibre cuts. This can be achieved by alternate routes, as illustrated in Figure 65.

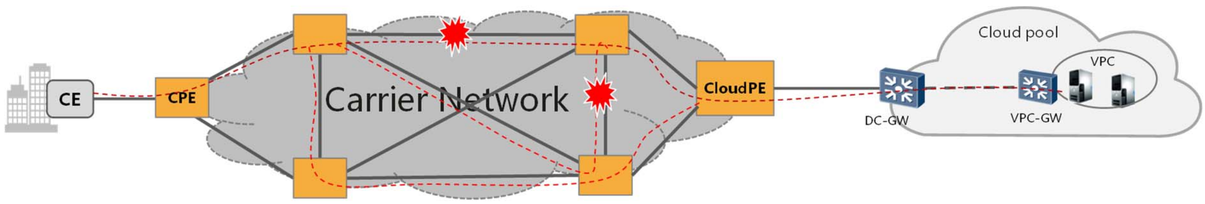


Figure 65: Protection against multiple fibre cuts on the carrier network

7.2.2.2 Motivation

Premium private line access to multiple Clouds enables users in various industries to enjoy high-quality Cloud access service experience. The main advantages are:

- Accelerating the development of high-quality Cloud services: based on slicing, large bandwidth, and low latency, the network operators can provide flexible and convenient Cloud connection capabilities.

- Reduces the need to lease multiple private lines. A single private line or private network can provide multipoint to multipoint Cloud access, potentially reducing the enterprise private line cost.

- Automated provisioning will improve Cloud access provisioning efficiency as well as user experience. E2E Cloud and network services automated provisioning, can reduce the carrier's OPEX, improve the user experience, and accelerate the TTM of users' Cloud services.

7.2.2.3 Pre-condition

Before enabling a multiple Clouds private line, the following conditions need to be met:

- The enterprise branch CE is deployed and is connected to a network CPE.
- The Cloud PE is connected to the network and the Cloud is connected to the Cloud DC gateway.
- The network has allocated sufficient bandwidth resources.
- A management system that can manage the O&M of these network devices (Access Network devices and Transport Network devices may have different management systems) is deployed. A Cloud management system can schedule Cloud resources to enable Cloud service connections. An orchestrator is used to collaborate with the network device management system and Cloud management system

7.2.2.4 Operational flow of actions

Figure 66 shows the process of provisioning the premium private line service in multiple Clouds scenarios.

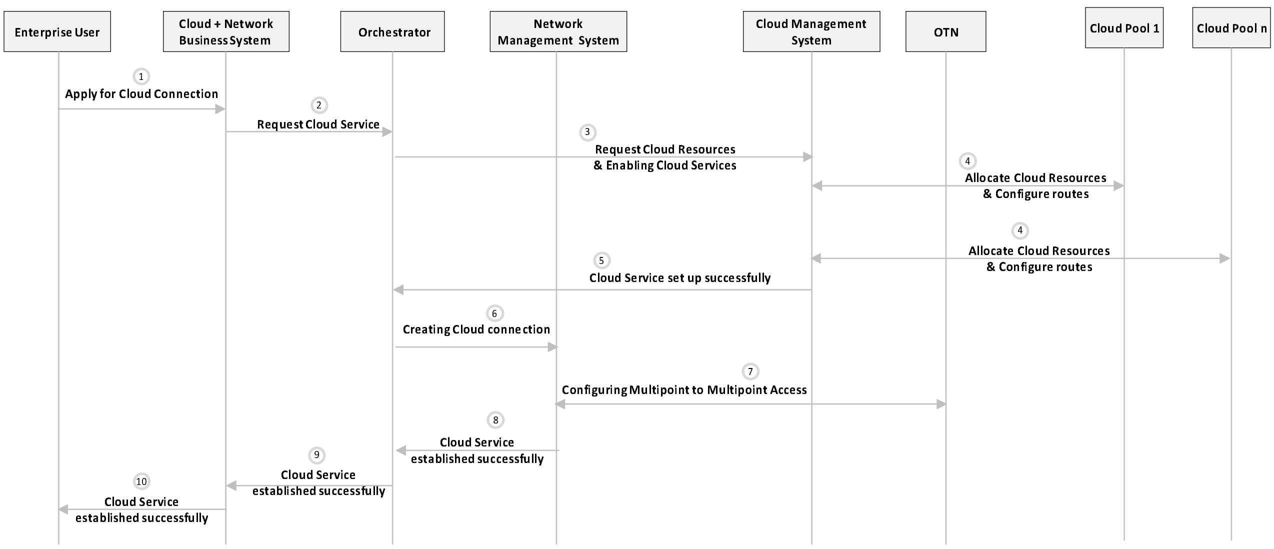


Figure 66: Cloud-network integration service provisioning process

1) The Enterprise IT department applies for Cloud connections. Depending on the size of the company it will require coordination with other IT groups in the organization to set up multi Cloud access.

2) The Cloud + Network business system creates a request for a new Cloud service.

3) The Cloud-network Orchestrator applies for the necessary Cloud Resources and if they are available the service will be enabled.

4) The Cloud management system allocates the appropriate Cloud resources in one or more Cloud pools and configures the routes.

5) The Cloud management system informs the Cloud-network Orchestrator that the service is established.

6) The Cloud-network Orchestrator request network management system to establish private line connectivity for multiple branches to access multiple Clouds.

7) The network management system configures Multipoint-to-Multipoint Access.

8) The network management system informs the Cloud-network Orchestrator, that the E2E Cloud access private line is set up successfully.

9) The Cloud-network Orchestrator relay back to Cloud + Network business system that the Cloud access private line is set up successfully.

10) Cloud + Network business system informs the Enterprise IT department, that the Cloud connection was successful.

7.3 Use case #17: Premium home broadband connectivity to multiple Clouds

7.3.1 Use case context

There is an increasing demand for premium home broadband Cloud-based services such as Cloud VR education, Cloud VR gaming, and Cloud gaming. These home broadband services impose stringent requirements on the network such as high bandwidth, low latency, and low packet loss rate. When users go online, the VR manager dynamically schedules user server access, based on their SLAs. The Transport Network needs to provide a single-point service access capability which can flexibly connect to different Clouds.

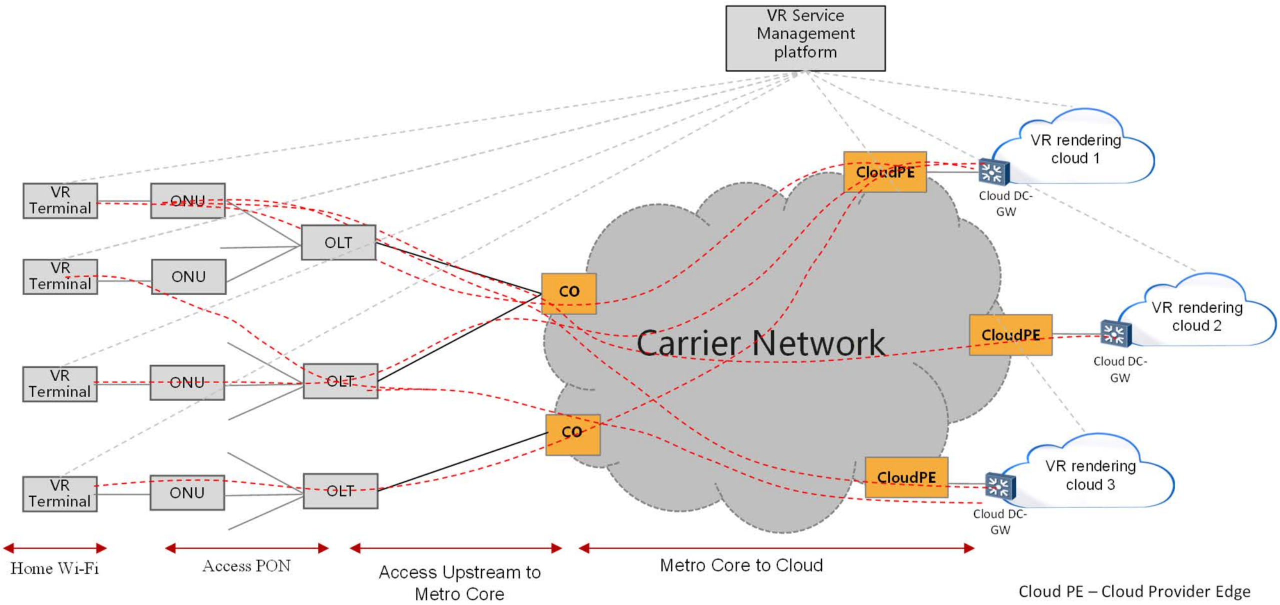
This use case describes the application scenario for premium home broadband users connecting to multiple Clouds.

7.3.2 Description of the use case

7.3.2.1 Overview

7.3.2.1.1 General

Figure 67 shows a typical networking scenario for deploying premium home broadband services, such as Cloud VR education, Cloud VR gaming and Cloud gaming.



NOTE: Figure 67 does not show all possible connection.

Figure 67: High-quality home broadband services to multiple Clouds

7.3.2.1.2 Service Establishment

When a user wishes to establish a connection with a VR application, the VR service management platform dynamically allocates a Cloud VR rendering node that provides the service based on the agreed user policy. The IP address of the rendering node is returned to the VR terminal. The VR terminal uses this IP address to send a connection request to the rendering server. In the home broadband scenario the multiple Clouds access is a dynamic allocation and scheduling process. Instances of the same application may be installed at different Cloud nodes. An example process flow is shown in Figure 68.

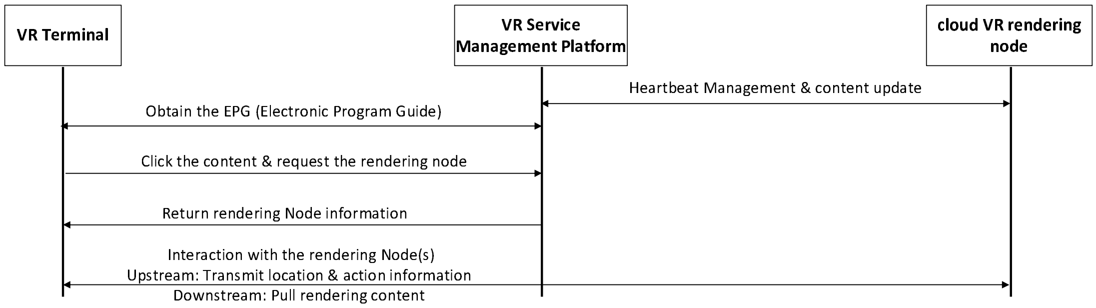


Figure 68: Example process for a strong-interaction VR service

7.3.2.1.3 Network Performance

When considering the provision of multiple Clouds connection services for premium home broadband, it should be noted that a very large number of home broadband users may need access to multiple Clouds via a large number of OLTs. So the interconnection model is point-to-multipoint or multipoint-to-multipoint.

When VR services are deployed on multiple Clouds, the network should meet the performance requirements for strong-interaction VR services.

Table 8: Cloud VR strong interaction services Network specifications

Immersed experience Levels (see note 1)	Cloud VR Phase 1	Cloud VR Phase 2	Cloud VR Phase 3	Cloud VR Phase 4
Screen resolution of mainstream terminals	2-3K	4K	8K	16K-
Average bit rate	≥ 40 Mbps	≥ 65 Mbps	≥ 270 Mbps	≥ 770 Mbps
Bandwidth Requirements	≥ 80 Mbps	≥ 130 Mbps	≥ 540 Mbps	≥ 1,5 Gbps
Network RTT (see note 2)	≤ 20 ms	≤ 20 ms	≤ 10 ms	≤ 8 ms
Network jitter requirements	≤ 15 ms	≤ 15 ms	≤ 10 ms	≤ 7 ms
Network Packet Loss Requirements	≤ 10 - 5	≤ 10 - 5	≤ 5 × 10 - 6	≤ 1 × 10 - 6

NOTE 1: Cloud VR Immersion level experience
Cloud VR Phase 1 (Initial Immersion 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 (Partially Immersive 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 (Deep Immersion 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 1080 pixels or higher on traditional TV.
Cloud VR Phase 4 (Full immersion 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.

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

The entire network consists of the home network, Access Network, and metro/backbone network.

Table 9: Cloud VR Service Jitter requirements

Immersed experience Levels	Cloud VR Phase 1	Cloud VR Phase 2	Cloud VR Phase 3	Cloud VR Phase 4
Total Network Jitter	< 15 ms	< 15 ms	<10 ms	< 7 ms
Home Wi-Fi®	< 8 ms	< 8 ms	<6 ms	< 3 ms
Access PON	< 2 ms	< 2 ms	<1 ms	< 1 ms
Access Upstream to the Metro Core	< 2 ms	< 2 ms	<2 ms	< 2 ms
Metro Core to Cloud	< 3 ms	< 3 ms	<1 ms	<1 ms

When Cloud Games are deployed in multiple Clouds, the network should meet the performance requirements of strong-interaction VR services.

Table 10: Cloud Gaming Network Requirements

Display Terminal	Network Metrics	Cloud Games Phase 1	Cloud Games Phase 2	Cloud Games Phase 3
Computer display screen	Bandwidth	≥ 32 Mbps	≥ 48 Mbps	≥ 88 Mbps
	Network RTT	≤ 30 ms	≤ 20 ms	≤ 15 ms
	Network jitter	≤ 16 ms	≤ 7 ms	≤ 4 ms
	Packet loss rate	≤ 1 × 10 - 5	≤ 1 × 10 - 5	≤ 1 × 10 - 6
TV display	Bandwidth	≥ 32 Mbps	≥ 96 Mbps	≥ 320 Mbps
	Network RTT	≤ 30 ms	≤ 20 ms	≤ 15 ms
	Network jitter	≤ 16 ms	≤16 ms	≤ 8 ms
	Packet loss rate	≤ 1 × 10 - 5	≤ 1 × 10 - 5	≤ 1 × 10 - 6
Mobile phone display	Bandwidth	≥ 10 Mbps	≥ 32 Mbps	≥ 64 Mbps
	Network RTT	≤ 30 ms	≤ 20 ms	≤ 15 ms
	Network jitter	≤ 33 ms	≤ 16 ms	≤ 8 ms
	Packet loss rate	≤ 1 × 10 - 3	≤ 1 × 10 - 5	≤ 1 × 10 - 6
NOTE: Cloud Games VR differ in the following phases and the network metrics needed are different depending on the screens used. Cloud Games Phase 1: Initial Immersion Experience. Cloud Games Phase 2: Comfortably Immersive Experience. Cloud Games Phase 3: Full Immersion Experience.				

7.3.2.1.4 Slicing

The bandwidth of a traditional Transport Network is shared by multiple services. It is difficult to avoid service traffic conflicts and ensure low latency for latency-sensitive services. The sensitivity of the VR service to bandwidth and latency needs to be considered when establishing the connections.

When different users want to access the same or different services (such as VR education and Cloud gaming) via the same or different OLTs, the network provider needs to take into account that the different services may impose different requirements on the network.

To ensure these different services perform efficiently, the network provider needs to separate these services to eliminate network resource conflict. This will prevent network parameters such as bandwidth, packet delay, and packet delay variation from impeding the service requirements. For example, different VLANs can be used to identify services, and different network slices can be used to separate services. This is illustrated in Figure 69.

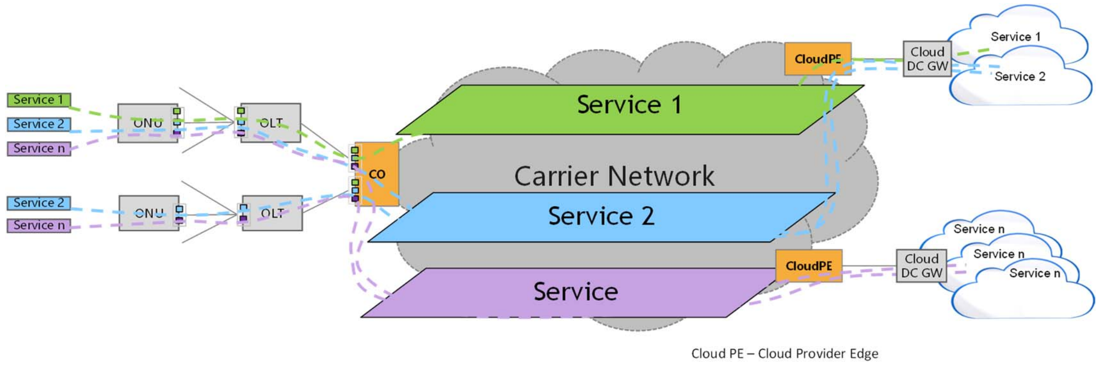


Figure 69: Network slicing mechanism for different services

7.3.2.1.5 Redundancy and Protection

VR rendering or gaming Clouds may provide Cloud services for a large number of home users at the same time. Therefore, the nodes and the links connected to the Clouds need to have high availability. The Cloud PEs on the Transport Network connected to the Cloud gateway need to support cross-node dual-homing protection to ensure that services can be protected and restored when and if a Cloud PE fails. The DC-GW interconnection with the dual-homed active and standby Cloud PEs needs to use separate links. The PEs should be physically separated from each other to prevent simultaneous failures. The active and standby service routes from the OLT or CO to the dual-homed active and standby Cloud PEs on the Transport Network need to use alternate paths to prevent simultaneous failures. This is illustrated in Figure 70.

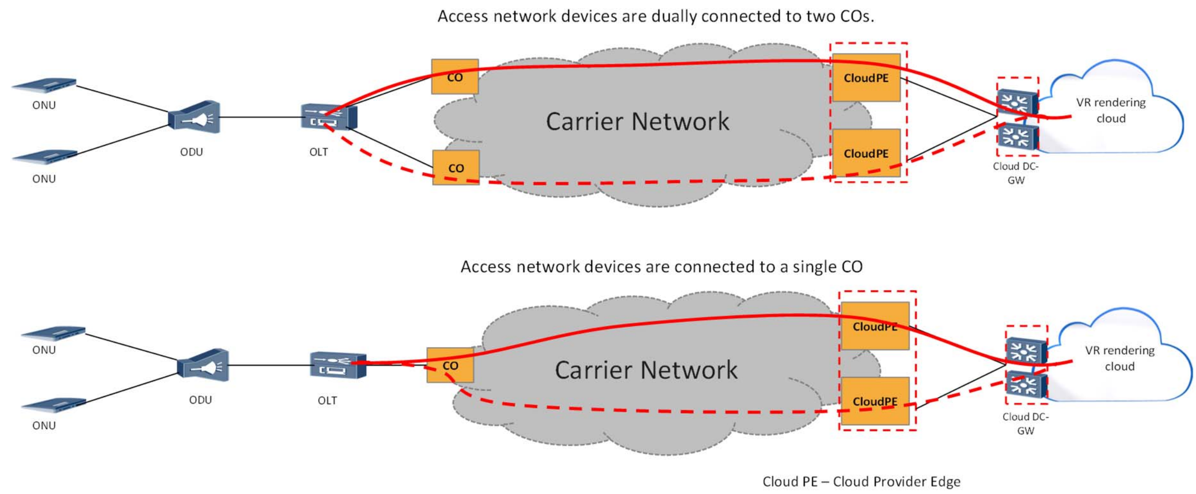


Figure 70: Dual-homing protection for Cloud interconnection

7.3.2.2 Motivation

Premium home broadband connectivity to multiple Clouds, enables users to enjoy a high-quality service experience. The main advantages are:

- Accelerate the development of high-quality Cloud services with slicing, large bandwidth, and low latency, enabling thousands of users to enjoy differentiated experience of high-quality Cloud access services.
- Automated provisioning will improve Cloud VR service provisioning efficiency, as well as user experience. E2E Cloud and network services automated provisioning enables fast service provisioning and improved user experience, also reducing the carrier's OPEX.

7.3.2.3 Pre-condition

The prerequisites for enabling premium services for home broadband users are as follows:

- ONUs have been deployed in the home network.
- The Cloud PE is connected to the network and the Cloud PE is connected to the Cloud DC gateway.
- Sufficient bandwidth resources and low latency routes are allocated in the network.
- A management system that can manage the O&M of these network devices (Access Network devices and Transport network devices may have different management systems) is deployed. A Cloud management system that can schedule Cloud resources to enable Cloud service connections is deployed. An orchestrator that can collaborate with the network device management system and Cloud management system is deployed.

7.3.2.4 Operational flow of actions

Figure 71 shows an example of the process of provisioning a premium home broadband service.

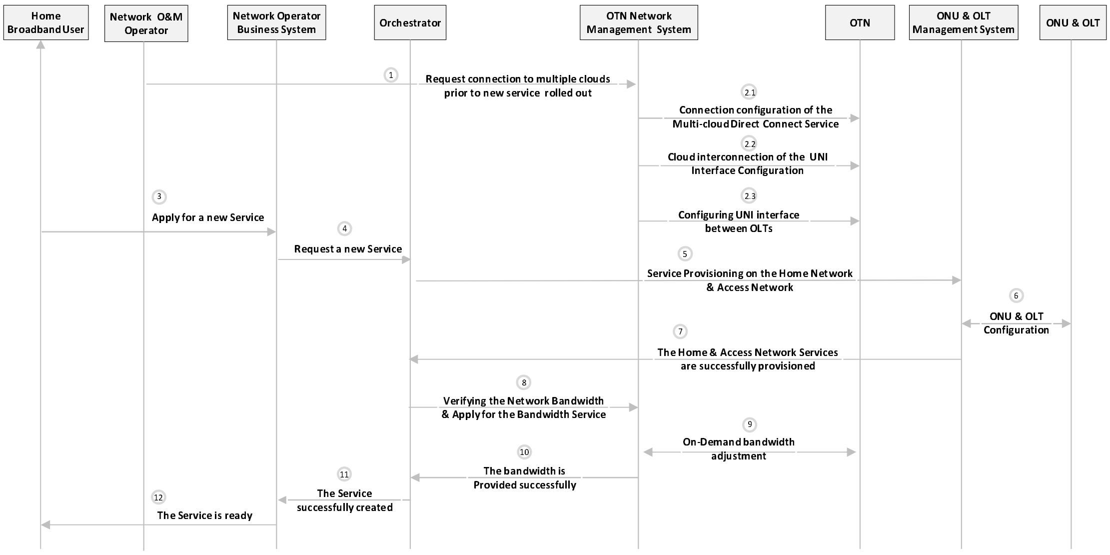


Figure 71: Example process of applying for and provisioning a premium home broadband service

1) The Network O&M operator requests the OTN Network Management system to establish connections to the multiple Clouds prior to allowing a new access to the services.

2) The OTN management system:

   2.1) Configures the multi Cloud direct connections service.

   2.2) Configures the Cloud interconnection of the UNIs and interface.

   2.3) Configures the UNI's interface between OLT.

3) The residential user applies for new service.

4) The network operator business systems request a new service.

5) The orchestrator provisions the service on the home and Access Network.

6) The OLT management system configures the OLT and the ONU.

7) OLT management informs the Orchestrator that the home and Access Network are successfully provisioned.

8) The Orchestrator Verifies the Network Bandwidth & Applies for the Bandwidth Service.

9) The OTN management system adjusts on demand bandwidth.

10) The OTN management system informs the Orchestrator that bandwidth is provided successfully.

11) The Orchestrator inform the network operator business systems that the service setup is successfully.

12) The Network operator business systems informs the user that the service is ready.

7.4 Use case #18: Virtual Music

7.4.1 Use case context

Virtual music can be defined as sharing and creating music in real time by different parties that are not in the same location. Currently, this is hardly possible. The reason for this is that to play music or sing together in a band or choir, has strict synchronization and latency requirements. This already becomes apparent in large physical orchestras, where the relative distances between some musicians cause a notable delay in arrival of the sounds. Experienced musicians compensate for this by timing their performance. A similar effect occurs but more pronounced when musicians play together via the internet, where buffering and transmission delays are caused by software latencies and the network.

To illustrate the virtual music use case the following examples are used.

- Virtual Orchestra

In this case the orchestra conductor and the musicians are geographically separated. Current conferencing tools can aid in the realization of such an orchestra, however network latency (assuming the latency caused by tools can be minimized) will lead to synchronization issues between the participants. The realization of such an orchestra needs low latency fibre networks, minimal buffering and processing delays.

- Virtual Music Classes

A virtual music class is defined as a music class or lesson where the teacher and the student(s) are at different locations. For an effective class, the teacher and the student(s) should be able to play together. This is not possible with current online meeting tools. The network latency between the teachers and the student(s) as well as buffering/processing delays prevents effective classes.

- Virtual concerts

Performers can work together interactively to broadcast live music sessions even when they are at different locations. With high uplink capacity and low latency fibre connections the performers can stream their music over the network. Fans can then enjoy the concert in real time, and possibly in an immersive VR session.

7.4.2 Description of the use case

7.4.2.1 Overview

7.4.2.1.1 Latency requirements

To realize the use case described in the previous clause, the end to end connection between musicians needs to meet certain synchronization requirements. The assumption is that this translates primarily into latency requirements. To derive a latency requirement, a hypothetical situation can be considered, where musicians are collocated, but they cannot see each other or a conductor (no visual coordination). They will have to rely on their hearing as they are not able to compensate visually for latency. Therefore, in order to synchronize effectively, the maximum distance between musicians is 10 meters as illustrated in Figure 72. To travel this distance sound waves take approximately 30 ms. A platform to share music over the Internet needs to replicate this with low latency connections. Thus, the maximum unidirectional end to end latency between each pair of musicians is 30 milliseconds.

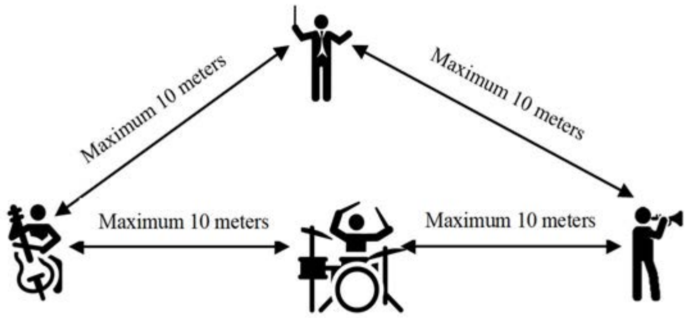


Figure 72: Maximum distance between musicians to share music effectively in real time

7.4.2.1.2 Latency contributions in the end to end chain

Figure 73 illustrates the decomposition of the end to end latency between the musicians. This includes the latency created at the device connected to the music instrument (1, 2 and 6, 7 in Figure 73), home network (3 and 5 in Figure 73) and most importantly, the network connection between the participants (4 in Figure 73). Additional latency is introduced to compensate for packet jitter in the underlying network. Latency at the end points is typically caused by encoding and decoding of signals and overhead due to buffering and error correction.

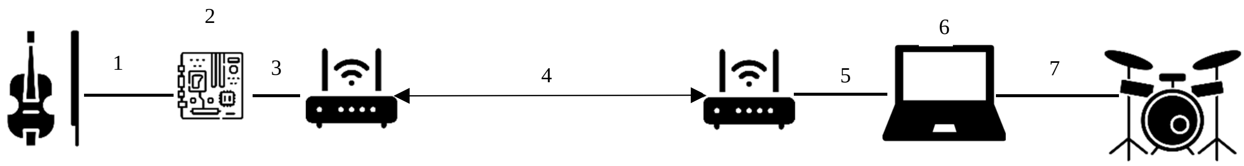


Figure 73: End to end latency created at various points between musicians

7.4.2.1.3 Impact of network topology on latency

Overall effectiveness of shared music among participants also depends on the topology of the connections. Two models are considered:

A client-server model

As illustrated in Figure 74 a), each performer is connected to a central entity, this central entity processes these inputs and sends a common output to each performer. Each endpoint only needs to send one stream and receive one (combined) stream. The central unit takes care of the mixing and optionally equalizing the delays where needed. The processing and redistribution of all streams will introduce a certain amount of delay. In the client server model (see Figure 74 a)), musicians A, B, C and D connect to a central entity O.

A peer-to-peer model

As illustrated in Figure 74 b), there is no central entity, but a copy of the music generated is sent from each party to every other party. There is no delay due to central processing. However, at the end points, more processing and potential delay adaptation has to be performed. This will also introduce some delay and added complexity. In the peer to peer model, each musician is connected to every other musician (see Figure 74 b))

NOTE: In the peer to peer connection of Figure 74 b), arrows from C and D have been intentionally omitted to improve readability.

The peer to peer model offers the opportunity to optimize the transmission delay. Because there is no central entity, additional processing needs to be added at the end points. The peer to peer model is suitable for a smaller number of musicians, while the client server model is more suitable for a larger number of musicians. Currently, both models are considered, and the optimum configuration may depend on the specifics of a particular scenario.

a) Client server connection between musicians

b) Peer to peer connection (arrows from C and D have been intentionally left out to improve readability)

Figure 74: Different network topologies

7.4.2.1.4 Audio and video channels

These strict latency requirements are specifically applicable for the audio generated by the participants while the video traffic may tolerate some additional latency in cases where no conductor is present.

Thus, the audio generated by musicians may be routed through a low latency channel, while the video traffic may be sent through the same or another channel on the network as shown in Figure 75. This was tested successfully over a short distance between participants.

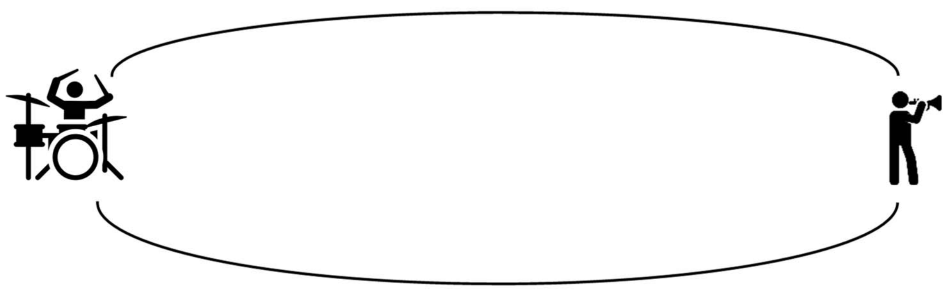


Figure 75: Audio and video sent over different channels

7.4.2.1.5 Applications state-of-the art

There are various applications that can help musicians create music together over the Internet by streaming uncompressed audio with low latency and low overhead. Some of them support the client server model and others support peer to peer connections. The virtual music applications are combined with hardware based solutions to reduce the endpoint (devices/laptop/PC of musicians) latency to as low as 1 ms. However, these solutions still needs low latency network connections between the endpoints.

One advantage of the client server model is that the processing and bandwidth (both uplink and downlink) requirements for the musicians is independent of the number of participants. In this model, the central entity is referred to as audio server. Such audio servers have specialized software and sometimes hardware to enable low latency collection and distribution of music. An efficient mechanism (see note 1) with shared memory buffering leads to negligible additional latency in the order of microseconds. In the case of a peer-to-peer model, the functionality of the audio server needs to be part of each musician's setup.

NOTE 1: Zero copy semantics.

In the case of a client server model, the audio mixer is part of the central unit (audio server). A hardware based analogue mixer at a musician's premise adds almost zero latency. The latency effect of the audio mixer in client server and the peer-to-peer model is for further study (see note 2).

NOTE 2: Since there are potentially different ways to implement it, either software based or hardware only or a combination of both.

NOTE 3: It is assumed that echo cancellation is handled by the application (just like typical audio or video communication).

There are various best practices that musicians can choose for an optimum setup to achieve high-quality virtual music, and a set of options can be seen in Table 11.

Table 11: Options to perform music remotely for various points in the end-to-end chain in Figure 73

Position in end to end channel (see Figure 72)	Indication of feasibility for virtual music ← Difficult to Achieve			Easy to achieve →	Latency range (estimate) (highest to lowest)
1 and 7	Bluetooth™ Headset	Wired connection to built-in computer hardware	Low latency external audio interface and wired headphones		100 - 5 ms
2 and 6	Laptop/PC with Windows™ OS	Laptop/PC with Linux™	Raspberry Pi™ with customized operating system	Dedicated hardware (with low latency sound card) and optimized software	100 - 1 ms
3 and 5	Wi-Fi®		Wired connection		6 to < 1 ms
4	4G/DSL	5G/Cable	Fibre/F5G		See below

So, today, musicians can reduce the delay at various points in the end-to-end chain except in the network. From Table 11, the lowest latency estimate for the end-to-end chain without the network is 7 ms. That means that given the overall latency requirement of 30 ms, the latency budget for the network is 23 ms in best case situation.

To reduce latency in the network, fibre plays an important role. Fibre networks provide low latency, and low packet jitter connectivity between these endpoints. Fibre connectivity requires less overhead for error correction compared to copper-based networks. F5G networks will have to provide the musicians with the lowest possible latency, this would mean the possibility of guaranteed latency which remains constant throughout the music session. A low latency dedicated slice could achieve virtual music. The F5G architecture will reduce the end-to-end network latency.

To illustrate the effect of latency reduction, a hypothetical optical link without any switching or routing is taken. Assuming an effective refractive index of about 1,5, the speed of light in optic cable is approximately 200 km/ms. Every millisecond latency reduction in the F5G network connecting the musicians allows the distance between them to increase by up to 200 km. This may allow musicians more degrees of freedom in creating a setup to make music together remotely.

7.4.2.2 Motivation

The virtual music use case is an example of how F5G networks can help overcome the limitations that currently make it difficult for musicians to interactively create music together through a remote connection.

The challenge of virtual music is real and being addressed by industry and academia alike. Although solutions to optimize latency are available, they do not address the network. However, it can be argued that there is a lot to be gained in reducing network latency being achieved by the F5G network architecture.

The relevance for F5G lies in the fact that this use case brings requirements that are difficult if not impossible to meet with current networks, specifically with the expected requirements on low latency and the possibility to offer separate channels for audio and video data.

Enabled by F5G technology, musicians can overcome geographical barriers thereby making shared real time music a reality.

7.4.2.3 Pre-condition

The following preconditions apply for this use case:

- For audio, musicians need to have specialized software applications and hardware to optimize the latency generated at endpoints (devices/laptop/PC).
- Wired connection from the device to a router, low latency audio interfaces, and wired headphone need to be used depending on the scenario.

7.5 Use case #19: Next Generation Digital Twins

7.5.1 Use case context

Even though digital twins are already being used across many industries, the global market for digital twins is still rapidly expanding. Fast innovation and wide scale digital transformation are opening new doors for n*ext generation digital twins*, that can radically transform the way to handle today's big societal and environmental challenges. However, to enable smooth operation of these *next generation digital twins*, strict requirements on the communication infrastructure have to be met. This use case gives an overview of current and potential future types of digital twins, some examples in the different domains, and how this translates into recommendations regarding connectivity.

7.5.2 Description of the use case

7.5.2.1 Overview

7.5.2.1.1 Definition of digital twin

A Digital Twin (DT) refers to a digital replica of physical assets, processes, and systems. In the following, the term physical object is used as the real world object of any type. DTs integrate Artificial Intelligence, machine learning, and data analytics to create living digital simulation models that are able to learn and update as well as represent and predict the current and future conditions of the corresponding physical objects [i.30]. The DT includes all information that can be obtained from the physical objects. Between the DT and the physical objects a bidirectional data communication is established, allowing the DT to act as a controlling instance of the physical object. A change in state of the physical object leads to a change in state of the DT and vice versa.

Current state-of-the-art DTs can not only mirror products, but also processes, systems, organizations, people or any other abstraction. A way of categorizing DTs is to look at the physical object they represent: it could be at the level of a *component*, an *asset*, a *system*, or a *process*:

- A component twin is the smallest unit of a DT.
- An asset twin combines multiple components or their twins, to gain insights into the interaction between them.
- A system twin involves multiple assets or their twins that together describe an entire system. They provide information on the interaction between assets, and could carry out performance enhancements.
- A process twin reveals how multiple systems or their twins work together in e.g. an entire production facility, a building, or a (smart) city.

It is important to note that DTs are more than just data -- they also include simulations, (machine learning) algorithms and reasoning to help decision-making based on the data. Data from multiple DTs can be aggregated for a complete view across a number of real-world entities, such as a power plant or an entire city, and their related processes. In summary, a DT has two purposes:

1) *understanding* the physical world by providing insights into the status of the physical object it represents; and

2) support *decision-making* that helps to adapt and improve the physical object.

7.5.2.1.2 Next generation digital twins

The *next generation digital twin*, is a set of DTs that could work together, with each DT having a well-defined objective on its own [i.29]. The DT of a city can e.g. have bidirectional interaction with the DTs of buildings by exchanging information and making cooperative decisions. The provisioning of DTs can be achieved in different ways: DTs can run in different distributed Clouds, in the same (local) Cloud, on local compute resources, or a combination thereof. These different implementations have different requirements on the connection between the DTs, and with their physical object. Ideally, (sensor) data is exchanged and processed in real-time, which is feasible if the DT is deployed local to the sensor. However, if the data first need to be collected by a Cloud application, synchronization and proper delay management become more important due to different time constants, especially if multiple DTs are involved. A reliable communication network with a consistent performance is required in these situations.

An alternative categorization of DTs is to look at their levels of sophistication, from least to most. DTs can be:

- *Descriptive* (a live version of design and construction data);
- *Informative* (has an added layer of operational and sensory data);
- *Predictive* (uses operational data to gain insights);
- *Comprehensive* (simulates future scenarios and "what-if" questions); or
- *Decisive* (has the ability to learn and act on behalf of users).

DTs that are either *descriptive* or *informative* are already being used, and DTs that are *predictive* or *comprehensive* are currently being developed. DTs that are truly *decisive*, i.e. that have the autonomy to make decisions without interaction of the operator, need further study.

The *next generation DTs* is a combination of all those five sophistication aspects. These next generation DTs are currently on the horizon with challenges of resiliency, autonomy and privacy.

7.5.2.1.3 Domains

DT technology has applications in many different domains, such as manufacturing or process industry (for a single robot, an assembly line, or a complete factory), automotive/transportation (for a digital replica of a car/train, vehicle platoon, or highway/railway system), energy (for power generation, power consumption and smart grids), healthcare (for medical machines and body sensors to remote surgery), and urbanization at city level (for providing monitoring and control at system, building and city level [i.29]). It goes without saying that this list is far from complete, but it shows the variety among DTs in both domain and scope.

The application of DT technology in industry is moving from the (one-time) engineering and construction phase to the (continuous) operations and maintenance phase e.g. in industrial automation via Cloud-based digital twins in Industry 4.0 [i.28]. It is anticipated that Industry 4.0 will have an increasing number of field devices with sensors and the virtualization of distributed control functions in a local or centralized automation Cloud. *Next generation DTs* will benefit from F5Gs support for real time distributed control via low latency communication (shown in Figure 76).

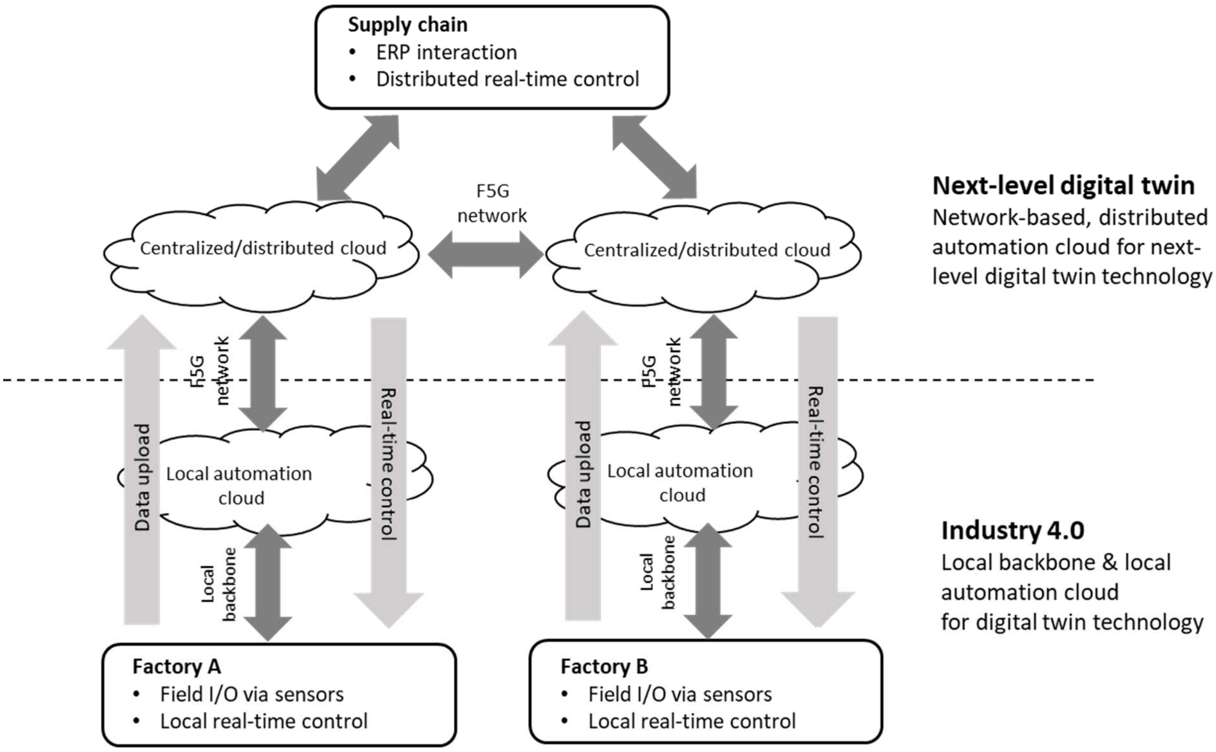


Figure 76: Transformation of industrial networks (Industry 4.0) with next-level digital twin technology

In smart cities a similar trend is visible and Figure 77 shows an example for DT connections in a smart city between DTs of individual systems (like traffic light and road sensor DT at system level), DTs at street/building level (like a traffic management DT) and further up towards a city DT with corresponding exchange of information and control.

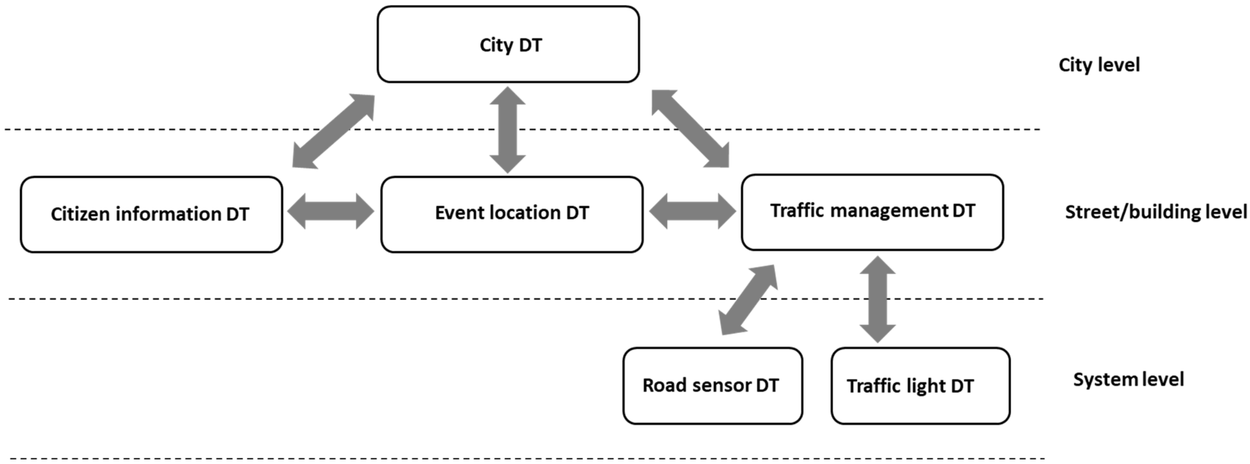


Figure 77: Example of DT connections and hierarchy among different levels for DT in a city

7.5.2.1.4 F5G network challenges

The challenges for today's DTs are related to e.g. collecting data and data interoperability, when it comes to the compositional nature of DTs. It is assumed that *next generation DTs* are a combination of multiple assets, systems and processes in a distributed Cloud-based architecture. Depending on their application, they are massive in scale (e.g. cities instead of a single building or road), they require real-time data (e.g. industry automation), and they are an integral part in managing real world processes.

This means that *next generation DTs* will pose challenging requirements on F5G networks, in terms of data (large scale data, real time data, and high quality image-based sensor data), latency (real-time control in time-sensitive networks of 100 µs - 2 ms) and reliability (monitoring and control of industrial processes depend on the DT).

As an illustrative example, Table 12 summarizes five different traffic types and their related industrial automation requirements. These traffic types have been defined by several organizations such as 3GPP, IEEE and IIC. The table is adopted from [i.28]. It is clear that the communication network need to allow for a mix of service requirements that range from critical real-time traffic to best-effort traffic, with varying reliabilities, periodicities and data sizes.

Table 12: Example of different traffic types and related requirements in industrial automation (extract from [i.28])

Traffic type	Periodic / sporadic	Typical period	Typical data size (bytes)	Criticality
Isochronous	Periodic	100 µs - 2 ms	Fixed: 30 - 100	High
Cyclic	Periodic	500 µs - 20 ms	Fixed: 50 - 1 000	High
Events	Sporadic	10 ms - 50 ms	Variable: 100 - 200	High
Network control	Periodic	50 ms - 1 s	Variable: 50 - 500	High
Audio / video	Periodic	Frame rate	Variable: 1 000 - 1 500	Low

Since the estimated data sizes are given per application message, the total data rate scales linearly with the number of application messages. If the number of application messages grows, for example in a factory with many different robots and assembly lines, the data volume becomes challenging to support on current infrastructures. Especially if a DT consist of multiple DTs, as in Figure 77, it is the aggregation points in a distributed Cloud (local/edge/central) that are the bottlenecks.

Also the interconnection of multiple *next generation DTs* in a distributed Cloud architecture (local, edge and central Cloud) and the support of multiple *next generation DTs* over a shared (F5G) network infrastructure is required.

7.5.2.2 Motivation

Digital Twin technology is being deployed today in multiple domains. The main motivation behind the usage of next generation digital twin technology is to improve the performance of assets, systems or processes.

The use case provides examples of how to deploy future digital twin technology in a flexible distributed architecture with multiple Cloud computing infrastructures, which are scalable and flexible to meet specific business needs. High-performance networks support the next generation digital twin deployments.

Today, industrial automation is a frontrunner in the use of digital twin technology. F5G networks are expected to support next generation digital twin technology in this domain.

7.5.2.3 Pre-conditions

This use case requires:

- One or more locations, where a distributed Cloud infrastructure (local/edge/central) is deployed, capable of supporting multiple interconnected DTs (in terms of compute, storage and networking).
- A highly available, (near-) real-time communication link, or a network of communication links, between the real-world object(s) and the location(s) in a distributed Cloud architecture where the DTs are realized.
- Support of multiple DTs over the same communication link or a network of communication links.

7.6 Use case #20: Media Transport

7.6.1 Use case context

The global 4K/8K UHD (Ultra-High Definition) video industry is developing rapidly. 4K/8K and HDR (High Dynamic Range) features are revolutionising the user experience. The exponential growth of definition and data volume imposes strict requirements on the Transport Network (such as bandwidth, latency, and packet loss), which is driving the Transport network technology and architecture to be upgraded to match these new requirements. The current media network needs to support SD (Standard Definition, e.g. 480P) and HD (High Definition, e.g. 1 080P), but also needs to support even higher definition and more applications. The media network needs to ensure high-quality experience, higher available bandwidth (e.g. > 100 Gbps), and lower latency (e.g. < 10 ms).

This use case gives a brief introduction of 4K/8K media applications but focuses on the production aspect on the fixed Transport Network.

7.6.2 Description of the use case

7.6.2.1 Overview

Live broadcast of large-scale events is evolving from on-site production in stadiums to remote and Cloud-based production. The live video is collected and sent to the IBC (International Broadcasting Centre) or to the remote studio for production, no need for onsite TV vehicles. Production and broadcast personnel can produce programs in a production centre under better conditions. The advantages are low cost, ease of production and better production and broadcast effects.

The media network requires the Transport Network to have high bandwidth, predictable and low latency, and high clock precision capabilities.

- Network bandwidth: New services such as 6G-SDI (Serial Digital Interface) and 12G-SDI require a bandwidth of greater than 100 Gbit/s.
- Service latency: Multiple devices, IP forwarding, and signal compression on the Transport Network will cause unpredictable and high latency for E2E services. The impact is quite obvious in the case of live TV.
- Transmission quality: A high-precision clock is required to ensure the high transmission quality, no signal loss, and good user experience.

Figure 78 shows an overview of media video collection and transport architecture.

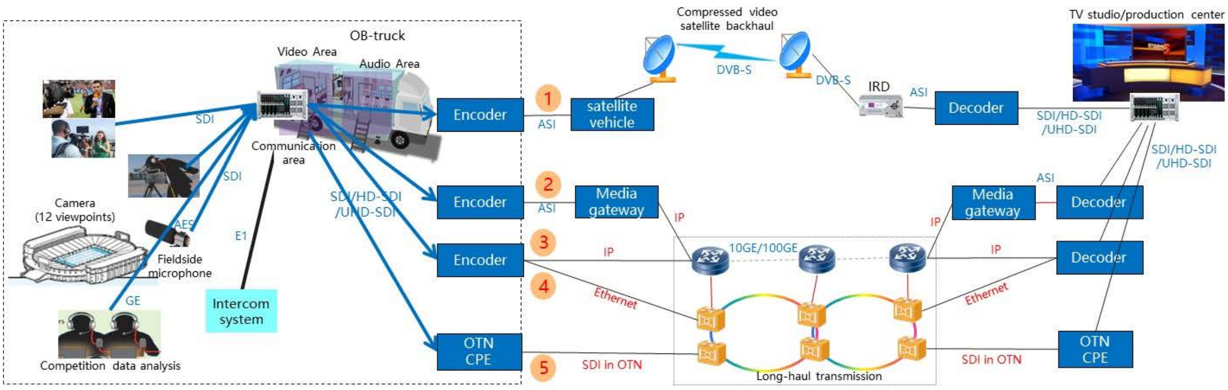


Figure 78: Media video collection and transport architecture

In Figure 78, the media video collection and Transport network include satellite backhaul network, IP/Ethernet backhaul network, and the OTN/DWDM backhaul network. Five options are shown in Figure 78.

- Option 1: The video signal (SDI/HD-SDI/UHD-SDI) is compressed and converted to ASI (Asynchronous Serial Interface) by an encoder. After that, the ASI signal is backhauled through the satellite network. It may also use microwave, or bundled 4G and 5G wireless network.
- Option 2: The encoded ASI signal is first converted to IP packets by the media gateway and then backhauled through IP network. Leased line were used initially for stadium collection and production.
- Option 3: The video signal is directly encoded to IP packets by an encoder. During the encoding, light compression can optionally be used. The encoded IP signal is backhauled through IP network.
- Option 4: The encoded IP packets are carried over Ethernet. The Ethernet signal is transparently transported over OTN/DWDM.
- Option 5: The video signal is directly transparently transported over OTN/DWDM. It saves the encoder and decoder devices and has a lower latency.

Higher performance and quality requirements on the Transport Network are needed to support 4K/8K transmission. The current network has insufficient bandwidth, unpredictable and high delay, long codec time, and packet loss. To ensure the ultimate experience of UHD, video signals over OTN/DWDM is the best option. It can provide the large bandwidth (e.g. N x 100 Gbps), one-hop transmission for low-latency, codec-free devices, zero packet loss, and 99,999 % reliability. Reliability can be enhanced by using dual fibre paths/routes as shown in Figure 79.

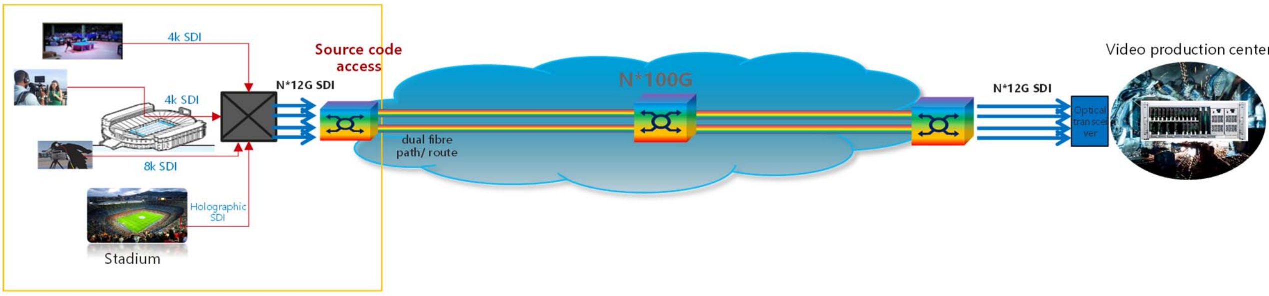


Figure 79: Media video collection and transport via OTN/DWDM

NOTE: The fibres in the figures are assuming different fibre path/routes.

7.6.2.2 Motivation

The main advantages and drivers for 4K/8K ultra high definition media video development includes:

- Improvement in user experience. 4K and HDR features provides revolutionary improvements in user experience.
- 4K technologies are currently realized by the content, network, and device industries. The efforts of these three parties are helping to promote the overall development of the industry.
- Acceleration of UHD commercial take-up. The UHD video industry is entering a rapid development phase in most countries. The video collection and Transport Networks need to be upgraded.

7.7 Use case #21: Edge/Cloud-based visual inspection for automatic quality assessment in production

7.7.1 Use case context

The use of Artificial Intelligence (AI) has significantly improved the efficiency of production lines and quality management systems. The combination of powerful capabilities of AI, real-time video streaming systems, and high-speed, low-latency telecommunications networks enable various industrial automation functions. This use case focuses on remote quality control on the factory shop floor and on centralized quality control management of distributed production sites using edge/Cloud compute nodes. Modern distributed/federated learning frameworks enable distributed machine learning at different, geographical locations. Contrary to the centralized learning approaches, where the data has to be available at a single location, federated learning uses localised machine learning model training. These local models are then used to generate a global model. This approach both relieves the company communication infrastructures and increases data security. This is because the transport of a large volume of sensitive data from the production sites to a central data processing facility is no longer necessary.

Private edge Clouds are becoming increasingly important for real-time, secure, robust and low-latency communication in production plants. This approach is used by larger manufacturing companies to implement a private/proprietary, real-time communication and data processing infrastructure for their production facilities. SMEs cannot afford such infrastructures due to the high investment costs. Therefore, a public edge Cloud connected via a real-time communication network offers, new and economically attractive opportunities, especially for SME manufacturing companies. For real-time support of distributed, urban production sites, a real-time, low-latency, fibre optic broadband infrastructure is needed, enabling highly innovative new approaches and unlocking the added value of edge Clouds.

This use case covers edge/Cloud-based visual inspection in the production environments using AI-assisted video analytics. Industrial-grade video cameras monitor produced objects in the visual inspection stations embedded in production lines. These video streams are transported in real-time to an edge data centre and processed by AI-assisted video analytics edge/Cloud services in order to evaluate the produced part quality metrics. Based on these metrics, automatic quality control measures are taken on the factory shop floor, such as controlling robotic actors to handle the defect parts.

Figure 80 shows the automation pyramid which provides an overview on the hierarchical levels of industrial production. The lowest level, the Field Level, contains the physical manufacturing equipment on the factory shop floor such as motors, actuators, video cameras and other sensors. Connectivity on the Field Level is heterogeneous based on different field bus systems. The second level, the Control Level, receives sensor and monitoring information from the devices in the Field Level. Based on that information, decisions are taken and control signals for the devices in the Field Level are generated, e.g. by using Programmable Logic Controllers (PLC). The Supervisory Level contains the Supervisory Control and Data Acquisition (SCADA) systems, which provide visualization and process control via Human Machine Interfaces (HMI). The Planning Level employs the Manufacturing Execution Systems (MES) to monitor the whole production process in a factory from base materials supply logistics to final products. The Management Level describes the administration of the whole Enterprise Resource Planning (ERP) processes.

This use case focusses on the two lower levels (Field Level and Control Level) of the automation pyramid, shown in Figure 80. Industrial production is moving towards virtualized control functions such as virtual PLCs (vPLCs) running in edge/Cloud environments.

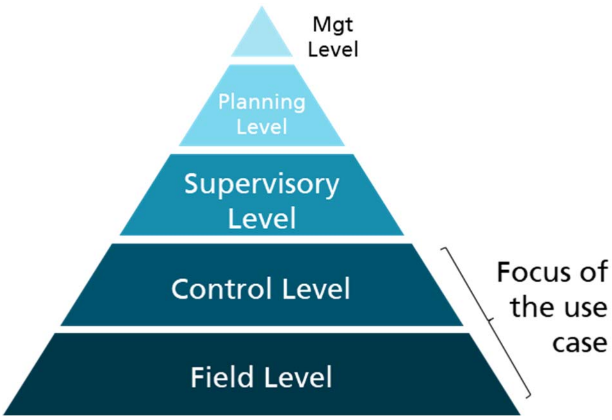


Figure 80: Focus of the use case in the context of the industrial automation pyramid

7.7.2 Description of the use case

7.7.2.1 Overview

7.7.2.1.1 General

The manufacturing industry is keen to adopt the new industry 4.0 concepts. That implies a trend towards a digital factory, where many functions, such as control logic, run in edge/Cloud environments. The equipment on the factory shop floor such as cameras (or other sensors) and robots needs to communicate in real-time with the edge/Cloud. The benefits are manifold. The virtualization of control functions alleviates the need for costly and often proprietary solutions for local PLCs on the shop floor, where cooling, power consumption, space and environmental effects are critical issues. The virtual control functions run as vPLCs on an edge/Cloud infrastructure composed of standard off-the-shelf IT equipment. This essentially removes the need for dedicated hardware PLCs on the shop floor and enables communication between many vPLCs.

This use case looks at camera-based vision inspection, where the video analytics functions and the control logic is moved into the edge/Cloud. A schematic overview of the use case is shown in Figure 81. Industrial video cameras located in a vision inspection station of a production line monitor the produced parts. Their video streams are transported in real time to a data centre, providing IT resources for running edge/Cloud services for video analytics. The control of and the communication with the Field Level equipment uses industrial Ethernet protocols. Based on the results of the video analytics service, the vPLCs control the actuators/robots at the production line to take appropriate actions. A critical metric is the minimum achievable cycle time, which is determined by the time required for the vPLC to send all control signals to its assigned targets and to receive all of their feedback. Typical vision inspection applications require a maximum cycle time of 5-10 ms, while some very time-critical vision inspection scenarios may require 2 ms or less.

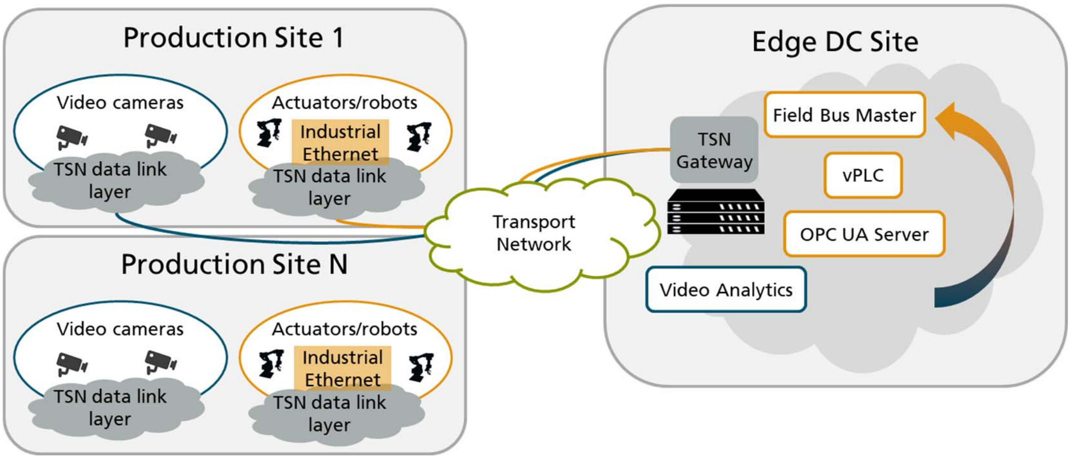


Figure 81: Schematic overview on edge/Cloud-based visual inspection for automatic quality assessment in production

The locations of one or more production sites and of compute and storage resources site (in the following referred to as edge DC site) are important in this use case. The production sites may be different factory buildings on the same campus or geographically distributed sites. The edge DC may be located on-premise (On-Premise Edge), or off-premise e.g. in shared locations of colocation providers (Colocation Edge) or hosted by a CSP (Public Edge). A Transport Network provides data communication between the sites. Depending on the location of production and edge DC sites, urban or regional scenarios may apply with respect to the distances between the sites. Table 13 summarizes the maximum distances for the different scenarios. Due to the stringent latency requirements of the use case, and due to the cycle time constraints, the roundtrip Transport Network latency needs to be less than 1 ms. Thus, centralized DC locations, which may be located hundreds of kilometres away from the production sites, are not within the scope of this use case.

Table 13: Typical distances between production site and edge data centre locations

On-Premise Edge	Colocation/Public Edge	
	Urban	Regional
<10 km	<50 km	<80 km

7.7.2.1.2 Video Cameras

Currently video cameras for industrial applications provide resolutions greater than 1 Megapixel and support GiGE Vision® [i.4] and/or USB3 Vision™ [i.5] interfaces. These standards allow for precise synchronization and/or real-time operation of multi-camera systems, e.g. for 3D vision. To time synchronize the cameras, these standards use IEEE 1588 precise time protocol (PTP) [i.6]. The interfaces also provide power supply to the cameras, e.g. based on PoE in case of GiGE Vision®. The GiGE Vision® Control Protocol (GVCP) is used to establish reliable data connections over the User Datagram Protocol (UDP) between cameras and compute resource. The GiGE Vision® Stream Protocol (GVSP) specifies UDP for video streaming and includes the option to resend lost packets in order to avoid frame losses [i.4] Typical state-of-the-art cameras are able to utilize the complete bandwidth of the interfaces, i.e. 1 Gb/s in case of GiGE Vision® and 5 Gb/s in case of USB3 Vision™. The number of cameras per vision inspection station ranges from one to four, in order to cover the inspected parts from different angles. This means that the upstream aggregated data rate per vision inspection station ranges from1 Gb/s to 20 Gb/s. The data rates are asymmetric, since the downstream control signals have a comparably negligible data rate.

7.7.2.1.3 Video Analytics and Compute Resource Requirements

At the edge DC, the camera video streams are processed by AI-assisted video analytics solutions based on Machine Learning (ML). Training and inference of the ML models have different requirements concerning the available compute, storage, and network resources. Typically, supervised ML model training is performed offline. However, there are also cases where it may be necessary for the ML model to dynamically adapt to new patterns in the video data. This necessitates algorithms to handle real-time (online) or near real-time training of the models. These algorithms have been in use for other applications such as recommendation systems. For manual and semi-automatic AI annotation in supervised learning, the video streams are recorded and a subset of the recorded frames is used to generate labelled data sets for training. The privacy of these data sets is of utmost importance to enterprises as they contain valuable information on the production processes. A special case of training that takes into account these privacy issues is the distributed/federated learning paradigm. Distributed/federated learning enables enterprises with multiple geo-distributed production sites to train global ML models without transporting the data between locations. It can also act as an enabler for cross-enterprise collaborative training of ML models while guaranteeing the privacy of the data and minimizing data communication to centralized DC locations.

Inference of the ML models is generally performed online. The video analytics processing chain needs to be optimized for the lowest possible latency and highest possible reliability. Lossless and timely video frame delivery ensures correct identification of defective production parts. Therefore, the network needs to transport the video streams in real time from the camera to the processing unit at the edge DC location. Although state-of-the-art GPUs are capable of processing several video streams in parallel, there is a trade-off between the number of processed video streams and the complexity of the ML models with the probability for frame losses. Typically time-critical tasks are therefore overprovisioned, e.g. 1 GPU per camera or an average load of 50 %. Compared to that the compute resources for the control software stack are modest.

7.7.2.1.4 Industrial Ethernet over TSN Approach

This is a particular approach, which does not exclude other standards that could provide equivalent features.

For this use case isochronous communication, low latency and deterministic data exchange between cameras, data centre and actuators/robots is needed. Time Sensitive Networking (TSN) as described by a set of standards developed by the TSN task group of IEEE 802.1 [i.7], is considered as the data link layer technology in the framework of this use case. In particular, TSN provides a standard for timing and synchronization for time-sensitive applications [i.8] and profiles for industrial automation [i.9]. TSN also has the benefit that different traffic types may coexist, while timing requirements of real-time traffic are fulfilled at all times.

There are a number of real-time capable industrial Ethernet protocols, such as ProfiNET® [i.11], EtherNet/IP™, EtherCAT®, Sercos® III and Ethernet POWERLINK™. There are ongoing activities for integration with TSN. For example, ProfiNET® over TSN can scale in data rate from 10 Mb/s to 10 Gb/s [i.11], while traffic priorities are maintained.

ProfiNET® over TSN makes use of the following TSN features [i.11]:

- Time synchronization (IEEE 802.1AS [i.8]).
- Interspersing express traffic (IEEE 802.3br [i.33]).
- Frame replication and elimination for reliability (IEEE 802.1CB [i.34]).
- Enhancements for scheduled traffic (IEEE 802.1Qbv [i.35]).
- Frame pre-emption (IEEE 802.1Qbu [i.36]).
- Station and media access control connectivity discovery (IEEE 802.1AB [i.37]).

Based on these features and the wide adoption in ongoing joint standardization activities (in particular [i.9] and [i.11]), TSN is becoming the de-facto standard for industrial automation applications. Therefore TSN needs to be supported by the Transport Network that connects production sites to edge Cloud sites. However, this is not excluding other potential future standards that may evolve and provide the required features.

7.7.2.1.5 Automation Control Layer

The automation control layer leverages the Open Platform Communications Unified Architecture (OPC UA) [i.12], which provides a standardized information exchange in industrial communications, e.g. between machine-to-machine and between Information Technology (IT) and Operational Technology (OT). An OPC UA Server is used to communicate with the video analytics service and virtual Programmable Logic Controllers (vPLC), e.g. according to IEC 61131-3 [i.13]. The communication of the vPLC control signals between the control level and the field level equipment potentially leverages Industrial Ethernet over TSN in conjunction with OPC UA. This is described in the companion specification OPC UA for ProfiNET® [i.14].

7.7.2.2 Motivation

This use case demonstrates the trend towards the efficient implementation of industry 4.0. The edge/Cloud approach is more efficient and cost effective due to AI-based analytics. The F5G network connecting the production site to the data centre needs to provide significant data rates in the upstream direction over distances greater than a few hundred meters (see Table 13) which may rule out copper based solutions.

7.7.2.3 Pre-condition

To help achieve this use case the following pre-conditions are necessary to be in place:

- A data centre (e.g. on-premise edge or colocation edge) providing an edge/Cloud environment to run the video analytics and the virtualized control functions (vPLC).
- A real-time communication between the equipment on the factory shop floor and the data centre location where the edge/Cloud environment is running.

7.7.2.4 Operational flow of actions

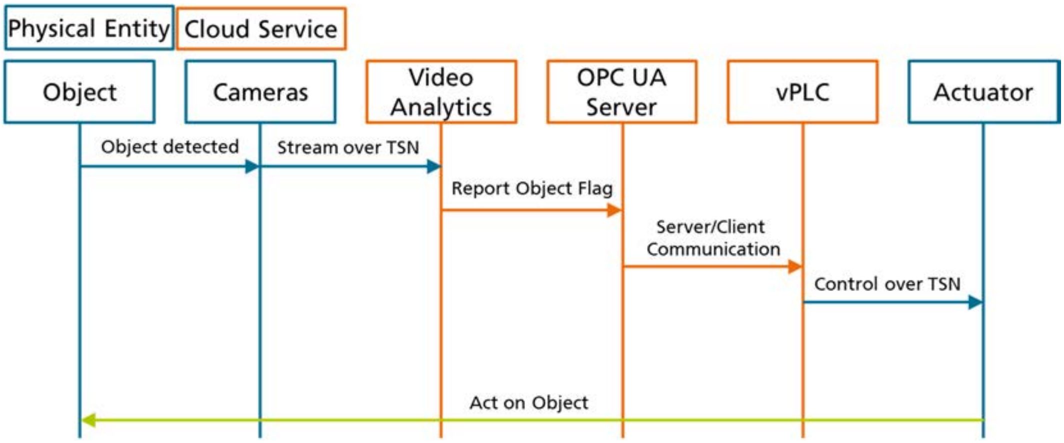


Figure 82: Operational flow of the edge/Cloud-based visual inspection

1) At the production line, the object is detected by the cameras, which are part of the visual inspection station.

2) The video streams are transported in real time e.g. over a TSN data link to the edge DC location where the edge/Cloud services are running.

3) The video analytics edge/Cloud service performs AI-assisted classification of the object's quality and reports to an OPC UA Server.

4) In case that insufficient quality was detected, a vPLC is activated by the OPC UA Server to take the required actions and send the necessary control signals e.g. via TSN to the physical actuator in the production line at the factory shop floor.

5) The actuator takes the necessary prescribed actions on the object and thus completes the control loop.

7.8 Use case #22: Edge/Cloud-based control of automated guided vehicles (AGV)

7.8.1 Use case context

An industrial communication use case is mobile robotics such as Automated Guided Vehicles (AGV). Digital production facilities will support on-demand product customization enabled by cost-efficient manufacturing of small lot sizes. AGVs, i.e. small mobile transport robots, are essential to distribute materials and production parts inside the factory and also between different buildings on an industrial campus. However, navigation in partially structured environments, such as factories, requires high computing power, which is a challenge to implement on battery-powered AGVs. Therefore, outsourcing the navigation and control algorithms to an edge/Cloud is an attractive solution. At the same time, Cloud-based navigation enables the exchange of captured maps between multiple robots and AGVs. This means that they can take current obstacles into account during path planning, for example, an aisle blocked by maintenance work.

7.8.2 Description of the use case

7.8.2.1 Overview

7.8.2.1.1 General

AGVs will play an increasingly important role in future factories as the workhorses for intra-factory logistics. However, reliable and secure navigation in complex environments requires high computation power (see note). Furthermore, AGVs need to be integrated in the flexible production processes, which support on-demand customization and thus fast reconfiguration of production processes and consequently supply lines. The navigation, guidance control system, and other services of the AGVs are moved to the edge Cloud. This removes the need for costly and power hungry computing resources on AGVs and extends their battery life. The move to Cloud technology enables the AGVs control and management system to interact with micro-service oriented control processes.

NOTE: Typically, navigation requires 16 CPU Cores, 32 GB RAM and 200 GB HD per AGV. For additional services such as object detection and localization an additional GPU is required.

Figure 83 provides an overview of this use case. AGVs perform transportation of goods, materials and other objects to and between robotic production cells. AGVs and robotic cells provide individual sets of micros services, which are hosted on an edge Cloud. These micro services can be flexibly chained into complex production processes by various process controllers. In particular, the navigation of the AGVs is performed on the edge Cloud by a guidance control system. The end-to-end roundtrip latency between AGV → edge data centre → AGV needs to be less than 30 ms including processing. The data rate for control messages is about 400 kbit/s per AGV, while transmission of video from the AGV to the Cloud may require 10 Mbit/s or greater.

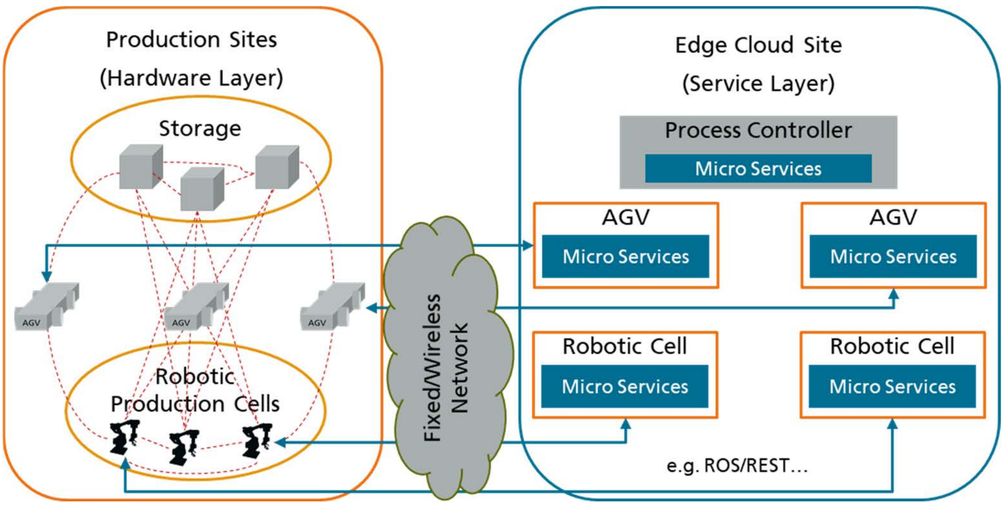


Figure 83: Overview of edge/Cloud-based control of AGV

The AGVs are communicating via a wireless network, while the robotic production cells are connected by a wired network with specific requirements (see clause 7.7). The wireless access points are connected by a wired network. In order to derive fixed network requirements, the wireless network options for this use case need to be discussed.

7.8.2.1.2 Wireless Network Options

The AGVs need a reliable wireless network to support their seamless mobility. Several standardization bodies have identified AGVs or in general mobile robots as an important use case for industrial scenarios. For example, the IETF has started a working group on Reliable and Available Wireless (RAW), which addresses Layer 3 aspects supporting applications needing high reliability and availability for different underlying wireless network technologies such as Wi-Fi® and 5G [i.16]. One of their use cases focusses on wireless for industrial applications [i.18].The relevant requirements for equipment and process control services and mobile robotics services are summarized in [i.18].

Three wireless network options are briefly discussed below.

1) 5G Campus Networks

For 5G networks, both 3GPP and 5G ACIA consider AGVs within the general use case of mobile robots [i.19] and [i.20] respectively. 5G ACIA classifies mobile robots and AGVs as a soft real-time use case, meaning that "Cycle times and latency are moderately critical, i.e. approximately one second" [i.20]. 3GPP deals with the use case of mobile robots (including AGVs) in more detail. In particular, three distinct communication cases are identified [i.19].

a) Communication between mobile robot and guidance control system.

b) Communication between mobile robots.

c) Communication between mobile robots and peripheral facilities.

Cases a) and c) are most relevant to this use case, since the guidance control system and the control systems for peripheral facilities (such as the robotic production cells) are located in the edge Cloud. The following table summarizes the requirements for the 5G network as specified in [i.19].

Table 14: Requirements for the 5G network as defined in [i.19]

Parameter	Value
Cyclic data communication service cycle time	10 - 50 ms
Jitter	< 50 % of cycle time
Data rate per mobile robot	> 10 Mbit/s (only for video streaming)
Communication service availability	> 99,9999 %
Max number of mobile robots	100

2) Wi-Fi® Access

Another option for industrial grade wireless networks are the current and upcoming generations of Wi-Fi®, namely Wi-Fi® 6 (IEEE 802.11ax) and Wi-Fi® 7 (IEEE 802.11be).

- Wi-Fi® 6 already implemented several functions, which are relevant for industrial deployment scenarios. For example, the Target Wake Time (TWT) feature enables longer runtime of battery-powered AGVs and at the same time enables planned access to the communication channel [i.21].

- Wi-Fi® 7 is expected to provide support on bounded latency and TSN features [i.22].

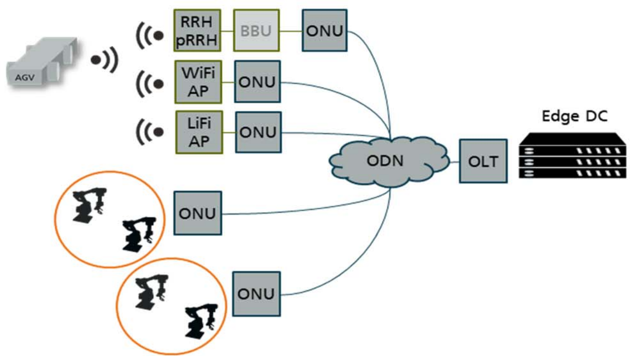
3) LiFi Access

A third option is LiFi, i.e. optical wireless communication, which has been proposed to meet the requirements of industrial wireless networks [i.23]. In particular, it may provide additional precise positioning information about the AGV to the guidance control system. The IEEE 802.11bb has specified industrial wireless as a usage model. The LiFi communication requirements are summarized in Table 15 [i.24]. However, LiFi performance depends on a Line of Sight (LoS) channel between the AGV and at least one LiFi access point. In an environment with lots of movement, such as on a factory shop floor, where LoS channels may be blocked, reliable communication with the AGV might be difficult to achieve. LiFi is considered an evolving technology and this problem might be resolved in the future.

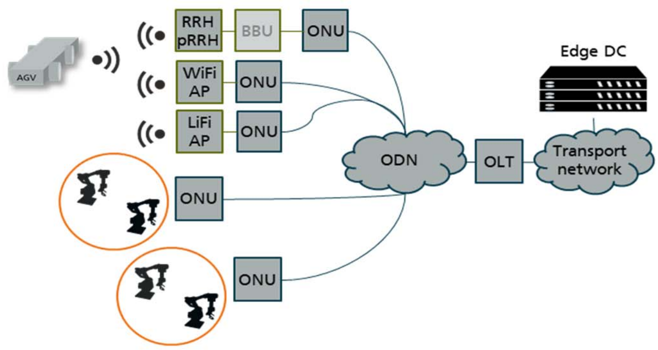
Table 15: LiFi communication requirements for industrial wireless usage model according to [i.24]

Parameter	Value
Distance to LiFi Access Point	< 20 m
Throughput	10 Mbit/s - 1 Gbit/s
Latency	< 1 ms

7.8.2.1.3 Deployment Scenarios



(a) on-premise edge



(b) A colocation/public edge

Figure 84: Possible deployment scenarios

Figure 84 shows two exemplary deployment scenarios based on Passive Optical Networks (PON) for this use case, differentiating between an on-premise edge in Figure 84(a) and a colocation/public edge in Figure 84(b). Typical distances for the two scenarios are available in Table 13 (clause 7.7.2.1.1). For the on-premise edge, PON as a Customer Premises Network (CPN) has to bridge distances of up to 10 km for large factory areas. In the colocation/public edge scenario, the PON CPN connects to a Transport Network to bridge distances to the edge data centre of up to 50 km (urban) or 80 km (regional). The latter scenario also applies to enterprises with several production sites, where only a subset of these sites may be equipped with data centres.

7.8.2.2 Motivation

The use case provides an application example, which is relevant to Industry 4.0. AGVs will play an increasingly important role in future factories. Moving the control system of the AGVs to the Cloud, makes them more agile and enables them to efficiently interact with the production processes.

To make this use case viable, it will depend on F5G network deployment. A high-quality connectivity is needed between access points of the industrial wireless network (which is used by AGVs for communication), the edge data centre site and the robotic production cells (which are usually connected by a wired communication network).

7.8.2.3 Pre-condition

The following are pre-conditions for this use case:

- There needs to be a deployed wireless network (e.g. 5G, Wi-Fi® or LiFi), which provides basic industrial wireless connectivity and the required specifications to support AGV use case.
- There needs to be a data centre (e.g. on-premise edge or colocation edge) providing an edge/Cloud to run the AGV control systems.
- There needs to be a real-time network between the equipment on the factory shop floor and the data centre location.

7.9 Use case #23: Cloudification of Medical Imaging

7.9.1 Use case context

The cloudification of medical imaging uses systems such as Picture Archiving and Communication System (PACS) or Radiology Information System (RIS). To ensure optimal experience, the imaging system requires high bandwidth, low latency, low packet loss rate, high security, high reliability, and flexible scheduling capabilities. This use case describes the key components, and service data flows in the Cloud-based medical imaging system.

PACS is a medical imaging technology, which provides storage and convenient access to images from multiple medical imaging equipment. Electronic images and reports are transmitted digitally via PACS. The universal format for PACS image storage, transfer, and management is the Digital Imaging and Communications in Medicine (DICOM) standard.

PACS consists of four major components:

- The imaging equipment such as X-ray plain film, Computed Tomography (CT) and Magnetic Resource Imaging (MRI).
- Secured network for the transmission of patient information.
- Workstations for interpreting and reviewing images.
- Archives for the storage and retrieval of images and reports.

7.9.2 Description of the use case

7.9.2.1 Overview

7.9.2.1.1 General

The migrating of medical images to the Cloud allows for remote access, and all-round PACS services for medical institutions. It also allows for resource sharing needed for AI-based image processing. Figure 85 gives a high level overview.

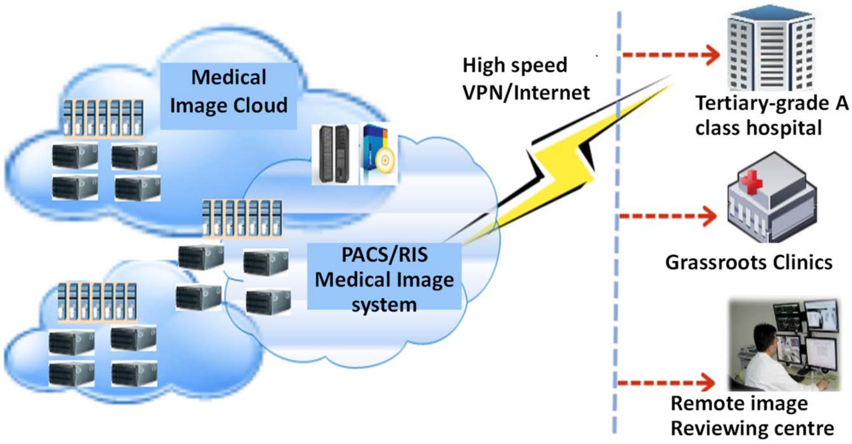


Figure 85: Medical image migration to the Cloud

This migration provides a wide range of applications such as medical image data storage, image retrieval via a doctor's desktop and mobile terminals, diagnosis and treatment assistance, and training material for medical institutions.

7.9.2.1.2 Key components and data flows

Figure 86 illustrates the key components (A1 to A4), networks (N1 to N2) and the main data flows (F1 to F3) involved in the Cloud-based medical imaging. Different imaging types generate different size image data. Patient's image data can be as large as 2G Bytes.

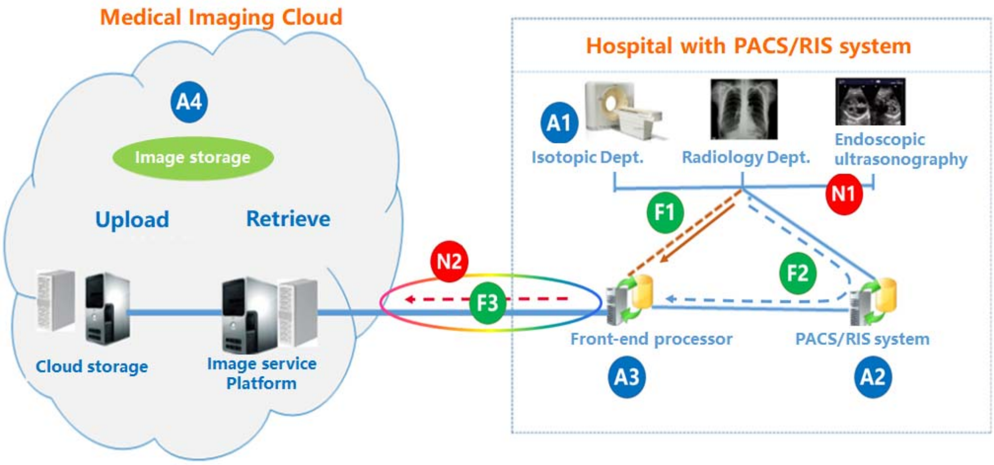


Figure 86: Key components, networks and data flows in the Cloud-based medical imaging

1) Key components

The followings are the key components in the Cloud-based medical imaging:

- A1- Image terminal: It generates image data in either DICOM or non-DICOM format. Non-DICOM format is converted to DICOM format by the front-end processor before upload to the medical imaging Cloud.
- A2- Medical imaging system: It is an IT system that stores medical image data locally in the hospital.

  NOTE: In the case of highly reliable Cloud-based system with low latency, secure and reliable access to the Cloud, the medical imaging system can be replaced by direct access to the Cloud services.

- A3- Image Cloud front-end processor: It processes the local image data before upload to the image Cloud. The front-end processor mainly performs the following functions:
  - Image transmission and backup
  - Providing a temporary local PACS for the hospital when the Cloud PACS network has a fault
  - Non-standard DICOM image conversion
- A4- Medical imaging Cloud: It is a data centre where compute and storage servers are deployed to provide Cloud storage and retrieval services.

2) Networks

The followings are the networks involved in the Cloud-based medical imaging:

- N1 network: It is a hospital campus Local Area Network (LAN) with a coverage area of several km^2 and provides communication service within the hospital.
- N2 network: It is the hospital cloudification network, which connect the image Cloud front-end processor and image Cloud. N2 Network is either owned by the hospital itself or provided by a network operator.

3) Main Data Flows

- The followings are the main data flows in the Cloud-based medical imaging:F1 data flow: For hospitals without local medical image storage systems, the data flow generated by image terminals is sent directly to the front-end processors deployed in hospitals.
- F2 data flow: For a hospital that has a local medical image storage system, the data flow generated by the image terminal is first stored in the local medical image storage system. Then the data is sent to the front-end processor deployed in the hospital.
- F3 data flow: After local image data is processed by the front-end processor in the hospital, the image data is uploaded to the medical imaging Cloud deployed outside the hospital.

7.9.2.1.3 Data Security

In addition to the security provided by PACS, consideration needs to be given to data and communication security. The hospital campus communication system is LAN based and the internal link data security needs to be considered. The connection from the Front end processor to the Data centre may also need data level and or link level security.

7.9.2.1.4 Flexible Bandwidth allocation

Hospital have regular visit from non-resident specialist consultants. These consultants move from hospital to hospital on a regular basis. These onsite visits can increase the demand on Cloud service for the duration of their visit. This will necessitate a temporarily increase in bandwidth to meet the additional Cloud data access of patients image data. This additional bandwidth is only required for the duration of the visit and the available bandwidth needs to return to normal once the visits are over to keep hospital IT cost down. This technique can be referred to as "bandwidth calendar", see Figure 87. This means the network service provider or operator need to support flexible bandwidth allocation to match the needs of the Hospital.

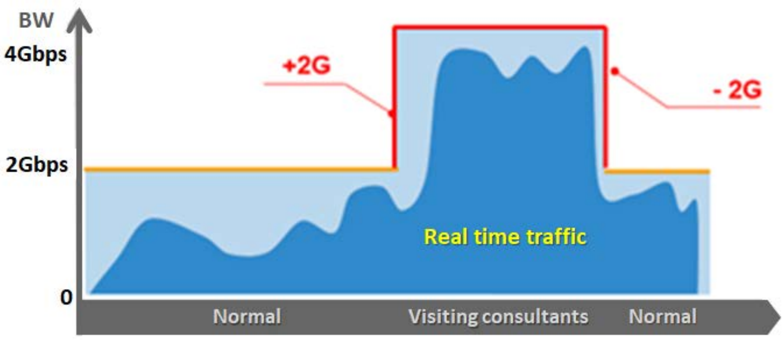


Figure 87: Bandwidth calendar for medical image access to the Cloud

DICOM is a TCP/IP-based application protocol, so network link quality, especially the packet loss rate and delay, impedes transmission efficiency of medical image data. The DICOM protocol stack is shown in Figure 88.

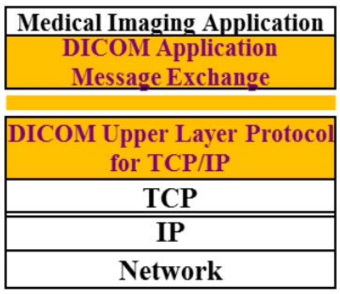


Figure 88: DICOM protocol stack

Digitalized medical images require high accuracy and need to meet the diagnostic-level image quality requirements. To ensure the quality of medical images, it is recommended that the image data should not be compressed for transmission and storage. Therefore the network bandwidth and storage requirements are high. Medical image classification, characteristics, and experience evaluation criteria are shown in Table 16.

Table 16: Medical Image Classification Table

Image Type	Image characteristics	Image operation	Experience evaluation criteria
CR/DR	• 16 MB per file • Typically 2 image files per patient • The image gray level is extremely detailed.	• Image reading • 2D image processing	• Image reading: second-level viewing of a single image/second-level opening of a single image; First video display time; Initial image file cache time and image cache rate • 2D image processing: operation response time and frame freezing • The gray scale definition cannot be determined by naked eyes. The first screen time is not concerned.
CT	• 512 KB per file • Each patient has hundreds to 1 000 image files, • Image size of 100 MB to 1 GB.	• Image reading • 2D image processing • 3D image post-processing	• Image reading: second-level viewing of a single image/second-level opening of a single image; First video display time; Initial image file cache time and image cache rate • 2D image processing: operation response time and frame freezing • 3D image post-processing: operation response time, and whether frame freezing or mouse drift occurs when the mouse is moving.
MRI	• 512 KB per file • Each patient has hundreds to 1 000 image files, • Image size is about 100 MB to 1 GB.	• Image reading • 2D image processing • 3D image post-processing	• Image reading: second-level viewing of a single image/second-level opening of a single image; First video display time; Initial image file cache time and image cache rate • 2D image processing: operation response time and frame freezing • 3D image post-processing: operation response time, and whether frame freezing or mouse drift occurs when the mouse is moving.
DSA	• Large single file, up to 10 GB • An image file contains multiple sequences. • Each sequence supports animation playback and frame-by-frame viewing.	• Viewing an Image Frame by Frame • Animation Play	• Frame-by-frame image viewing: second-level video viewing and first video display completion time; Initial cache time of image files; Image cache rate • Animation playback: no frame freezing occurs.

Image Type	Image characteristics	Image operation	Experience evaluation criteria
PET-CT	• Single file size similar to CT image file, 512 KB • The number of image files per patient is large, • Total image size is larger than 2 GB.	• Image reading • 2D image processing • 3D image post-processing • image fusion post-processing	• Image reading: single-picture viewing time; Initial loading time of the first screen; Image file cache time; Image cache rate • 2D image processing: operation response time and frame freezing • 3D image post-processing: The initial loading time, operation response time, and mouse movement are not affected. • Post-processing of image fusion: initial loading time, operation response time, and whether frame freezing and mouse drift occur when the mouse is moving. • Video playback: whether the video is frozen.

Given a certain medical image data size, the network bandwidth directly affects the transmission efficiency of the image data to and from the Cloud. Network degradation, such as network packet loss and higher network latency, will delay image transmission, and prolong transmission time, and will diminish image processing experience to and from the Cloud.

Depending on the size of the imaging department and the number of medical personnel in the hospital, the number of patients that the hospital can processed will vary with the size of the hospital. Table 17 lists some suggested network bandwidths for hospitals of different sizes to access the imaging Cloud.

Table 17: Network bandwidths of hospitals with different scales

Hospital Size	Daily outpatients/patients	Image and image reading terminal in the hospital	Network bandwidth for image storage to the Cloud/Mbit/s
Large hospital	20 000	2 000	15 840
Medium-sized hospital	7 000	800	6 336
Small hospital	1 000	100	792

7.9.2.2 Motivation

The medical image Cloud provides medical imaging services. The main features of the medical imaging service are data collection, conversion, integration, storage, back up, archiving, verification and access control.

Medical image Cloud provides services for remote consultation, specialist imaging diagnosis, image teaching, mobile image reading/consultation, and image big data analysis services. These services enable medical personnel to quickly query and search medical records, improving their work and scientific research efficiency.

The medical image Cloud provides necessary resources for AI-based image analytics.

7.9.2.3 Pre-conditions

1) The IT application systems of medical institutions have been deployed on the Cloud and provide access channels for various end users.

2) The network between medical institutions, healthcare image Cloud, and end users is in operation and can be accessed.

3) The management and control system has been deployed to manage related devices.

After the above mentioned pre-conditions are met, medical imaging Cloud access private line services can be quickly provisioned, e.g. within days.

7.10 Use case #24: F5G for Intelligent Mine

7.10.1 Use case context

The traditional mine production uses Ethernet switches to provide the communication networks for services such as video backhaul, remote control, security surveillance, and personnel positioning data backhaul in the underground mines. This network typically uses multiple aggregation switches in a ring topology with multiple cascaded 100 M/Gigabit switches. This ensures all end devices are connected.

The current mine production networks have following shortcomings:

1) Aggregation switches are usually deployed in explosion-proof boxes. According to some mine safety regulations (e.g. in coal mine regulation), explosion-proof boxes cannot be deployed in fully-mechanized tunnels with high gas concentration, consequently network services are unavailable. In areas where explosion-proof boxes are allowed, they will be powered-off, when the surrounding gas concentration increases. This will cause network interruptions. The explosion-proof box is large and heavy, and the installation and deployment are difficult and costly.

2) Multi-level cascaded gigabit/100 M access switches have a large bandwidth convergence ratio, which does not meet the increasing bandwidth requirements for intelligent mines. In addition, network congestion and non-deterministic delays are becoming more problematic. These access switches are usually unmanaged, which makes it difficult to remotely monitor and diagnose network failures.

3) When the aggregation or access switches fail, the service in the cascaded access switch chain will also be interrupted. Access switches usually do not support dual-path optical fibre redundancy protection.

4) The deployment of downhole optical fibre networks is provided by a large number of high-temperature fibre splicing operations, and this has a safety risk for potential accidents.

5) The underground optical fibre network is complex. When the optical fibre network fails, the operation and maintenance personnel need to go underground to locate the fault. Therefore, the optical fibre network operation and maintenance efficiency is low.

In order to solve these shortcomings, some mining companies are starting to deploy F5G industrial optical ring network solutions based on PON technology. The deployment of anF5G PON can simplify the mine network topology by significantly reducing the number of active network nodes and potentially enhancing safety. This network provides high reliability, low latency, and easy maintenance. F5G will support the acceleration of intelligent processes for mine production.

7.10.2 Description of the use case for the mining industry

7.10.2.1 Overview

In order to meet the special requirements of the mine industry networks, the mine ODN usually deploys a ring network topology to improve network reliability. This kind of network is called Industrial Optical Ring (IOR). The mine network is usually composed of three parts as shown in Figure 89:

- Optical Ring Head (ORH) equipment.
- Optical Ring End (ORE) equipment.
- Optical Ring Passive (ORP) network.

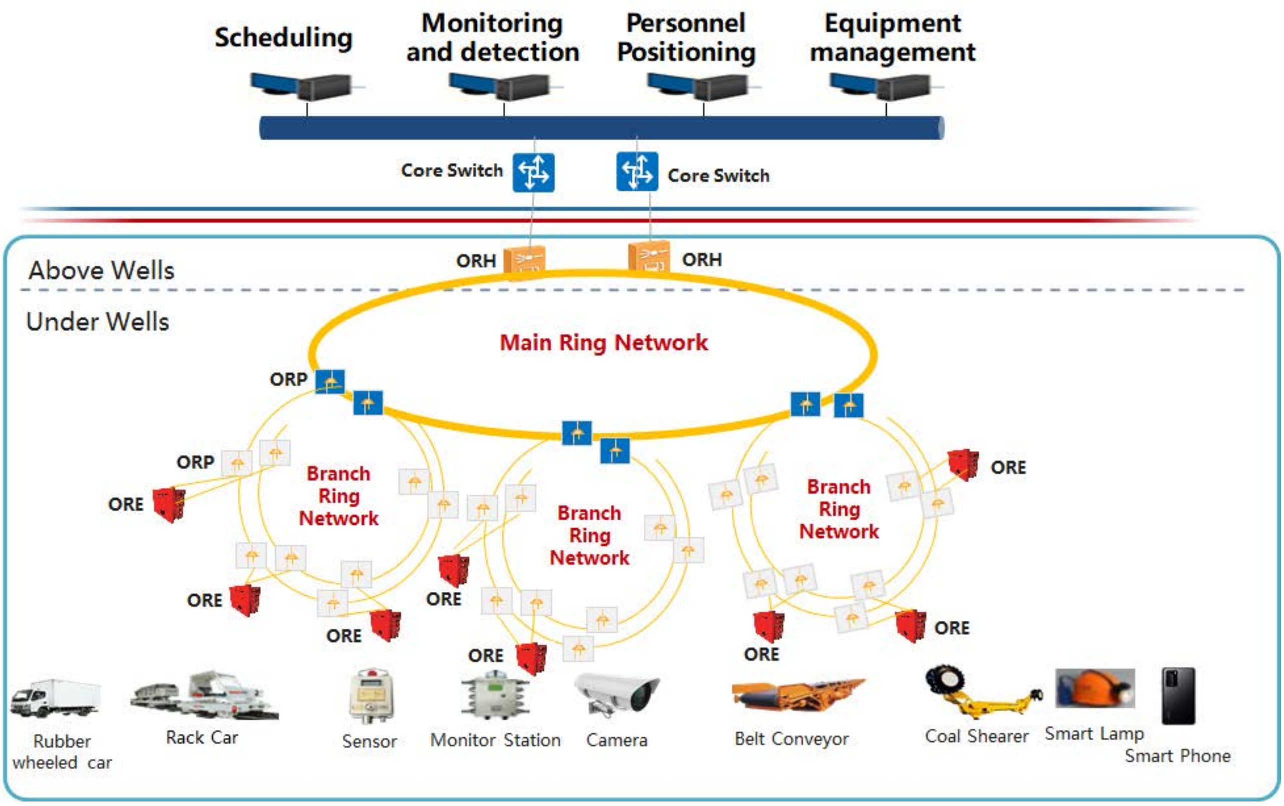


Figure 89: F5G IOR (Industrial Optical Ring) Network Topology

It can be seen from Figure 90 that ORP and ORE in the F5G industrial optical ring network replaces the aggregation and access switches in the traditional solution. ORH connects up to the core switch (this connection is only shown in Figure 89). The ORH and ORE support Ethernet or IP addressing schemes. The user side (ORE) provides Ethernet interfaces and Wi-Fi® while the network side (ORH) provides Ethernet interfaces.

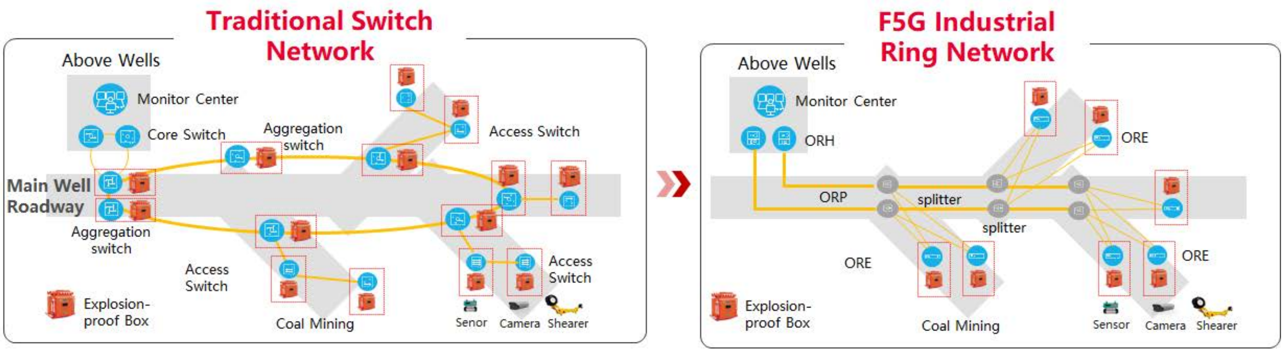


Figure 90: F5G Industrial Ring Network and traditional Switch Network Comparison

The F5G IOR network needs to meet the following requirements for the mine production networks:

1) Electric safety: Based on a passive optical network architecture, the aggregation switches are replaced by ORP equipment. The ORP need to be made of anti-static and flame-retardant materials that meet the mine safety regulation requirements. Compared with the traditional network solutions, ORP saves the use of explosion-proof equipment and explosion-proof boxes. ORE can adopt explosion-proof and intrinsically safe circuit design (Intrinsically safe circuit means the circuit itself will not produce sparks). Intrinsically safe ORE can be deployed in areas of high gas concentration such as fully mechanized mining interfaces and heading interfaces in mines, effectively reducing the risk of underground sparks.

2) High network reliability: Each ORE in the F5G IOR network is connected to two independent ORPs. Each ORP is directly connected to an ORH above the wells with dual optical fibre redundant protection. This kind of network topology is highly resilient to multi-point failures, and the network failure self-healing time is less than 30 ms, which meets the requirements of the mining industry.

3) Construction safety: To avoid the high-risk of fibre fusion under the well, the F5G IOR network can use pre-connected optical components, which are manufactured in the factory. This enables the plug and play of optical fibres on site, improving the safety and efficiency of the underground optical fibre deployment.

4) Maintenance security: F5G IOR network uses a PON centralized management architecture. The ORE operating status and traffic statistics can be monitored in real-time by the network management system. This can improve the maintenance efficiency of the underground network. The F5G intelligent optical fibre diagnostic technology supports remote fibre fault localisation within minutes in the well. It improves fibre repair efficiency under the wells.

5) High-bandwidth/high-quality network: F5G IOR network uses 10G PON technology and can evolve to higher PON rates. The ORE can support at least 10 Gigabit access uplink (for evolved PON) meeting the requirements of the mining industry for a high bandwidth network and long-term evolution. The OREs are connected to the ORHs through fibre, so the network latency is less than 5 ms.

There are three typical application scenarios in the underground mine environment for F5G industrial optical ring network: video surveillance network, production control network and safety monitor network.

1) Video surveillance network scenario

Video surveillance is widely used in underground mine workplaces. With the continuous development of the intelligent construction in mines, the importance of video surveillance increases. The main locations that need to transmit video in underground mines include: the belt conveyor (head, middle and tail), the material drop point, the material receiving point, the power distribution rooms and points, the pump room, the drainage point, and the gas drainage drilling yard (front, middle, and rear), mining face mounted video, on board video of mining machine, on board video of inspection equipment such as robots, intelligent recognition of important areas in underground sites, and other application scenarios.

F5G IOR can provide a reliable transmission network for video surveillance services, as shown in Figure 91. ORE can have built-in Wi-Fi® APs for data transmission of Wi-Fi® cameras.

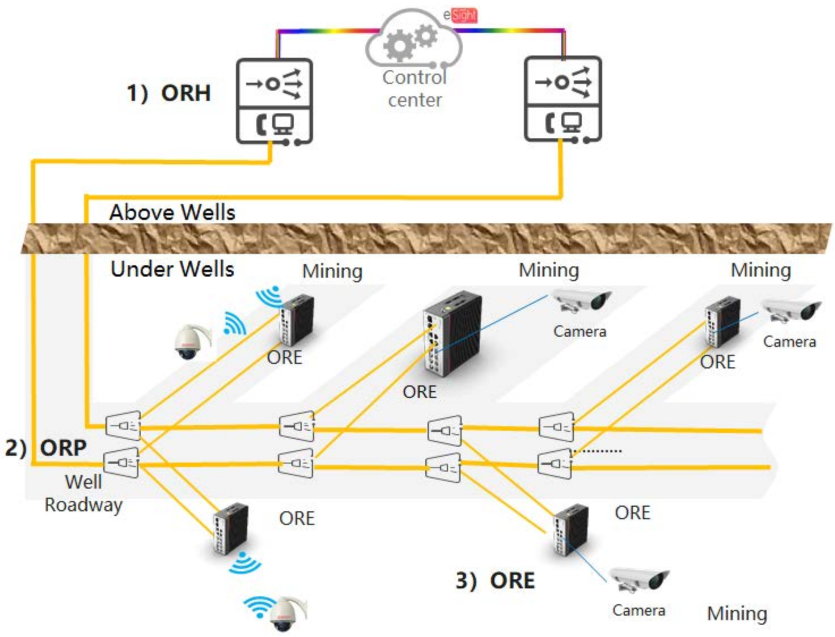


Figure 91: F5G IOR Video surveillance network

2) Production control network scenario

There are several underground areas, such as the mining face (material shearer, hydraulic support, and road header), the substation, the water pump room, the belt conveyor, etc., that need monitoring and control. They all need to connect to the remote, centralized control system via a reliable network.

F5G IOR can provide a reliable transmission network for the production control system. Figure 92 shows the production control network access terminal equipment. The ORE needs to support GE (Gigabit Ethernet) interface, industrial RS232/RS485 interface and an industrial controller gateway or controller docking station. In addition, the ORE need to provide open resources to support third-party APP customized development to realize the functions of industrial gateways.

The production control network needs to ensure low latency, low packet jitter, low packet loss ratio and high bandwidth. These are essential for the compliant transmission of industrial protocols (such as EtherNet/IP™ or ProfiNET®). Therefore, the F5G IOR needs to support QoS for the complete production control network.

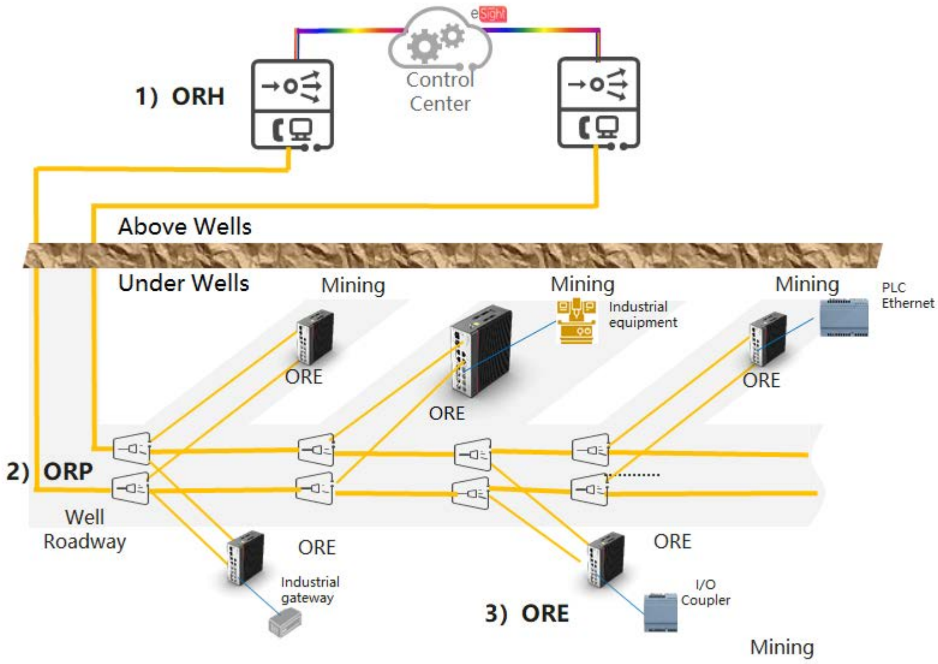


Figure 92: F5G IOR Production Control Network

3) Safety monitor network scenario

The mine safety monitoring system is mainly used to monitor methane concentration, carbon monoxide concentration, carbon dioxide concentration, oxygen concentration, hydrogen sulphide concentration, mine dust concentration, wind speed, wind pressure, humidity, temperature, power supply status, damper status, air duct status. The system is used to start and stop the fans, etc. The system also needs to generate the methane over-limit sound, light alarm, power outage, and methane wind power lockout control. In addition, F5G IOR needs to ensure the independence of the security monitoring network from other network resources. F5G network slicing could achieve that.

Many mining industries can benefit from this type of solution. Certain aspect might only be relevant in particular cases such as, coal mining regulations.

7.10.2.2 Motivation

10G PON technology has been widely used worldwide for a large number of telecommunication users. It has the advantages of being a mature technology, having a simple topology, high reliability, and with strong economic benefit. These advantages make 10G PON technology a preferred choice for the construction of industrial production networks (such as intelligent manufacturing and intelligent mines).

10G PON technology, combined with the F5G IOR network architecture, can effectively improve the underground network electrical, production, construction, and maintenance safety, while providing network services with large bandwidth and low latency.

10G PON network, combined with network slicing, can be used to meet the requirements of underground video transmission, remote control, safety monitoring, personnel positioning and other services. These services can operate independently of each other, improve production efficiency and quality, reduce costs, and enhance the production management and intelligence level.

7.10.2.3 Pre-condition

Several preconditions for the application of F5G industrial optical ring network solutions in mines:

1) F5G industrial optical ring network equipment has passed the mine safety certification.

2) Deployment of the ORP.

7.11 Use case #25: Enhanced optical transport network for Data Centre Interconnections

7.11.1 Use case context

Cloud services are usually supported by multiple interconnected Data Centres (DCs). These DCs need Data Centre Interconnect (DCI) with stringent requirements on capacity, latency, reliability and flexible scheduling. This use case describes the application and capabilities of advanced optical network for DCIs.

Figure 93: Simple view of DCI

7.11.2 Description of the use case

7.11.2.1 Overview

7.11.2.1.1 General

Cloud infrastructure consists of the following concepts:

1) Data Centre (DC): A DC is a physical facility consisting of multiple bays of interconnected servers (server farm), that performs computing, storage, and communication needed for Cloud services. Infrastructure-as-a-service may be deployed in both public and private Clouds, where virtual servers and other virtual resources are made available to users on demand and by self-service.

2) Point of Delivery (PoD): A PoD is located on a Layer 2 network used to differentiate virtual resource pools (including computing, storage, and network resources). A PoD only resides in one DC, however a DC may have multiple PoDs. Intra-DC connection between PoDs is outside the scope of this use case.

3) Availability Zone (AZ): An AZ is a logical Data Centre in a region and consists of multiple discrete data centres with redundant and separate power, networking, and connectivity to provide highly available, fault tolerant, and scalable Cloud services. There are typically 2~5 AZs in a region of a public Cloud. Inter-AZ connections refer to intra-city or adjacent city DCs connections that are within 100 km of each other.

4) Region: A region is a geographic area within a Cloud infrastructure that contains multiple data centres. In public Cloud infrastructure, a region can cover multiple provinces or even multiple countries. In a private Cloud infrastructure, a region may cover just one DC or a few DCs within a short distance (e.g. tens of kilometres) of each other. Inter-region connections refer to connections between large regions that are greater than 100 km apart.

7.11.2.1.2 AZ DCI

One typical scenario for AZ interconnection is the Intra-city DCs, which communicate with each other via the intra-city DCI network to meet the high availability requirements. The active-active and Virtual Machine (VM) migration services, which require low latency are provided by the intra-city DCI network. The intra-city DCI network supports the public and/or the private Cloud services, such as video, games, desktop Cloud, and Cloud Internet cafe services. To ensure low latency, intra-city DCI network is deployed in the same city or adjacent cities. The distance is typically less than 100 km and more likely to be less than 50 km. One city may have several large DCs.

Ideally, DCs are interconnected through Layer 3 switches or routers with full mesh connectivity. However, due to optical fibre resource limitations, the physical topology may be a ring or a chain.

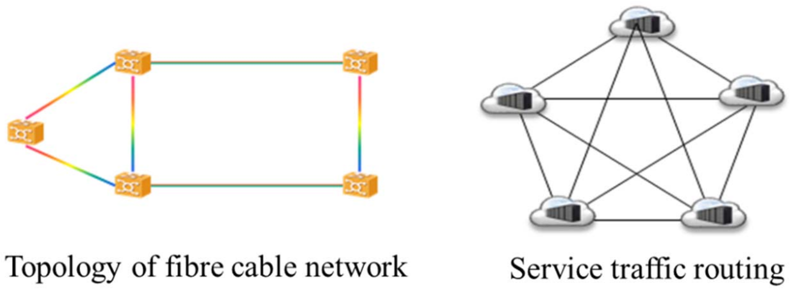


Figure 94: Ideal Router connectivity verses Physical Fibre topology

The active-active, synchronization, VM migration operations, disaster recovery and backup services between intra-city DCs require tens of terabytes/second transmission capacity. Due to insufficient optical fibre resources and the high costs associated with deploying new fibres, the single fibre transmission capacity need to be enhanced.

The service response time and storage performance between DCs are closely related to latency, lower latency leads to higher performance. Adjacent DCs need to be located as close as possible to each other, and the processing latency needs to be as low as possible. Table 18 describes the impact of latency on the reading/writing performance in an active-active storage system.

Table 18: Impact of latency on the reading/writing performance in RAC active-active storage

Distance between DCs	Latency constraint of I/O	Max. reading/writing performance
Local < 500 m	0,4 ms	100 %
25 km	0,8 ms	90 %
50 km	1 ms	55 %
100 km	1,5 ms	53 %

7.11.2.1.3 Region DCI

A region generally covers a cluster of cities in a large metropolitan area. A large amount of data is exchanged between DCs across regions.

A remote DC located in a low cost rural region can provide remote disaster recovery and backup, for example, backing up data from a large city DC. Some services, such as a commerce services, have no stringent latency requirements. However, to improve interaction efficiency as well as service experience, the latency is still expected to be as low as possible. Figure 95 shows the service flow between the remote DCs and the large city DC cluster.

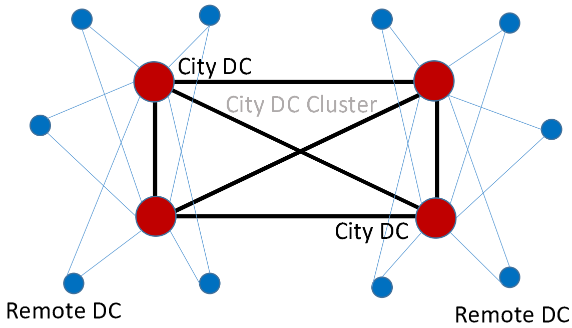


Figure 95: Service flow between the remote DCs and the large city DC cluster

Because the backbone optical fibre network is difficult to deploy, each physical site has around three to four optical fibre directions. It is not always possible to realize full mesh connectivity by having direct optical fibre connections among all the DCs, so one optical fibre may need to transmit services for multiple destination DCs.

The transmission distance between DCs ranges from hundreds of kilometres to thousands of kilometres. For services with short transmission distances, optical-layer grooming is used to reduce the number of switching nodes within the transmission system. For services with long transmission distances, electrical-layer grooming is used to increase the transmission distance and reduce wavelength conflicts.

Cross region DCI transmission capacity between large cities can exceeds 20 Tbit/s, and the transmission capacity between remote DCs and DCs in large cities can reaches hundreds of Gbit/s. In both cases the network capacity and single fibre transmission capacity is high.

The transmission distance between regions is large, typically greater than 1 000 km, so repair of backbone optical fibre can takes a long time when a fault occurs. Multiple optical fibres may suffer service disruption at the same time.

Virtualized computation has different traffic patterns and the Cloud infrastructure needs to perform different tasks depending on the time of the day (such as backups, large volume data synchronization, scheduled migration of workloads for upgrading, etc.). This means that the network services need to flexibly adapt to traffic demand changes.

7.11.2.1.4 Summarized DCI needs

Inter-DC needs full optical interconnection to meet the high-speed interconnection requirements between DCs. DCI is required to meet service requirements such as:

- Active-active operation: Active-active operation needs at least two data centres. Each DC serves as an active site of the other. This means the application continues to be accessible even if parts of the network or servers fail unexpectedly.
- Remote storage: Remote data storage provide reliable, secure, redundant, connectivity and space for storage of important data.
- VM (Virtual Machine) migration: VM migration is the process of moving a running virtual machine or application between different physical machines without disconnecting the client or application. Memory, storage, and network connectivity of the virtual machine are transferred from the original guest machine to the destination machine.
- Disaster recovery and backup: Disaster recovery is the plan and process for quickly restabilising access to applications, data and resources after an unexpected outage. Backup is the process of making an extra copy of data.

These services require high-capacity and low-latency communications, and improved availability to meet high reliability requirements.

7.11.2.1.5 Suggested optical network enhancements

From the preceding discussion, the optical Transport network need to be enhanced to provide the following DCI capabilities:

1) Higher single-wavelength data rate: The single-wavelength data rate for intra-city DCI is desired to be between 400 Gb/s and 800 Gb/s in order to meet the ultrahigh capacity requirements.

2) Ultra-long-haul transmission distance: It is desired to realize transparent optical transmission distances of greater than 1 500 km for inter-region DCI to remove the latency, power consumption and cost associated with optical-electrical-optical conversions.

3) Large single-fibre transmission capacity: The single-fibre transmission capacity can reach 48 Tbit/s for intra-city DCI. To achieve high single-fibre transmission capacity, spectrum expansion need to be considered. Figure 96 shows an example on how to achieve high single-fibre transmission capacity by using the super-C-band with 6-THz spectral bandwidth, which is 25 % greater than the extended-C-band with 4,8-THz spectral bandwidth. The allowed 50-GHz-spaced dense wavelength-division multiplexing (DWDM) channels are increased from 96 to 120.

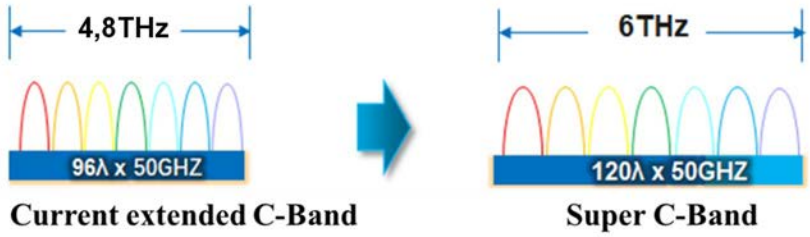


Figure 96: Spectrum expansion by considering super C-Band and extended C-Band

4) Optical-layer wavelength-level grooming: Large service nodes need to support simultaneous grooming of multiple optical directions with high capacity. OXC (Optical Cross-Connect) can be used to support optical-layer wavelength grooming without electrical-layer switching, effectively reducing latency, electrical-layer switching costs, and power consumption. Advanced OXC techniques can be applied to improve integration density and achieve "zero" manual fibre connections to save site space and reduce operating cost.

5) Low latency and jitter: The optical fibre transmission latency can be reduced by using optical-layer switching instead of electrical-layer switching whenever possible. The processing latency and jitter need to be managed so that it is low, predictable and measurable.

6) High reliability: It is essential to support highly reliable DCI for Cloud services. With advanced optical Transport network protection and automatic recovery technologies, services can still run properly even when multiple fibre cuts occur in the DCI network.

7) High flexibility: Since the traffic patterns and matrices might change a lot depending on the workloads and operational task, the change of bandwidth and traffic might need to be flexibly allocated.

7.11.2.2 Motivation

All optical interconnection between DCs have the following benefits by using technologies such as ultra-large single fibre transmission capacity, ultra-long-haul transmission, OXC-based wavelength-level grooming, and protection restoration.

- Low cost: High-speed lines effectively reduce the cost per bit. Spectrum expansion technologies improve single fibre transmission capacity and reduce investment in optical fibre and auxiliary facilities. OXC-based wavelength-level grooming reduces electrical-layer grooming costs at intermediate nodes.

- Low latency and jitter: The optical layer is directly connected, and the shortest route is selected for transmission. In addition, the WDM network enables low latency and jitter, meeting the stringent latency and jitter requirements for DCI.

- High reliability: Multiple optical-layer and electrical-layer protection, rerouting and restoration mechanisms are used to achieve high reliability of services, and in turn improves the reliability level of services between DCs, and increase the availability.

7.11.2.3 Pre-conditions

Once these preceding conditions are met, inter-DC services can be quickly provisioned, e.g. within days.

- Optical cross-connection, grooming devices and OTN/WDM devices are pre-deployed in the DC.
- Optical-layer links between DCs are available.
- The management and control system has been deployed to manage related devices.

7.11.2.4 Operational flow of actions

The processes of provisioning inter-DC optical interconnection services are as follows.

1) The DCI network provider completes the optical-layer network design based on optical fibre availability and status.

2) The DCI network provider designs and provides the optical layer protection and electrical-layer protection based on the fibre fault rate and inter-DC service reliability requirements.

3) The management and control system delivers services with different SLA requirements on demand.

7.12 Use case #26: Enhanced Point to Point optical access

7.12.1 Use case context

Optical Access Networks use either Point to Multi-Point (based on TDMA PON) or Point to Point interfaces. All these interfaces may be supported on the Optical Line Terminal (OLT) shelf with dedicated cards and ports. The focus of this use case is on the OLT uplink Point To Point (P2P) connection to the Aggregation edge node and for access connection to customers such as enterprises, and mobile antennas. The existing OLT P2P market is focused on mobile backhaul (OLT linked to cell site gateway) and business (OLT linked to business gateway). Another promising market could be the mobile fronthaul (Digital Unit (DU) linked to Radio Unit (RU)) through an OLT. With the evolution of bit rate and power reduction of P2P interfaces, the existing interfaces should be upgraded and replaced.

7.12.2 Description of the use case

7.12.1.1 Overview

7.12.2.1.1 General

A variety of P2P transceiver module types are used today for the pluggable form factors (like SFP, SFP+, SFP28, XFP and QSFP, QSFP+, QSFP14, QSFP28, CFP, CFP2, etc.). Each transceiver is associated with a unique interface name and port number. Concerning the last mile fibre connectivity network (fixed Access Network to reach antennas), a BiDi (Bidirectional - a single fibre in single-mode) transceiver is the preferred fibre approach. The BiDi transceiver simplifies operations, reduces cost, reduces fibre cable dimensions, and potentially reduces path delay asymmetry. The interoperability between the transceiver at the customer site and the OLT needs to be guaranteed to ensure a multi-vendor supply chain.

7.12.2.1.2 Supervision

The operational expenditure for the transport medium and related equipment needs to be considered. The purpose of supervision is to reduce the operational expenditure of the transport systems, without significantly increasing the capital expenditure, by including as much test and diagnostic capability as possible. Naturally, this should be achieved without compromising the service available bandwidth. Therefore test and diagnostics need to be non-service affecting. Currently, all transceivers or optical interfaces include RSSI (Received Signal Strength Indication) for optical line supervision. The resolution, accuracy, repeatability and response time of this metric is needed to increase the performance of the network supervision algorithms.

The ability to reliably differentiate between optical medium and equipment electrical faults and to determine if the faults are associated with the optical medium or the electronics is a key operator requirement. Error inference can usually be made from the presence (i.e. power or equipment failure), or absence (i.e. fibre failure), of the Dying Gasp alarm.

Several key points of supervision including suggested improvements are summarized as follows:

- Optical medium monitoring/checking: monitoring and on-demand checking of the optical medium health independently from a transport system is important to differentiate optical medium failures from transport system failures. It is desirable that such monitoring and checking is available regardless of whether the transport equipment (e.g. an antenna site) is in service or even connected. Several implementations could be considered:

  - The optical monitoring solution as proposed by Recommendation ITU-T G.697 [i.15] to detect anomalies, defects, degradation and faults affecting the quality of the optical Transport.

  - The use of an Optical Time Domain Reflectometer (OTDR), which is a powerful tool for diagnosing such faults in the optical medium.

  - Power meter and light source can also be used to aid in this monitoring process.

    Research is ongoing in several demarcation devices to further improve the optical medium monitoring and checking.

- Transport system would benefit from the ability to automatically and autonomously detect and locate optical medium faults (optical medium segments: patch panel at the hub or antenna site, optical fibre cable in ducts or on the poles, etc.).

- End-to-end performance monitoring up to the Ethernet layer: end-to-end performance monitoring enables operators to diagnose and determine where traffic may have been dropped or throttled. Higher layer tools, such as Ethernet performance monitoring, need to support the capability of monitoring and verification of ingress and egress traffic flows in Transport Network elements.

- Proactive versus reactive repair: transport systems with their monitoring and control systems will allow operators to use either proactive or reactive fault repair. It is of course up to the operators to decide how to use the transport status reports.

Key performance indicators of optical transport supervision could be made available to a network orchestrator via a layer of abstraction.

7.12.2.1.3 Point to point link reach

Consideration need to be given to the fact that the OLT is localised in a central office. The coverage of this central office is defined by the Optical Distribution Network (ODN). The typical maximum reach values of ODN are:

- For high density area about 10 km.

- For medium density area 20 km.

- For low density area 60 km.

7.12.2.1.4 Optical infrastructure operations

Based on a "replacement type" network operations approach, the P2P optical access operation could be split in two optical infrastructure operations:

1) Dedicated fibre

The dedicated fibre scenario can also be split in two other sub-categories: dual or single fibre links:

- Dual fibre links: The dual fibre transceivers are based on IEEE 802.1 [i.7] and MSA specifications. F5G could take the initiative to drive the improvement in supervision with a generalization of dying gasp, and accuracy of optical digital diagnostic values (for an efficient data mining diagnostic). F5G could also propose power saving mechanism by decreasing the number of wavelength and/or line rate for multi-wavelength logical link.

- Single fibre link (bidirectional): The bidirectional transceivers are based on IEEE 802.1 [i.7] and ITU-T SG15 Q2 specifications. F5G could drive the specification for bit rates > 50 Gbit/s. Currently 100 Gbit/s and higher line rate are not being driven by optical Access market but the demand will come from OLT uplinks and O-RAN fronthaul use cases. Currently the bidirectional solution is not being proposed. F5G could drive the future of network operation by proposing technical solution for bidirectional 100 Gbit/s and higher line rate. Most 100 Gbit/s interfaces are based on fixed multi-wavelength (typically 4 wavelengths per stream), F5G could propose a bidirectional solution with two half-duplex bands. Also, power saving mechanism could be discussed based on active wavelengths (powering off emitter and receiver).

2) Shared fibre

For P2P operation, the solution to allow sharing one or two fibres for multiple logical P2P links is to use Wavelength Division Multiplexing (WDM). Currently, 100 Gbit/s or higher technologies use several wavelengths for one logical link. The WDM shared fibre scenario can also be split in two sub-categories: fixed wavelength allocation (also named passive WDM) and flexible wavelength allocation (also named active WDM).

- Fixed wavelength allocation are based on several wavelength spectrum allocations: CWDM, DWDM, and MWDM. Passive optical multiplexer and de-multiplexer are already deployed in the optical infrastructure. The migration to 100 Gbit/s and higher line rate per logical link needs to be considered in the existing passive wavelength multiplexer. F5G could drive the future of passive WDM Access Network operation by addressing:

  a) Wavelength allocation for 100 Gbit/s or higher line rate per logical link through single or multi-wavelength allocation channels per stream.

  b) Bidirectional or dual fibre WDM transceivers and passive optical multiplexer ports.

  c) Supervision and optical digital diagnostic values.

  d) Working optical reach and attenuation classes.

  e) Power saving mechanism by decreasing the number of active wavelength channels and line rate.

  f) Others.

- Flexible wavelength allocation could be achieved by either a transponder (typically OLT cards) or embedded in pluggable transceivers with typically auto-wavelength allocation. Several MSA and standardization groups propose implementations of such wavelength management. Auto-tuneable wavelength allocation simplifies inventory management. Each wavelength channel is tuned via an embedded control channel. This control channel need to be interoperable so as to ease network operations. F5G could drive the future of active (automatic) WDM Access Network operation by addressing:

  a) Wavelength allocation for 100 Gbit/s or higher line rate per logical link through single or multi-wavelength flexible allocation channels per stream.

  b) Bidirectional or dual fibre wavelength tuneable transceivers and passive optical multiplexer ports.

  c) Supervision, optical digital diagnostic values.

  d) Wavelength management interoperability.

  e) Working optical spectrum, reach and attenuation classes.

f) Power saving mechanism by decreasing the number of active wavelength channels and line rate.

g) Other.

7.12.2.2 Motivation

The optical fibre technology is widely used in Access Network not only for residential customer but also for other customers. The motivations to address the use of enhanced P2P optical Access is driven by Mobile xHaul, Enterprise, and OLT uplink (backhaul) to the Aggregation edge node markets. With wide-spread optical fibre infrastructure deployment, the optical technology is mandatory to serve all types of customers.

For all these motivations the technical topics of enhanced optical P2P could be summarized as follows:

- The capacity to support 100 Gbit/s or higher line rate per wavelength pair with wavelength management when it is required.
- To save the number of fibres required to achieve one or several P2P links.
- To have optical line supervision parameters corresponding to the network supervision algorithms.
- To have P2P administration and monitoring similar to what is defined by PON, based on OMCI and pPLOAM.

7.13 Use case #27: Rural Scenarios

7.13.1 Use case context

PON technology has been used for many years as the main solution in the Access Networks due to its advantages such as high performance, higher reliability and low cost. With the increase of PON usage in the Access Networks, it has become advantageous to use OLTs as backhaul for some other solutions. This use case will give a brief introduction to scenarios for extending PON to rural areas with the assistance of a Fixed Wireless Link (FWL) at different locations depending on the deployment scenario.

Rural cable deployment may have higher cost in cases where there is a small number of distributed customers, where there is a government service obligation or areas with hard geographic situations to deploy cables. In such cases, ISPs can use a combined PON and FWL solutions. For PON + FWL solutions, there are different scenarios for deployment depending on the requirements and customer base.

The performance of FWL technologies varies depending on the scenario (e.g. line-of-sight), the distance, the frequency, the licenced or unlicensed spectrum, or the radio technology used. This use case assumes either a point-to-point or a point-to-multi-point FWL, but does not assume any specific FWL technology.

7.13.2 Description of the use case

7.13.2.1 Overview of P2P (Point to Point) Solutions

7.13.2.1.1 General

In P2P solutions, there will be one FWL receiver for each FWL transmitter. The PON systems can be deployed with SFP ONUs where the FWL transmitters are located. Because of their small size and that they do not need an additional power supply, the SFP ONUs are suitable for the PON + FWL solution.

There are different solutions on the customer side depending on the number of customers or the ISP's obligation.

7.13.2.1.2 PON P2P FWL HGW (0-10 Customer)

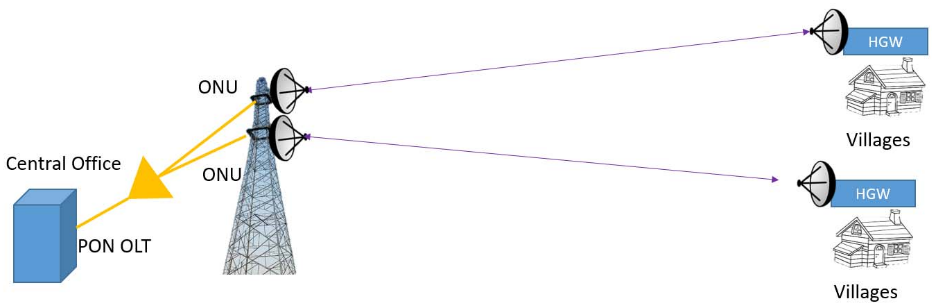


Figure 97: P2P wireless HGW

PON P2P FWL HGW solution can apply in rural locations where the number of distributed customers is between 0 and 10. Each customer will have a HGW as the end devices. In case, Wi-Fi® is used as FWL technology, the HGW can act as a Wi-Fi® receiver and an additional Wi-Fi® receiver will not be needed.

7.13.2.1.3 Wireless P2P scenarios

In the following scenarios, there is a network connecting the customers, and depending on the scenario different technologies can be used.

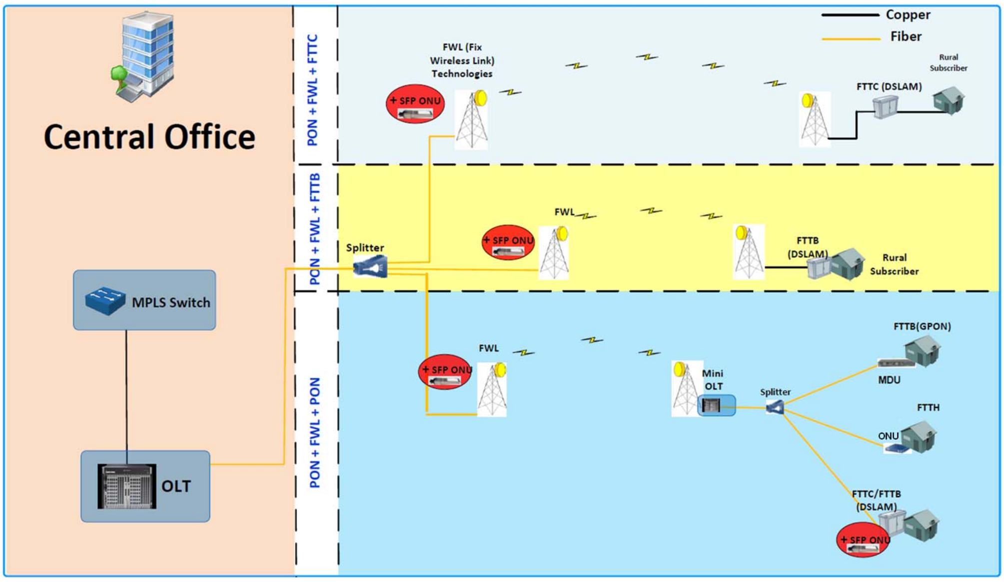


Figure 98: Overview of wireless P2P scenarios

PON - P2P - FTTC (10-100 Customer): PON-P2P-FTTC solution can apply in rural locations, which have between 10 and 100 distributed customers. After the FWL receiver, a FTTC DSLAM will be used to provide services to the customer.

PON - P2P - FTTB (5 - 100 Customer): PON-P2P-FTTB solution can apply in rural locations, which have between 5 and 100 customer in the same building. After the FWL receiver, FTTB DSLAM will be used to provide services to the customers.

PON - P2P - PON (>100 Customer): PON-P2P-PON solution can apply in rural locations, which has greater than 100 customers. In this solution, a Mini OLT, which has 1-2 slots can be used. For this solution the rural area should be suitable for fibre deployment between OLT and ONU/MDU/SFP ONU.

7.13.2.2 Overview of P2MP (Point to Multi Point) Solutions

7.13.2.2.1 General

In P2MP FWL solutions, there is only one FWL transmitter for all FWL receivers. PON systems can be deployed with SFP ONUs, where the FWL transmitter is located. Because of their small size and that they do not need an additional power supply, the SFP ONUs are suitable for PON + FWL solution. For the P2MP solutions, the bandwidth can be lower and the latency better than in the P2P solution. There are different solutions on the customer side depending on the number of customer or the ISP's obligation.

7.13.2.2.2 PON P2MP FWL HGW (0-10 Customer)

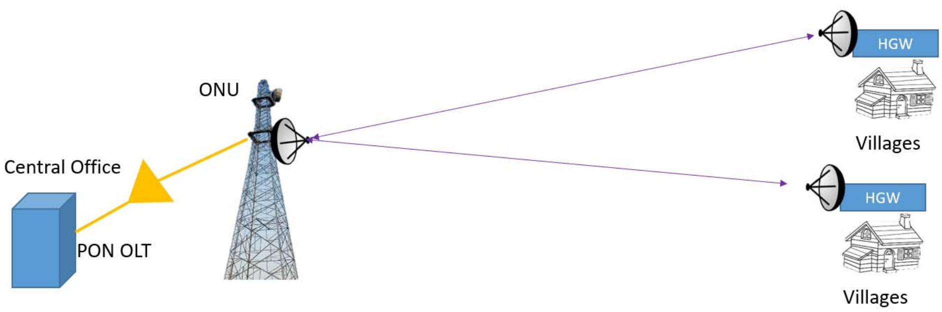


Figure 99: P2MP Wireless HGW Scenario

PON P2MP FWL HGW solution can apply in rural locations, which have between 0 and 10 customers. Each customer will have a FWL HGW as the end devices. In case, Wi-Fi® HGWs will be used as a Wi-Fi® receiver and an additional Wi-Fi® receiver will not be needed.

7.13.2.2.3 Wireless P2MP scenarios

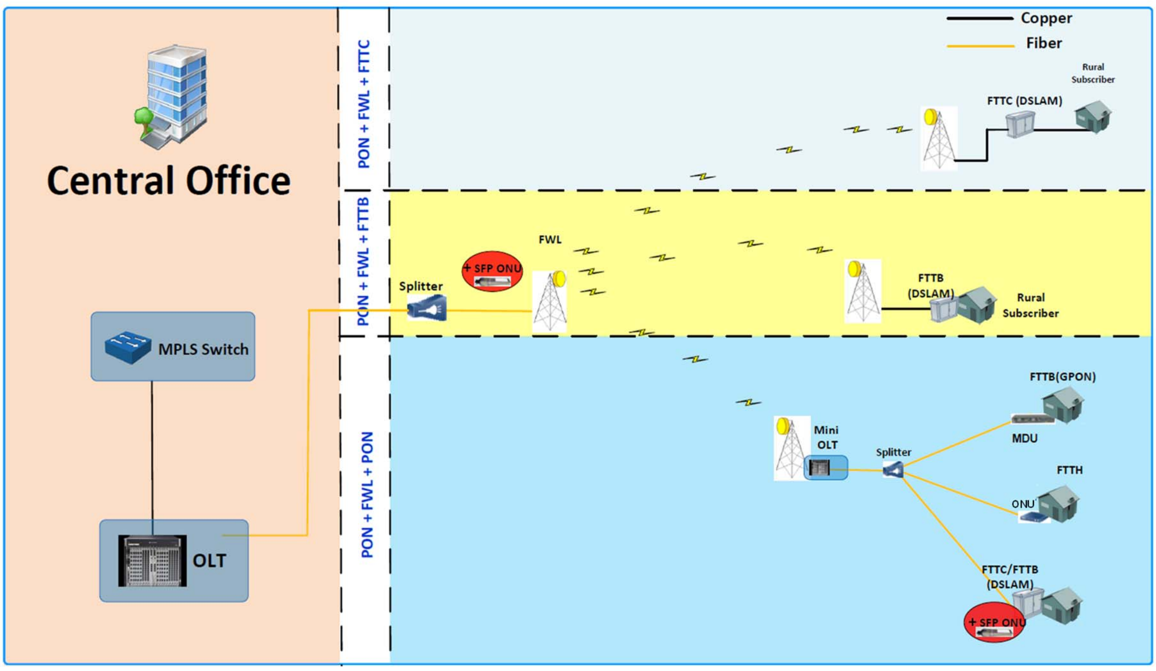


Figure 100: Overview of P2MP wireless scenarios

PON - P2MP - FTTC (10-100 Customer): PON-P2MP-FTTC solution can apply in rural locations which have between 10 and 100 distributed customer. After the FWL receiver point FTTC DSLAMs will be used to provide services to the customer.

PON - P2MP - FTTB (5 - 100 Customer): PON-P2MP-FTTB solution can apply in rural locations which have between 5 and 100 customer in the same building. After the FWL receiver point FTTB DSLAM will be used to provide services to the customers.

PON - P2MP - PON (>100 customer): PON-P2MP-PON solution can apply in rural locations which have greater than 100 customers. In this solution the Mini OLTs which has 1-2 slots can be used. For this solution the rural area should be suitable for fibre deployment between OLT and ONU/MDU/SFP ONU.

7.13.2.3 Overview of Services

Since PON + FWL solutions will be used in rural areas, mainly residential services will be needed. The technology of FWL can be selected according to bandwidth needs. The bandwidth of FWL technologies is dependent on several factors such as distance and spectrum, among others.

Type of the services provided in the rural area include:

- VoIP: Voice over IP service is often a government regulatory requirement.
- HSI: High-Speed Internet (HSI) services can be provided by PON + FWL solutions. Speeds and tariffs can be identified according to the bandwidth of the PON + FWL solution.
- IPTV: IPTV services technically can be provided by PON +FWL solutions. But because of the high bandwidth demands of IPTV services, this can be optional.

7.13.2.4 Motivation

ISPs can use the combination of PON and FWL as a solution for rural locations for the following reasons:

In the cases in which there are a small number of customers or where there is government service obligation, and the cost of cabling is too high.

In the case that it is hard to deploy cables because of difficult geographic situations, ISPs can use combined PON and FWL solutions.

7.14 Use case #28: High-speed Passive P2MP Network Traffic Aggregation

7.14.1 Use case context

In any type of Aggregation Networks such as OLT backhaul, mobile xHaul or enterprise access, multiple Remote Nodes (RNs) need to be bidirectionally connected to a central node. The traffic is essentially point to multi-point and multi-Point to Point, so a P2MP technology is beneficial. In optical networks, the aggregation of network traffic is traditionally a point-to-point (P2P) topology, as shown in Figure 101.

An example of such a topology is, a 5G mid-haul network connects N Distributed Units (DU) nodes with their corresponding Central Unit (CU) node using P2P optical connections and one Electrical Aggregation Unit (EAU). This topology requires 2N optical transceivers for the N connections between the EAU and the N DU nodes and 2 full-band transceivers for the connection between the EAU and the CU node. Moreover, the EAU requires an additional power supply and an equipment room. Thus, it is desirable to improve the cost effectiveness and energy efficiency of an Aggregation Network. In high-speed passive Point-to-MultiPoint (P2MP) network traffic aggregation, a central node is connected to multiple remote nodes through a passive optical splitter. This is a promising approach to realize traffic aggregation in a cost-effective and energy-efficient manner, as shown in Figure 102.

Frequency-Division Multiple Access (FDMA) can be used to flexibly partition the network traffic to and from the remote nodes [i.25] and [i.26]. From an operational perspective, the flexibility to partition the traffic depending on the remote nodes resource requirements is important for the efficient use of existing resources. In addition, the ease of upgrading capacity without changing the whole Aggregation Network is important for leveraging existing investments. Therefore, increasing the system capacity by only changing one interface is appealing for a future-proof Aggregation Network technology.

7.14.2 Description of the use case

7.14.2.1 Overview

In the downlink direction, the central node transmits a high-bandwidth multi-carrier signal to the remote nodes, while each remote node receives a subset of these carriers. In the uplink direction, the central node receives a high-bandwidth multi-carrier signal that contains modulated carriers from multiple remote nodes, each of which only transmits a subset of these carriers. For the example network case shown in Figure 101 and Figure 102, there are eight RNs. Assuming an interface bit rate of 25 Gb/s per RN for each direction (downlink or uplink), sixteen 25-Gb/s connections are needed, resulting in a total bi-directional data rate of 400 Gb/s.

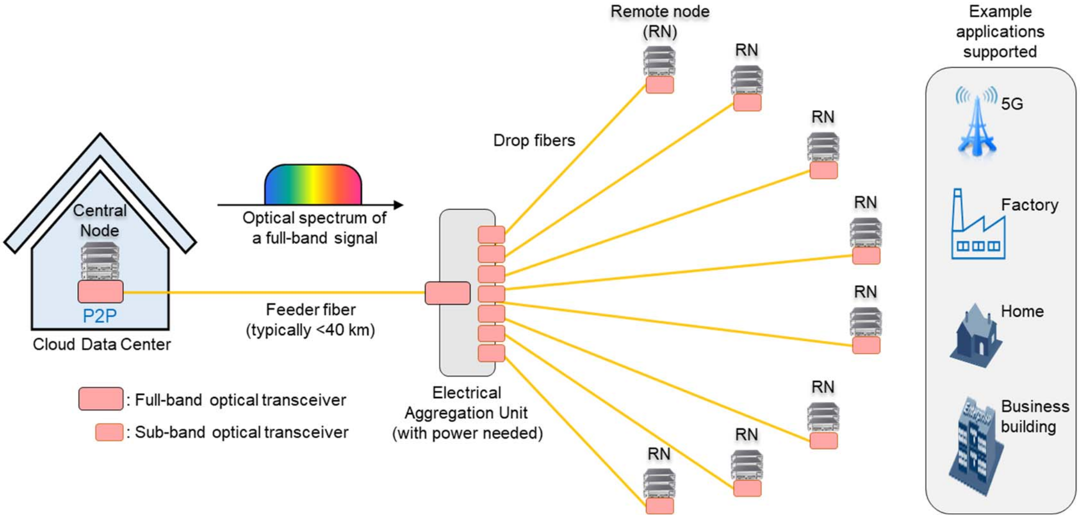


Figure 101: Conventional P2P optical connections between multiple Remote Nodes (RNs) and their corresponding central node

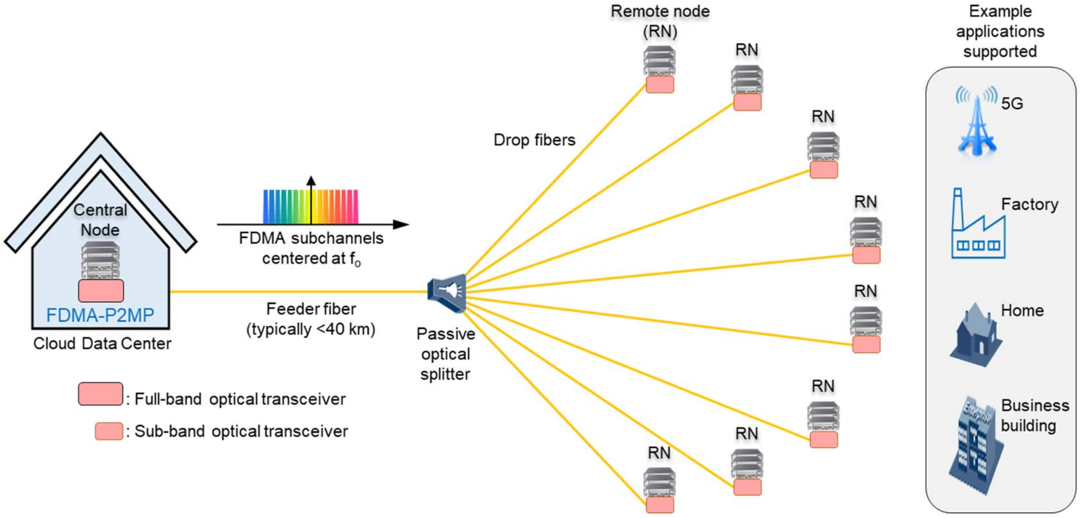


Figure 102: FDMA-based passive P2MP optical connections between multiple Remote Nodes (RNs) and their corresponding central node

To achieve a total FDMA data rate of 400 Gb/s, an optical bandwidth of 64 GHz to carry sixteen 4-GHz-spaced sub-channels is used, as shown in Figure 103. Assuming Nyquist spectral shaping with a roll-off factor of 0,1, each sub-channel can be modulated at 3,6 Gbaud and carry a raw data rate of 28,8 Gb/s via Polarization-Division Multiplexed (PDM) 16QAM. Excluding the overhead for Forward Error Correction (FEC) of ~15 %, payload data rate of each sub-channel can reach 25 Gb/s, leading to an aggregated payload data rate per FDMA channel of 400 Gb/s.

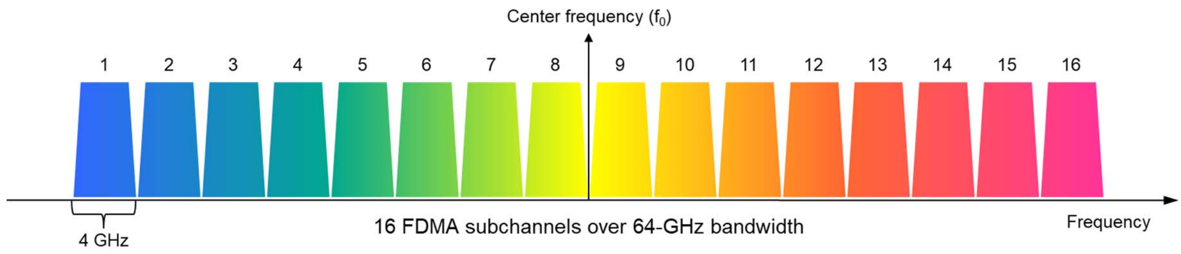


Figure 103: Optical spectrum of a 400-Gb/s FDMA channel consisting of sixteen 4-GHz-spaced sub-channels each carrying 25-Gb/s payload data rate

At the central node, a coherent full-band transceiver can be used to transmit (receive) all the downlink (uplink) sub-channels to (from) the connected RNs, as shown in Figure 104. At each RN, a coherent sub-band transceiver can be used to receive a subset of sub-channels in the downlink direction and transmit a neighbouring subset of sub-channels in the uplink direction, also shown in Figure 104. In each coherent transceiver, a common laser is used as the Optical Local Oscillator (OLO) and the transmitter laser [i.27], and bidirectional transmission over a single fibre can be enabled by the use of a circulator. When receiving a downlink sub-channel, the OLO is accurately locked to a pre-determined frequency offset from the centre frequency of the downlink sub-channel. So, the same laser can be modulated by a coherent I/Q modulator to generate an uplink sub-channel whose centre frequency is locked to the received downlink sub-channel with an intended frequency offset. As an example, when the intended downlink sub-channel and uplink sub-channel for a RN are next to each other, the laser frequency of the sub-band transceiver can be set in the middle of these two sub-channels. Doing so minimizes the RF bandwidth requirement of the sub-band transceiver to the sub-channel bandwidth, which is 4 GHz in the case shown in Figure 103.

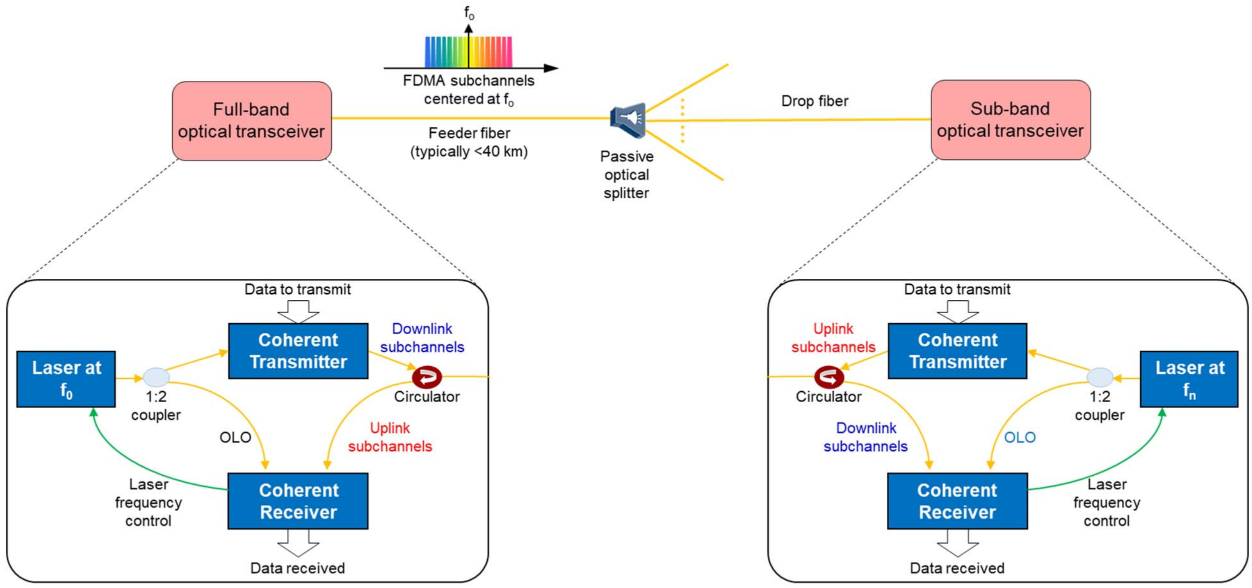


Figure 104: Coherent full-band and sub-band transceivers supporting bidirectional transmission with the downstream signal centred at f_0 and the upstream signal centred at f_n

It is also feasible to allow the sub-band transceiver to transmit and receive multiple sub-channels by increasing its RF bandwidth. For example, when the RF bandwidth of the sub-band transceiver is increased to 16 GHz, 4 adjacent downlink sub-channels can be received and another 4 adjacent uplink sub-channels can be transmitted, at 100-Gb/s payload data rate per direction. This indicates the flexibility in the implementation of the sub-band transceiver to address different data rate requirements in the access nodes.

Instead of single-fibre bi-directional transmission, two fibres can be used to support bi-directional transmission. In this case, the circulator used in the coherent transceiver is omitted. With unidirectional transmission in each fibre, Erbium-Doped Fibre Amplifiers (EDFAs) can be readily used to extend the reach of the Aggregation Network (e.g. to 200 km or greater). With bi-direction transmission over two fibres, the use of ring topology for network traffic aggregation can also be supported.

7.14.2.2 Motivation

The use case of high-speed passive P2MP network traffic aggregation offers a highly cost-effective and energy-efficient means to achieve traffic aggregation. The coherent FDMA-based P2MP approach further offers the following benefits:

- High capacity: supporting high-capacity traffic aggregation (e.g. 400 Gb/s per FDMA channel) from multiple access nodes to a core node.
- Long reach: supporting long-distance transmission (e.g. greater than 400 km) without dispersion penalty because of the dispersion compensation capability of coherent detection.
- Flexible bandwidth allocation: supporting flexible and dynamic bandwidth allocations to match downstream and upstream traffic demands.
- High scalability and upgradability: allowing the increase of aggregated system capacity by only upgrading the equipment at the core node (e.g. by increasing the aggregation capacity from 400 Gb/s to 800 Gb/s per FDMA channel), and potentially allowing the increase of the capacity of each RN by software-defined sub-band transceiver upgrade.
- Ability to be used over ring-based fibre deployments: leveraging the use of the popular ring topology for network traffic aggregation.
- Reduced CapEx: reducing the number optical transceivers by 50 % as compared to the traditional P2P approach and eliminating the active electrical aggregation unit. In addition, it eliminates the extra power supply and equipment room needed for the active electrical aggregation unit.
- Reduced OpEx: it allows for a higher degree of remote operations through the system flexibility.

7.14.2.3 Pre-condition

The following pre-conditions apply for this use case:

- Architectural designs of FDMA-based passive P2MP network traffic aggregation.
- Specification of the FDMA channel partition for interoperable operations.
- Control and management of each FDMA channel including DBA, power control, and software-defined system capacity upgrade, etc.

7.15 Use case #29: Orchestration of B2B services in xPON networks

7.15.1 Use case context

The xPON technology for FTTH networks has evolved over recent years and is now in mass deployment by many operators. It is one of the pillars on the EU Recommendation for a European Gigabit Society, giving access to broadband services to the B2C market, targeting speeds up to 1 Gb/s in every European household by 2025.

The Europe penetration ratio average is at 43 %, with some countries above 70 % and others already beyond 90 %. Other than households, this coverage is also reaching B2B sites like commercial buildings, factories, enterprises, business-oriented facilities (e.g. technology parks) and public facilities (e.g. amusement parks, sea ports, sport stadiums).

For the SME market, price targets for communication services are of significant importance. xPON is becoming the first choice for communications services due to the bandwidth/price ratio, and in some markets represents between 15 % and 18 % of total fibre Access.

The operator solutions for this market tend to make an offer using distinct equipment, although most of the time, commercial service packages use less bandwidth than B2C ones. One of the reasons is related to branding; (it is more appealing to sell an enterprise-like branded equipment then a generic one). Another reason is performance.

This approach results in distinct Access Network connectivity service definitions and OSS terminal equipment modelling. The approach generates well-defined provisioning workflows and delivery processes with increased time-to-market, when compared to B2C solutions on the same Access Network. One of the reasons is that for the residential market, that require mass provisioning, data models are stable and well defined. The residential equipment used is fully compliant, as compared to B2B CPEs, which are not fully compliant

7.15.2 Description of the use case

7.15.2.1 Overview

The goal of this use case is to define, a common Access Network connectivity service model, which serves B2B needs, using a unified CPE device (EG including ONU) and specifically defined B2B service VLANs at the OLTs SNI (Service Node Interface).

The Enterprise Gateway (EG) will be a L2/L3 device, which is integrated with an ONU for cost reduction and it uses well established data models for management automation. The unified CPE will function as a universal device with several roles, serving different connectivity purposes.

The network connectivity model is exposed to upper OSS layers by the resource orchestrator northbound API. The OSS layer is responsible for informing the CPN and Access Network controllers of the service requests. The user expresses its service intent through the provided customer portal as shown in Figure 104. Additional services, like security features or on-demand bandwidth changes can be requested by a user through this digital channel portal.

This represents an opportunity to leverage and standardize a common set of Access Network services, for mass deployment scenarios, for both business customers, and telco operators:

- VPN connectivity
- Internet Access
- Edge Compute Data Centre Direct Connectivity
- 4G/5G Small Cell direct connectivity to 5G SA Core
- Sensor / Surveillance Devices Connectivity

The customer digital interaction through these portals is a key differentiator for operators in the B2B market. It facilitates transparent customer relations, provides control of their services, and presents an opportunity for new value added service revenue streams for the operator. The portal can reside either on the CPE device or on the operator´s edge computing platforms.

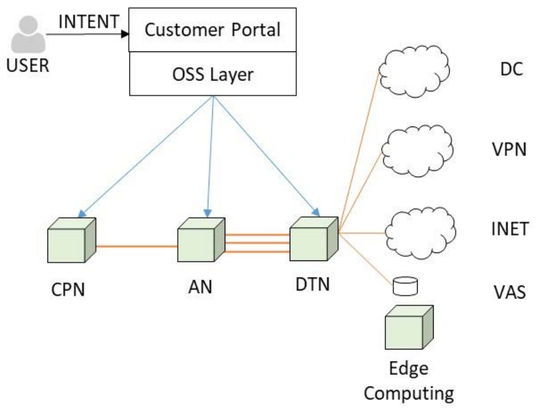


Figure 105: Customer portal and B2B service connectivity flows

The overall solution can be achieved using an ecosystem of the following three components as shown in Figure 106.

Customer Self Service Portal: a digital interface which relates to the user's intent to request changes to the network contract parameters. These parameters can be related to general QoS features like bandwidth, connection class of service, routing protocol, or add/change LAN IP range or VLANs.

Enterprise Gateway: Is a L2/L3 device that has the capability to manage the provisioning of business specific connectivity services. It can interface with additional device functions such as Wi-Fi®, Cellular Radio or an IoT protocol stack that could be combined in the CPE device. It is physically integrated in a CPE.

Multi-Service Connectivity Orchestrator (MSCO): this is the software piece of the ecosystem. It is a network services orchestrator, that has the capability to expose B2B services as 'Network as a Service' to the higher layers. It also ensures the management of multiple CPEs and their roles, combining service definition of the ONU and EG functions. One example is, a VPN access service that terminates in an OLT SNI that connects to the PE. Another example is, a connectivity service that terminates in a specific OLT SNI that connects to a service VPN responsible for L3 routing up to the 5G SA Core UPF function.

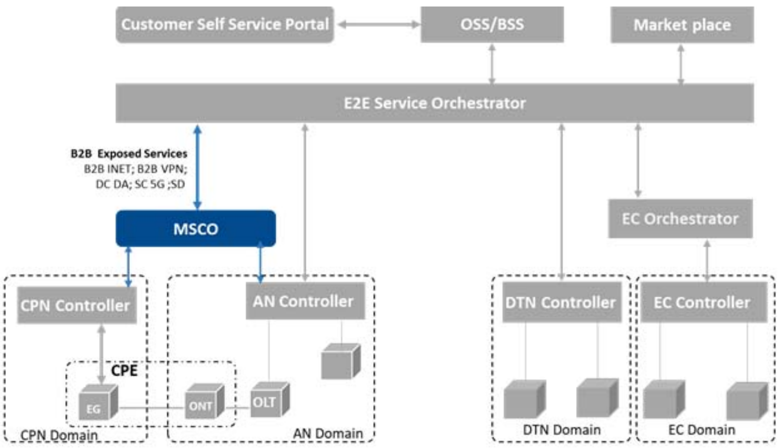


Figure 106: B2B Enhanced connectivity architecture

The typical scenarios are:

- B2B and B2C bundle services in the same OLT.
- Managed connectivity characteristics such as bandwidth and Class of Service (CoS).
- Providing Value Added Services (VAS) by using service chaining over instantiated functions in the operators edge computing data centre.
- Mass deployment of small cells using the xPON Access Networks.
- Public video surveillance in dense areas with FTTH coverage.

7.15.2.2 Motivation

- Lower OSS integration costs by defining a common set of B2B connectivity services, combining CPN and Access Networks.
- Reducing the cost of customer devices by using a modular CPE, for mass deployment of multiple B2B services over xPON.
- Reducing human error and achieve zero touch provisioning using a centralized controller.
- Reducing site intervention costs and simplify the customer premises network operation by combined ONU and EG in a single CPE device.
- Providing full user control and a digital channel VAS by means of a customer self-service portal.

7.15.2.3 Pre-condition

The CPE need to be compliant with and fully support standard data models used by the MSCO and CPN and Access Network controllers.

7.15.2.4 Operational flow of actions

The customer places an order via the Customer Self-Service Portal.

The E2E Service Orchestrator decomposes the order into several Resource Facing Services (RFS). One or more RFS uses the services exposed by the Multi-Service Connectivity Orchestrator.

The Multi-Service Connectivity Orchestrator maps the orchestration resource service parameters order, into API calls for EG configuration via CPN controller (e.g. IP address, Routing protocol, shaping rate, CoS, VXLAN ID, LAN IP range, active/proxy DHCP, etc.) and OLT/ONU via Access Network controller (e.g. SNI VLAN, Customer VLAN, Uplink speed, Downlink speed, etc.).

7.16 Use case #30: Bandwidth on Demand

7.16.1 Use case context

In current fixed broadband services, the bandwidth allocation to subscribers is typically static. However, many subscriber services, such as gaming updates, video downloads or periodic data backups need variable bandwidth. Allowing subscribers to request a temporary service bandwidth increase for a limited period of time (hours, minutes, seconds, or even milliseconds) can significantly improve their experience. This could help optimize the network bandwidth utilization. End to end bandwidth availability will be taken into account when granting a subscriber's bandwidth on demand change request.

7.16.2 Description of the use case

7.16.2.1 Overview

For fixed broadband services, network planning is such that it is highly unlikely that the network bandwidth is fully utilized and saturated.

Currently, most broadband services use a static bandwidth for the majority of the time. The end users could benefit from a temporary bandwidth increase for a predefined time and/or duration. Examples of such services are:

- **Online gaming:** when playing a game, the user needs around 25-50 Mbps. A typical game update size is in the order of 50 GB, which would take approximately 2 hours at 50 Mbps.
- **Periodic data backups:** differential backups are relatively low bandwidth usage, but a full backup can easily be several orders of magnitude larger.
- **Premium video streaming service:** users that have a subscription that supports regular-sized (e.g. 2K HD) videos, could be interested in using more bandwidth to stream 4K/8K UHD videos every once in a while.
- **Newspaper download:** digital newspapers can be significant in size. Based on typical broadband service bandwidth it would take several minutes to download a complete digital newspaper. Bandwidth on demand can significantly improve the download time with a temporary speed boost of a few seconds.
- **Pre-Recorded Video Content Download:** many platforms allow for downloading video content for offline viewing. Since content might be large and often users want shorter download times, so bandwidth on demand is a suitable solution.

Users of these types of services are unlikely to upgrade their existing subscription permanently, for momentary bandwidth boosts, which are sporadic in nature. However, they might be interested in temporarily boosting their bandwidth depending on the business model, if the underlying network allows for it.

The user can request such bandwidth boosts in two main ways:

- **Manually:** the user requests a temporary increase, for example, by clicking on a button in a service provider application.

- **Automatically:** the user specifies (e.g. via a service provider application) which applications require the F5G network (usually by the F5G network management system) to perform bandwidth boosts. There could be agreements on specific time of day and other aspects that are not specified here. The network could, for example, detect that the user's bandwidth is being capped by a fixed bitrate profile, while there are resources available to provide additional bandwidth temporarily.

The telecom operator can offer a temporary increase in bandwidth to its subscribers in two possible ways:

- **Spontaneous:** the subscriber needs the increase in bandwidth right away, for example, for downloading a 4K video. Whether the request can be granted depends on the current load of the network and the duration of the desired bandwidth boost.

- **Scheduled:** the subscriber needs the increase in bandwidth at some point in the foreseeable future, for instance for downloading a game update, which can happen overnight. The service management platform can check the available capacity and schedule the update when it fits best.

NOTE: In this use case, the service characteristic only considers bandwidth, however, other characteristics like guaranteed service on demand, etc., are for further study.

7.16.2.2 Motivation

A bandwidth on demand functionality offers several advantages, for instance:

- Network operators can optimize their available resources.

- Network operators/service providers can develop new business propositions for end-users.

- The quality of experience for end-users may improve.

7.16.2.3 Pre-conditions

The following pre-conditions need to be in place:

- The subscriber or application can request a temporary increase in bandwidth.

- The network management system has the functionality to assess whether there is sufficient capacity available in the network to complete the bandwidth change.

- There is a service management platform in place that provides the on-demand bandwidth allocations in the network.

7.16.2.4 Operational flow of actions

Figure 107 shows an example of an operational flow for bandwidth on demand. In this particular example, the user requests to temporarily use more bandwidth in the network. It should be stressed that there will be many other possible operational flows that may depend on the business proposition or implementation.

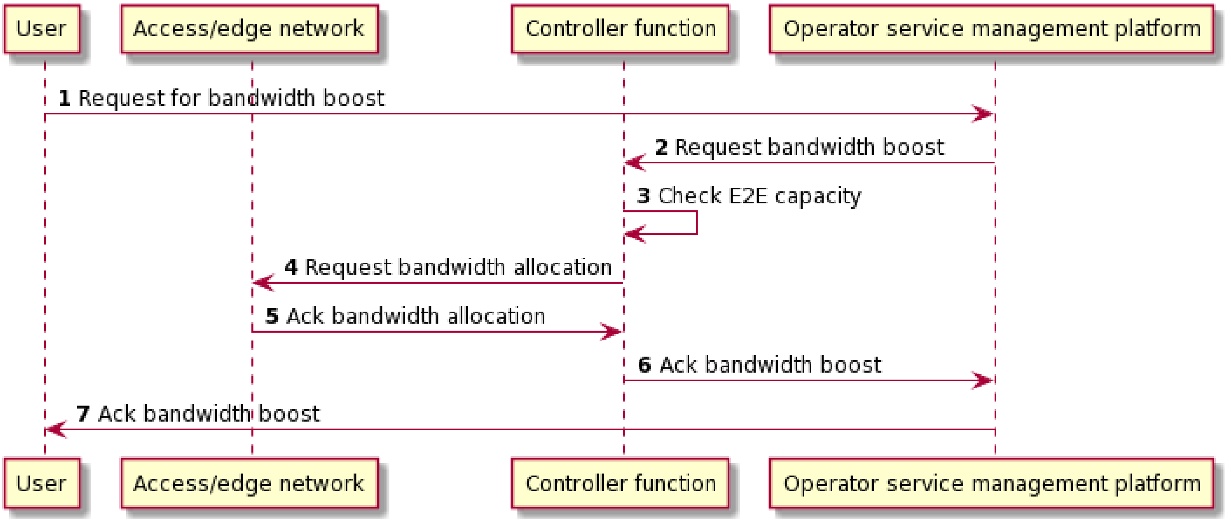


Figure 107: Example of an operational flow of bandwidth on demand in case of a client-driven request

1) The user sends a request to the operator service management platform for a temporary increase in bandwidth. The request includes at least the desired bit rate. Optionally, the request can include:

- A specific starting time: either the current time (user wants to download something immediately), or sometime in the future (user wants to watch a movie at 10 PM).

- A specific ending time: this is either the projected ending time of the service (like the end of the movie), or a deadline before something has to be finished (like backups that need to be completed before midnight).

2) After authentication and authorization actions, the operator service management platform sends a request with the bandwidth boost parameters to the controller function.

3) The controller function verifies if the E2E network capacity is sufficient for the requested boost

4) The controller function performs a request to the Access/edge networks (this is the Access and Aggregation Network up to the Aggregation Edge Node) with different options:

- A specific start time including from now on and duration.

- When bandwidth is available in the future (the controller function checks when the extra bandwidth can be allocated).

5) The Access/edge network applies a temporary bandwidth profile and acknowledges this to the controller function.

6) The controller function acknowledges the boost to the service management platform.

7) The service management platform acknowledges the bandwidth boost to the user with information such as duration and pricing.

7.17 Use case #31: Intelligent Optical Cable Management

7.17.1 Use case context

Optical cables are non-intelligent resources as they only consist of passive components. The cable routing, fault detection and quality monitoring are usually performed manually. As a result, optical cable network management efficiency is low. The accuracy and consistency of the optical cable network management is not absolutely correct, because of the human intervention, and fault detection is reactive and slow. For example, during service provisioning, two optical cables that belong to different physical cable routes can be assigned to one service. One is classified as the working link and the other is classified as the protection link. However, occasionally both of them may be allocated to the same cable route by mistake as illustrated in Figure 108, which effectively results in no service backup. In the case, when the cable is cut, both working and protection paths may be cut simultaneously causing service outage. This collocated cable route issue is detected manually, which implies low efficiency.

For an F5G network to guarantee service availability, intelligent optical cable network management is needed. It accurately identifies the same cable and same duct information of optical fibres, and proactively provides troubleshooting assistance and continuous quality monitoring.

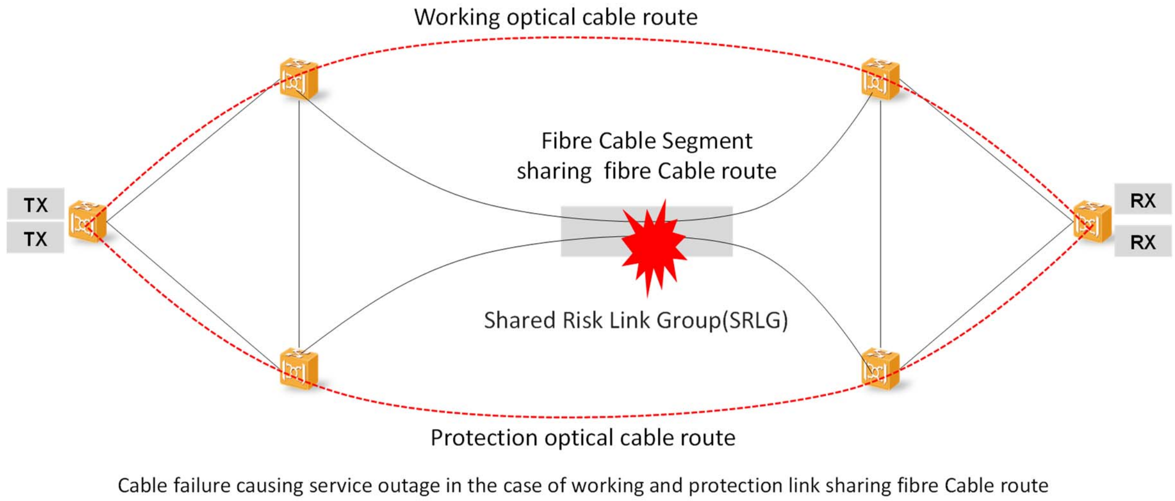


Figure 108: Service outage caused by cable failure when both working and protection link sharing fibre cable route

7.17.2 Description of the use case

7.17.2.1 Overview

7.17.2.1.1 General

Some practical problems that cannot be ignored in the current optical cable network management system:

1) Optical cable route information is managed and maintained manually, which makes it difficult to ensure its accuracy. A service with shared cable route information is not totally reliable (e.g. working and protection link of a given service are collocated in the same cable, same trench or same duct). As a result, the service availability cannot be guaranteed, and services run the risk of service outages.

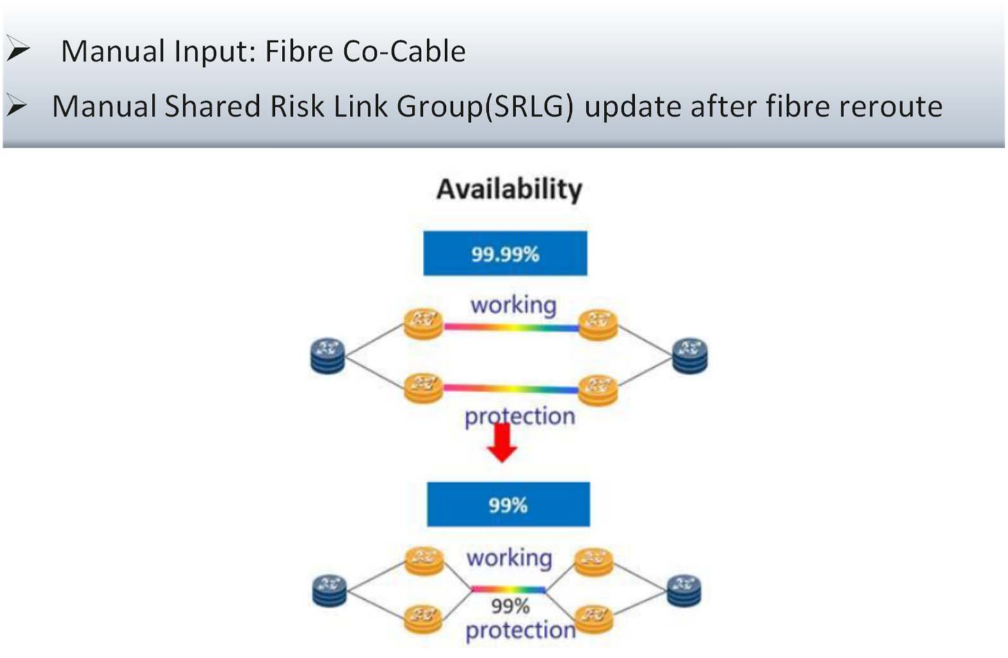


Figure 109: Availability degradation do to shared cable colocation

2) Optical cable routes are not currently associated with GIS (Geographic Information System) information: so as a result, optical cable faults cannot be located accurately.

   Currently, if a fault occurs within a few kilometres (in fibre length) from a given optical node, it can be identified (by using Optical Time-Domain Reflectometer: ODTR) but due to the deployed optical cable route and service loops, the geographic location of the cable fault may not be derived from the fibre length. Therefore, the repair team needs to manually locate the actual fault.

3) Optical cable quality is monitored manually: Therefore, optical cable degradation cannot be predicted and detected in a timely manner, leading to reactive maintenance, after the fault occurs, being the usual response.

   In summary, current optical cable management accuracy and troubleshooting efficiency is low, which increases the risk to service operation and may have a significant impact on service availability.

   Take a WDM systems for example, which can carry multi-Tera bits/s of traffic data. For such a systems optical cable management accuracy is extremely important. For optical fibre cables that support WDM systems, the automatic identification of the shared route (collocation in same cable, same trench or same duct) is critical. It uses GIS-based optical cable management and fibre quality monitoring. The health prediction can effectively guarantee service availability and improve operation and maintenance efficiency.

7.17.2.1.2 Key points to be addressed

1) Automatic identification of shared-route: During service provisioning and rerouting, the working and protection route need to be automatically and physically separated from each other. The service availability will be accurately evaluated based on actual shared-route information. The shared-route status between the working and protection route can be automatically detected. An early alarm mechanism can trigger on-demand optimization and automatic separation determination.

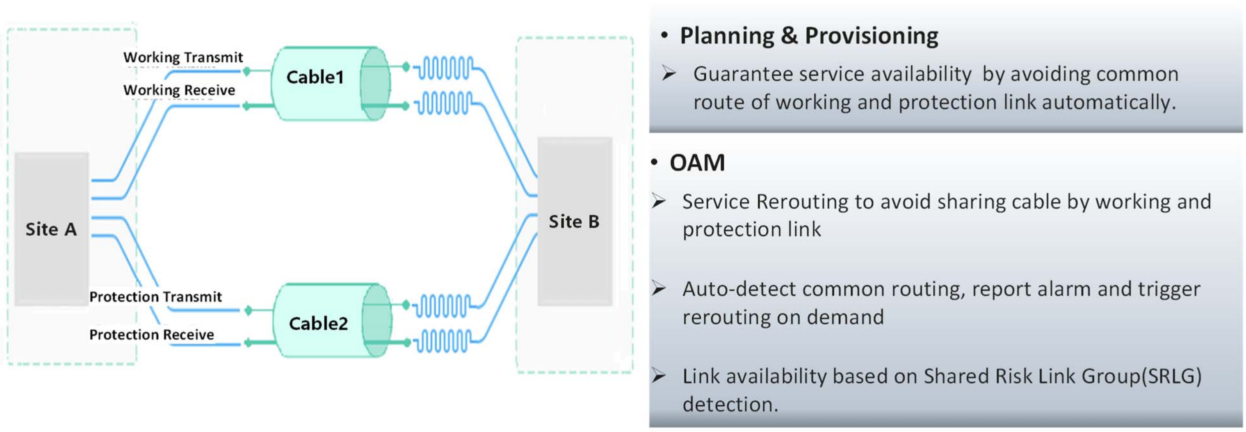


Figure 110: Example of duplicate-routing optical cable

2) GIS-based optical cable management: The GIS information of optical cable routes can be manually recorded or automatically discovered. It can use, for example, AI + proactive perturbation (imposing vibration on the cable) that allows the automatic correlation of the fibre cables that share the same route. Figure 110 illustrates an example of the optical cable topology based on GIS information, which support fault location to street level in minutes.

Figure 111: GIS based optical cable topology management (Example)

3) Real-time fibre quality monitoring and health prediction: collects optical performance in real time, calculates fibre attenuation and continuously monitors the Fibre quality. In the case of a degrading fibre, it gives advance warning of a possible failure occurrence (allowing traffic to be moved to a different fibre), with prediction of fault time derived from the trend of fibre degradation (e.g. hour/day/week/month). This enables proactive O&M by prompting cable maintenance before cable fault occurs and therefore preventing service outage.

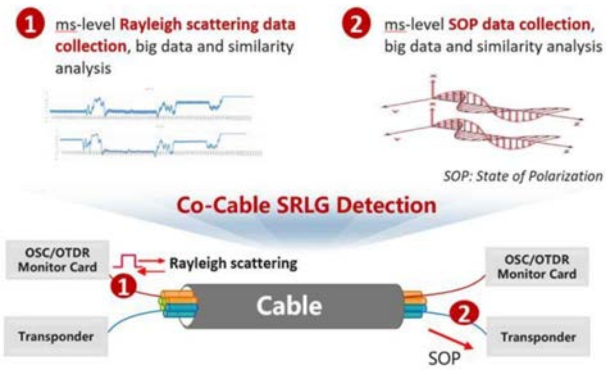


Figure 112: Co-Cable Shared Risk Link Group (SRLG) detection

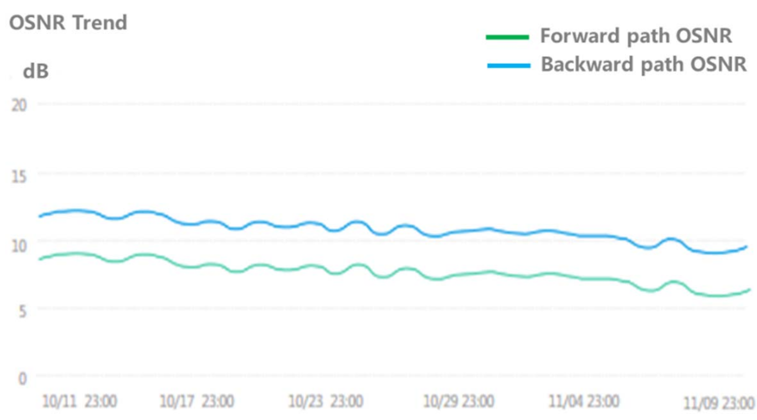


Figure 113: On-line real-time optical channel performance

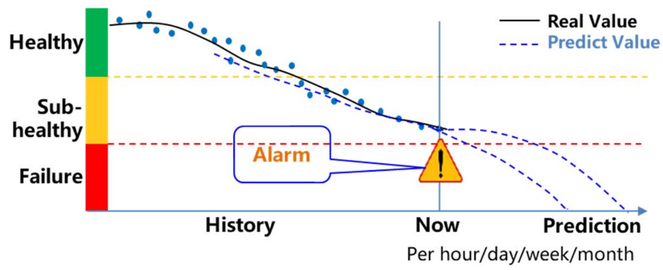


Figure 114: Optical fibre degradation prediction

7.17.2.2 Motivation

- Automatic identification of shared-route optical fibres, guarantees higher service availability.
- Association of the optical cable with GIS information improves OAM efficiency and accuracy, supports locating cable faults in minutes.
- Monitor optical fibre quality and predict degradation, supports proactive maintenance and reduces service outages.

7.17.2.3 Pre-condition

- Install intelligent optical cable network management APP in the NMS.
- Input the GIS information of optical cable routes (or automatically detect the GIS information).

7.17.2.4 Operational flow of actions

1) The operator installs the intelligent optical cable network management APP in the NMS.

2) The operator generates corresponding SRLG (Shared Risk Link Group).

3) The operator needs to input GIS information of the optical cable network, and the NMS associates the optical cable with GIS information and generates overall optical cable network topology.

4) The NMS re-allocates service automatically during service provisioning, to avoid working route collocation with protection route in the same cable, trench or duct.

7.18 Use case #32: AI-based PON optical path diagnosis

7.18.1 Use case context

Traditional optical path fault repair process in PON has low efficiency and low accuracy. This is due to inaccurate ODN data and inefficient fibre provisioning. Therefore, in order to improve the efficiency of Access Network management, an enhanced ODN data collection mechanism, fast diagnostics and repair is needed.

Traditional methods, such as OTDR (Optical Time Domain Reflectometer), needs additional hardware and system upgrade, and is not applicable to existing systems. This use case focuses on AI-based PON optical path diagnosis which works on existing systems.

7.18.2 Description of the use case

7.18.2.1 Overview

7.18.2.1.1 Current issue

PON optical path fault is a major fault contributor in Access Networks. Currently, PON optical path diagnostics relies on an EMS alarm and manual troubleshooting, which is inefficient and costly, due to onsite inspection. In addition, the fault location needs to be analysed manually based on the alarms, the ODN splitter information, and the ONU information. When the ODN resource information in the operator's management system is inaccurate, the real ODN topology cannot be accurately determined by manual analysis. This will increase the difficulty of troubleshooting, and further leads to the incorrect issuing of work orders. Therefore, in the current situation, the fault processing time is long, user satisfaction declines due to long service interruption.

7.18.2.1.2 Benefits of AI-based PON optical path diagnosis

The collected optical path fault information is used to train an AI platform. The AI platform learns the fault characteristics and accurately models the ODN data with PON optical path data.

It can accurately identify the root cause of a PON optical path fault and quickly locate the fault. The optical path performance degradation can be monitored and performance degradation identified before service interruption actually occurs.

The associated work order system automatically sends orders in advance for optical path fault repair to prevent customer service interruption. In this way, the efficiency of optical path fault repair is obviously improved. The PON optical path fault diagnosis is shown in Figure 115.

7.18.2.1.3 Implementation

PON optical path fault intelligent diagnosis relies on the optical path data acquisition. Data transport between AI platform and OLT may use telemetry technology which is highly efficient. The AI platform performs fault diagnosis.

Optical path data acquisition includes (see Figure 115):

1) ONU statistics: type of optical module, current, voltage, temperature, receiving and launching power;

2) OLT statistics: LoS (Loss of Signal), BIP (Bit-Interleaved Parity) errors, FEC (Forward Error Correction) corrected and non-correctable errors, packet loss, transmitting/receiving rate, transmitter/receiver capacity, transmitting/receiving packet numbers;

3) Alarm data: optical path alarm, etc.

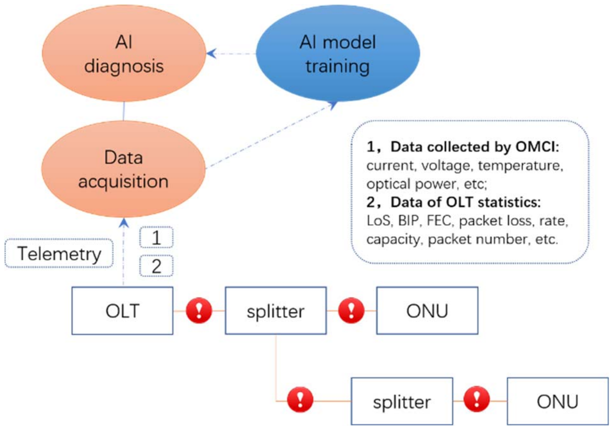


Figure 115: PON optical path diagnosis

The AI platform continuously monitors and analyses the Access Network optical path status using the collected data, such as packet loss and optical power, etc. and outputs an optical path status chart.

Optical path fault results, such as weak light, frequent flash failure, optical path termination, etc. can be accurately identified using models such as a fault tree model.

AI model training (mainly offline training which has higher accuracy compared with online training which is vulnerable to incorrectly identified alarms) is responsible for providing updated fault tree models.

Some causes of optical path faults are:

1) PON board fault.

2) OLT optical module fault.

3) Feeder optical fibre fault, distribution optical fibre fault, drop optical fibre fault.

4) ONU fault, etc., can be accurately located using algorithms such as, correlation clustering algorithm.

Based on the diagnosed position of the fault, the number of online users, etc., fault impact and priority are evaluated accurately and intelligently. The associated work order system automatically sends alarms and orders supporting efficient operator maintenance.

7.18.2.2 Motivation

- Intelligent and timely analysis of optical path fault, enable automatic service provision.
- Provides a real-time display of optical path status.
- Supports proactive troubleshooting of optical path faults, and improve troubleshooting efficiency.

7.18.2.3 Pre-conditions

- Data acquisition module is available.
- Telemetry techniques are supported by OLT.
- The network has an AI diagnosis platform including fault tree model training.
- Availability of AI training data.
- The operator provides locations of Access Network elements, such as ONU, OLT and ODN.

7.18.2.4 ODN deployment operation flow

1) The operator deploys a data acquisition function and AI diagnosis function.

2) The AI-enhanced management system collects optical path faults, uses the fault information to train the AI system and learns the fault characteristics.

3) The AI-enhanced management system automatically reports optical path fault alarm information and issues maintenance work orders.

4) The AI-enhanced management system displays the optical path status near real-time.

History

Document history		
V1.1.1	June 2022	Publication