ETSI GR F5G 002 V1.1.1 (2021-02)

GROUP REPORT

Fifth Generation Fixed Network (F5G); F5G Use Cases Release #1

Disclaimer

Reference

DGR/F5G-002_use_cases

Keywords

customer premises networks, F5G, fixed networks, use case

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 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is 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 IPR Policy, no investigation, 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.

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 a first set of use cases to be enabled by the Fifth Generation Fixed Network (F5G). These use cases include services to consumers and enterprises as well as functionalities to optimize the management of the Fifth Generation Fixed Network. The use cases will be used as input to a gap analysis and a technology landscape study, aiming to extract technical requirements needed for their implementations. Fourteen use cases are selected based on their impact. 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] ETSI GS F5G 003: "F5G Technology Landscape F5G Technology Landscape".

[i.5] ETSI GS F5G 004: "F5G Network Architecture Specification F5G Network Architecture Specification".

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

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:

AI	Artificial Intelligence
AP	Access Point
API	Application Programming Interface
AR	Augmented Reality
ATM	Automatic Teller Machine
B2B	Business to Business
B2C	Business to Customer
BBU	Base Band Unit
BNG	Broadband Network Gateway
CAPEX	CAPital EXpenditure
CCTV	Closed Circuit TeleVision
CDN	Content Delivery Network
CE	Customer Edge
CO	Central Office
CPE	Customer Premise Equipment
CR	Core Router
CT	Communication Technology
CU	Central Unit
DBA	Dynamic Bandwidth Allocation
DC	Data Centre
DIM	Dynamic Integrity Measurement
DSLAM	Digital Subscriber Line Access Multiplexer
DU	Distributed Unit
E2E	End to End
EMI	Electro-Magnetic Interference
EPC	Evolved Packet Core
F5G	Fifth Generation Fixed Network
FAT	Fibre Access Terminal
FFC	Full-Fibre Connection
FGW	Fibre GateWay
FPS	First Person Shooter
FTTB	Fibre To The Building
FTTB/C	Fibre To The Building/Curb
FTTH	Fibre To The Home
FTTR	Fibre To The Room
GE	Gigabit Ethernet
GPON	Gigabit-capable Passive Optical Network
GRE	Guaranteed Reliable Experience
HD	High Definition
HDTV	High Definition TeleVision
HIS	Hospital Information System
HQ	HeadQuter
HSI	High Speed Internet
HW	HardWare
IIoT	Industrial Internet of Things
IP	Internet Protocol
IPTV	Internet Protocol TeleVision
IT	Information Technology
LAN	Local Area Network
MAC	Media Access Control
MAN	Metro Area Network
MDU	Multiple Dwelling Unit
MOBA	Multiplayer Online Battle Arena
MOOC	Massive Open Online Course
NFV	Network Functions Virtualisation
NMS	Network Management System
OA	Office Automation

OAM	Operation And Maintenance
ODN	Optical Distribution Network
OLT	Optical Line Termination
ONT	Optical Network Terminal
ONU	Optical Network Unit
OPEX	OPerational EXpenses
OSS	Operation Support System
OT	Operational Technology
OTN	Optical Transport Network
P2P	Point to Point
PACS	Picture Archiving and Communication Systems
PC	Personal Computer
PLC	Programmable Logical Controller
PoE	Power over Ethernet
POL	Passive Optical LAN
PON	Passive Optical Network
PoP	Point of Presence
RA	Remote Attestation
RAN	Radio Access Network
RRH	Radio Remote Head
RTT	Round Trip Time
RTU	Remote Teminal Unit
RU	Radio Unit
SDN	Software-Defined Network
SD-WAN	Software-Defined Wide Area Network
SFP	Small Form Pluggable
SLA	Service-Level Agreement
SME	Small and Medium Enterprises
STP	Shielded Twisted Pair
TCP	Transmission Control Protocol
TPM	Trusted Platform Module
TSN	Time-Sensitive Networking
TV	TeleVision
UAC	User Application Client
UAS	User Application Server
UHD	Ultra-High Definition
URLLC	Ultra-Reliable and Low Latency Communications
UTP	Unshielded Twisted Pair
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VR	Virtual Reality
VR/AR	Virtual Reality/Augmented Reality
VTM	Video Teller Machine
WAP	Wireless Access Points
WIFI	Wireless Fidelity
WLAN	Wireless Local Area Network
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 include improved speed, capacity, coverage, responsivity, density, reliability, availability, security, operational efficiency, energy efficiency and spectral efficiency 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, fourteen use cases are described. 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 the document on generation definitions [i.1], 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, and
- all dimensions of the F5G system architecture are needed to implement the use cases.

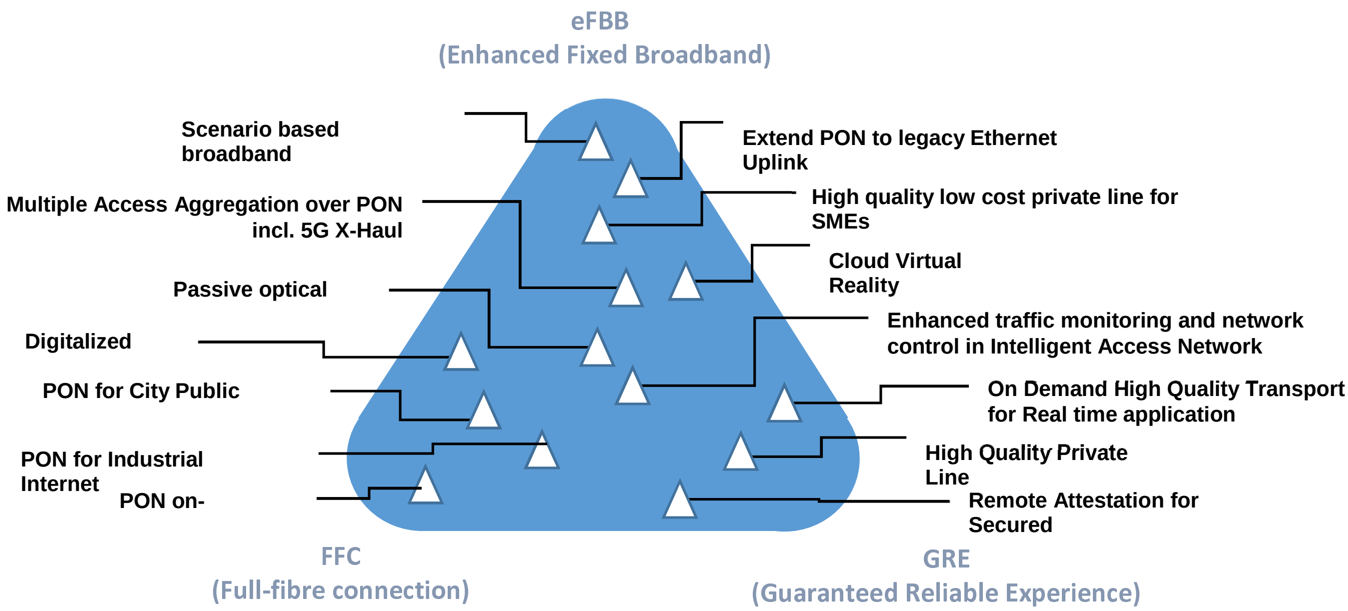


Figure 2: F5G use cases driving the three dimensions of F5G, the enhanced Fixed BroadBand (eFBB), Full-Fibre Connection (FFC), and Guaranteed Reliable Experience (GRE)

5.2 Application Area Perspective

A key motivation for F5G is leveraging technologies of current fibre optical networks to benefit more application areas namely extending the business to cover new fields, including numerous applications in the vertical industries.

The use cases described in the present document cover the major anticipated areas including residential applications, business applications, network internal topics such as network optimizations and the use of F5G for mobile front, midhaul, and backhaul, and finally vertical applications oriented use cases. Many use cases will address topics that may be applicable in different application areas, therefore features and solutions needed by one use case may benefit other areas as well.

Use cases may be classified from the application and business area perspective. For each of the three main technical drivers eFBB (speed), GRE (latency), and FFC (density), additional subcategories on the application and business area are introduced. 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 1.

Table 1: Mapping use cases into application categories

Technical driver	Application category	Corresponding use cases
eFBB (speed)	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)
	Customer premises networking	6.4 Use case #4: PON on-premises) (6.5 Use case #5: Passive optical LAN)
	Physical networking	6.14 Use case #14: Digitalized ODN/FTTX
GRE (latency)	Immersive experiences	6.1 Use case #1: Cloud Virtual Reality
	Time-sensitive applications	6.12 Use case #12: On Demand High Quality Transport for Real time applications
	Reliable communications	6.2 Use case #2: High Quality Private Line 6.13 Use case #13: Remote Attestation for Secured Network Elements
FFC (density)	High-density endpoints	(6.4 Use case #4: PON on-premises) (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
	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
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 are 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 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.

6 Description of use cases

6.0 Introduction

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.

In the present document each use case includes the context of the use case and a detailed description.

The use case context introduces the background of each use case, providing a quick overview of the covered application and associated challenges.

The description of the use case provides more detailed information. It includes the overview (what is the use case), motivation (the benefits the use case provides), actors/roles (who will be involved in the use case and what they will do in the use case) and precondition (what should be ready before the use case is running).

All the use cases in the present document are identified in Table 2, grouped into 3 use case types - new/enhanced services to users, expanded fibre infrastructure and services, management and optimization.

Table 2: List of Use cases

New/Enhanced Services to Users
6.1 Use case #1: Cloud Virtual Reality
6.2 Use case #2: High Quality Private Line
6.3 Use case #3: High quality low cost private line for small and medium enterprises
Expanded Fibre Infrastructure and Services
6.4 Use case #4: PON on-premises
6.5 Use case #5: Passive optical LAN
6.6 Use case #6: PON for Industrial Manufacturing
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
Management and Optimization
6.10 Use case #10: Scenario based broadband
6.11 Use case #11: Enhanced traffic monitoring and network control in Intelligent Access Network
6.12 Use case #12: On Demand High Quality Transport for Real time applications
6.13 Use case #13: Remote Attestation for Secured Network Elements
6.14 Use case #14: Digitalized ODN/FTTX

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.

The order of use cases in the subsequent clauses follows the order in Table 2.

6.1 Use case #1: Cloud Virtual Reality

6.1.1 Use case context

Based on cloud computing and rendering technologies, Cloud Virtual Reality (VR) applications introduce vast amount of data exchange between the terminal and the cloud server. It will place stringent requirements on the bearer network (e.g. bandwidth, latency, jitter, and packet loss), which will require 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 experience, much higher available and guaranteed bandwidth (e.g. > 1 Gbps), lower latency (e.g. < 10 ms) and lower jitter (e.g. < 5 ms) are required.

This use case gives a brief introduction of Cloud VR applications and the required capabilities on fixed bearing network.

6.1.2 Description of the use case

6.1.2.1 Overview

Cloud VR offloads computing and cloud rendering in VR services from local dedicated hardware to a shared cloud infrastructure. Cloud rendered video and audio outputs are encoded, compressed, and transmitted to user terminals through fast and stable networks. In contrast to current VR services, where good user experience primarily relies on the end user purchasing expensive high-end PCs for local 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 influence the achieved sense of reality, interaction, and pleasure, which are related to the network properties (e.g. bandwidth, latency 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 jitter.

Cloud VR implements computing and rendering in the cloud. Any latency from remote processing compromise the sense of interaction, including latency in loading, switchover, and joystick operations. The most important effect of high latency in VR is the user becoming sea-sick or dizzy. Note that high jitter will cause VR play-out to not being smooth and frames might be distorted or lost.

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

The sense of pleasantness 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, need to meet the requirements to realize pleasurable experience.

Figure 3 shows an overview of Cloud VR network architecture.

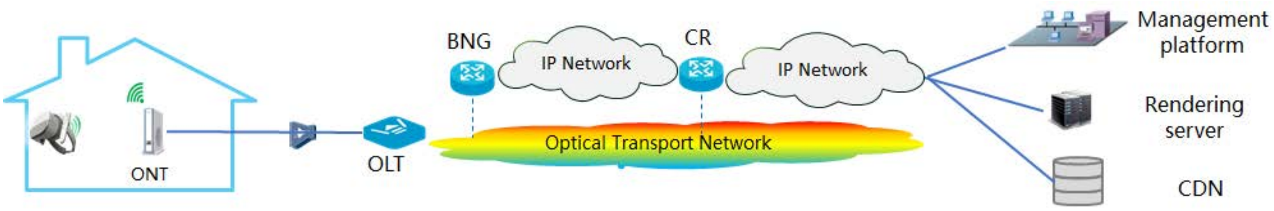


Figure 3: Cloud VR network architecture

As depicted in Figure 3, the Cloud VR bearer network includes the home network, access network, metro IP network, and an 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 home networks through OLT.
- The metro network provides the IP bearer function, and it is connected to the Cloud VR management platform, rendering server and CDN through backbone network.

Cloud VR places stringent requirements on the network. It can be transported with current Internet services, however they will-affect each other's 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 assures the desired performance and 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 transport network. From the server side, Cloud VR traffic is transported via the same independent channel. A general view is shown in Figure 4.

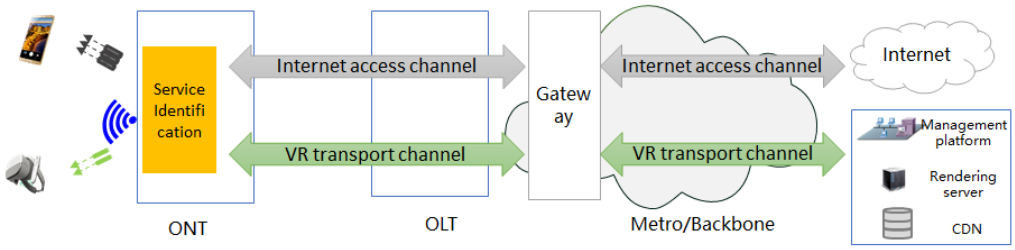


Figure 4: Cloud VR transport in independent channel

6.1.2.2 Motivation

The key features of Cloud VR are cloud-based rendering and delivery of VR content. 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 on 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 will show the process with Cloud VR service bearer in 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 5.

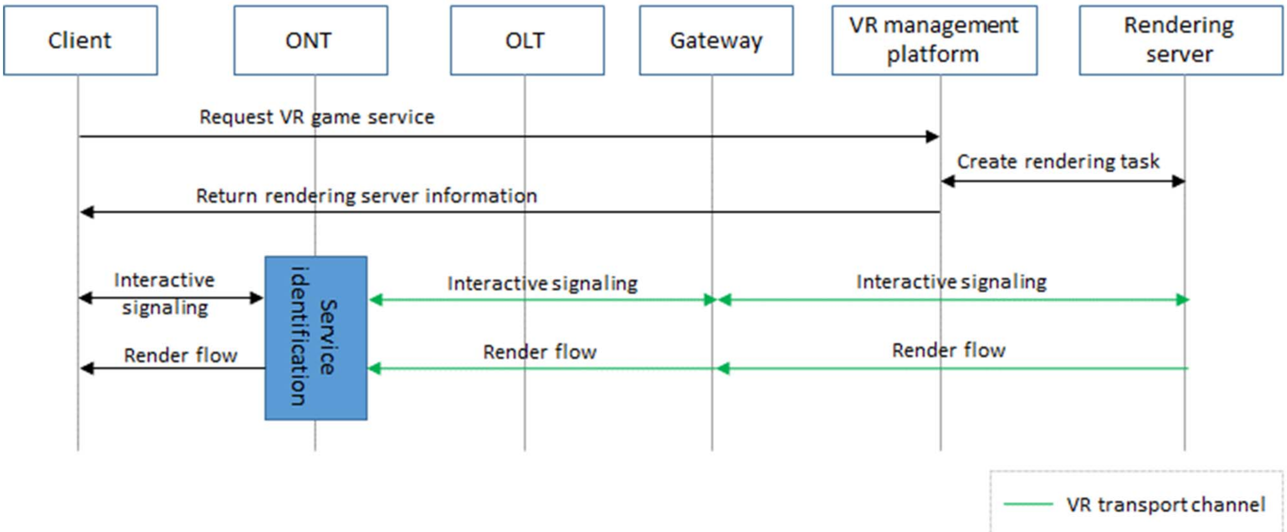


Figure 5: Operational flow of Cloud VR game service

1) When a user starts the game, the client sends a request to VR management platform for gaming service. VR management platform returns the rendering server information after the rendering task was created. 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 ONT, and 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 then will be further directed to the Cloud VR transport channel in Metro/Backbone 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

A high quality private line is strongly demanded in certain scenarios. High quality private line has 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

The government institutions, financial organizations, and medical organizations require private lines with high quality. 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 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 necessary bandwidth.

- Financial Organizations:

  Financial organizations include banking and financial services:

  a) Banking: Digital transformation has brought unprecedented challenges to traditional banking business, while also putting tremendous pressure on the infrastructures, requiring 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, which means that high-quality private lines are required. The evolution of the banking network architecture is shown in Figure 6.

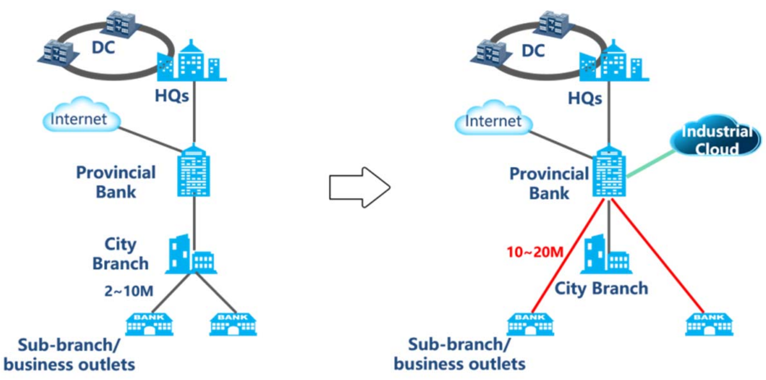


Figure 6: Banking network architecture evolution

The bank's internal network is divided into an office network and a production network. An office network services include: OA (Office Automation) system, mail system, video conference system, video surveillance system, etc. 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 connection to a provincial branch is being upgraded from 2 ~ 10 Mbps to 10 ~ 20 Mbps. Assuming a large number of branches belonging to a provincial level branch, the total bandwidth of all its private lines 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 the trading hours, each branch office has redundant connections to the headquarters; there are also redundant lines within the headquarter. One possible typical networking architecture is shown in Figure 7.

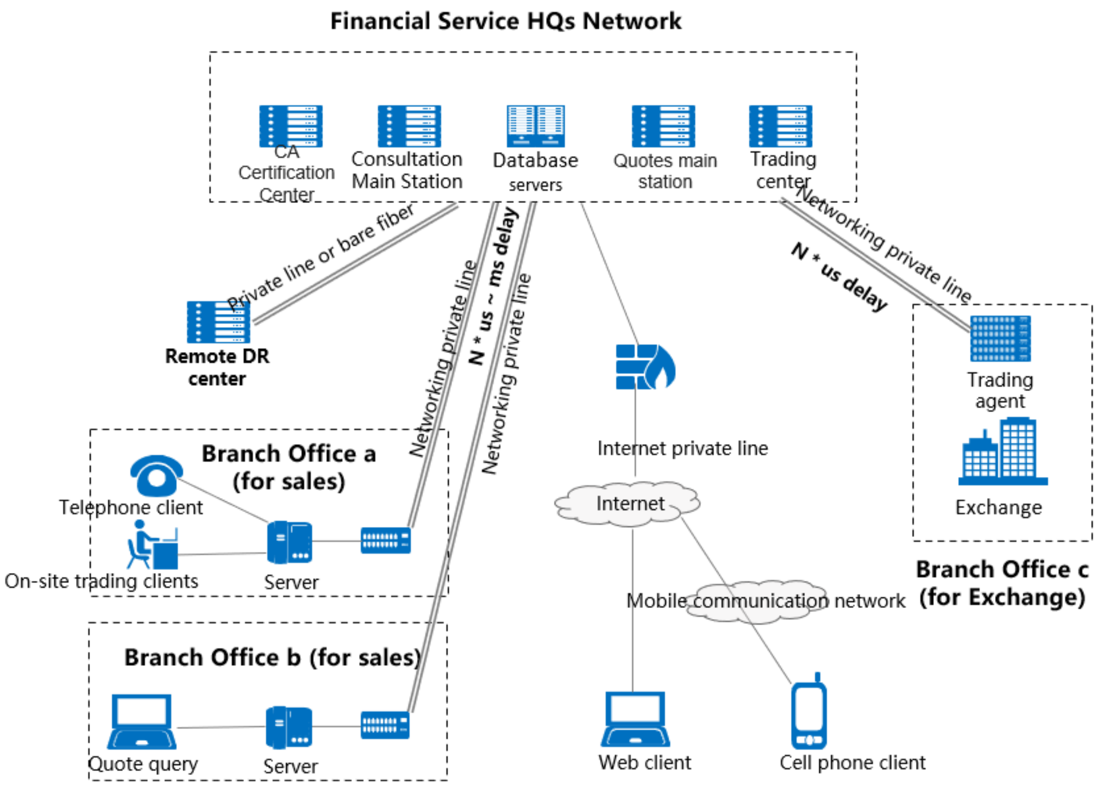


Figure 7: Typical network architecture for financial services

The typical network topology of the financial services is Hub-Spoke. All sites managed by HQ go through to the HQ for transaction and market query.

Typically digital private lines are used for data exchange between branch offices and headquarters, as well as data exchange between headquarters and 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 exchanges for orders and market inquiries. The security level of the production network is very high; therefore it 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. Now 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, bringing advantages of 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. At the same time, 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, 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 of exclusive use for organizations to allow for higher security and performance.

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

- Medical cloud:

  To ease the on-premises asset burden, many medical associations are migrating the 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 typical applications preferably deployed on the cloud.

  A large amount 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 huge, which normally needs higher than 1 Gits/s speeds to ensure good experience during upload and download. The images need to be stored on the Cloud for months or even for years, which demands for high storage volume and high reliability at the cloud.

  HIS is used to record the patient's diagnosis and treatment data. This information is highly confidential and requires a dedicated network from 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 the cloud desktop for reducing assets in operations 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 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 high quality of the 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 the scenario of competition with Internet Service Providers (ISPs), carriers use multiple technical means 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 above scenarios, a high quality private line is supposed to have the following capabilities:

a) Guaranteed bandwidth: the bandwidth is absolutely guaranteed. Private line bandwidth granularity can be flexibly configured from 2 M to 100 G 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 reaches the carrier-class 50 ms, and the link availability can reach 99,999 %.

c) Business security: physical equipment isolation; L1 hard pipe isolation; L2 logical pipe 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, which may reach vast amount of connections in some larger 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) Quick 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: private line service can be quickly provisioned in days or even minutes. Therefore, E2E service provisioning and O&M, plug-and-play private line CPE, and automatic and fast provisioning of combined Cloud-network services are required to simplify the configuration of CE devices in enterprises.

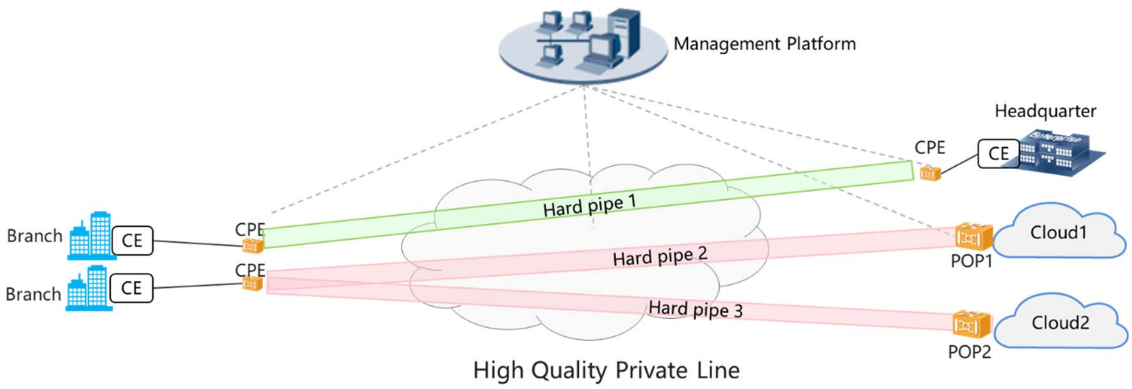


Figure 8: High quality private network

As shown in Figure 8, 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 transmission 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 for any type of 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 reduce heavy 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 opening of the high quality private line, the following preconditions are required:

- CE equipment 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 9.

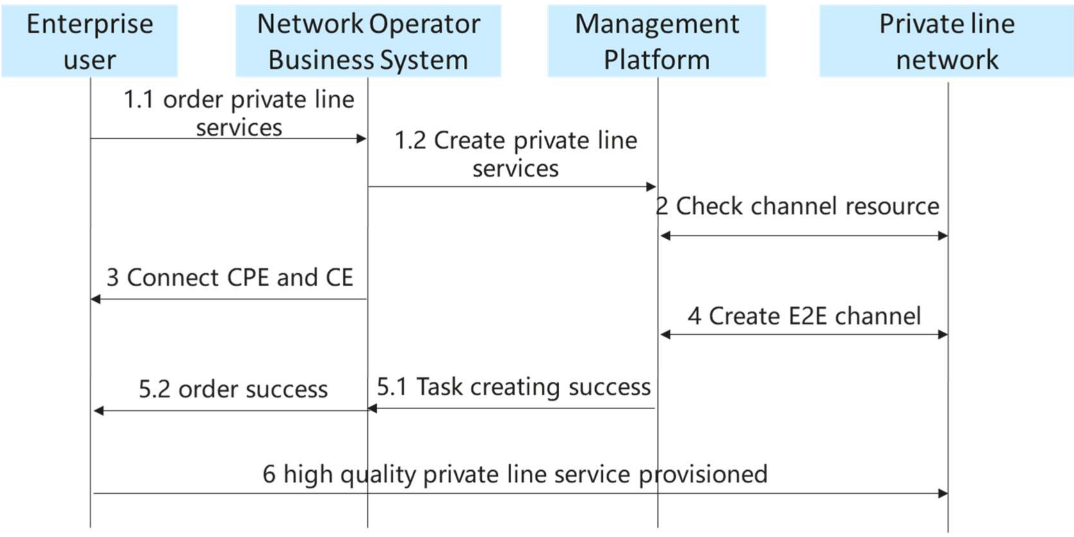


Figure 9: Provisioning process of high quality private line

1) The enterprise purchases 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 hard pipe resources (2);

3) If resources are available, the operator deploys CPEs, connects CPEs to the CE, and performs necessary configurations;

4) The management system creates a hard pipe to the Private line Network, 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 met by currently available solutions such as better service quality according to 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. Legacy leased 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:

1) Internet access: 32 ~ 128 terminal devices need to be connected to the operators' CPE. The Internet access bandwidth should be assured.

2) Cloud service: Micro enterprises need Cloud-based virtual desktop based on 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.

3) 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 should be secure and reliable.

4) Telephony services: Multiple telephony clients need to be supported.

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

a) Wide coverage: The network and the SME private line service needs to cover a wide geographical area.

b) 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.

c) Connecting up to 128 terminals (many of which are wireless devices).

d) Supporting 99,99 % network availability and 1 Gbit/s to 10 Gbit/s bandwidth.

e) Supporting the four key services mentioned above over a single SME private line service subscription.

f) Isolating SME users from home broadband users, as they may share the network infrastructure with residential customers.

g) Fast provisioning.

h) Plug-and-play CPE and quick trouble shooting.

To meet 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 10.

- 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).

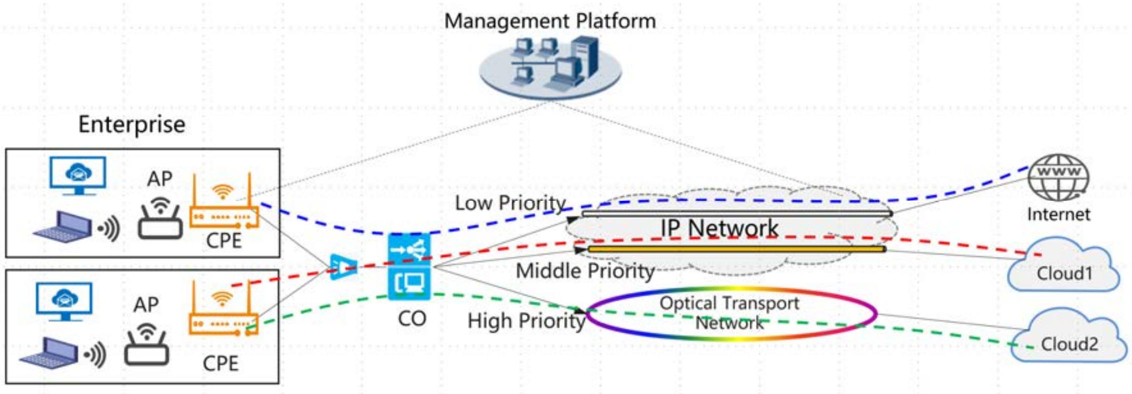


Figure 10: SME private line service identification and distribution of application traffic

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, and 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 exploring 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 11.

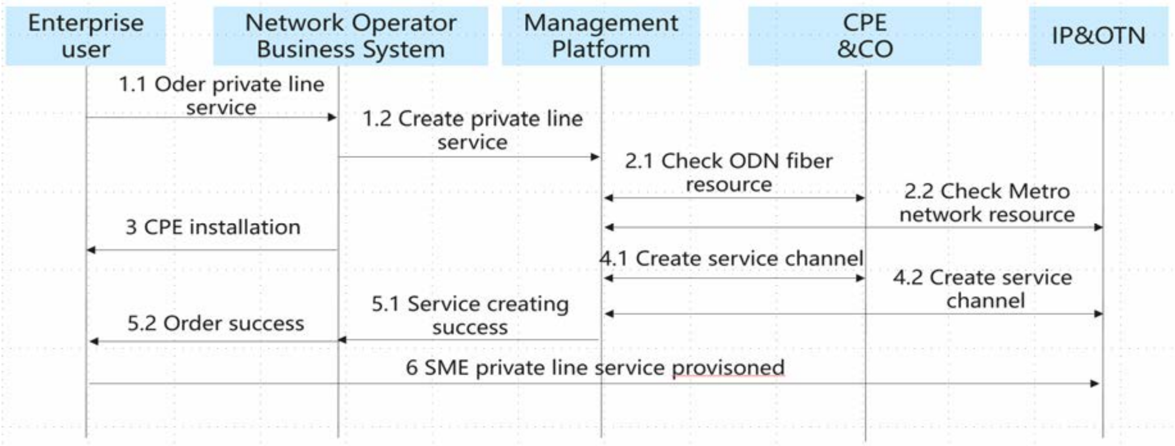


Figure 11: Flowchart of SME private line service provisioning

1) When SMEs need a private line service, they purchase 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 metro area network (MAN) resources (2.2).

3) In case the resources are available, the operator installs CPEs, connect 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 priorities of different services (4.1). Create service channels on the MAN devices to forward service data traffics with different priorities (4.2).

5) After the access network and MAN 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: PON on-premises

6.4.1 Use case context

XG(S)-PON standard (Recommendation ITU-T G.987 [i.3]) has been published in 2010 and XG(S)-PON is a commercially available solution for the access network. With XG-PON, each user can obtain more than 1 Gbps bandwidth. However, end user devices are usually not directly connected to the access network but instead, to the on-premises network. In order to take full advantage of the access network capabilities, the on-premises network should be matched with the access network. The current connections in the house are mostly copper or wireless based, and they suffer from limited capacity due to the restricted frequency range and limited spectrum resource. In this case, users would like to deploy new media for the on-premises network. Fibre is a preferred upgrade choice for the on-premises network due to its future proof capabilities.

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 two typical scenarios of fibre on-premises network that will be shown as good examples in the context of this use case.

- PON for home area network.

- PON as a supplement in FTTB/C for Apartment houses in dense residential areas.

6.4.2.1.2 PON for in-home networking

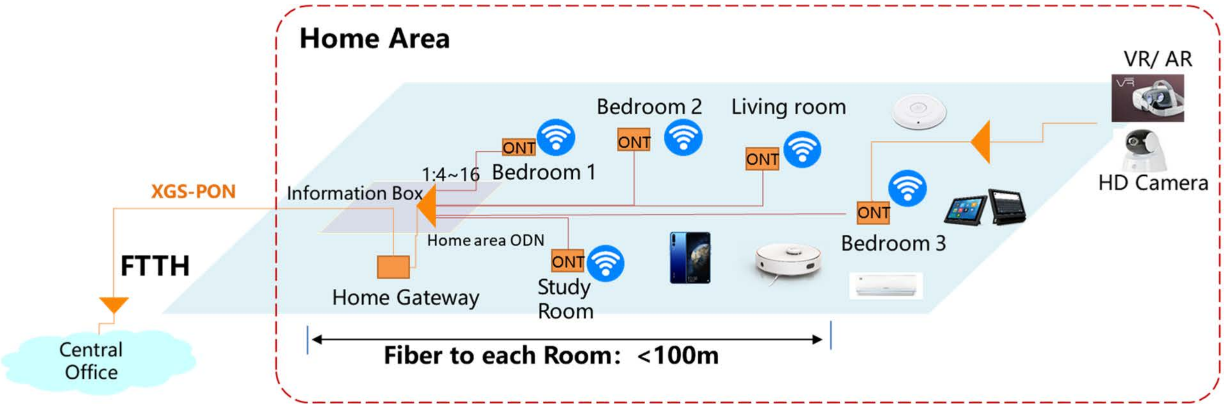


Figure 12: PON in Home

As known, Wi-Fi® is widely used in home networks due to its convenience of connection. 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 maximal 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 also 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 cable can be small, light and flexible, so it is easy to deploy fibre in the home area. Figure 12 shows a simplified PON system for home network. From the central office to the home gateway, there is an XG(S)-PON system that can deliver Gigabit access bandwidth from the network operator. From the home gateway, Wi-Fi® and simplified PON is used in home area network for the access 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 quality. The simplified PON system can connect to Wi-Fi® Access Points in several rooms of the home area network. In order to optimize the performance of the Wi-Fi®, coordination of the Wi-Fi® APs is supported by the simplified PON system if possible.

6.4.2.1.3 PON as a supplement in FTTB/C for Apartment houses in dense residential areas

Figure 13: PON for dense residential area

In some dense residential areas, the fibre for the access network is deployed to the building or curb (FTTB/C). From the access point in the building or curb to each apartment, copper cabling is still 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-based medium. An XG(S)-PON can be deployed from the central office to the building or curb, and then another PON system can be deployed from this point on inside the building for each individual apartment. In this way, the operator could reuse the deployed fibre and sites, and the users can enjoy an excellent network experience.

6.4.2.2 Considerations for on-premise devices

In order to deploy PON on premise, OLT function needs to be integrated inside the premise device, in place of the legacy LAN side Ethernet ports. For example, a typical Home Gateway has 4 Ethernet ports. Once a PON-based FTTR is deployed, these 4 Ethernet ports are replaced by one PON port. Potentially, the size of the device can be even smaller. The uplink of this Home Gateway is still PON, and a new kind of ONU may be proposed, consisting of a miniaturized OLT embedded in an intelligent home ONU. The cascaded PONs could have common management tools and cooperative mechanisms to forward the customers' traffic (i.e. a shared media access control (MAC) function).

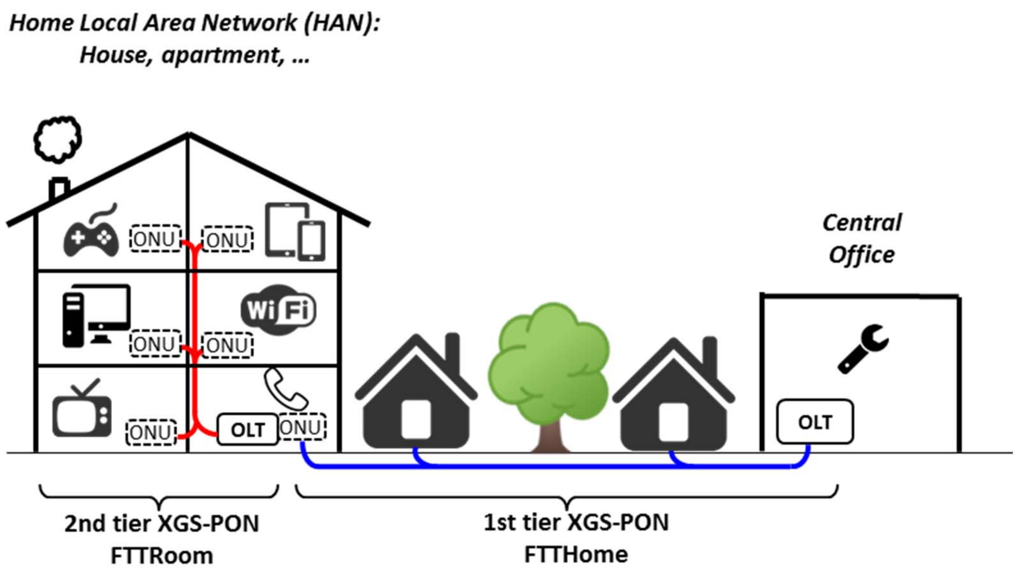


Figure 14: Cascaded PONs with new on-premises devices

6.4.2.3 Motivation

Using fibre connection (single mode fibre as an example) within home brings several advantages:

- The bandwidth can be sensibly upgraded, rendering this medium future proof.
- 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 divided transmission channels for different services.
- The optical signal in the fibre is immune to electro-magnetic interference (EMI).
- The fibre is lightweight and in small size, leading to an 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 PON on-premises networking, there are several pre-conditions as follows:

- Fibre has been deployed on-premises.
- Efficient solutions to extend the XG(S)-PON service to the on-premises network.

6.5 Use case #5: Passive optical LAN

6.5.1 Use case context

Legacy LAN networks are used in business areas, campus, 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 traditional 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:

1) The bandwidth is insufficient to meet the traffic requirements of new applications.
2) Copper wire deployment costs are high and not effective for future network upgrades.
3) The power consumption is high and the equipment occupies a large area.

To cope with these challenges, some forward-looking enterprises have used 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 connection, but also supports all functions provided in 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 15, 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. 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.

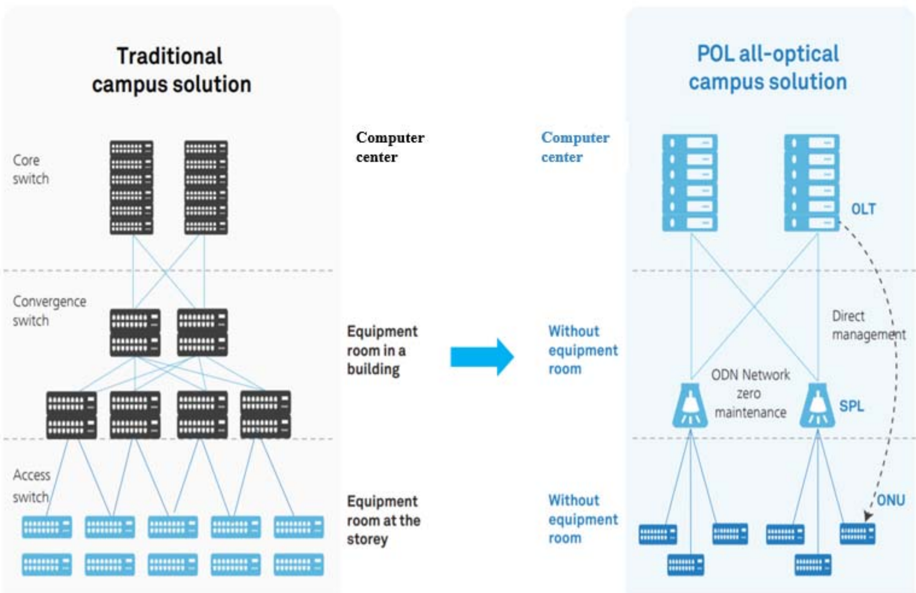


Figure 15: The POL all-optical solution compared with traditional campus solution

POL can be used in different scenarios. The location of OLT and ONU in different scenarios could be different. Table 3 to Table 5 describe the following three typical scenarios of POL.

- 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

Typical Case	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

Typical Case	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 fiber 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 fiber distribution subsystem area.	Students' dormitories and small office buildings	

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

Typical Case	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, resorts, railways/highways and shopping centres.

6.5.2.1.2 Hotel

In the hotel, the overall architecture is shown in the Figure 16. In this architecture there are the following features:

- One single fibre infrastructure for all the services required at the hotel.
- One Fibre Gateway (FGW), a ONU with integrated router and WiFi capabilities, per guestroom providing all the services (internet, Wi-Fi®, Voice, TV and IPTV).
- ONUs spread 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.
- One single vendor/integrator for OAM/Support.
- One OLT can support all the end points required at the hotel.
- Web Management Portal.
- VoIP Server included.
- IPTV Server/Streamer.

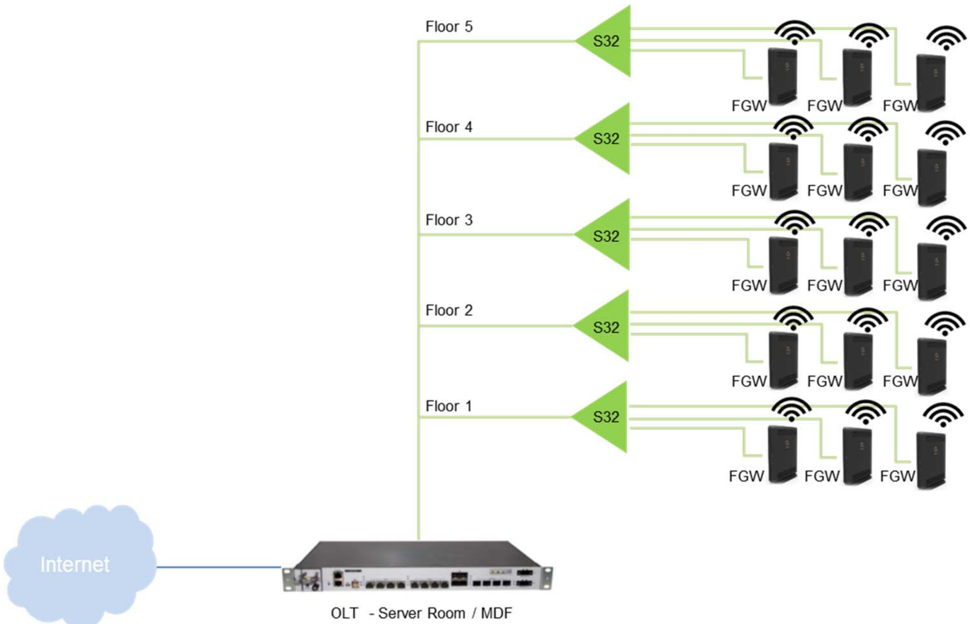


Figure 16: Overall PON architecture in the hotel

Figure 17: ONU at each guestroom

In the hotel each guestroom uses ONU, providing HSI, TV, IPTV and phone as shown in Figure 17. Spread across the hotel, there will also be ONUs with added services such as hot-lines for emergency situations and IP cameras for surveillance as shown in Figure 18. As ONUs can provide both standard Ethernet outlets as well as connectivity for Wireless Access Points (WAPs), this avoids the need to install two devices (ONU and WPAs) for the common areas (lobby, hallway, stairs, pool, gym, etc). This ONU has be capable of supporting multiple Wi-Fi® users, in the 2,4 GHz and 5 GHz bands, independent streams of data, provide QoS based on L2 or L3 as well as WLAN roaming.

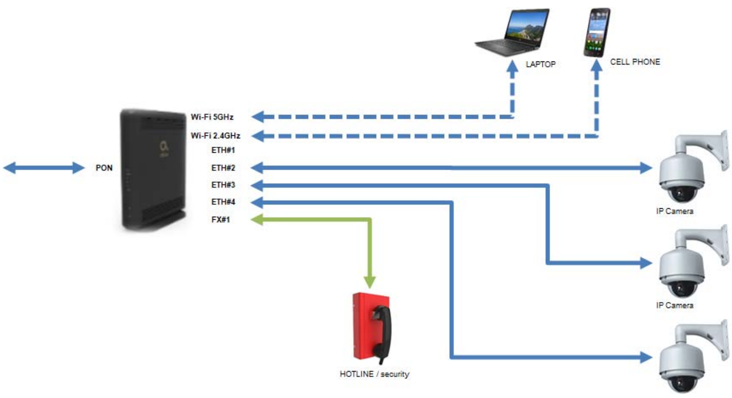


Figure 18: ONUs spread across the hotel for common services

6.5.2.1.3 Stadium

In the stadium, the overall architecture is shown in the Figure 19. In this architecture there are 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 spread 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.
- One single vendor/integrator for OAM/Support.
- One OLT can support all the end points required at the stadium/arena.

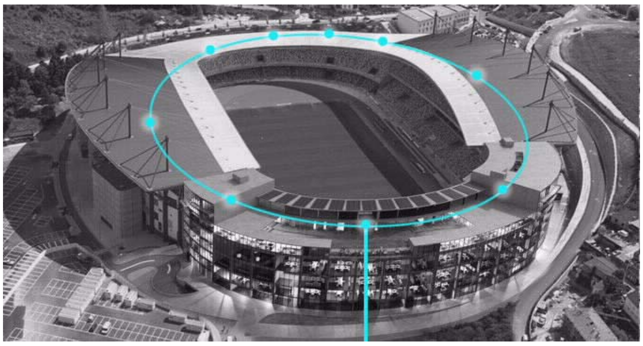


Figure 19: Overall PON architecture in the stadium

6.5.2.1.4 Holiday Resort

In the holiday resort, the overall architecture is shown in the Figure 20. In this architecture there are 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 spread 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.
- One single vendor/integrator for OAM/Support.
- One OLT can support all the end points required at the resort.

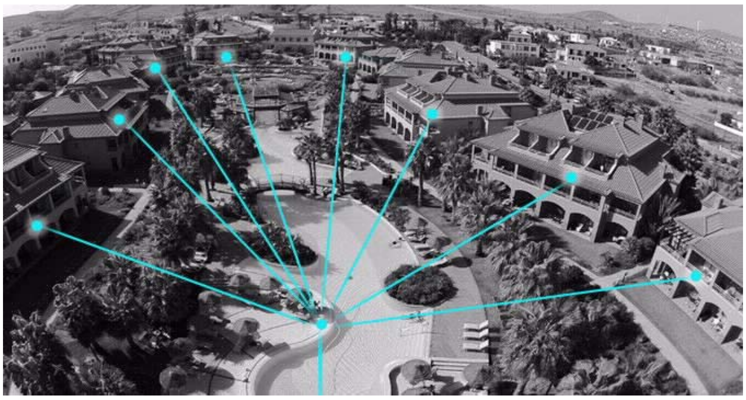


Figure 20: Overall PON architecture in the resort

6.5.2.1.5 Railways/Highways

In the railways/highways case, OLT with less PON ports will be installed along the railway or highway at each 60 km. Along those 60 km ONUs will be installed with unbalanced splitters. This system will provide the proper telecom infrastructure to build a secure LAN infrastructure for the railway or highway operator, which will be able to transport data coming from CCTV cameras (High Definition), be used for telemetry, road signals, and display panels and also VoIP (SOS/hotlines).

6.5.2.1.6 Shopping Centre

In the shopping centre an OLT could be installed in a central technical room of the facility and from there multiple fibres would reach not just all the stores but also places across the mall 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 mall, depending on the desired split ration and configuration of the shopping centre. This fibre will be used for all telecom needs of the mall, meaning internet, intranet, CCTV, voice, TV, IPTV and Wi-Fi™. All services would be separated by means of assigning different VLANs. Each store would receive an ONU with embedded gateway functionality and that would be the demarcation point of the mall infrastructure. The network would allow bitstream services (also supported with an 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) during transmission.
- Fibre cannot be oxidized and has a longer service life. It adopts a point-to-multipoint networking topology which can save a lot of backbone fibre resources. Active equipment centralized within Building Network Rooms, with a centralized exploitation of the LAN from the OLT.

6.5.2.3 Pre-condition

In order to deploy POL, there is 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.

Meanwhile, 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 need to be upgraded to support the new cloud-based production machine control system. The end-to-end equipment networking feature within the production including data collection and data transport is the fundamental feature of factory intelligence.

PON technology has become a major direction for factories intra-plant network innovation, as a novel network platform built from advanced passive optical fibre communication technology. When it is combined with factory automation systems, the future 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 shopfloors.

2) Supporting of fundamental network and data services for enterprises cloud connecting.

3) Supporting of abundant 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 described in Figure 21.

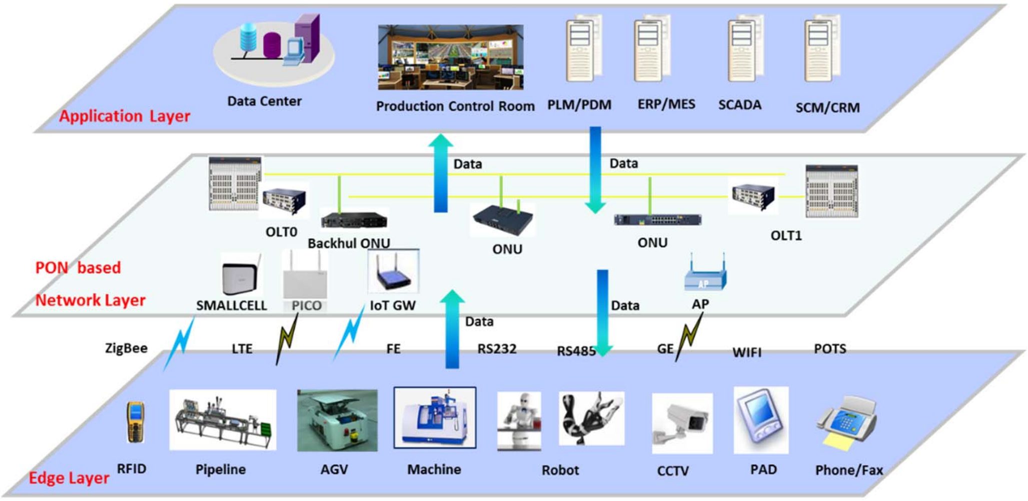


Figure 21: PON based industrial network solution overview

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: realize low-cost all-in-one multi-service carrying PON system, simplifying the factory intra-plant network architecture and lowering the network transmission latency when necessary.

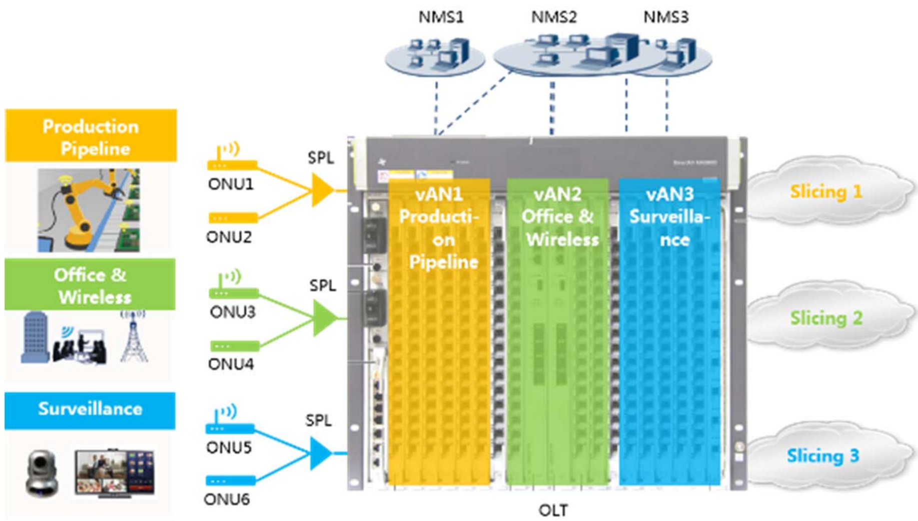


Figure 22: Schematic diagram of PON slice

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 inside 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 1ms in some specific applications. Besides, time synchronization function is available when necessary. Time Sensitive Networking (TSN) features will be supported in the future.

6) Network resilience and availability: Implementation of protection switching (restoration time expected to be less than 50 ms), targeting 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 into the industrial world:

- Electromagnetic Isolation using fiber optics only. This guarantees connectivity in a very noisy electromagnetic environment (electric motors, Variable Frequency Drives, Inverters, etc.). To avoid this problem, traditional networks based on structured cabling use expensive shielded cabling (STP).

- Conventional copper cables require a large amount of pipeline resources which make future network expansion or scaling difficult. The copper cables also have several reasonable problems: the replacement and updating should be covered within short-term (3 years in some cases) due to the deteriorating characteristics of copper cables such as oxidation. Unlike the metallic cables, PON network based on optical fiber has advantages of both lifetime and volume, for example, optical fiber generally has long lifetime for around 20 years, which means stable network and lower OPEX.

- Extend communications through a passive network up to 20 km. This ends with the limitations of 100 meters typical of traditional structured cabling and switching systems, which hardly 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 shown in Figure 23.

Industrial PON includes simultaneously three typical scenarios or networks:

- Industrial Process Field Data network.

- Office network.

- Surveillance network.

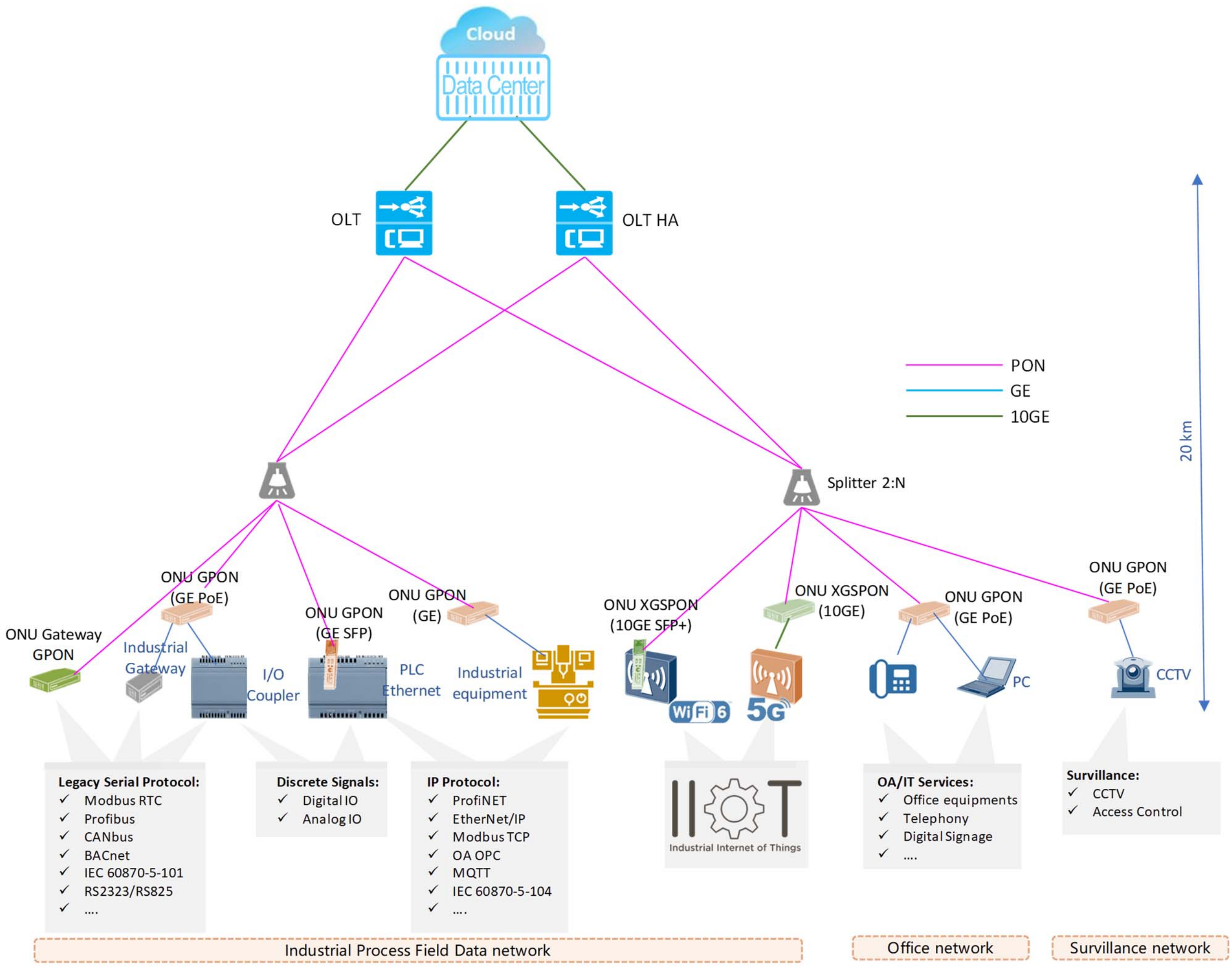


Figure 23: Industrial PON

1) Industrial Process Field Data network

The transport of enterprises factory intra-plant process data files is a crucial application scenario for industrial PON as shown in Figure 23.

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

- Connectivity services through PON interfaces: The carrying of enterprises factory intra-plant fieldbus services is a crucial application scenario for industrial PON as shown in Figure 23. 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 also support integrated open sources or client customized industrial applications, which can be employed to provide customization of industrial data collection and conversion process, with the interaction with industrial cloud platform, to realize the entire interconnection between devices and information systems.

- Connectivity services through GE (Gigabit Ethernet) interfaces:

  - 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.

  - IP Industrial protocols (ProfiNET, EtherNet/IP, Modbus TCP, etc.) from PLC or other Industrial Equipment.

- IIoT devices: The explosion of connectivity in Industry 4.0 will come from these devices and their connectivity will be mostly wireless through Wi-Fi6® and 5G services. Industrial PON provide xhaul services that allow the deployment of WIFI6 or 5G networks.

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

As shown in Figure 23, for the integration of these services, industrial grade ONU will be used, which have the mechanical and environmental characteristics of the industrial environment: degrees of protection (dust, water, etc.), extended temperature ranges. Types of ONU:

- GPON Gateway ONU with industrial physical interfaces and built-in gateway functions
- GPON ONU with GE (Gigabit Ethernet) interfaces and PoE functionality.
- XGS-PON ONU with 10GE interfaces needed for AR/VR applications or 5G/Wi-Fi6® xhaul.

Likewise, the use of ONU in SFP/SFP+ format is especially important for Industrial PON, allowing its direct integration in industrial equipment: PLC, Access Point Wi-Fi6®, etc.

2) Office network

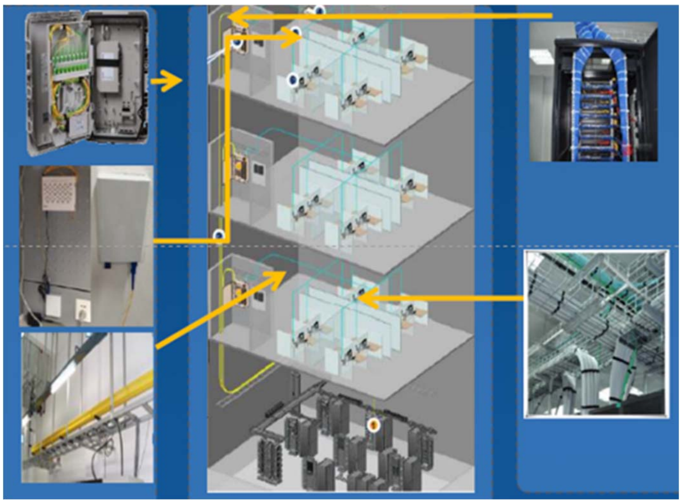


Figure 24: PON for office network, the internal networking in the office park with internet/intranet, telephone, fax services

Industrial PON is capable of carrying official OA (Office Automation) traffic, telephony system and etc. in office area as shown in Figure 24. Conventional office networks are typically constructed by Ethernet switches, which needs to be configured and managed independently, resulting in complex and inefficient services configuration. Also, Ethernet switches lack mature unified network management systems. Hence their maintenance, performance monitoring and troubleshooting are often causing problems in network operation.

By industrial PON, with unified services configuration and management, fast troubleshooting can be achieved.

3) Surveillance network

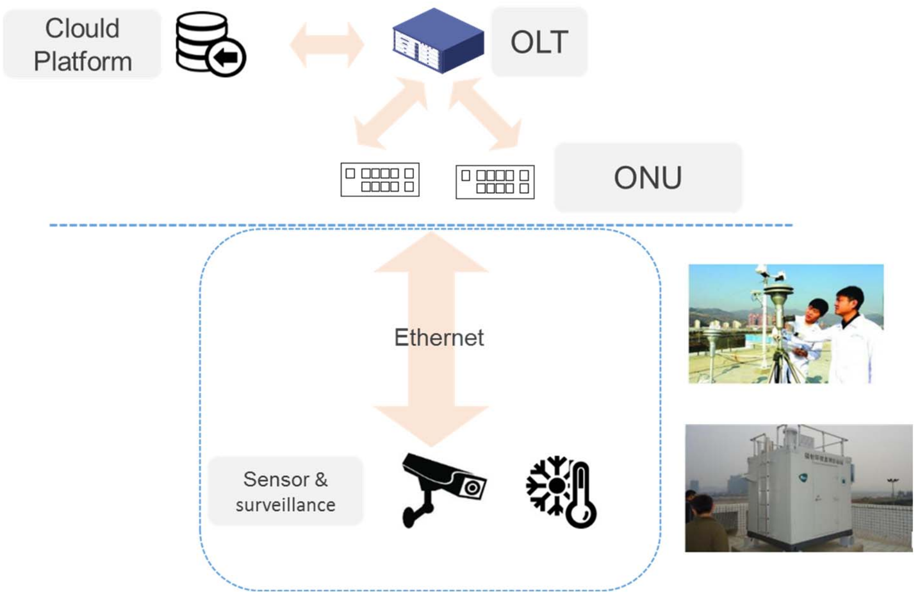


Figure 25: PON for sensor & surveillance network overview

Industrial enterprises have strong requirements in real-time applications such as video monitoring and environment sensing. The industrial PON can provide fully support for these sensing services as shown in Figure 25. PON ONU is capable of PoE (Power over Ethernet) function when necessary to provide both network connection and electricity supply for remote video monitoring cameras, flexible supporting the full scene installation of the cameras. Other capabilities such as WiFi AP can also be set inside the PON ONU to realize the data carrying and transmission for several kinds of sensors.

6.6.2.2 Motivation

There will be several advantages with PON used for industrial application:

- PON technology is widely used worldwide to construct FTTH network for a huge number of residential users, which has been proven to be 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 be easily built in to enhance the network capability, such as integrating diversified industrial protocols, and full interconnection among all equipment in factories, a uniform intra-plant factory network capable of any traffic generated in a factory.
- PON can deliver long distance connection, low-density layouts, and EMI immunity.
- The discontinuity between the factory production management network and production shopfloor or field network can be overcome, with increased production efficiency and quality, reduced costs, improved of production management and 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 should be well-prepared.
- 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 quite a promising method for a basic network in the context of city public service, and a typical scenario could be using PON in a smart city network. Technologies used in smart city 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 usually viewed as a good support 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:

1) meet the requirements of urban landscape and environmental constraints;

2) the placement of poles should be reasonably selected to meet the objectives of effective coverage of the target area, taking into account the effective coverage of each installed device, combined with the needs of users and services;

3) the poles should 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 room-saving connections with high performance and high energy efficiency. Furthermore, benefiting from the massive deployment of PONs in access network for years, PON systems can be cost effective, and can be extended to other scenarios. Figure 26 shows a practical example of PON use for connecting smart light poles.

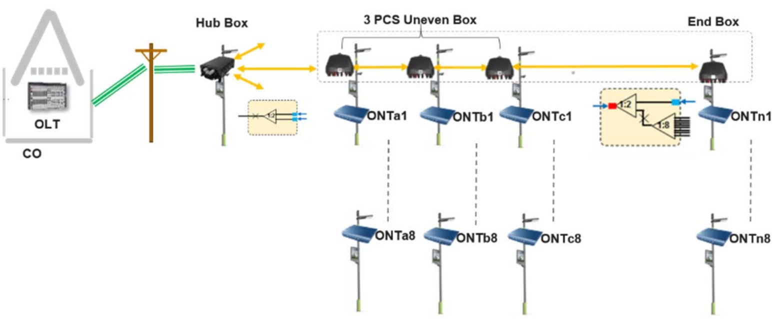


Figure 26: PON based connection for smart light poles

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 topology 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 are required for the high density needs of 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, lower number of fibre termination, CO space reduction, and lower power consumption, while guaranteeing a high quality of service and customer experience.

One of the main challenges to 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.

GPON technologies are 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. Current (XGS-PON) and future (25/50G-PON, NG-PON2, etc.) PON technologies could in fact be adapted to implement the 5G mobile xHaul scenarios.

This use case focuses on the support of mobile x-haul 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 27 describes the multiple access aggregation over PON.

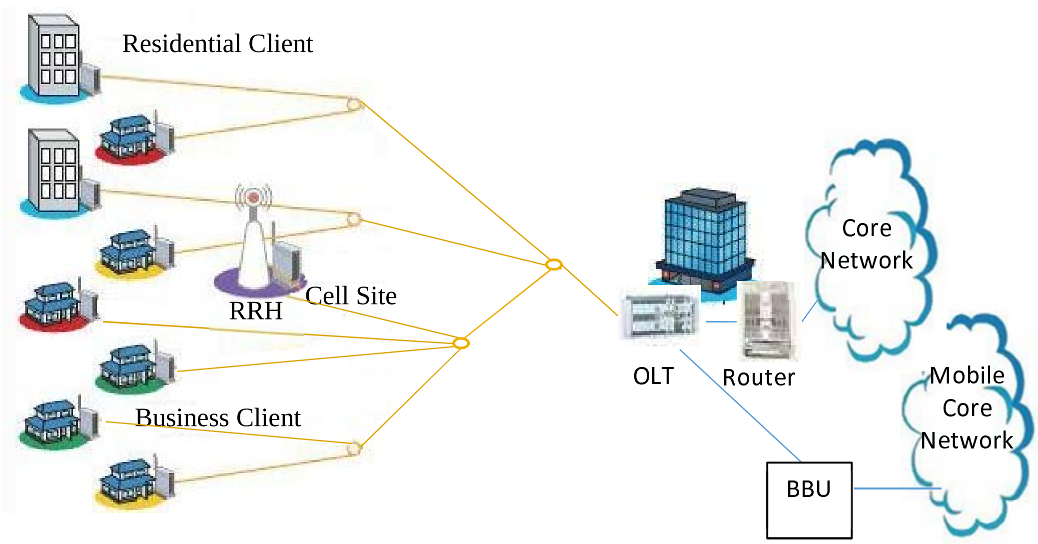


Figure 27: Overview of the multiple access aggregation over PON

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 28 illustrates the three main access network goals that F5G will need to address:

- network QoS;
- network availability;
- network densification.

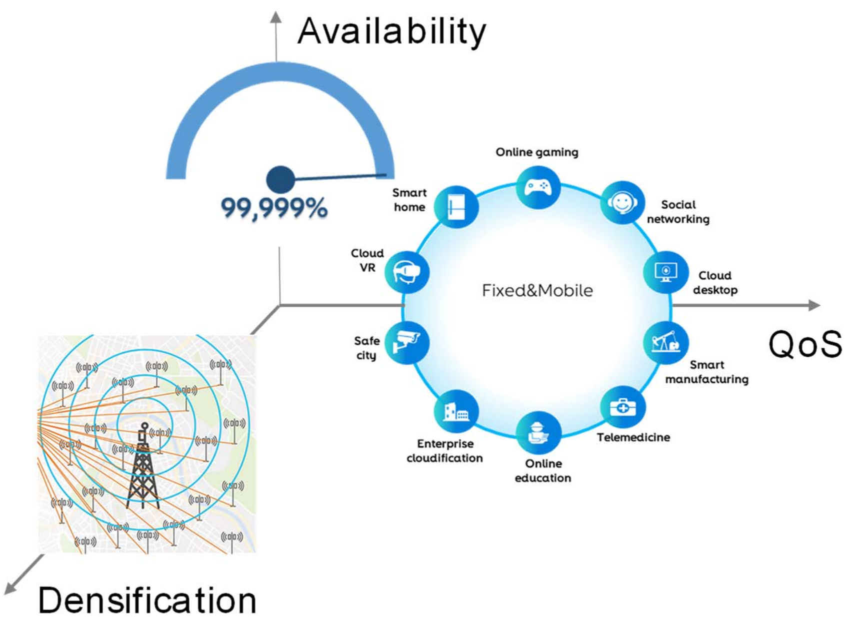


Figure 28: Main features of the multiple access aggregation over PON

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 Market, Enterprise Market 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 the same transmission medium (fibre and/or radio) or via a different medium. 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 clear reason for SDN/NFV deployment, as this is the most efficient management of different PONs terminations and services requirements on distinct OLTs (HW protection/selection) giving QoS and SLA 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 in a converged view of Fixed and Mobile and 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 29. 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.

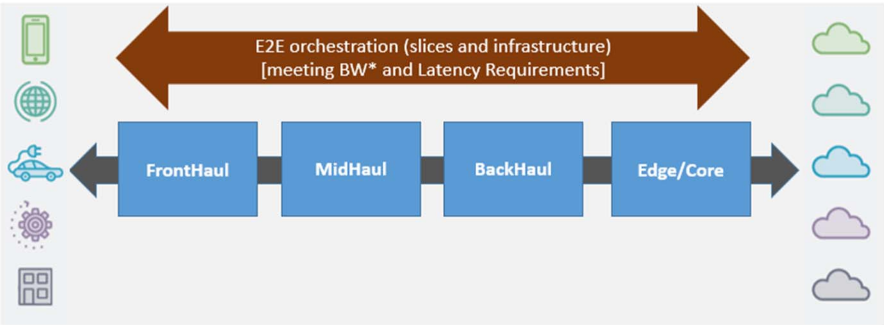


Figure 29: End-to-end Orchestration

3) Network densification

The diverse QoS, availability and massive Points of Presence needed, affect the way fibre can be deployed. With densification, the PON solution has the advantage to reduce significantly 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, 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 instead 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 split 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 30.

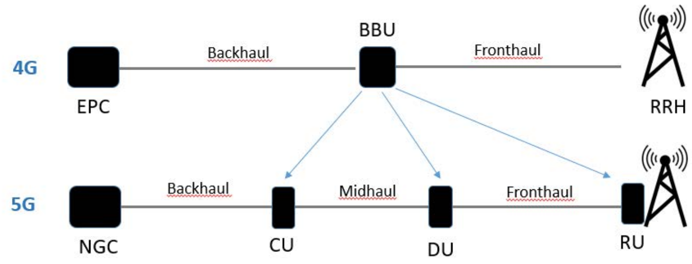


Figure 30: RAN Evolution from 4G to 5G

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 31.

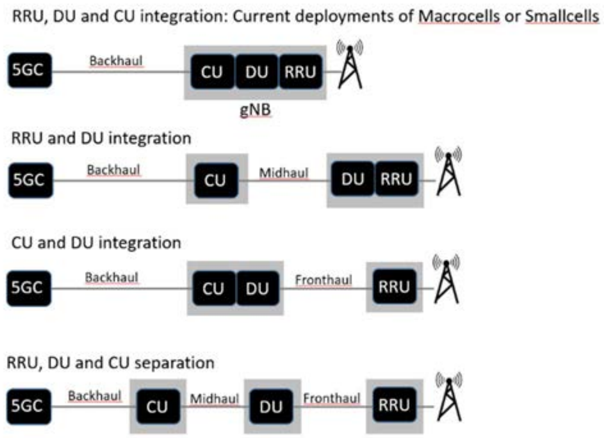


Figure 31: Different options for gNB modules integration/separation

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 largely used in Access Network for many years. Nowadays people are planning to deploy 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 as 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 and 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, and may require PON devices different from those adopted by the traditional access markets.

6.9.2.1.2 DSLAMs - Switches - Routers

DSLAM systems are still deployed for the access networks. With OLT usage increasing in the network, it will be more useful to deploy DSLAM's with SFP ONUs. In some outdoor DSLAM applications, there should 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 and operational issues. PON equipment (ONUs, MDUs) and DSLAM Backhaul equipment can be separated by using different OLT cards or PON ports. Figure 32 shows the differences between DSLAM Backhaul and current DSLAM.

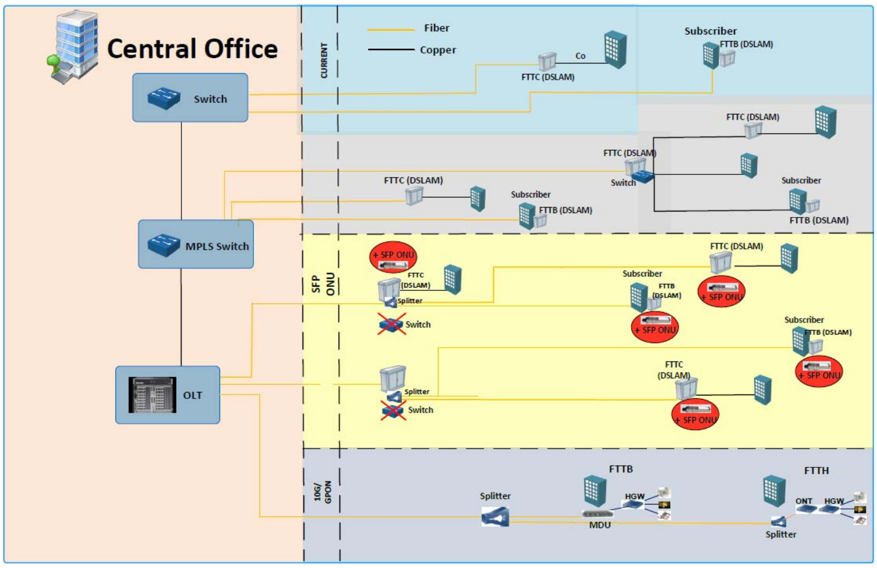


Figure 32: Extend PON to DSLAM Ethernet Uplink

6.9.2.1.3 Wifi AP backhaul

Wi-Fi® has been widely deployed for its convenience for network connection. 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 based on 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 used so that existing Wi-Fi® AP devices can still be used. By using PONs, the Ethernet switches are replaced by OLTs and optical splitters that reduce power consumption and cost. In addition all the Wi-Fi® APs are managed and controlled by the OLT as shown in Figure 33.

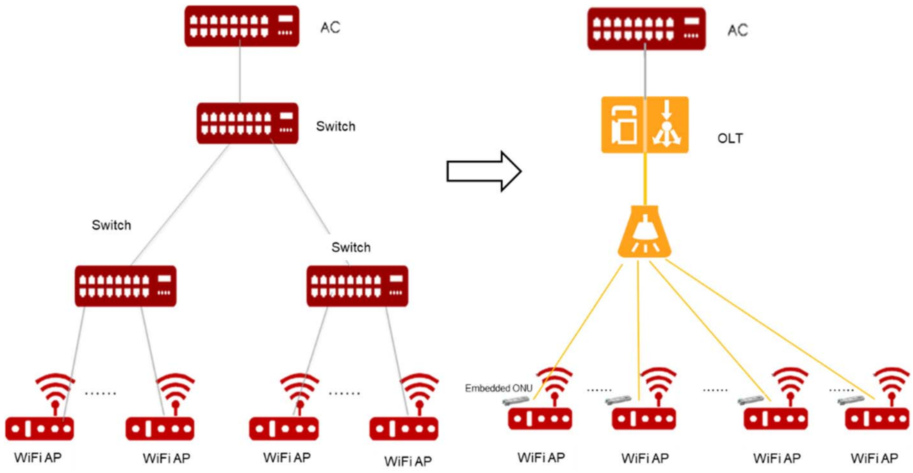


Figure 33: Extend PON to AP Ethernet Uplink

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 of a surveillance camera is Ethernet. However, from Figure 34, it can be observed that the distance from a camera to the surveillance centre could be greater than 10 km in big cities. The topology from the surveillance centre to each camera is a point-to-multi-point, which suits a PON system's topology. In addition, the PON system could support distances of at least 20 km or even up to 40 km. The OLT can support the split ratio of 1:128, which is very suitable for the 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 the local power supply is unavailable.

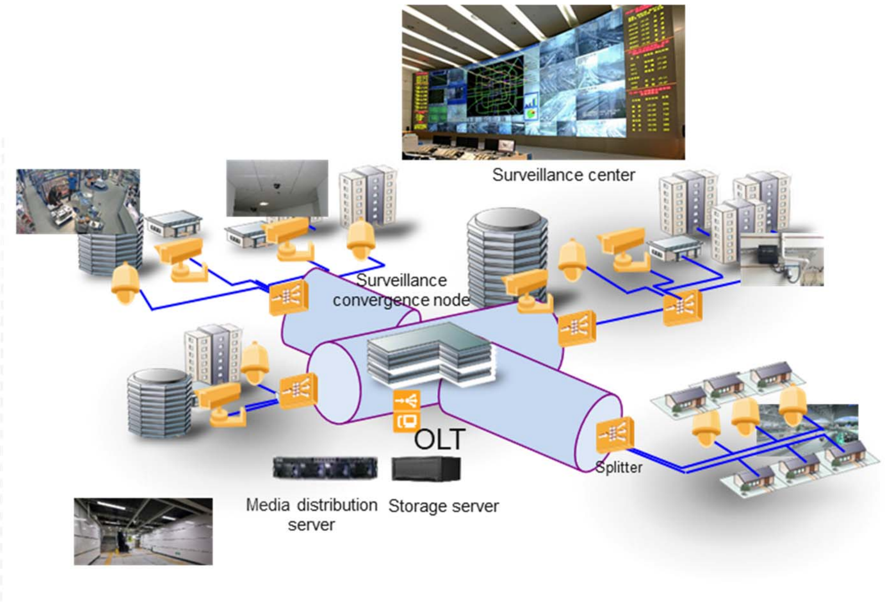


Figure 34: Extend PON to Video surveillance backhaul

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:

a) using ONUs to interface Ethernet-based devices to the PON network;

b) 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 network. With wide deployment, the technology is quite mature and the device cost is quite low. In order to enjoy the benefits brought by the 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 meeting 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 35, high value broadband applications are identified by the broadband network components, distinguished from the ordinary Internet traffic and high quality network resources are allocated between the application terminal and the application Cloud to guarantee the user experience. All the network operations are managed by the E2E management plane.

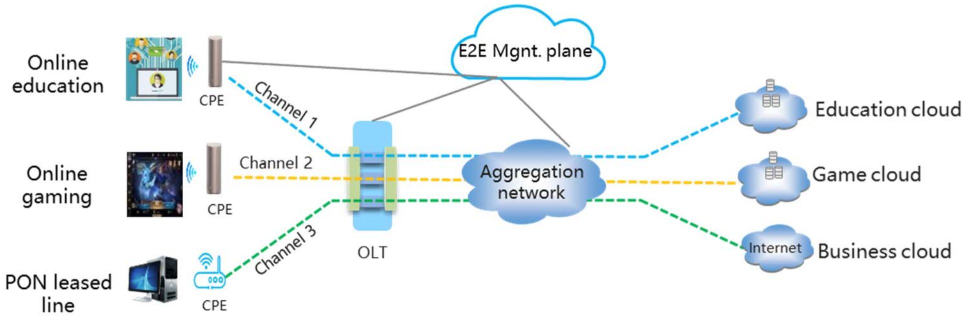


Figure 35: Multiple applications carrying on the network

Broadband network users often experience unstable network connections 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 applications' Cloud and the device have different requirements on the network performance. In order to provide a good quality experience to users, on top of the high bandwidth of the fibre networks several other parameters have to be considered and supported in the network such as automatic application identification, low latency, high reliability, application elasticity and adaptation, automatic application quality measurement and assurance.

New Internet applications and new broadband devices are attached to the network frequently. The broadband network needs to adapt to the changes flexibly and automatically without manual adjustment. The changes to the broadband applications and user behaviour should be detected by the network management system that should take actions when necessary to guarantee the network performance matching the corresponding broadband applications.

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 capable to handle the unpredicted changes. With the technological advancements in Artificial Intelligence, the 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 36. The most frequently used broadband applications are education, gaming, media streaming, and ordinary best-effort Internet (browsing, and Email). Different applications could be identified by the network with its embedded Artificial Intelligence functions by which the applications' feature could be distinguished from each other. The network resources will be allocated to the identified high value applications according to their demands on the network, including the home network segment. To support the flexible changes of the broadband application in the Internet, the AI learning centre learns the high value applications, which are to be guaranteed.

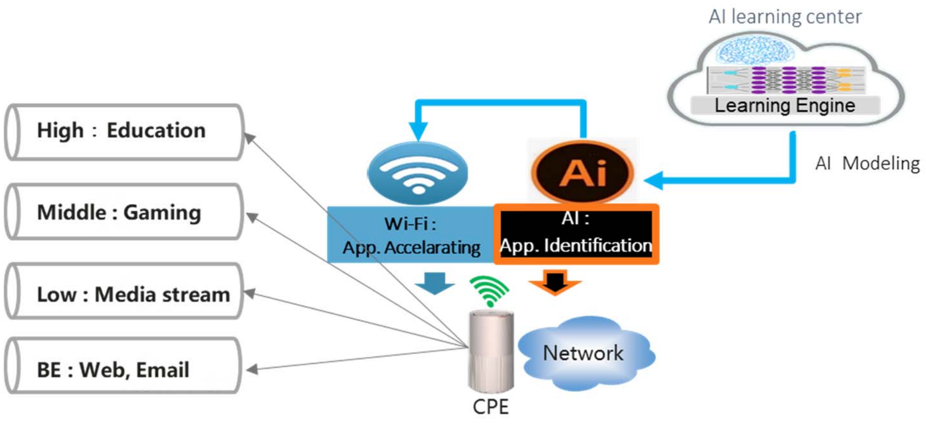


Figure 36: Overview of the scenario based broadband

The scenario based broadband use case may be relevant to any possible broadband application when its quality is essential to the end broadband 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 game 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, playing PC games or game stations, should 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 37.

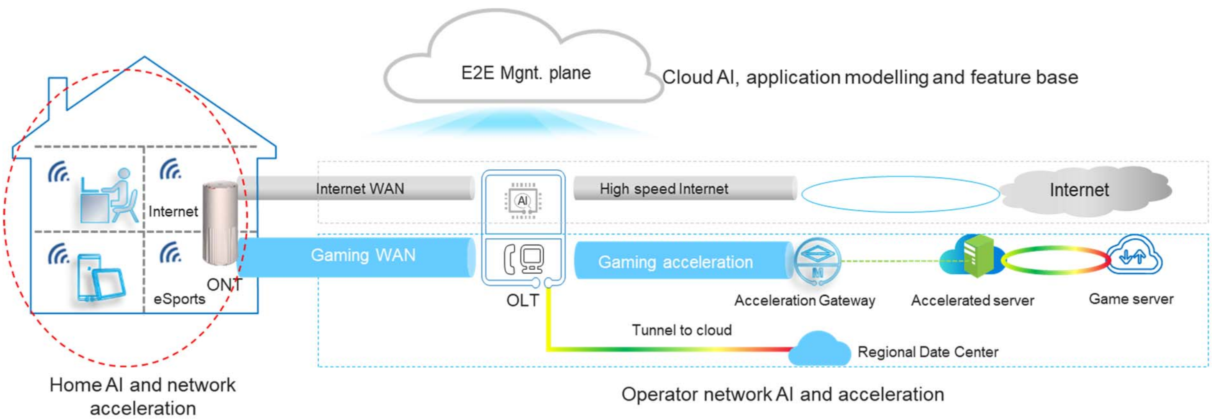


Figure 37: Network architecture for gaming

The high-end games need good network performance. Bandwidth is one of the performance factors. The installation software kit of the 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. Please 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 as strict as 30 ms or even 10 ms E2E.

Table 6: Latency impacts to the experience

	Excellent	Good	Medium	Poor
Latency (ms)	0~50	51~90	91~150	> 150
Experience description	Smooth without feeling delay	Normal game operation without obvious delay	Capable to play with feeling pause	Pause frequently, drop line occasionally

The gaming broadband requires to improve the network performance, especially reducing the network latency for guaranteed experience. The traffic model and feature base of the popular Internet games are established and updated by the AI engine embedded in the home network and operator network automatically and are stored on the E2E operator's 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 as a supplemental method to the traditional school education. Nowadays it is changing gradually into one of the main stream methods similar to classroom education.

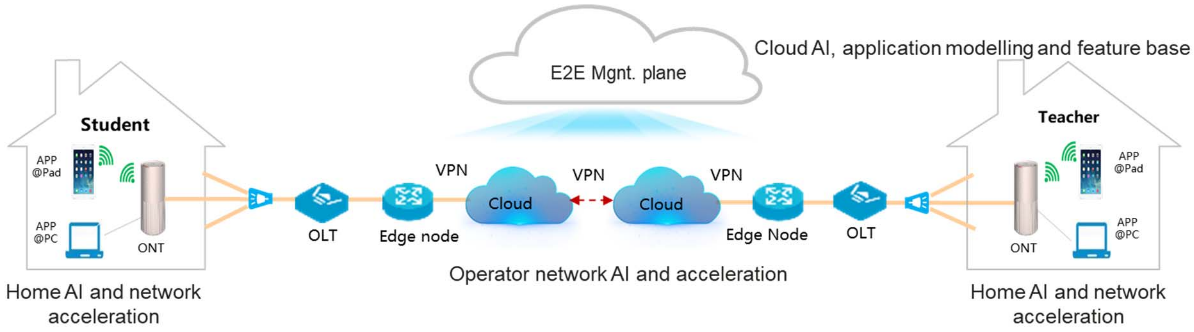


Figure 38: Network architecture of the on-line education

The end to end education broadband network is shown in Figure 38. 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 more critical parameters.

The traffic model and feature base of the popular education applications are established and updated by the AI engine embedded in the home network and operator network automatically 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

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 freely. 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 network of a home office broadband is shown Figure 39. 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 data model and feature base of the popular home office applications of enterprise VPN software are established and automatically updated by the AI engine embedded in the home network and operator network and it is implemented in the E2E operator's management plane. The key network component received 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.

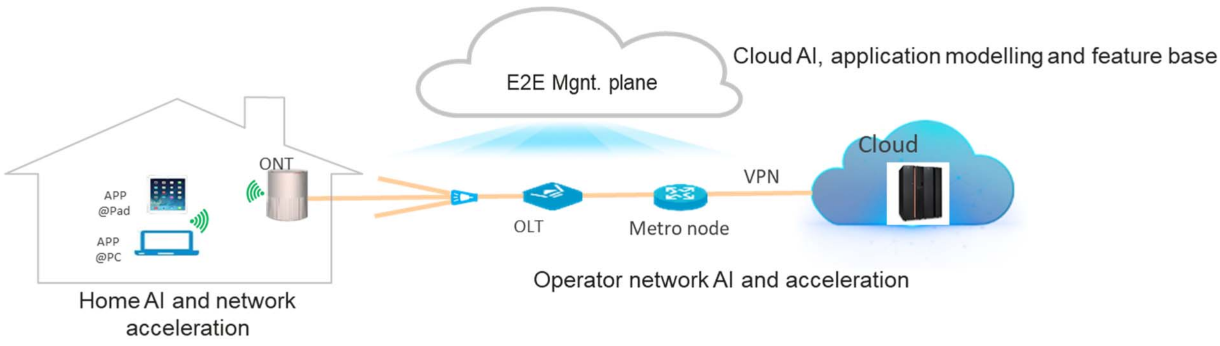


Figure 39: Network architecture of the on-line meeting

6.10.2.1.5 PON leased line

Business leased line is used by small and medium enterprise customers, such as small shops and branch offices etc., as shown in Figure 40. There are two kinds of broadband services needed, Internet leased line and business leased line. Normally the business leased line is a high SLA demanding service in terms of bandwidth, latency, stability and reliability. It is getting more important when more business applications are deployed on the Cloud, including public Cloud, operators' Cloud and the private Cloud of the enterprise themselves. 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 also, with large capacity access, network redundancy, self-management, etc.

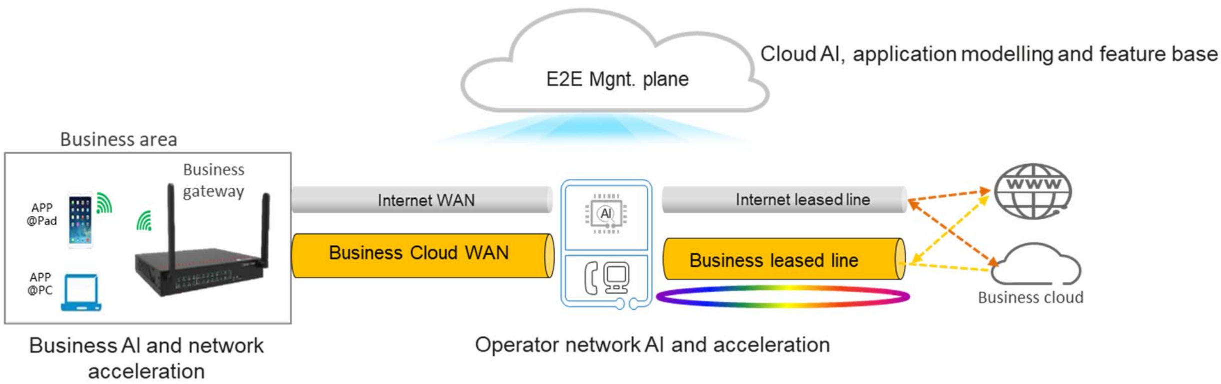


Figure 40: Network architecture of the PON leased line

The data model and feature base of the business applications or enterprise VPN software are established and updated by the AI engine embedded in the customer premise network and operator network automatically and is stored at the E2E operator's 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 kept increasing in the past decades, reaching Gigabits level in F5G era. 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 treated nearly the same as the so called HSI (High Speed Internet) services and transported on the broadband network in general. It prevents the network operators to improve their service level to broadband users. The requirements from applications and behaviours from users have to be considered and differentiated to provide the adequate network services and solutions. That leads to the scenario based broadband services which are actually to setup a common network architecture to support multiple application scenarios of the users.

The user behaviour and application change alongside with the Internet further developing. The scenario based broadband network also needs to be a self-healing system to keep up with the application development automatically.

6.10.2.3 Pre-conditions

- The network components are designed in a high reliable manner.
- The network resources are sufficient especially to the high SLA demanding applications.

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, 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 due to coarse granularity of traffic monitoring data collection. That coarse granularity of monitoring displays flattening of traffic bursts within a monitoring period and is not sufficient to determine the actual traffic status, leading to miss traffic anomalies. Figure 41 gives an illustration of the case.

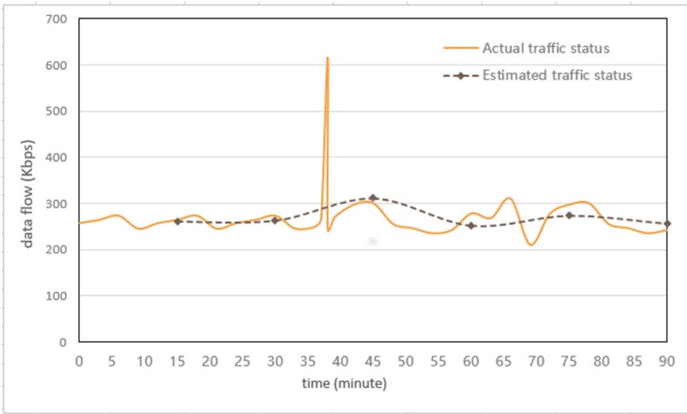


Figure 41: Example diagram of micro traffic burst

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 42. Several functions are included in the management layer, such as access network data collection used by the access network management system and OLT control.

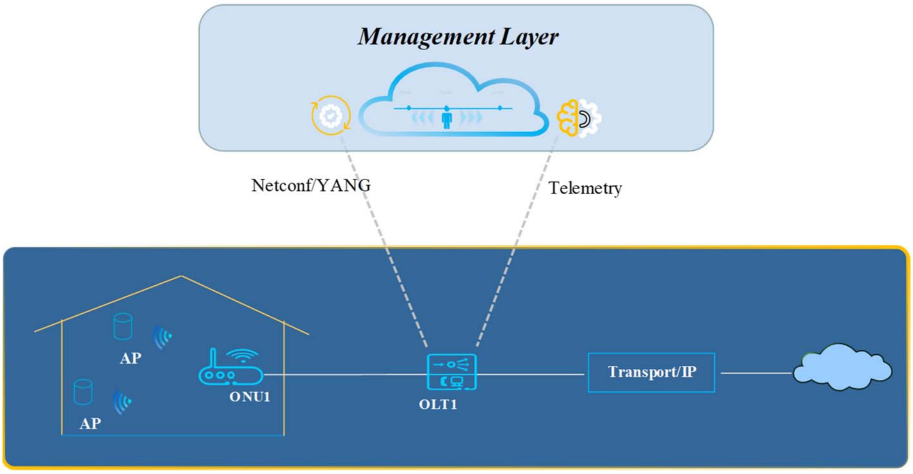


Figure 42: Example of enhanced traffic monitoring and network control for intelligent access network

In general, an intelligent access network can be applied to application scenarios such as FTTH. It can be extended by cascading PON systems and applies to both the access network segment (tier 1 PON) and the customer premises network (tier 2 PON) to achieve better traffic monitoring, operation, and maintenance capability as shown in Figure 43. The management layer for cascaded PONs provides comprehensive support to cover lower tier cascaded PON. One example is the automatic setup of the second tier 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 case of cascade PON, end-to-end orchestration enables the control and management of the customer premises network.

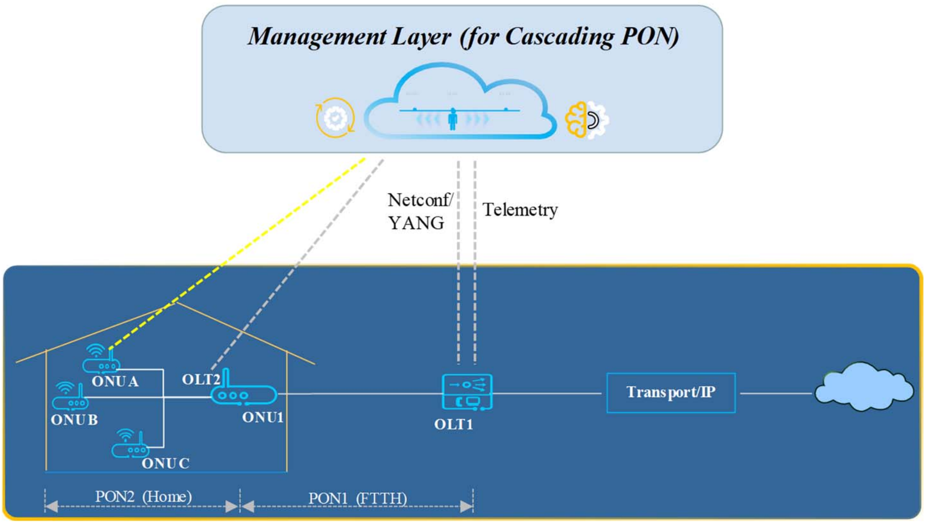


Figure 43: Example of enhanced traffic monitoring and network control for cascading PON

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 static encoding to data-driven dynamic machine learning algorithm, to realize the network automation including 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 framework and interface should be supported by the OLT.
- Telemetry interface and model should be supported by the OLT.

6.11.2.4 Operational flow of actions

Flow chart is shown in Figure 44.

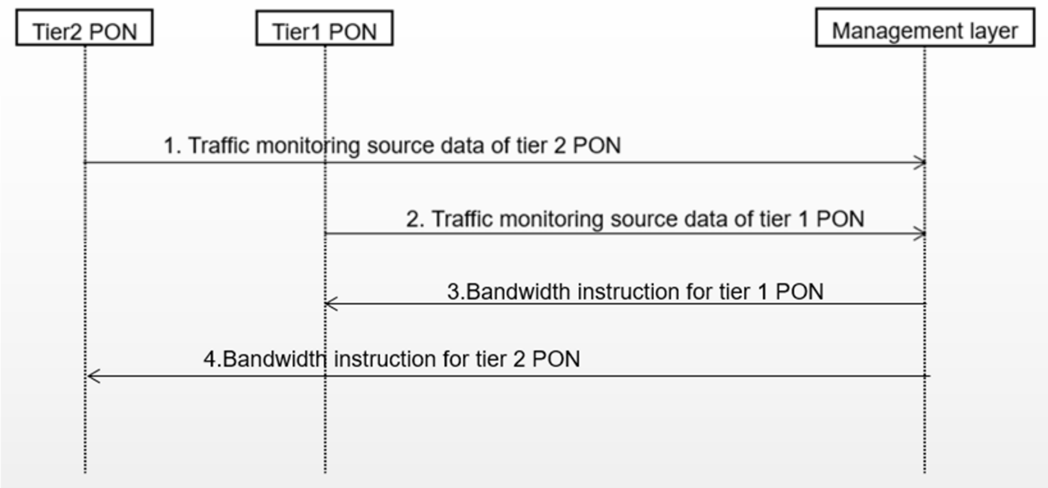


Figure 44: Operational flow of bandwidth dynamic adjustment in Intelligent Access Network

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 WiFi 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 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 inside the network. This performance cannot be deterministically reached on a shared resource, where communication are concurrent. In fact, simultaneous communications will create some 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 deteriorate consumer's 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

The 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 45:

- 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.

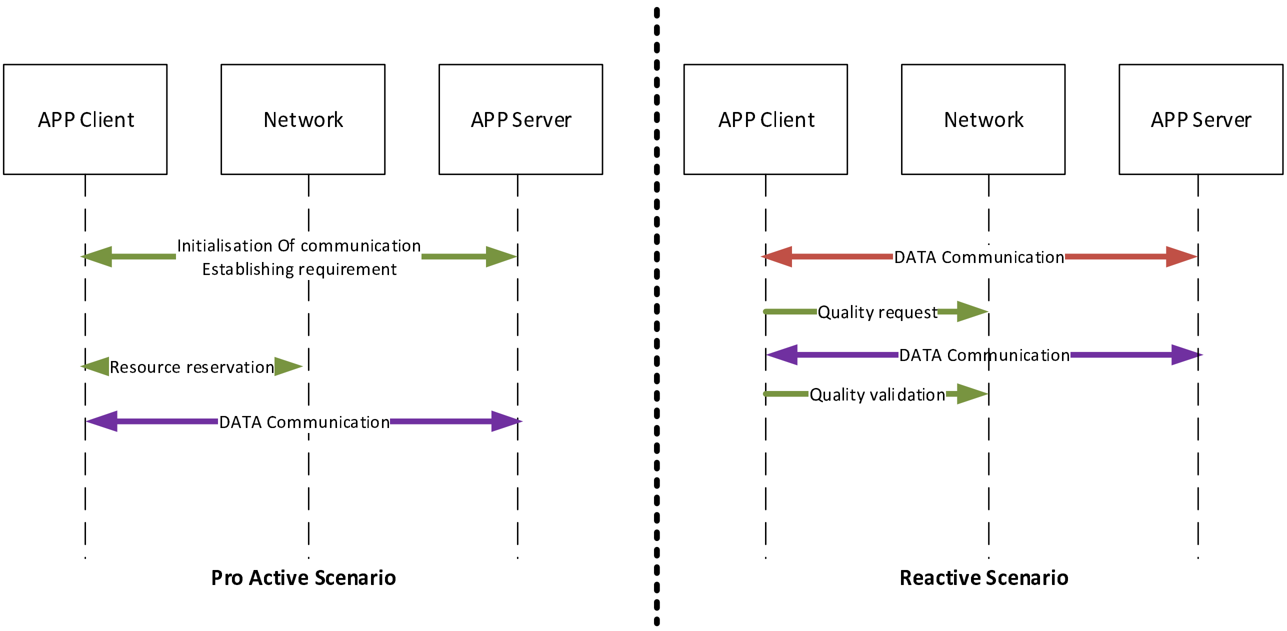


Figure 45: Dedicate Resource scenarios

Figure 46 gives an example based on communication established by Cloud VR Application using pro-active resource allocation mechanisms.

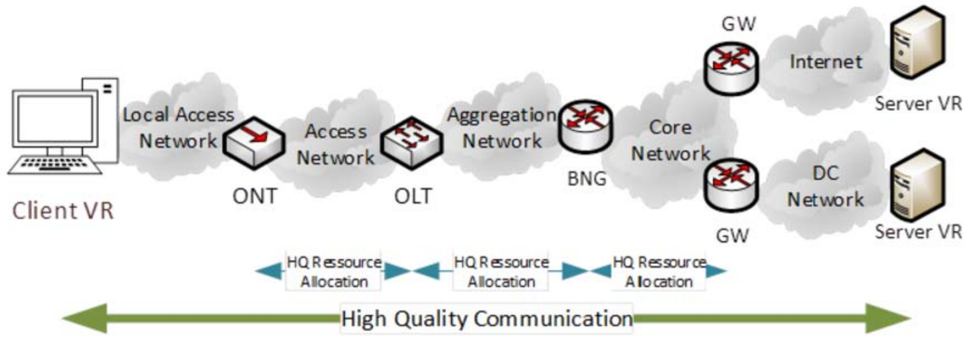


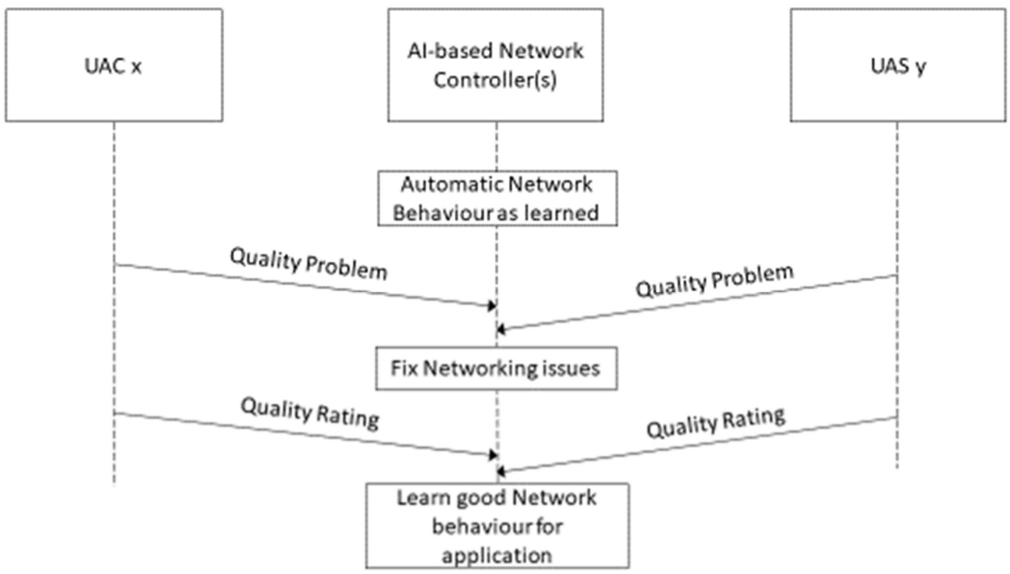
Figure 46: Initialization of dedicated transport channel

During the initialization of the communication between application server and the application client, the application client will request a high-quality communication. 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. This request will be granted, based on policies and depending on the service agreement, segment by segment in the network.

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



NOTE: This is an example using reactive network controller mechanism based on AI.

Figure 47: 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, they send a notification to the network controller, which 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 the mechanism are introduced.

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, 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 48 shows the network architecture and the deployment position of RA client and RA server.

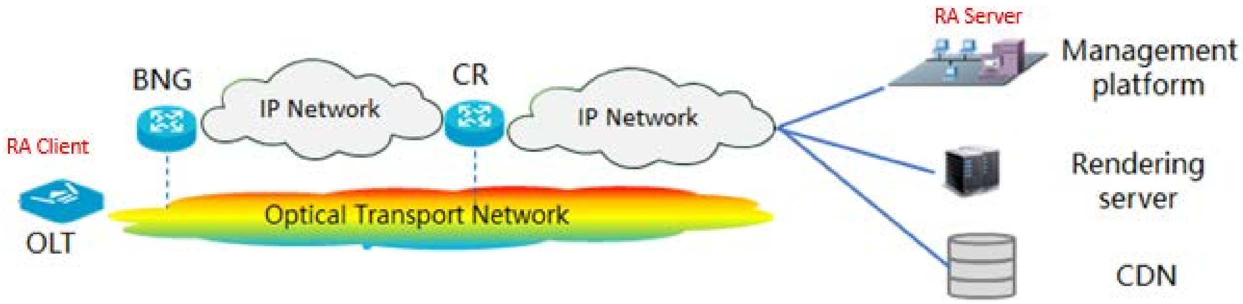


Figure 48: Remote Attestation Network Architecture

Figure 49 introduces the process of measured booting with remote attestation applied.

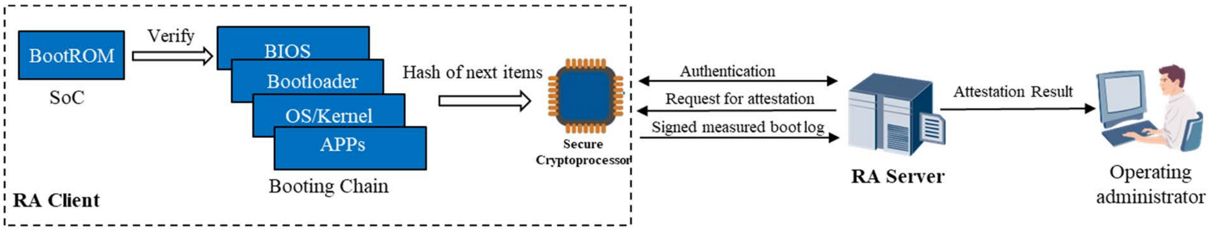


Figure 49: Measured Boot with Remote Attestation

As depicted in Figure 49, 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 operator gets 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 50 shows the DIM process with remote attestation to determine the integrity of the running programs.

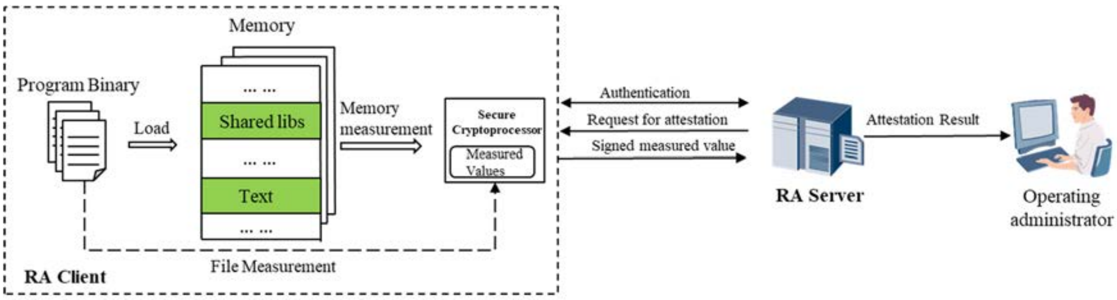


Figure 50: DIM With Remote Attestation

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:

- Keeping the integrity status of network devices. With measured boot and remote attestation, devices with tampered software can be detected and software recovery or isolation processes will be triggered.
- Improving the efficiency of network device management. 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 51 introduces the operational flows of remote attestation. 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.

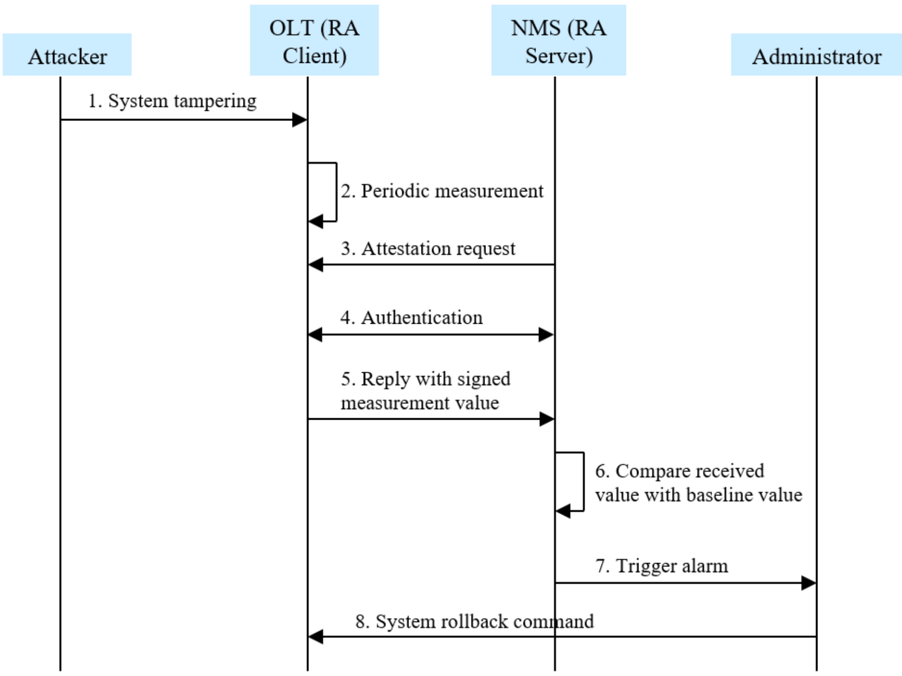


Figure 51: Operational flow of remote attestation

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, ODN should allow fast deployment and accurate and efficient resource management.

6.14.2 Description of the use case

6.14.2.1 Overview

Nowadays paper and plastic labels are usually used on ODN network components. However, they cannot be updated in a timely manner. Also, being exposed to high temperature and high humidity during life time, 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) normally will not be disconnected after the ONU is removed. For example, as shown in Figure 52, 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 52: The challenges of paper labels

It is essential to ensure the accurate identification and recoding of ODN resources. The digitalized ODN and intelligent management of information makes ODN resources more visible and manageable in the network deployment phase and user service provisioning phase. In this way, ODN resources can be managed more accurately and used more efficiently.

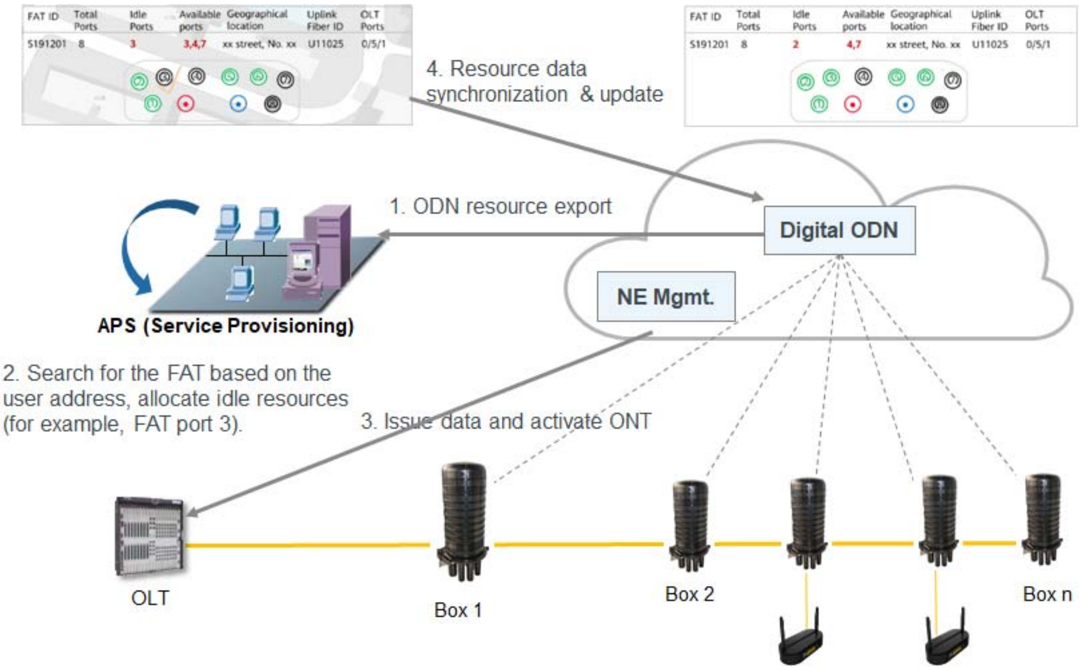


Figure 53: Digitalized ODN enables automatic service provisioning and accurate resource management

In some scenarios, such as in smart cities or vertical industries, the fibre resource management (such as resource database entries recording and retrieving) should be handled by skilful and qualified ODN technicians, which are scarce and costly. The digitalized ODN can support real time resource recording and database update, port status monitoring, automatic resource allocation and automatic service provisioning. Therefore, the efficient use of the fibre resources and its management can greatly improve.

6.14.2.2 Motivation

- Digitalized and intelligent identification of ODN labels, achieving 100 % accurate resource recording and digital management, enable automatic service provision.
- Real-time visualization of ODN topology and resource management.
- Quick ODN deployment and easy maintenance.

6.14.2.3 Pre-conditions

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

6.14.2.4 ODN deployment operation flow

1) Use optical cables and appropriate components with digital labels to quickly complete the network infrastructure deployment based on the network plan.

2) 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) Provision services and display fibre resource usage.

7 Relationship with other F5G work items

ETSI ETSI GS F5G 003 [i.4] (F5G Technology Landscape) will specify the technical requirements and the gap analysis derived from the use cases captured in the present document

ETSI ETSI GS F5G 004 [i.5] (F5G Network Architecture Specification) will consider the requirements generated from the use cases.

History

Document history		
V1.1.1	February 2021	Publication