ETSI GS F5G 014 V1.1.1 (2023-05)

Fifth Generation Fixed Network (F5G); F5G Network Architecture Release 2

Disclaimer

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

Reference
DGS/F5G-0014

Keywords
architecture, F5G

ETSI

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

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

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

Contents

Intellectual Property Rights 5
Foreword 5
Modal verbs terminology 5
Introduction 5
1 Scope 6
2 References 6
2.1 Normative references 6
2.2 Informative references 7
3 Definition of terms, symbols and abbreviations 8
3.1 Terms 8
3.2 Symbols 10
3.3 Abbreviations 10
4 Business requirements for network architecture 12
4.1 Business requirements overview 12
4.2 Business requirements driving the F5G architecture 13
5 Network architecture 14
5.1 Architecture design principles 14
5.1.1 Multi-Service Network Platform 14
5.1.2 Dynamic and Flexible Service Creation 14
5.1.3 Decoupling Service Plane and Network Plane 15
5.1.4 AI-based Control, Management and Analytics 15
5.1.5 Security by Default 15
5.2 Architecture overview 15
5.3 Network topology and interfaces 17
5.3.1 Network Overview 17
5.3.2 Definition of Interfaces 19
5.3.2.1 T interface 19
5.3.2.2 T' interface 19
5.3.2.3 T" interface 19
5.3.2.4 U interface 19
5.3.2.5 U' interface 20
5.3.2.6 B interface 20
5.3.2.7 V interface 20
5.3.2.8 V_o interface 20
5.3.2.9 A10 interface 21
5.3.2.10 A10' interface 21
5.3.3 OTN Control Interfaces 21
5.3.4 FTTR control interface 23
5.4 Key enabling features 24
5.4.1 Network Slicing 24
5.4.1.1 Introduction 24
5.4.1.2 Concepts 24
5.4.1.3 Network Slicing Applicability 26
5.4.1.4 F5G Slicing Architecture 27
5.4.1.5 Network Slice Management 28
5.4.1.6 Traffic Steering in the Context of Slicing 29
5.4.1.7 Fibre-wireless coordination 29
5.4.1.8 Wi-Fi® Slicing 30
5.4.1.9 PON Slicing 31
5.4.1.9.1 Introduction 31
5.4.1.9.2 User Group Oriented Slicing 31
5.4.1.9.3 Service-Oriented Slicing 32
5.4.1.10 OTN Slicing 32

5.4.1.11 IP AggN Slicing 34
5.4.2 Traffic Steering 35
5.4.2.1 Overview 35
5.4.2.2 Traffic Steering Architecture 35
5.4.2.2.1 High-level Framework 35
5.4.2.2.2 Management Control and Analytics (MCA) functions 36
5.4.2.2.3 Access Network Element Based Functions 37
5.4.2.2.4 Aggregation Network Element Based Functions 38
5.4.2.3 Example for Traffic Steering 38
5.4.3 Separation of Services Plane and Underlay Plane 39
5.4.3.1 Introduction 39
5.4.3.1.1 Purpose of service and network separation 39
5.4.3.1.2 Implementation of separation between service and network 40
5.4.3.2 The Underlay Plane 41
5.4.3.2.1 Introduction 41
5.4.3.2.2 Bearer Technologies 42
5.4.3.2.3 Summary and Analyses 44
5.4.3.3 The Service Plane 44
5.4.3.3.1 Introduction 44
5.4.3.3.2 Traffic encapsulation for the Service Plane 45
5.4.3.3.3 Signalling for the Service Plane 45
5.4.4 The Aggregation Network Fabric 46
5.4.4.1 IP/Ethernet Fabric 46
5.4.4.2 OTN Fabric 47
5.5 Management, Control and Analytics (MCA) 49
5.5.1 Overview 49
5.5.2 Autonomous Management and Control 49
5.5.3 Digital Twin and Telemetry 50
5.5.4 Network Abstraction and Model-driven Design 50
5.6 Security 51

6 Network devices/equipment requirements 51
6.1 Customer Premises Network requirements 51
6.2 Optical Access Network requirements 52
6.2.1 Access Network System Requirements 52
6.2.2 ONU Requirements 52
6.2.2.1 Functional Requirements 52
6.2.3 OLT Requirements 53
6.2.3.1 Functional Requirements 53
6.2.3.2 Interface Requirements 54
6.3 Optical Transport Network requirements 54
6.4 IP Network requirements 55
6.5 F5G Security requirements 55

7 Network migration 55

Annex A (informative): How the F5G Architecture addresses the Gaps 58

History 61

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

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

BLUETOOTH® is a trademark registered and owned by Bluetooth SIG, Inc.

Foreword

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

Modal verbs terminology

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

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

Introduction

The F5G network, as described in ETSI GR F5G 002 [i.2], has committed to three characteristics for extending and enhancing fixed networks, eFBB, FFC and GRE. These characteristics are derived from the F5G use cases (ETSI GR F5G 008 [i.1]) that require these enhancements. To implement these characteristics, the F5G architecture has introduced new design principles and new features. Such features include separation of data plane into Underlay Plane and Service Plane, dual network fabrics for the Aggregation Network, comprised of an IP/Ethernet and an OTN fabric, and the seamless and combined usage of PON and OTN, E2E slicing, etc. Based on these design principles and new features, F5G networks can provide a variety of services for residential and enterprise customers over one physical network with guaranteed SLAs. The new F5G architecture balances performance and operational efficiency through a higher degree of flexibility and choice. Network services can be carried by an IP/Ethernet or an OTN fabric depending on the network characteristics and the performance requirements and allowing for independent changes of the Underlay or Service Planes to match the needs of applications, services or users. Using EVPN as the unified Service Plane technology simplifies the Service Plane protocols and management. This Service Plane is easily programmable to adapt

to market needs and it supports different cloud-oriented Information and Communication Technology (ICT) architectures.

1 Scope

The present document specifies the End-to-End network architecture, features and related network devices/elements' requirements for F5G, including on-premises, Access, IP and Transport Networks. The present document defines new features and enhance existing ones.

2 References

2.1 Normative references

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

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

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

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

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

[2] Recommendation ITU-T G.709/Y.1331: "Interfaces for the optical transport network".

[3] Recommendation ITU-T G.709.1/Y.1331.1: "Flexible OTN short-reach interfaces".

[4] Recommendation ITU-T G.709.3/Y.1331.3: "Flexible OTN long-reach interfaces".

[5] IETF RFC 8402: "Segment Routing Architecture".

[6] IETF RFC 8986: "Segment Routing over IPv6 (SRv6) Network Programming".

[7] IETF RFC 7209: "Requirements for Ethernet VPN (EVPN)".

[8] IETF RFC 8584: "Framework for Ethernet VPN Designated Forwarder Election Extensibility".

[9] IETF RFC 4760: "Multiprotocol Extensions for BGP-4".

[10] IEEE 802.11ax™: "IEEE Standard for Information Technology -- Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks -- Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 1: Enhancements for High-Efficiency WLAN".

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

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

[13] Recommendation ITU-T G.873.1: "Optical transport network: Linear protection".

[14] Recommendation ITU-T G.873.2: "ODUk shared ring protection".

[15] Recommendation ITU-T G.873.3: "Optical transport network - Shared mesh protection".

[16] Recommendation ITU-T G.8251: "The control of jitter and wander within the optical transport network (OTN)".

[17] Recommendation ITU-T G.8201: "Error performance parameters and objectives for multi-operator international paths within optical transport networks".

[18] IEEE 802.3.1™: "IEEE Standard for Management Information Base (MIB) Definitions for Ethernet".

[19] IEEE 802.1Q™: "IEEE Standard for Local and Metropolitan Area Networks–Bridges and Bridged Networks".

[20] ETSI GS F5G 006 (V1.1.1): "Fifth Generation Fixed Network (F5G); End-to-End Management and Control; Release #1".

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

[22] ETSI GS F5G 012 (V1.1.1): "Fifth Generation Fixed Network (F5G); Security; F5G Security Countermeasure Framework Specification".

[23] ETSI TS 103 924: "Optical Network and Device Security Catalogue of requirements".

[24] IETF RFC 7950: "The YANG 1.1 Data Modeling Language".

[25] IETF RFC 6241: "Network Configuration Protocol (NETCONF)".

[26] IETF RFC 8040: "RESTCONF Protocol".

[27] ETSI GS F5G 013 (V1.1.1): "Fifth Generation Fixed Network (F5G); F5G Technology Landscape Release #2".

[28] ETSI GS F5G 015 (V1.1.1): "Fifth Generation Fixed Network (F5G); F5G Residential Services Quality Evaluation and Classification".

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 008 (V1.1.1): "Fifth Generation Fixed Network (F5G); F5G Use Cases Release #2".

[i.2] ETSI GR F5G 001 (V1.1.1): "Fifth Generation Fixed Network (F5G); F5G Generation Definition Release #1".

[i.3] ITU-T Study Group 15/Q18, G.fin-SA: "High speed fibre-based in-premises transceivers - system architecture".

[i.4] IETF draft-ietf-ccamp-transport-nbi-app-statement: "Transport Northbound Interface Applicability Statement".

[i.5] IETF draft-ietf-teas-ietf-network-slices: "Framework for IETF Network Slices".

[i.6] IETF draft-ietf-teas-applicability-actn-slicing: "Applicability of Abstraction and Control of Traffic Engineered Networks (ACTN) to Network Slicing".

[i.7] IETF draft-ietf-ccamp-yang-otn-slicing: "Framework and Data Model for OTN Network Slicing".

[i.8] ITU-T Study Group 15/Q11 G.osu: "Optical Service Unit (OSU) path layer network".

[i.9] IETF draft-ietf-teas-enhanced-vpn: "A Framework for Enhanced Virtual Private Network (VPN+) Services".

[i.10] IETF draft-ietf-teas-ns-ip-mpls: "Realizing Network Slices in IP/MPLS Networks".

[i.11] ETSI GR IPE 005: "IPv6 Enhanced Innovation (IPE); 5G Transport over IPv6 and SRv6".

[i.12] IETF RFC 8655: "Deterministic Networking Architecture".

[i.13] IETF RFC 2702: "Requirements for Traffic Engineering Over MPLS".

[i.14] IETF RFC 3209: "RSVP-TE: Extensions to RSVP for LSP Tunnels".

[i.15] IETF draft-ietf-spring-resource-aware-segments: "Introducing Resource Awareness to SR Segments".

[i.16] IEC 61158: "Industrial communication networks -- Fieldbus specifications".

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

access node: network node which has connectivity by access network technology to the customers and is connected to the aggregation network

NOTE: The access node is the delineation between the access network and aggregation network. The access node might consist of several physical network elements.

AggN Edge Node: network node which has connectivity to several access nodes and is connected to the core network

NOTE: The AggN Edge Node is the delineation between the aggregation network and the core network. The AggN Edge Node might consist of several physical network elements.

aggregation fabric: network connecting the access node and the AggN Edge Node

application list: list of applications and the associated attributes to identify the application in a network element

bearer connection: network connection instance in the Underlay Plane with particular QoS characteristics, transporting the traffic according to the service or network requirements

Dedicated Network (D-Net): set of preconfigured paths or bearer connections established on a shared networking infrastructure

NOTE: D-Nets operate independently from each other, are fully isolated from other paths and bearer connections, and meet the SLA requirements of the tenants. A D-Net can be managed by an independent management plane or several D-Nets can be managed by a single management plane.

digital twin: model of the network, including available resources and configurations and containing a real-time, equivalent model of the running network

EtherCAT (Ethernet for Control Automation Technology): Ethernet-based fieldbus system

NOTE: The protocol is standardized in IEC 61158 [i.16] and is suitable for both hard and soft real-time computing requirements in automation technology.

isolation: several levels of isolation including on data level, resource level and several mechanisms for soft and hard isolation

NOTE 1: On the data level, each instance has its own isolated data instance. On the resource level, it means isolation which includes tenants having their own basic resources like databases, logs, alarms, and networking resources. There is also soft isolation of resources like buffers, queues, control-plane processes, forwarding processes and hardware isolation like boards and ports, CPU cores, forwarding chips and sub-racks.

NOTE 2: Different isolation levels and mechanisms have different characteristics and complexities.

Management, Control and Analytics (MCA) plane: sub-system, which is responsible for the management, control and analytics of the complete end-to-end F5G network

network slice: logical network that achieves specific service requirements

Network Service Providers (NSPs): business entity which provides a logical or physical network or connectivity service

NOTE: The NSP defines network services including the network functions and the required E2E network resources including topology, transmission links, and ODN resources that can be exclusively used, and resources such as boards and ports of each Network Element (NE).

Network Slice Instance (NSI): instantiation of a network slice with particular defined network capabilities (e.g. QoS, OAM, reliability) and a set of resources

NOTE: The network slice instance is characterized by multiple parameters and covers management, control, and forwarding requirements of the services. The network slice instance is an end-to-end concept.

Network Slice Template: data structure with different parameters of the network slice instance's characteristics

Service Access Point (SAP): function that provides and controls the customer access to the service

NOTE: The SAP is a component in the Service Plane.

Service Mapping Point (SMP): function that maps the service traffic to a specific Underlay Plane infrastructure

NOTE: The SMP is a component in the Service Plane.

service plane: plane for the connectivity services to customers

NOTE: Connectivity services can be dynamically created, deleted and adapted, and provides the service with a customer agreed quality.

Service Processing Point (SPP): function that performs service specific processing

NOTE: The SPP is a component in the Service Plane.

Service Slice Type (SST): data structure that defines an expected network behaviour in terms of features and services (e.g. specialized broadband for a particular application) of a slice

tenant: business entity using and controlling a network slice

NOTE: The tenant can be different entities depending on the context and business relationship.

EXAMPLE: A tenant can be a Virtual Network Operator (VNO) or a Network as a Service (NaaS) user.

traffic steering: function deciding what traffic is steered to what destination or next node

NOTE 1: The traffic needs to be identified such that it can be steered.

NOTE 2: A bearer connection can be a tunnel or a native network connection depending on the technologies used.

trust domain: collection of entities between which there is either direct, delegated or transitive trust

NOTE: The trust is in the authenticity of identifiers and respecting the privacy requirements that share a set of security policies that mitigate any risk of exploit to the grouping and/or collection within the trust domain boundary (see ETSI GS F5G 012 [22])

underlay plane: physical network of the physical network elements and the interconnecting links

3.2 Symbols

Void.

3.3 Abbreviations

For the present document, the following abbreviations apply:

ACTN	Abstraction and Control of Traffic-Engineering Network
AEL	Aggregation Edge Leaf
AgF	Aggregation Fabric
AggN	Aggregation Network
AI	Artificial Intelligence
AL	Access Leaf
AN	Access Network
AP	Access Point
API	Application Programming Interface
ARPU	Average Revenue Per User
ASG	Access Service Gateway
BGP	Border Gateway Protocol
BNG	Broadband Network Gateway
BSS	Business Support System
BYOD	Bring You Own Device
CE	Customer Equipment
CNC	Customer Network Controller
CPE	Customer Premises Equipment
CPN	Customer Premises Network
CPU	Central Processing Unit
CR	Core Router
CSMA/CD	Carrier Sense Multiple Access/Collision Detection
DC	Data Centre
DC-GW	Data Center Gateway
DetNet	Deterministic Networking
DSCP	Differentiated Services Code Point
E2E	End-to-End
E-CPE	Enterprise CPE
EDCA	Enhanced Distributed Channel Access
eFBB	enhanced Fixed BroadBand
E-LAN	Ethernet Virtual Private LAN
E-Line	Ethernet Virtual Private Line
E-O-CPE	Enterprise-OTN-Customer Premise Equipment
ETH	Ethernet
E-Tree	Ethernet Virtual Private Tree
EVPN	Ethernet VPN
FEC	Forward Error Correction
FFC	Full Fibre Connection
FlexO	Flexible Optical transport network
FTTH	Fibre-To-The-Home
FTTR	Fibre-To-The-Room
GEM	GPON Encapsulation Mode
GMPLS	Generalized Multi-Protocol Label Switching
GPON	Gigabit Passive Optical Network

GRE	Guaranteed Reliable Experience
HGW	Home Gateway
ICT	Information and Communication Technology
IE	Industrial Equipment
IoT	Internet of Things
IP RAN	IP Radio Access Network
IP	Internet Protocol
IPTV	Internet Protocol Television
IT	Information Technology
L2VPN	Layer 2 VPN
LAN	Local Area Network
LDP	Label Distribution Protocol
LSP	Link State Protocol
MAC	Media Access Control
MAN	Metropolitan Area Network
MCA	Management, Control, and Analytics
MDSC	Multi-Domain Service Coordinator
MEF	Metro Ethernet Forum
MP2MP	Multi-Point to Multi-Point
MP-BGP	Multiprotocol Extensions for BGP
MPLS	Multiprotocol Label Switching
MPLS-TE	MPLS Traffic Engineering
MS-OTN	Multi-Service OTN
NaaS	Network as a Service
NAT	Network Address Translation
NE	Network Element
NFV	Network Function Virtualisation
NMS	Network Management System
NSI	Network Slice Instance
NSP	Network Service Provider
O&M	Operation and Maintenance
OAM	Operation, Administration and Maintenance
OAM&P	Operation, Administration, Maintenance and Provision
ODN	Optical Distribution Network
ODU	Optical Data Unit
OLT	Optical Line Terminal
OMCI	ONU Management and Control Interface
ONU	Optical Network Unit
OSS	Operations Support System
OSU	Optical Service Unit
OTN	Optical Transport Network
OTUCn	Optical Transport Unit-Cn
OTUk	Optical Transport Unit (k = 0 to 4)
OXC	Optical Cross-Connect
P2MP	Point to Multi-Point
pBNG	physical Broadband Network Gateway
PBX	Private Branch Exchange
PC	Personal Computer
PCP	Priority Code Point
PCS	Physical Coding Sublayer
PDH	Plesiochronous Digital Hierarchy
PE	Provider Edge
PHY	Physical layer
PLC	Power Line Communication
PNC	Provisioning Network Controller
POL	Passive Optical LAN
PON	Passive Optical Network
PPPoE	Point-to-Point Protocol over Ethernet
QoE	Quality of Experience
QoS	Quality of Service
RFC	Requests for Comments
RG	Residential Gateway

RoT	Root of Trust
RSVP-TE	Resource Reservation Protocol-Traffic Engineering
RU	Radio Unit
SAP	Service Access Point
SDH	Synchronous Digital Hierarchy
SDN	Software Defined Networking
SID	Segment Identifier
SLA	Service Level Agreement
SME	Small and Medium Enterprises
SMP	Service Mapping Point
SPP	Service Processing Point
SR	Segment Routing
SRH	Segment Routing Header
SRv6	Segment Routing over IPv6
T-CONT	Traffic Container
TDM	Time Division Multiplexing
TDMA	Time Division Multiple Access
TID	Traffic IDentifier
TOS	Type Of Service
TSN	Time-Sensitive Network
VCPE	Virtual Customer Premises Equipment
VLAN	Virtual LAN
VNF	Virtual Network Function
VNO	Virtual Network Operator
VoIP	Voice over IP
VPN	Virtual Private Network
VR	Virtual Reality
VTP	Virtual Transport Path
VxLAN	Virtual extensible Local Area Network
WAN	Wide Area Network
WDM	Wavelength-Division Multiplexing
WG	Wireless Gateway
WMM	Wi-Fi® multimedia
XC	Cross-Connect
XGS-PON	10-Gigabit-capable Symmetric PON

NOTE: Also known as symmetric 10G-PON.

YANG	Yet Another Next Generation data modelling language

4 Business requirements for network architecture

4.1 Business requirements overview

When implementing a use case, the business requirements may be separated into a Physical Layer, a Network Layer and an Application and Management Layer. The focus of the present document is the F5G network architecture. This clause will summarize the business requirements of the network layer. However, this clause may also illustrate system-level requirements essential to network nodes and equipment for the F5G use cases. Other requirements not deduced from the F5G use cases may also be considered, such as network evolution trends.

4.2 Business requirements driving the F5G architecture

- Dual-Gigabit Networks:
  - The dual-Gigabit networks are represented by 5G mobile and fixed multi-gigabit optical networks (F5G), which provide fixed and mobile gigabit single user access capabilities. The dual-Gigabit network features ultra-high bandwidth, ultra-low latency and enhanced reliability. That means dual 5G and F5G networks need to be built for new application scenarios beyond the traditional applications. It is a key element for developing the digital economy, the digital society and the digital government.
- Rich set of Applications and Services for Different Market Segments:
  - The F5G architecture needs to support a rich and diverse set of application and service scenarios for a wide range of customer profiles including home users, large, medium, and small enterprises and specific vertical industries. Those applications and services for the different markets are ideally supported on the same infrastructure for improved operational efficiency of communication and networking services. This multi-service network shall allow flexible and dynamic service creation, development and deployment.
- F5G Infrastructure Convergence and Consolidation:
  - In the current fixed network business, the networking services are provided with dedicated networks and shared best-effort network infrastructure using copper- and fibre-based access networks. Consolidating and converging the fixed network infrastructure requires the overall infrastructure to enable a seamless connection between network segments (access, aggregation and core) and differentiate the services required by the different market segments and applications. The differentiation is expected over several dimensions, including bandwidth, latency, reliability, end-to-end delay assurance, and convergence through dynamic service awareness on a single, converged and agile management plane.
  - Also, studies show that enterprises from medium to small scale have a very diverse set of networking service requirements and are often co-located with other SMEs and residential housing. Sharing infrastructure on various levels is a suitable way of increasing operational efficiency.
- Converged Application Needs:
  - The line between home and enterprise networks is blurring since many more of those that work from home offices require enterprise-grade infrastructure. Also, industries and education institutions have moved more online and have massively digitized their processes, requiring the proper networking technology. On the other hand, some enterprises encourage Bring Your Own Device (BYOD), and some applications that the workforce are using are based on what they use at home. Also, enterprise networks are required to support residential oriented methods of working and processes, including on-demand ordering of communication services.
- Shift of Broadband Service Requirements:
  - So far, specifically for the residential markets, the services focus on the Internet Access Bandwidth. Also, in the enterprise markets, an important focus is on network bandwidth and reliability. For F5G, the assumption is that bandwidth is no longer the only dimension and that there is a shift from bandwidth to user experience to improve ARPU. This implies that the network needs to be more service-aware. Separation and isolation of user traffic from each other are a necessary mechanism to deal with guaranteed SLAs (e.g. through E2E slicing). More experience-based network policies are required to support more scenario-based broadband products for home, enterprise and verticals.
- Growing beyond Traditional Telecommunication:
  - The F5G architecture shall enable a wide range of services and functionalities, namely addressing specific vertical industries and other needs that support new business areas. For example, the functionality of E2E slicing and time-critical communication enables a larger set of industrial applications. In addition, the F5G architecture should support Passive Optical LAN (POL) as carrier-grade technology for campus and enterprise environments with the benefits of saving equipment rooms, having high-quality management capabilities, saving energy through passive optical technologies, removing radiation, and enhancing networking services in the customer premises.

- Increased Operational Efficiency:
  - The F5G architecture aims to improve operational efficiency by improving the quality of experience and better control over the quality of the services provided, such that potential user requirements are detected early and can be reacted upon. Integrating artificial intelligence and machine learning mechanisms into the F5G architecture will enable improved efficiency and more accurate network planning in terms of quality and capacity extension.
  - The F5G architecture is a unified architecture, which simplifies the O&M of the network. Decoupling the Service Plane and Underlay Plane using fabric networking simplifies and decouples capacity expansion from the service needs and improves bandwidth efficiency. Automatic operation and model-driven management simplify the interaction with different IT systems in the operator domain.
- Network Security:
  - The fixed network shall be a trusted infrastructure, requiring that the F5G architecture solves network security challenges. Secured networks and services are important for customer's trust in the network and make it a prerequisite for digitalization of industries and the society.

NOTE: The present document peripherally addresses security and privacy topics, but they are addressed in detail by ETSI GS F5G 012 [22] and ETSI TS 103 924 [23].

5 Network architecture

5.1 Architecture design principles

5.1.1 Multi-Service Network Platform

Multiple services for multiple customer types can be deployed based on the currently deployed broadband network architecture. However, it is not flexible, the deployment takes time, and the different customer requirements are difficult to fulfil cost-effectively. To enable flexible service deployment, SDN and NFV were introduced for network flexibility as tools to migrate fixed network architecture towards an SDN and NFV enabled F5G network architecture. SDN centralizes the control plane function and provides a concentrated network management functions. The management plane is now called the Management, Control and Analytics (MCA) plane; it enables more flexible and more efficient traffic route selection than a fully distributed control plane. NFV uses the virtualization technologies and cloudification to virtualize entire classes of network node functions into functions that are either stand alone or chained together to provide a communication service. This is especially beneficial for computing-based network functions, which can be easily deployed on IT-oriented cloud infrastructures.

NFV enables more flexibility to run the network functions and makes it easier to upgrade and enhance network services dynamically. The F5G architecture supports processing elements wherever needed including edge computing. However, the network's primary function is transporting bits at high speed, which means the base functionality of networking still requires major hardware support.

The multi-service network platform needs mechanisms to isolate a certain type of service traffic from other traffic. The platform should support guaranteed quality of service and a wide range of diverse services.

5.1.2 Dynamic and Flexible Service Creation

The F5G architecture is expected to support eFBB, FFC and GRE, which means ten times more speed, ten times more dense connections and ten times better SLAs. Besides fundamental features like SDN and NFV, the F5G architecture focuses more on flexible service enabling, reliable network performance guarantees, and autonomous service deployment.

The assumption is that customers can order or change their services on demand through a user interface (portal or API) to the OSS/BSS, which requires the Service Plane to be more flexible to adapt to a particular customer need.

5.1.3 Decoupling Service Plane and Network Plane

Therefore, broadband services shall be decoupled from the underlying network infrastructure. The decoupling allows for the independent upgrade of the network infrastructure without any effect or changes on the Service Plane. Also, the services can be adapted and changed without changing the basic network infrastructure. However, certain interdependencies will still exist, specifically in terms of what resources on the underlay can be used to provide a particular service. Also, in the cases of underlay network failures, these may affect the service quality.

5.1.4 AI-based Control, Management and Analytics

Artificial Intelligence shall be introduced on the Management & Control plane, making it a Management, Control & Analytics Plane, enabling more intelligent detection of faults and QoE degradation, network behaviour analysis and reaction to poor performing networks.

5.1.5 Security by Default

F5G applies the "security by default" paradigm, which means security claims for each element in the F5G system are verified. The connections and interfaces in the system (security-connections), which are potentially malicious, are verified to be secure. Details about the security design principles and directions are outlined in ETSI GS F5G 012 [22].

5.2 Architecture overview

Based on SDN and NFV principles, the F5G network architecture decouples services from the underlying physical network. Figure 1 illustrates an overview of the three planes of the F5G network architecture.

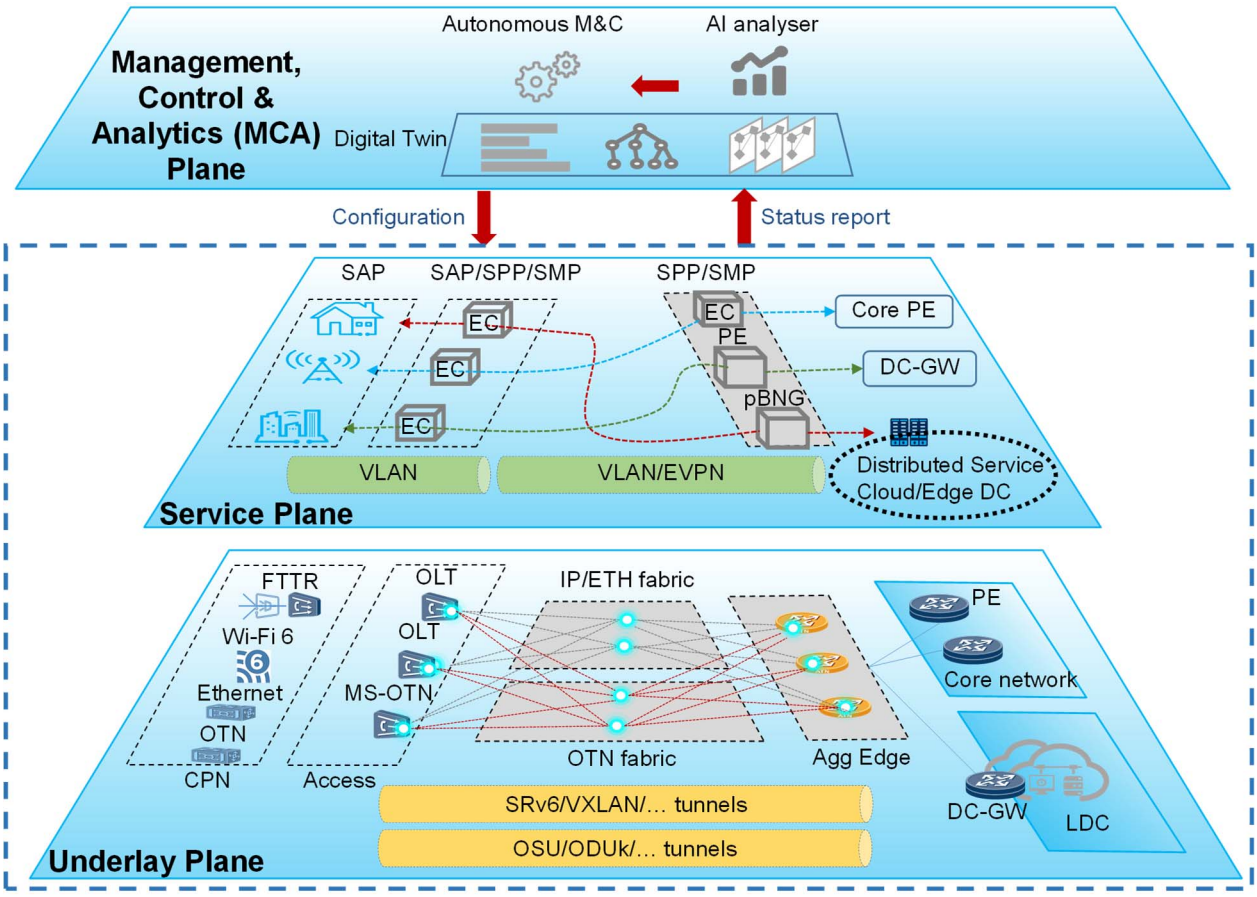


Figure 1: F5G network architecture

The F5G network architecture comprises three planes, an Underlay Plane, a Service Plane and a Management, Control & Analytics (MCA) Plane:

- Underlay Plane:
  - This is fundamentally the physical network plane, which comprises physical network nodes. The Underlay Plane provides connections and dynamic programmable path selection under the control of the F5G controller in the MCA Plane. The network switching capacity shall scale without interfering with the Service Plane.
  - The Underlay Plane has four segments, Customer Premises Network (CPN), Access Network (AN), Aggregation Network and Core Network. Various Technologies are used in the CPN, depending on the end-user requirements. For example, in Home Access, Wi-Fi® 6 and FTTR can be introduced as new technologies, while Enterprise Access can benefit from POL to gain easy deployment and high bandwidth. OTN can also be deployed in the CPN for customers requiring high-quality VPN service. The Access Network shall be based on XGS-PON technology and OTN, depending on customer type and service delivered. The Aggregation Network has two parallel fabrics, an IP/Ethernet fabric and an OTN fabric. The IP/Ethernet fabric comprises spine switches, while OTN fabric is comprised of OTN nodes. For the actual deployment of IP/Ethernet or OTN fabrics, there could be multiple physical fabrics of the same type co-existing in one network. Both fabrics have a common Aggregation Edge handover point to the Core Network. There might be multiple bearer connections between Access Network and Aggregation Edge, which go over either the IP/Ethernet fabric or the OTN fabric. There may be multiple paths through different nodes for differentiated bearer connection instances in one fabric with the required SLA. Typically, there is only one bearer connection instance for a certain SLA. The Access Network connects both IP/Ethernet fabric and OTN fabric.
  - The Underlay Plane and the associated network nodes shall support network slicing.
- Service Plane:
  - This plane provides service connectivity for customers and the broadband service above. Compared with coarse granularity bearer connections of the Underlay Plane, service connections on the Service Plane can be dynamically created when triggered by protocols, e.g. PPPoE, or configured from the MCA Plane.
  - A Service Access Point (SAP) provides customer service access. A Service Processing Point (SPP) performs L1/L2/L3 service processing, which may be enhanced by Edge Computing. A Service Mapping Point (SMP) is where traffic is directed to proper underlay fabric and channels. An Access Network typically contains SAP, SPP and SMP. Besides providing the access function, it also identifies services, adds or removes encapsulations, and directs the traffic to the proper underlay fabric and channels. An Aggregation Edge typically contains SPP and SMP, because it needs to perform service-specific processing and egress/ingress traffic mapping to appropriate underlay bearer connections.
  - A service connection refers to the service pipe between a Service Access Point (SAP) from the Access Network and the Service Processing Point (SPP) on the Aggregation Edge. Examples of SPP on the Aggregation Edge are pBNG, wholesale Gateway, VPN PE and VNF for value-added services. Internet service pipes between ONU and pBNG are typical service connections. The Service Plane also provides service connections between SPPs, e.g. a service chain between a VCPE instance and a Firewall instance, a VPN from the OLT to the Aggregation Edge. For IP based services, the SPP in the Access Network can perform subscriber authentication, while pBNG mainly terminates PPPoE services.
  - By defining new SPPs, new services can easily be created by programming service chains with SPPs.
  - The Service Plane is decoupled from the Underlay Plane. The Underlay Plane is unaware of changes in the Service Plane, e.g. adding, deleting and directing service traffic to SAPs and SPPs. The SAP and SPP can be scaled independently. The Service Plane can support multiple services with different SLAs. The requirements for deploying services on the Service Plane include connecting endpoints with guaranteed SLAs. The Service Plane shall negotiate resource requirements with the Underlay Plane, which is coordinated by the MCA Plane. It is unnecessary for the Service Plane to be aware of the creation of paths through network nodes, protection, etc.

- Management, Control & Analytics (MCA) Plane:
  - MCA Plane is the intelligent core of the network, which is in charge of management, control and analytics of the complete network. It is comprised of three logical components. However, the logical components can be implemented as distributed, centralized or hybrid mode. So the functional allocation to locations in the network topology is for further study:
    - Digital Twin: The digital twin of the network is the model of the network, including available resources and configurations. The digital twin also contains an equivalent model of the running network. A network digital twin is generated through the real-time collection of network status and combining that with network resources and configurations. Network statistics are continuously computed. A digital twin is the real-time status and configuration of the network, which is the input for autonomous operation and artificial intelligence-based analysis.
    - Autonomous Management and Control: This is the main function for network configuration, service deployment, and network operation. Besides the controllers for Service Plane and Underlay Plane, it also contains Intent Engine and Autonomous Engine:
      - Intent Engine: provides an Intent API for the OSS. The Intent API is an interface similar to natural language, describing "what I want". It is abstract and decoupled from specific network configurations. The Intent Engine can translate and understand the intent from the interface and drive corresponding operation, validation and feedback.
      - Autonomous Engine: implements operations such as resource management, device management, service deployment and bearer connection selections on the Underlay Plane. It also implements resource management, device management and service deployment on the Service Plane. One important function of the Autonomous Engine is the coordinated configuration of the planes, which enables plug and play of network nodes, and programmability of both underlay bearer connections and services.
    - AI analyser: analyses network data, identifies, locates and predicts network failures, provides management tools for QoE and analysis tools for network operations. It includes the Analysis Engine and the AI Engine:
      - Analysis Engine: a data management platform and algorithms for analytics. Analysing network digital twin enables optimal bearer connection selection on Underlay Plane, identifies and analyses network failures, and drives close loop control of the Autonomous Engine.
      - AI Engine: it performs reasoning and training using Artificial Intelligence. The Analysing Engine leverages the AI Engine for analytics and reasoning, in order to perform prediction of network failure and usage, and failure identification and analysis.

5.3 Network topology and interfaces

5.3.1 Network Overview

The F5G network architecture is developed based on the current fixed network deployment and provides more Full Fibre Connections (FFC) with high-quality user experience (GRE).

Compared with previous generations, the introduction of FTTR will be a major improvement in fibre connection numbers. FTTR is not restricted to residential customers but can also be applied to business customers. This will fundamentally change the network topology, flow model and management.

Considering GRE, E2E service quality relies on QoS for each network segment, where network topology and technologies play an important role. For example, for Cloud VR, Cloud VR terminal devices communicate with the Cloud VR Service Platform through the CPN, the Access network and the Aggregation Network. All three segments need to provide good quality to guarantee an E2E high-quality user experience.

PON can provide on-premises network connectivity and is considered part of the CPN (use case #4 in IETF RFC 8453 [1]). XG(S)-PON is the leading F5G Access Network technology. For the Aggregation Network, IP/Ethernet based network has been widely deployed for years. For residential customers, BNG is necessary for subscriber authentication, authorization and accounting. However, for business customers, especially Private Line customers, the BNG may not be required.

Provisioning and management of MPLS-based VPN is complicated, especially Traffic Engineering (TE), which typically needs manual configuration.

To improve the flexibility, efficiency and performance of the Aggregation Network in F5G, an OTN network is introduced to complement the IP/Ethernet-based network and build a full fibre E2E network. F5G requires differentiated carrier capabilities to support high-quality services with guaranteed bandwidth and latency, as well as low cost best-effort services. The IP Network can be improved with new IP technologies to meet the requirements of GRE and potentially simplify the management. OTN can be used to provide high quality carrier service, which is enhanced by adding fine granularity. There are several benefits with the addition of OTN, including supporting transparent transport, high bandwidth multiplexing, powerful OAM, etc.

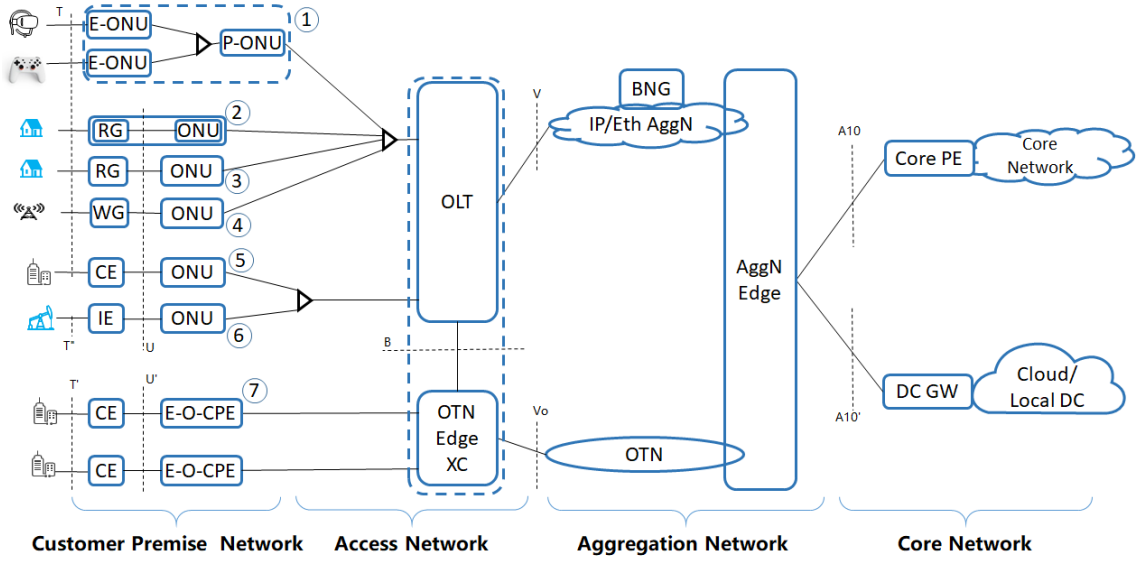


Figure 2: F5G Network topology

1) FTTR is comprised of a CPN Agent labelled P-ONU and a customer edge devices labelled E-ONU. The link between P-ONU and E-ONU is through P2MP passive optical network.

2) Integrated home Optical Network Termination comprising an adaptation function labelled RG (Residential Gateway) and an Access Network node labelled ONU.

3) Disaggregated home Optical Network Termination comprising an adaptation function labelled RG (Residential Gateway) and Access Network node labelled ONU. The difference between item 2 and item 3 is that the adaptation function is external.

4) Cellular Backhaul Optical Network Termination comprising an adaptation function labelled Wireless Gateway (WG) and Access Network node labelled ONU.

5) Small and medium-sized business Optical Network Termination comprising an adaptation function labelled CE (Customer Equipment), and Access Network node labelled ONU.

6) Industrial Optical Network Termination comprising an adaptation function labelled IE (Industrial Equipment), and an Access Network node labelled ONU.

7) Premium Private Line Optical Network Termination differs from item 2 to item 6, and it comprises an adaptation function labelled CE (Customer Equipment) and Access Network node labelled E-O-CPE (Enterprise-OTN-Customer Premise Equipment), which is OTN based and not PON bases.

Figure 2 shows the F5G network topology. The FTTR case labelled item 1 in Figure 2 uses a centralized Wi-Fi® access network architecture, facilitating coordination between fibre backhaul link and wireless link (Wi-Fi® connection between AP and end devices). Items 2 to 5 in Figure 2 have a customer-facing adaptation function and an Access Network node. The adaptation function and Access Network node are demarcated by the U interface. In the case of premium private line, an Enterprise-OTNCPE (E-O-CPE) represents the device that communicates with the OTN edge cross-connect (OTN Edge XC) on the network side. It is also the aggregation device for enterprise data. The enterprise network labelled CE in Figure 2 and the U' interface demarcates the Access Network. While SDN/NFV is considered in F5G, the OLT module in Figure 2 represents the data plane function of OLT and OTN edge cross-connect, whereas the control and management function of the OLT is not shown and is out of scope of the present document.

A BNG is a typical function in IP/Ethernet-based Aggregation Networks, which may be directly connected to an OLT or via other nodes. Even though there are some efforts to disaggregate the BNG or create a BNG pool, the module in the figure represents the BNG function. There may be an IP/Ethernet Aggregation Network between BNG and Core Network in some cases. OTN technology is an alternative to IP/Ethernet for the Aggregation Network. The OTN edge cross-connect aggregates the Access OTN traffic and will be a node on the OTN Aggregation Network. The Aggregation Network Edge represents the handover point between the Aggregation Network and Core Network. It needs to identify and direct the traffic in both directions.

The local DC and cloud services are getting more and more popular and can be considered an extension that expands the legacy core network. Even though the Core Network is not in the scope of the present document, the interfaces between Aggregation Network and Core Network need to be specified in the present document.

The interfaces in Figure 2 are described in clause 5.3.2.

5.3.2 Definition of Interfaces

5.3.2.1 T interface

The T interface is the handover point between E-CPE/Gateway/CE and the customer devices. This includes residential customers, business customers and wireless backhaul. Because of the diversity of customers, besides Ethernet and Wi-Fi® 6, there might be other types of interfaces like Bluetooth®. Such interfaces shall be translated to Ethernet/IP protocols on the CE devices.

The T interface for FTTR is the same as for FTTH. Other interfaces for FTTR are not addressed in the present document. They are for further study and for future versions of the F5G architecture. For example, the G.fin-SA project in ITU-T Study Group 15/Q18 [i.3] defines the FTTR system architecture.

5.3.2.2 T' interface

The T' interface is the handover point between the Enterprise customer devices and the CE. The primary interfaces from of Enterprise devices are Ethernet and Wi-Fi® 6. However, besides Ethernet and Wi-Fi® 6, there might be other types of interfaces such as for telephones connecting to a PBX or legacy SDH equipment.

5.3.2.3 T'' interface

The T'' interface is the handover point between IE and industrial network devices. There are many types of industrial protocols and interfaces, like EtherCAT, serial interface, etc. They shall be supported by the IE device depending on the scenarios. Such interfaces shall translate industrial protocols to Ethernet/IP protocols on the IE devices.

5.3.2.4 U interface

The U interface is the handover point between the Access Network and the CPN. For a PON based network, the ONU is considered an extension of the Access Network, even though it physically resides in the CPN. Therefore, the U interface is the user-facing interface of an ONU. It could be an internal interface if ONU and RG are integrated into one physical device.

5.3.2.5 U' interface

The U' interface is the handover point between the OTN Access Network and the CPN/CE. For an OTN Access Network, the E-O-CPE is considered an extension of that OTN Access Network, even though it physically resides in the Enterprise CPN. Therefore, the U' interface is the user-facing interface of E-O-CPE. The protocol stacks on the U' interface are depicted in Figure 3.

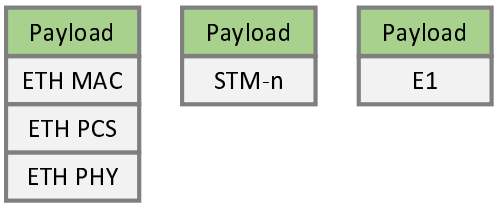


Figure 3: Protocol stacks on U' interface

5.3.2.6 B interface

The B interface is the handover point between the OLT Access Network node and the OTN Edge cross-connect (OTN Edge XC) node. This is an Ethernet interface, which will be mapped over an appropriate OTN container. The protocol stacks on the B interface are depicted in Figure 4.

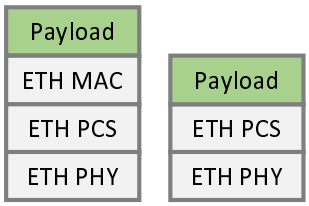


Figure 4: Protocol stacks on B interface

The B interface is only present in the case of OLT and OTN Edge XC being separated physical network equipment. Otherwise, it is an internal interface and does not necessitate a description.

5.3.2.7 V interface

The V interface is the IP/Ethernet-based handover point between the Access Network and the Aggregation Network. Compared with a legacy IP/Ethernet Aggregation Network, SRv6 and VxLAN are the primary technology for the Underlay Plane of IP/Ethernet Aggregation Network. At the same time, EVPN is used for the Service Plane. The protocol stacks on the V interface are depicted in Figure 5.

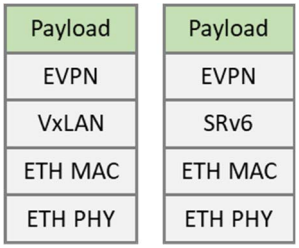


Figure 5: Protocol stacks on V interface

5.3.2.8 V_o interface

The V_o interface is the OTN based handover point between OTN Access Network and OTN Aggregation Network. The interface rate is dependent on the OTN bandwidth requirements of this OTN Access Node. The interfaces is either OTUk (k = 2, 3, 4) for bandwidth requirements between 10 G and 100 G or OTUCn/FlexO for bandwidth greater than 100 G. These are the primary technologies for the Underlay Plane of OTN Aggregation Network, while VLAN is used for the Service Plane.

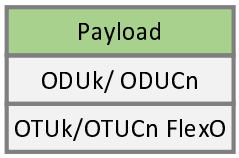


Figure 6: Protocol stacks on V_o interface

5.3.2.9 A10 interface

The A10 interface is the handover point between the Aggregation Network and the Core Network. Depending on the capability of Core PE, the handover protocol may be selected from EVPN, VxLAN, SRv6, MPLS, etc. Protocol stacks on A10 interface are depicted in Figure 7. Aggregation Edge may be required to implement protocol interworking between the Aggregation Network and the Core Network. PHY for A10 interface may be Ethernet PHY for the legacy network or OTN for a full optical network.

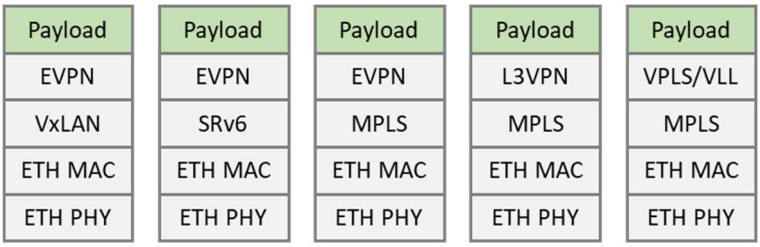


Figure 7: Protocol stacks on A10 interface

5.3.2.10 A10' interface

A10' interface is the handover point between the Aggregation Network and the Cloud or local DC. This interface is actually the interface between the Aggregation Edge and the DC Gateway. The link could either be Ethernet-based or OTN based. Protocol stacks on A10' interface are depicted in Figure 8.

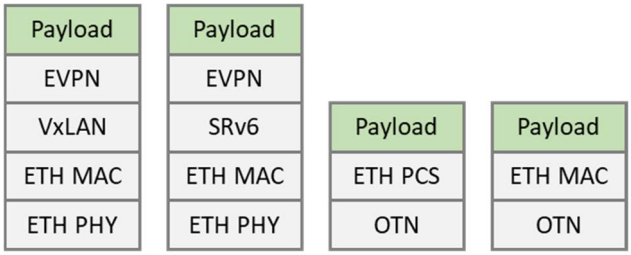


Figure 8: Protocol stacks on A10' interface

5.3.3 OTN Control Interfaces

In F5G, the OTN network can be used to carry high-quality services. To enable the automatic OTN bearer connection creation for these services, the OTN control plane shall be enhanced. The OTN control plane is separated from the data plane, and the interfaces in the OTN control plane are shown in the modified F5G network topology in Figure 9. Unlike the centralized MCA plane, the OTN control plane is a signalling plane running between OTN nodes.

The OTN control interfaces transmit the provisioning protocols for the OTN-based services. There are two OTN control interfaces types:

- The C1 interface is used to control the OTN network connections in the Underlay Plane.
- The C2 and C2' interfaces are used to control the OTN-based service connections in the Service Plane.

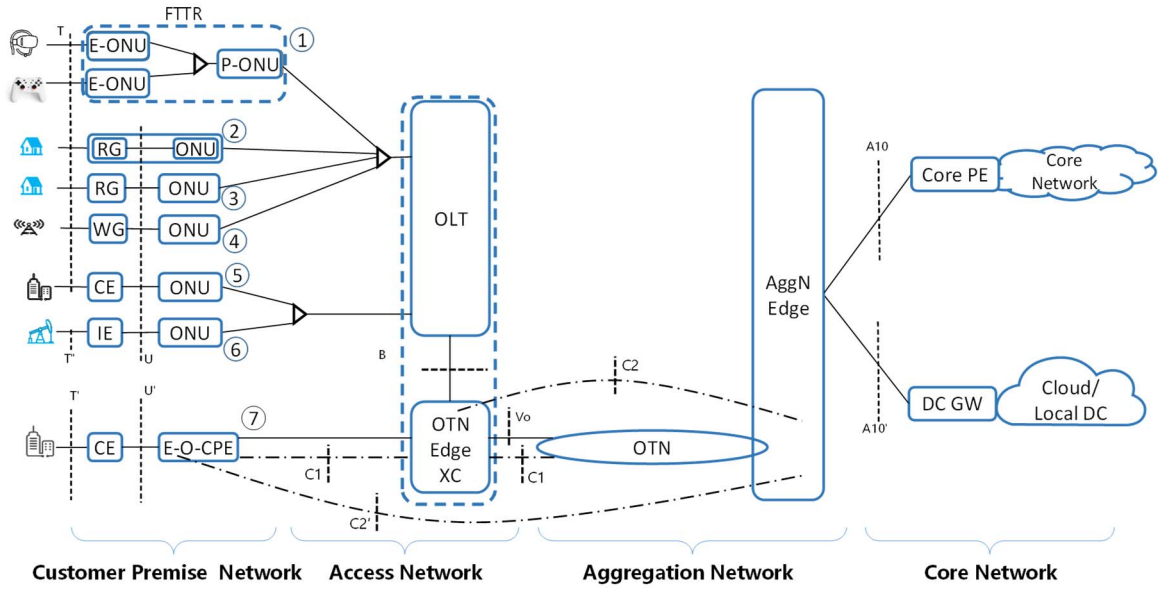


Figure 9: OTN control interfaces

The C1 interface is the control plane handover point between two network nodes, where the OTN-based links are used. The C1 interface exists between the OTN Edge XC and the OTN Aggregation Network, and between the E-O-CPE and the OTN Edge XC. For both locations, the C1 interface has the same control functions and is used to exchange the OTN signalling messages to control the OTN network connections across the network segments. The main functions of the C1 interface include:

- To transmit the signalling messages used to create, modify or delete OTN network connections automatically. The F5G management and control system will trigger this signalling process (not shown in Figure 9 for simplicity).
- To transmit the signalling messages used to adjust the bandwidth of the OTN network connections. A typical network scenario is the use case for premium home broadband service, supported by connecting to multiple clouds. The OTN Aggregation Network is used to transport the services of multiple users. The bandwidth adjustment of the OTN network connection is based on a change in the number of users, an adaptation of the user's bandwidth needs, or a shift in application bandwidth needs.
- To perform fast OTN connection recovery after network failures, specifically in the case of a large number of connections. The OTN network is being enhanced by the addition of finer granularity containers, therefore the number of connections in the OTN network will increase significantly. At the same time, compared with legacy GMPLS protocol, the C1 interface should also be enhanced with the ability to recover a large number of connections in a short and committed recovery time. This is required to meet the SLA requirements of the OTN-based services and ensure high-quality customer experience.

The C2 and C2' interfaces are the control plane handover points between the two ends of an OTN-based service connection in the Service Plane, where the service traffic is mapped into/de-mapped from an OTN network connection. The C2 interface exists between the OTN Edge XC and the AggN Edge and is mainly applied to the PON on-premises use cases (see items 1 to 6 in Figure 2). The C2' interface exists between the E-O-CPE and the AggN Edge and is mainly applied to the use case of Premium Private Line services (see item 7 in Figure 2). The C2 and C2' interfaces are used to negotiate between and configure the Service Mapping Point (SMP) in the Service Plane. The C2 and C2' may be different due to the provisioned services.

The main functions of the C2 and C2' interfaces include:

- To learn and exchange the MAC/IP addresses between the network endpoints, ,such as between the private networks in both the CPN/Access Network side and the Core Network side, signalling endpoints (OTN edge nodes). This helps the OTN edge nodes (i.e. the E-O-CPE, the OTN Edge XC and the OTN AggN Edge) to generate the appropriate service mapping/de-mapping rules. Such rules include the mapping of the service traffic into the OTN network connections and the de-mapping of the service traffic from the OTN network connections. Note that the exchange of MAC/IP addresses is per VPN service, i.e. the address exchange is only within each VPN of a specific service.

- To identify the destination address of the service traffic and map the service traffic into the appropriated OTN network connections according to the service mapping/de-mapping rules.

Note that, due to the differences of applicable use cases and service provided, the C2 and C2' interfaces may be slightly different in protocol design, although they have similar functions. The protocol design of the C2 and C2' interfaces are out of the scope of the present document.

Since the E-O-CPE is located on customer's premises, and its security may not be under the control of the network operator, the security aspects of the control interfaces (C1, C2') connecting the E-O-CPE and the nodes in the operator's network also need to be considered. This is for further study.

5.3.4 FTTR control interface

To guarantee customer experience, the FTTR network should ensure a close collaboration with Wi-Fi® network. Thus, dynamic coordination between the different E-ONUs should be achieved. This requires an architecture to reflect fibre and wireless integration within FTTR (shown in Figure 10), forming a single cascaded multiple link LAN, such as FTTR and Wi-Fi® network through centralized control.

To complete the centralized control procedure, a series of steps are described as following, and is shown in Figure 10:

- The P-ONU collects the Wi-Fi® status, such as data buffer level, air interface status, etc., from the E-ONU Wi-Fi® entity. Such status information are encapsulated by edge FTTR entity through the FTTR protocol (such as specification of G.fin) and sent to the main FTTR entity in the P-ONU. In addition, the coordination strategy from the controller is also extracted from edge FTTR entity in the P-ONU and sent to Wi-Fi® module.

- The controller collects the Wi-Fi® status from the Wi-Fi® module on one hand and send the coordination strategy to the Wi-Fi® module directly on the other hand.

- The F1 is the interface between the main FTTR (M-FTTR in the P-ONU) entity and the edge FTTR (E-FTTR in the E-ONU), enabling message transmission for data and control message transmission for coordination. The interface supports the exchange of Wi-Fi® status message in the up-link and coordination strategy in the downlink.

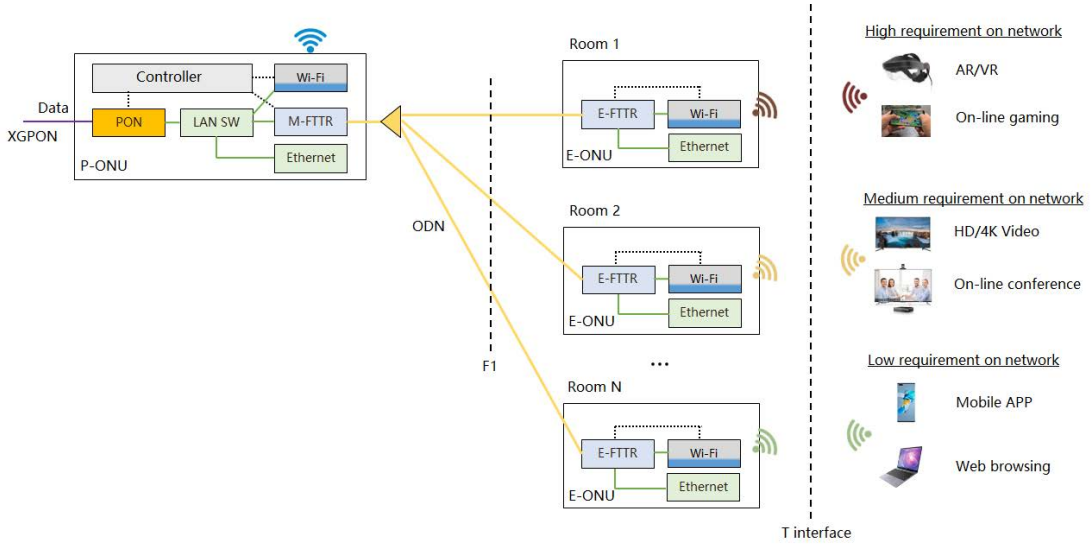


Figure 10: Centralized Wi-Fi® access network architecture through centralized control in FTTR

The FTTR control function focuses mainly on the coordination within the fibre connection network, which does not change the characteristics of T interface (such as physical layer properties, MAC framing, etc.). Specifically, Wi-Fi® specification in the air interface is defined by the IEEE 802.11 group. Other technology like Ethernet may also be dynamically managed. As a whole system, the P-ONU act as a master FTTR unit while the E-ONU act as a salve FTTR unit.

5.4 Key enabling features

5.4.1 Network Slicing

5.4.1.1 Introduction

A network slice is a logical network that achieves specific service requirements.

Network slicing provides a solution for differentiated services in a mode of operation such that multiple independent instances with different service requirements are provided on a shared infrastructure. With the flexible design of slicing functions in terms of performance, isolation and O&M, network service providers can create customized networks based on customers' requirements. Network slicing is an end-to-end concept that covers all network segments. The F5G architecture end-to-end slicing includes CPN, Access, Aggregation, and Core networks. It enables the concurrent deployment of multiple end-to-end logical, self-contained, and independent shared or partitioned networks on a common infrastructure platform. In-network slicing, forwarding resources are sliced, and network functions shall be sliced or allocated to different slices also. Slicing of network functions in Service Plane, e.g. SAP, SPP and SMP, are for further study.

Network Slicing is an important feature for F5G networks, which fulfils a set of high level F5G requirements that are summarized below:

1) The F5G system requires "guaranteed network service". The motivation for this requirement is that the service performance requirements will be more dynamic and differentiated. The handling of requirements along a various dimensions is needed to support those different service performances. Services with different SLAs can be carried on the same network through the slicing solution separating the traffic into different slices.

2) The F5G system requires isolation. The motivation for isolation is from a resource perspective to have guaranteed service, and it protects against the mixing of traffic and interference between different business entities and tenants. For example, resource isolation from other tenant networks is a basic privacy requirement for industry production networks.

3) The F5G system requires independent service operation. Network providers need to be able to open network functions to tenants so that tenants can manage, configure, and operate their own network slices (for the definition of tenant see clause 3.1).

4) The F5G system requires end-to-end slices covering customer premise, Access Network, Aggregation Network and Cloud resources.

5) The F5G system requires end-to-end slice management, ensuring resource reservation, configuration, protection and O&M management.

5.4.1.2 Concepts

In the following a set of concepts in the context of network slicing are used (see clause 3.1):

- Network Slice.
- Network Slice Instance (NSI).
- Network Slice Template (NST).
- Tenants.
- Dedicated Network (D-Net).
- Network Service Providers (NSPs).
- Isolation.

Typically, an application or service uses a network slice of a certain slice type. The tenant is the business entity providing the particular service or application to users.

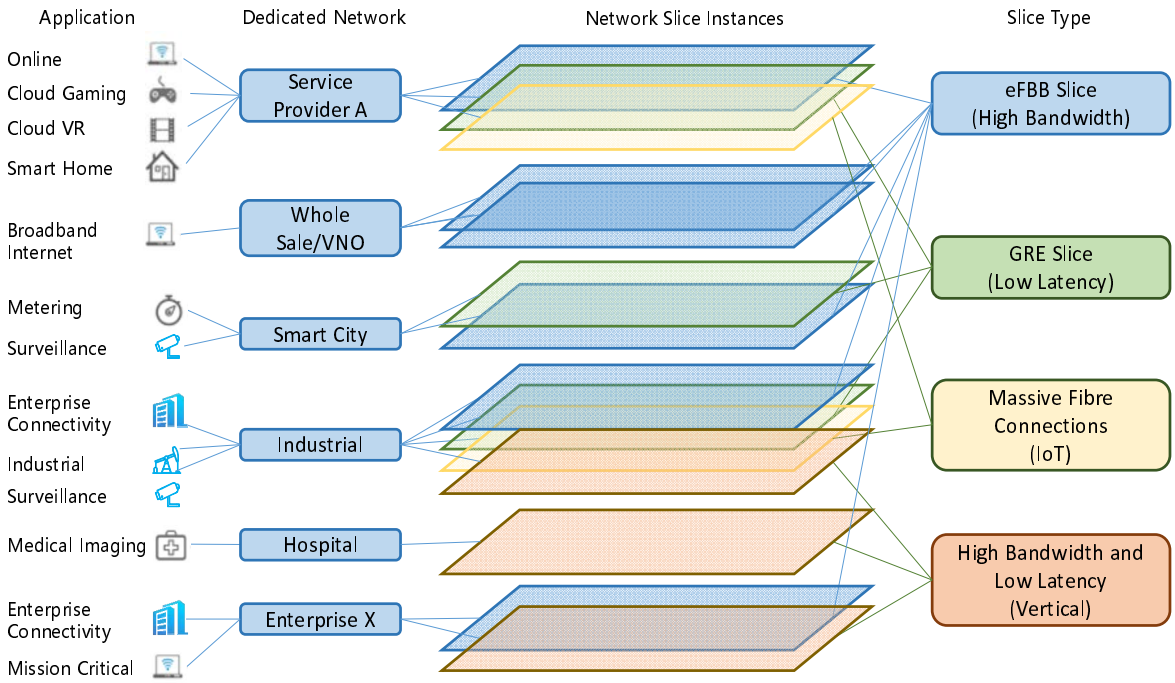


Figure 11: Network Slicing Concepts Example

Figure 11 shows an example of different network slicing concepts. Several slice types exist. In this example, 4 slice types are illustrated (eFBB, GRE, Massive Fibre Connections for IoT oriented application, and a combination of high bandwidth and low latency for vertical industry oriented services). Network Slice Instances can be of one of the pre-defined slice types. A Dedicated Network (D-Net) belongs to a particular tenant offering services to specific market segments like residential, wholesale, smart city, industrial, hospitals or any other enterprise-oriented segment. The Enterprise X in Figure 11 is a placeholder for any enterprise oriented services as described in the use case document. The particular market segment has a set of typical applications, which the Dedicated Network needs to support with the appropriate quality. For example, the residential oriented Dedicated Network supports traditional broadband, Cloud Gaming, Cloud VR, and Smart Home applications.

NOTE: There are use cases in the F5G use case document ETSI GR F5G 008 [i.1] not shown in Figure 11.

For the present document the following characteristics of network slicing are envisioned:

1) A network slice has several network capabilities. The network slice is defined by multiple parameters and covers management, control, and forwarding requirements.

2) A network slice template describes the network slice characteristics.

3) An instance of a network slice that is deployed on a network is referred to as a Network Slice Instance (NSI). The network slice instance is a service or service unit that can be independently operated and managed as a whole.

4) Network slice instances are implemented on a unified physical infrastructure, including computing, storage and network resources (what is used for providing a service is a matter of slice design). Resource occupation modes include shared priority-based scheduling, guaranteed resource reservation (which can be occupied by other services when not in use) and exclusive resource reservation.

5) A network slicing SLA can be met in several ways. From the perspective of network slicing, unified scheduling of E2E computing, storage and connection resources is important. For example, to meet the ultra-low latency requirement, a service can be deployed locally or an ultra-low latency hard pipe can be deployed.

6) The network slice SLA includes QoS guarantees.

7) A slice includes a data plane component. It consists of end-to-end logical connections and switching nodes. Logical connections and switching nodes can be classified into three types: shared priority-based scheduler, guaranteed resource reservation, and exclusive resource reservation. The switching nodes might include packet and TDM switching. The data plane of the Underlay Plane can have two types of technologies: priority scheduling and guaranteed resource reservation.

5.4.1.3 Network Slicing Applicability

Generally, there are two types of E2E slices in F5G. One is slicing the network into dedicated network resources according to SLA requirements for various tenants or operators, which may be applied to multiple industries or scenarios. The other is service-oriented slicing, where one network can be shared for different services with isolation and guaranteed QoS:

1) User group-oriented slicing: User group-oriented slicing refers to virtual operators, which implement the operation, management, and control of network nodes and virtual networks. It refers to several Dedicated Networks, where the virtual operator's network nodes are connected. The user group may be one with all users of the same type, for example, an enterprise user group (users of an enterprise) or a home broadband user group. It can also be a third-party virtual network leaser in a whole-sale scenario deploying its own devices connecting to the virtual network:

   - Different user group slices have basic features in terms of operation isolation, including forwarding isolation and management isolation. Implementing user group slicing simplifies communication network management, improves network communication quality and lays the foundation for differentiated services on a virtualized infrastructure.

2) Service-oriented slicing: Service-oriented slicing refers to the construction of multiple isolated logical networks with different SLA capabilities for different services of the same user group or tenant:

   - The slicing concept is applicable on different levels and might be hierarchical. Several service oriented slice instances can be within one user group oriented slice instance. For example, a home broadband user group uses both common Internet access services and VR services. A service slice is setup for each service. The traffic is separated and associated to its predefined slice type to meet the SLA requirements of common Internet access services and VR services. Different service slices have different SLA capabilities, and service slices have the characteristics of forwarding resource isolation.

To illustrate network slicing, an example scenario is shown in Figure 12. It shows three slice instances for residential high-quality video, education, and medical industry. Since network slicing is about sharing common infrastructure, the example shows different sharing approaches, depending on the use case:

1) For the residential high-quality video scenario, the Wi-Fi® network, the WAN port of the ONU, the PON network, the OLT, the OTN Nodes and the Gateway are shared but still have appropriate QoS characteristics for high-quality video services. This is a more service-oriented slice type since the service characteristics are the major influencing factor.

2) For the education scenario, the CPN is exclusive for the education site, and the ODN and PON tree are also exclusive. The OLT, OTN nodes, and the gateway are shared, however. Within the CPN, different applications as e-whiteboard and teaching equipment, including PC and projectors, might need to share the CPN and need certain QoS characteristics. Depending on the business arrangement and the education administration's willingness to control and manage the slice, it is more a dedicated network-oriented slice, which can be sub-divided into service-oriented slices for the different applications of the administration of the education. Or it can be seen more as a set of services provided by the operator. Then it can be regarded as more a service-oriented slice.

3) For the medical application scenario, the traffic from the CPE onwards is isolated from other traffic. Though the OTN nodes are shared, with hard isolation of slice instances from each other. Here the slice is a dedicated network provided to the medical institution with defined network QoS characteristics.

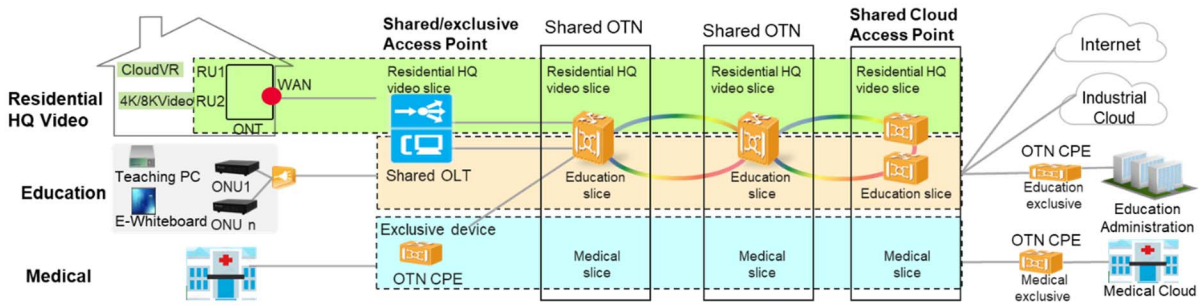
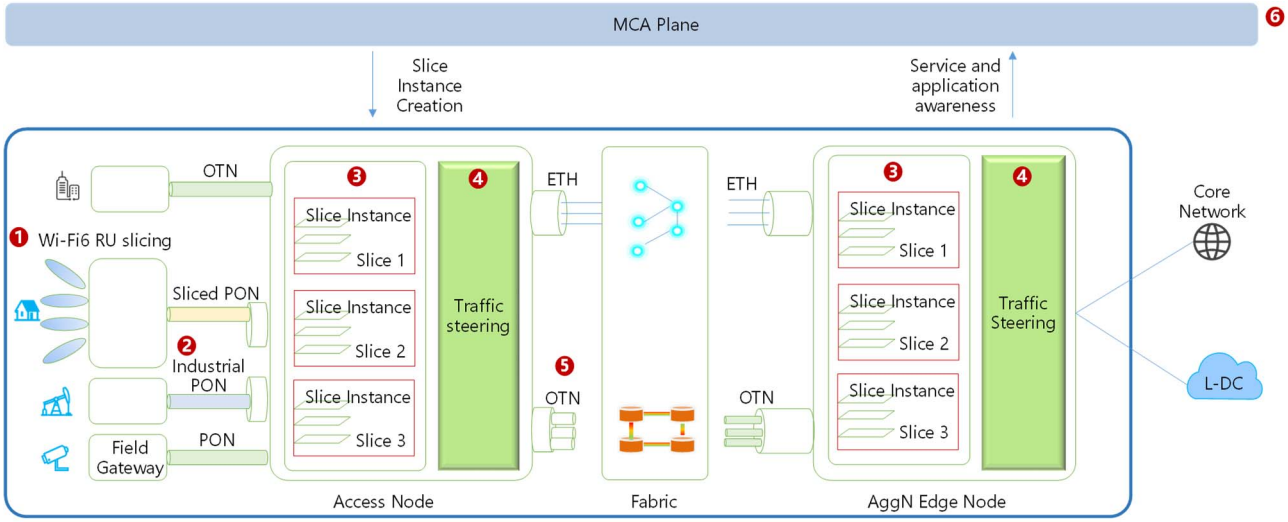


Figure 12: Example of Network Slicing

5.4.1.4 F5G Slicing Architecture

Figure 13 shows the F5G slicing architecture. Since slicing is end-to-end at several locations, slicing oriented functionality is needed. This includes the data plane as well as the control and management plane. There are different levels of isolation at the different locations.



NOTE: The location of features 3 and 4 in Figure 13 does not impose a particular implementation and only denotes those features available on the nodes.

Figure 13: F5G Slicing Architecture

In Figure 13, the following slicing features are shown:

1) Wi-Fi® 6 RU (Radio Unit) slicing: The Wi-Fi® 6 Radio Unit needs slicing functionality for isolating resources on the Wi-Fi® Radio part of the network. Also, the function for Wi-Fi® 6 network attachment plays a role in what slice a particular device is connected to. The decision on what slice a Wi-Fi® terminal is connecting to can be decided by the network or the terminal. Also, it can be transparent to the terminal, and the network can make intelligent decisions on-demand within the Customer Premises Network or in the Access Network.

2) In the Access Network, either PON or OTN features isolate traffic from different slices. If there is a need for resource isolation within a slice, the PON network or the OTN-based Access Network needs to handle that.

3) In the Access Nodes and AggN Edge nodes the network slices from the various slice types needs to be properly handled such that the service slice type characteristics are guaranteed. Traffic separation within a slice needs the appropriate handling in the Access Node.

4) Also, in the Access Node and the AggN Edge node, the characteristics of the path and the bearer connection used are selected. The traffic is steered to use OTN or IP/Ethernet depending on the required service characteristics.

5) In the fabric of the Aggregation Network, bearer connections have been established to carry the service traffic, guaranteeing the demanded characteristics to the appropriate place in the network. The traffic steering function needs to know what traffic is steered into those bearer connections.

6) Slice management deals with the creation/removal and monitoring of slice instances. Above the MCA plane are the tenant management systems that manage their tenant services and request slice instances. The northbound interfaces of the MCA plane need to be isolated from each other for management independence.

A key aspect of network slicing is resource isolation. So the specific functionality on the forwarding plane for resource isolation is the following:

1) The forwarding plane supports two forwarding modes: Packet and TDM. The resources of the two forwarding modes shall be independent.

2) The packet forwarding plane shall support multiple isolated resource pools for isolating the traffic. The TDM forwarding plane supports isolation inherently.

3) Resources in either forwarding planes may be allocated to one or more network slice instances.

Currently, independent dedicated networks are usually established for industries with high privacy requirements. An optimized and agile network construction is achievable with enhanced resource isolation and deployment flexibility of network slices. Therefore industries benefit from migrating from these privacy-oriented networks to network slices.

5.4.1.5 Network Slice Management

The details of the management architecture are out of scope of the present document, but a high level view of the slice management that is divided into layers and is described in this clause.

The first layer is the application layer, a service layer module where tenant VNOs can perform machine-to-machine or human-to-machine operations on slices and D-Nets. Tenants can manage and operate slices independently. The second layer is the network layer, which provides resource management, configuration management, performance management, and status management for network slices. The data in the network layer includes the predefined network function set, initial resource package, current resource data, and the slice running status. The NSP manages the life cycle of tenants, grants and withdraws resources, and grants and modifies network functions. The third layer is the NE management and control layer, which manages the functionalities of each network element.

A particular solution of network slice management is given by a standardized architecture, namely the Abstraction and Control of Traffic-Engineering Network (ACTN), as specified in IETF RFC 8453 [1]. ACTN is defined as a multi-domain, multi-technology network management architecture, as illustrated in the following Figure 14. The Customer Network Controller (CNC) of ACTN is the top layer, where tenants can manage their slices. Multi-Domain Service Coordinator (MDSC) is the second layer that manages E2E network resources and slice configuration. Provisioning Network Controller (PNC) is the third layer that manages network elements.

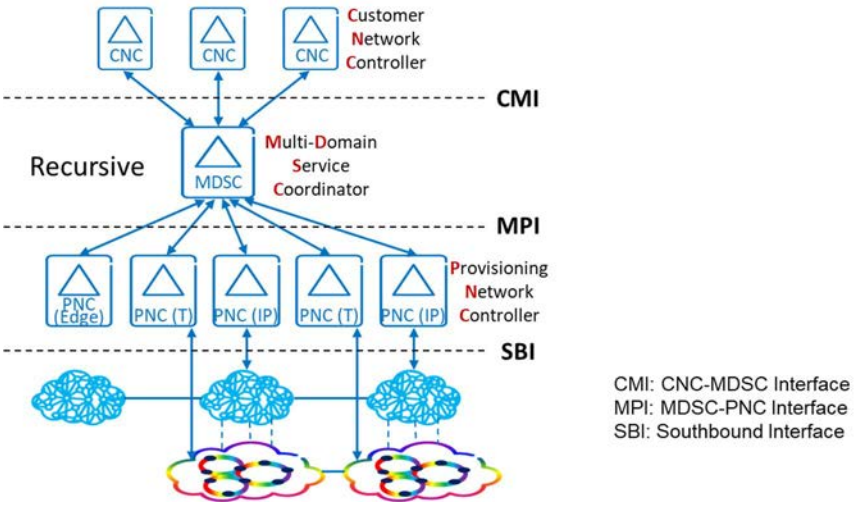


Figure 14: ACTN Architecture

The YANG models specified in the IETF are applicable to the ACTN architecture. The IETF draft-ietf-ccamp-transport-nbi-app-statement [i.4] provides guidelines on how the IETF YANG models are applied on ACTN interfaces for various functionalities including topology learning, bearer connection establishment and service delivery. ACTN has been identified by the Framework for IETF Network Slices (draft-ietf-teas-ietf-network-slices [i.5]) as a suitable basis for delivering and realizing IETF network slices. Further discussion on applicability, including YANG models, is ongoing in IETF draft-ietf-teas-applicability-actn-slicing [i.6]. Besides the current capability of OTN network management, the IETF is also developing YANG models for OTN slicing by draft-ietf-ccamp-yang-otn-slicing [i.7]. It is expected that the ACTN framework can be extended to cover F5G end-to-end slice management, which creates a lot of synergy among different SDOs.

5.4.1.6 Traffic Steering in the Context of Slicing

Traffic steering in the context of slicing deals with what traffic is mapped to what network slice instance. The traffic of different tenants or users is distinguished by some labels/tags/protocol header information in the service flows. In the network, the traffic is processed based on forwarding rules including QoS processing.

The control and management system authenticates and authorizes the access to an end-to-end slice instance and statically configures the mapping function for traffic to the appropriate network slice instance. The automated mapping function is for further study.

For further details on traffic steering, refer to clause 5.4.2.

5.4.1.7 Fibre-wireless coordination

The F5G, FTTR networking technology solves the Wi-Fi® interface collision problem to end device within the last 10 meters. This reflects the Guaranteed Reliable Experience (GRE) feature of F5G. The traditional networking technologies like Power Line Communication (PLC), Ethernet, etc. act as independent backhaul link compared to Wi-Fi® fronthaul interface. In many of these technologies, the on-premises network is cascaded by two independent link, which are the backhaul and the Wi-Fi® fronthaul links. The Wi-Fi® fronthaul functionality of E-ONU works by observing individual configuration, such as back-off counter, roaming mechanism (e.g. switching threshold), etc. This leads to a loose or no coordination between the backhaul network and Wi-Fi® network. Therefore, the air interface stability in multi-AP Wi-Fi® scenarios is still not achieved.

In such an architecture (shown in Figure 10 in clause 5.3.4), the Wi-Fi® status is first exchanged between the Wi-Fi® module in the E-ONU and FTTR entity (the controller directly collects the Wi-Fi® status information from Wi-Fi® module in the P-ONU). Furthermore, the controller should determine the coordination strategy based on the real-time Wi-Fi® status information input from the whole network (link service priority, Wi-Fi® status, business strategy of service operator, etc.). The strategy decision will be sent in time (such as to align with the air interface transmission) to all the Wi-Fi® module in the FTTR network. More importantly, the Wi-Fi® air interface time unit is 9 μs as specified by the IEEE 802.11 group (in IEEE 802.11ax [10] for Wi-Fi® 6).The shortest Wi-Fi® packet is tens of μs. Therefore, an extremely fast and latency guaranteed communication channel for the information exchange (status message and control command) is essential. The FTTR technology (i.e. G.fin) should provide dedicated protocol to support guaranteed latency channel to enable Wi-Fi® over fibre interface. The robustness of these messages should also be considered.

With the control interfaces of FTTR interacting with Wi-Fi® transmission, the on-premises fibre-based network behaves like a single network, which solves many of the current pain points of Wi-Fi® such as:

1) Air interface communication in the AP Wi-Fi® downlink could be coordinated. Specifically, making use of the trigger frame based mechanism defined by Wi-Fi® 6, the Wi-Fi® up-link communication could also be regulated.

2) Seamless roaming with zero switching time may be achieved based on the single fibre-wireless network.

3) Service QoE could be guaranteed in the Wi-Fi® network.

4) Others.

The complete integration of fibre and wireless required protocol convergence to avoid two cascaded processes in the on-premises network, is for future consideration.

To further demonstrate the benefit of centralized Wi-Fi® access network architecture, Figure 15 shows an example of coordination in Wi-Fi® air interface.

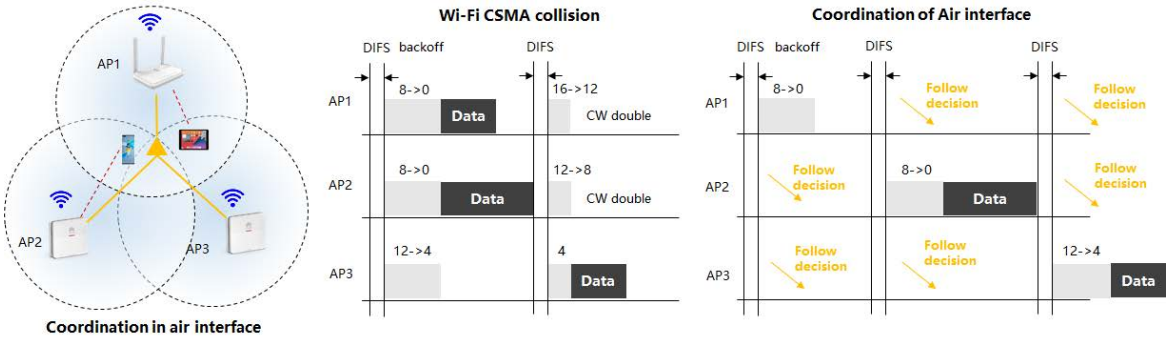


Figure 15: Example of coordination in Wi-Fi® air interface

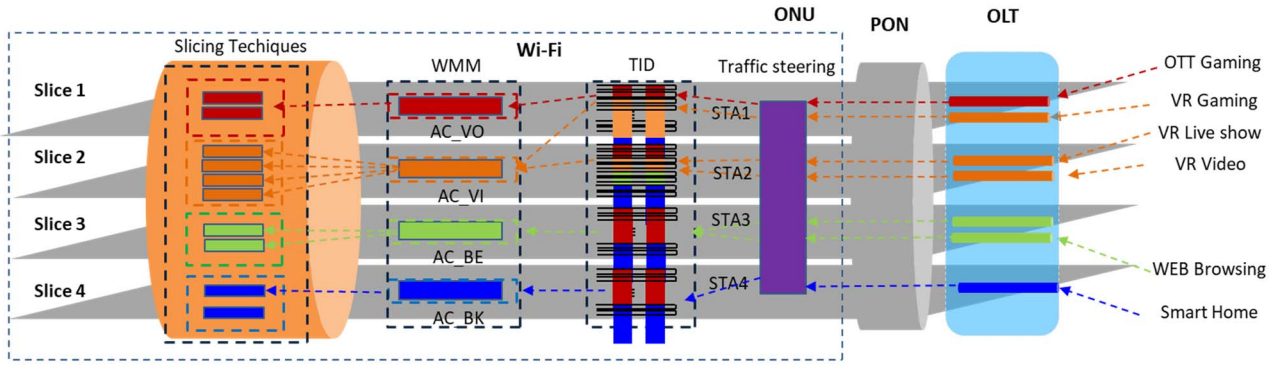
Since unlicensed spectrum are limited resources, especially for channel with large bandwidth (like 80 MHz, 160 MHz and 320 MHz). In these cases, the neighbouring AP are probably using the same channel (shown in the left picture in Figure 15). Therefore, collision due to a CSMA mechanism will significantly affect the spectrum efficiency. Avoiding collision could guarantee network stability (lower latency and lower network packet jitter), which is used to guarantee user experience.

The middle picture of Figure 15 shows an example of how collision takes place and how it affects the generation of additional transmission latency. Collisions create longer back-off duration. Currently, there is no coordination between multiple APs, each AP follow its own transmission decision (such as Enhanced Distributed Channel Access (EDCA) based mechanism). This is the reason why collisions occur. Therefore, a centralized controlled function is necessary in the P-ONU. Another reason mentioned above is the short time unit (9 µs). To dynamically coordinate the air interface, the process of dynamically collecting the network information, making the decision and informing each AP should be done within a short period of time.

It can be seen on the right-hand side of Figure 15, by following the coordination procedure, in which, the master AP should complete the whole estimation process and send the transmission decision to all of the AP in the network, before and AP sends a packet. All the AP will follow the command and the regulation of the air interface will be achieved.

5.4.1.8 Wi-Fi® Slicing

In F5G, many of the end-user devices in the network are connected to an ONU or Gateway through Wi-Fi®. Such Wi-Fi® links in the local area network are service-oriented. User traffic is classified with different traffic priority identified by a Traffic IDentifier (TID) for different service quality requirements. According to the TID, the traffic is mapped to Wi-Fi® Multimedia (WMM) queues, in which multiple slicing techniques can be applied to achieve Wi-Fi® slicing. To implement Wi-Fi® slicing, the Wi-Fi® air interface resource is divided into multiple groups and allocated to different users. These slicing techniques are for further study.



AC_VO voice
AC_VI video
AC_BE best effort
AC_BK background
STA station

Figure 16: Overview for Wi-Fi® Slicing

5.4.1.9 PON Slicing

5.4.1.9.1 Introduction

Aligned with the F5G E2E slicing concept, PON also supports user group-oriented slicing and service-oriented slicing. These two types of slicing may be combined in a PON Access Network. From the implementation perspective, the OLT node is comprised of PON, IP/Ethernet and OTN uplink. This clause will address the slicing of ONU and OLT nodes.

Figure 17 depicts an example of a combination of user group oriented slicing and service-oriented slicing. A specific user group uses a specific D-Net instance (D-Net1 and D-Net2). Figure 17 shows 2 D-Nets with different performance characteristics. The implementation of the differentiated performance characteristics is shown in the pipe symbols labelled D-Net1 (blue) and D-Net2 (green) in Figure 17. Each D-Net has two service oriented slices (slices 1 to 4). In each D-Net, there are multiple slices with different performance characteristics for different services. For example, in D-Net1, Slice 1 and Slice 2 represent two types of services and Slice 2 is shared by two users. Slice 2 and Slice 4 are two different slices but having the same service quality characteristics.

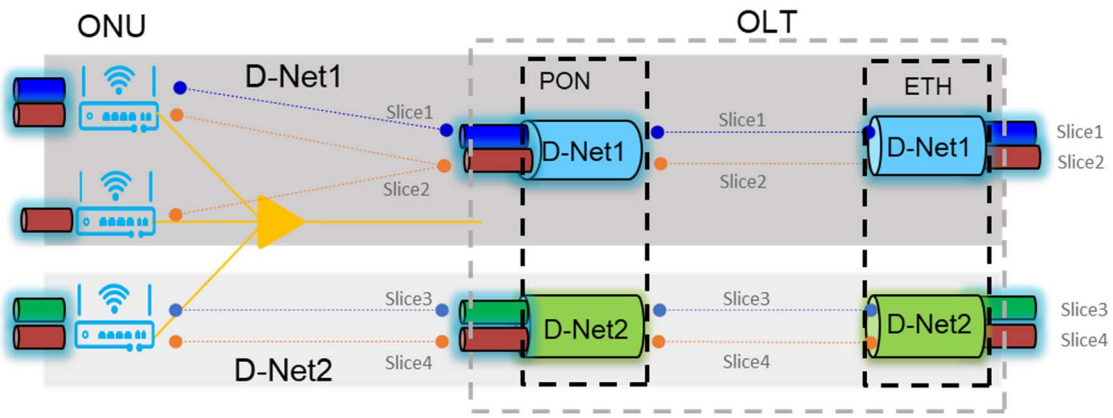


Figure 17: Overview for PON Slicing

5.4.1.9.2 User Group Oriented Slicing

In the context of PON, an ONU is part of a single user group, and therefore an ONU is part of a single D-Net instance. The user group shall be configured per ONU, and the uplink ports of an OLT shall be configured for all ONUs of the same user group.

On the PON port of the OLT, different user groups should perform bandwidth isolation. Each user group exclusively uses its own bandwidth. The OLT allocates the upstream bandwidth of all T-CONTs on a PON port in the same user group and isolates the upstream services of the user group. The OLT perform traffic shaping based on the user group of the user-side PON port to ensure bandwidth isolation.

When VLANs of multiple user groups are planned in the same scheme, the OLT should allow multiple user groups to share an uplink port. For different user groups, the OLT should be able to allocate bandwidth on the uplink port. Each user group exclusively uses its own bandwidth. The upstream port of the OLT supports traffic shaping for user groups to ensure bandwidth isolation.

The OLT shall have an independent forwarding domain for each user group. This requires that the forwarding entries of each user group are isolated, and VLANs can be reused across user groups. VLANs are planned independently for each user group.

Resource isolation between user groups includes:

- VLAN.
- ONU.
- Downstream bandwidth of the same OLT PON port.
- Queue resources of the same OLT PON port.

5.4.1.9.3 Service-Oriented Slicing

The service-oriented slicing on PON has finer granularity than the user group oriented slicing. Service-oriented slicing can be implemented per ONU, ONU LAN port or application Destination IP address. For upstream services, the OLT classifies service flows based on GEM port-IDs and VLANs and maps service flows to service-oriented slices. For downstream services, the service flows shall be classified and mapped to slices based on VLANs.

For service slicing, upstream bandwidth isolation is based on T-CONT time sequence on PON ports, and downstream bandwidth isolation is based on Hierarchical QoS (H-QoS).

Resource isolation between service slices includes:

- LAN port of the ONU.
- Downstream bandwidth of the same OLT PON port.
- Queue resources of the same OLT PON port.
- The upstream bandwidth of the ETH upstream ports on the OLT.

5.4.1.10 OTN Slicing

OTN is a TDM technology with no oversubscription or congestion issues, and client data is allocated to their container, and each container is exclusively allocated its bandwidth. By virtue of the fact that OTN is a TDM technology the OTN containers are totally isolated from each other. In OTN, lower-order containers are multiplexed into higher-order containers. For example, eight lower order ODU0 can be multiplexed into a higher ODU2, or ten lower-order ODU2 can be multiplexed into an ODU4. In general, a number of ODUj containers are multiplexed into an ODUk container where $j < k$ and $j,k = 0..4$. The ODU is the entity that is transported End-to-End. It may be de-multiplexed from ingress high order ODU and switched and multiplexed into a different high order ODU on the egress of an OTN cross-connects. So this hop by hop demuxing switching and muxing is the basic mechanism of OTN End-to-End path connectivity. The OTN management configures, monitors and tears down connections. The characteristics of the connection, such as bandwidth latency and End-to-End connectivity, are pre-configured by the OTN NMS.

In addition to an ODU container, ITU-T Study Group 15/Q11 [i.8] is developing an additional OTN container called OSU, which will support all client rates below 1 Gbit/s. In contrast, the ODU will support client rates above 1 Gbit/s. The OSU will be multiplexed into an ODU for transport through an OTN network. Same as ODU, OSU will be de-multiplexed switched and multiplexed again on a hop by hop basis. Depending on the capability of the cross-connect, it may only support ODU switching or may support both ODU and OSU switching. It depends on where the network switching is done.

So an OTN slice is an ODU/OSU with specific network characteristics matching the SLA. That ODU/OSU could be a single entity End-to-End, or it could be an ODU that consists of lower-order ODU and OSU with the same network characteristics requirement and destined for the same endpoint. As explained above, the higher-order ODU may change on a hop by hop basis, but the de-multiplexing, switching and muxing again are how the End-to-End path for a slice is formed. Also mentioned above, the OTN NMS determines the route taken through the OTN network and determines the characteristic of that route to form a slice instance matching the required SLA.

An OTN slice instance can originate in two locations in the Access Network. The first source of OTN slicing originates in the E-O-CPE, where client data is mapped into an OTN container such as an OSU. The VLAN tag and physical port are used to delineate the slice type. The user may join several different slice instances by allocating the appropriate traffic stream to the different OSUs/ODUs. These OSUs/ODUs are multiplexed into a higher-order ODUk and transported via an OTUk to/from the E-O-CPE to the edge cross-connect. These OSU/ODUs will be demultiplexed on the ingress of edge cross-connect, then switched to an egress line card and multiplexed into a different higher-order ODU and transported through the OTN Aggregation Network to the Aggregation edge, where they are either demapped back into client data most likely Ethernet and forwarded to the endpoint, or they may also remain as OTN and get forwarded to the far endpoint CPE for demapping. The second source of OTN slicing may originate in the PON network, where a VLAN tag delineates the slice type. In the OLT the SMP determines which fabric is used to transport the service through the Aggregation Network. In this case SMP directed this traffic to the OTN cross connect, where it is mapped into an OSU or ODU depending on the bandwidth requirements. Then it follows the same process as in the first case in that it is transported through the Aggregation Network. In this case, it may join an existing slice instance that matches its network requirements or start a new slice instance.

An important aspect of slicing is its ability to grow or contract depending on the bandwidth requirement of the slice. A slice member can be the originator of the slice formation or may join an existing slice with other members already present. In the latter case, there are two aspects to take into account. Firstly the ability to add a member to the slice by expanding the bandwidth of the slice without interfering or disturbing existing members, so there is a need for hitless slice expansion. The second is the ability to remove a member of the slice without interfering or disturbing existing members, so there is a need for slice bandwidth contraction when the member no longer needs the bandwidth, such as stopping playing a VR game or denial of service for non-payment of the service, or whatever reason. The bandwidth needs to be reduced to reduce waste and reduce the cost to the service provider. Again this bandwidth change needs to be done without interfering or disturbing existing members, so there is a need for hitless bandwidth reduction. OTN supports hitless bandwidth upgrades for both OSUs and ODUs, making it an ideal choice for slicing.

The example in Figure 18 illustrates OTN slicing. There are five different slices established in the figure, two for VR cloud services, a banking slice, a Data Centre slice, and connectivity to the core slice:

1) The banking slice: There are two separate bank branches labelled 1 and 2 requiring reliable and isolated connection to the headquarters. In bank branches 1, its local OTN CPE maps the client data into two OSUs, similarly in bank branches 2, its local OTN CPE maps the client data into two OSUs. The OSU from bank branches 1 and 2 are carried in an OTU0 to the edge cross-connect 2 and 1, respectively. In edge cross-connect node 2 bank branches 1 OSUs are muxed into an ODU0 and carried to node 4 via an OTU2, and in edge cross-connect node 1 bank branches 2 OSUs are muxed into an ODU0 which is carried to node 3 via an OTU2. Bank branches 1 OSUs are muxed into and ODU0 in node 4 and carried to node 6 via an OTU4, and bank branches 2 OSUs are muxed into, and ODU0 in node 3 and carried to node 6 via an OTU4. In node 6 the four OSUs are multiplexed into an ODU2 and carried to the edge cross-connect node 8 via an OTU2, and there they are multiplexed into an ODU2 and transported to the headquarters CPE in an OTU2.

2) Cloud VR slice: There are four home broadband users, and two sets of two share the same OLT. On the top of the diagram, the users are labelled Cloud VR 1 (orange) and 2 (grey), while at the bottom are labelled again labelled Cloud VR 1 (green) and 2 (purple). Green and orange users are associated with the VR rendering 1, while purple and grey are associated with VR rendering 2. Cloud rendering 1 slice formation is described here, but the same principle applies to Cloud rendering 2 slices. Cloud VR 1 (orange) is attached to OLT1, while Cloud VR 1 (green) is attached to OLT2. OLT 1 and 2 redirect Cloud VR 1 (orange) and Cloud VR 1 (green) to edge cross-connect 1 and 2, respectively, where Cloud VR 1 (orange) is mapped into the orange OSU and Cloud VR 1 (green) is mapped into the green OSU. The orange OSU is multiplexed into an ODU0 and carried via an OTU2 to node 3, while the green OSU is multiplexed into an ODU0 and carried via an OTU2 to node 4. The orange OSU is multiplexed into an ODU0 and carried via an OTU4 to node 6, while the green OSU is multiplexed into an ODU0 and carried via an OTU4 to node 6. In node 6, the orange and green OSUs are multiplexed together into an ODU0 and carried to node 8 via an OTU2. In node 8, the orange and green OSUs are terminated and demapped, and the user data is transferred to the VR rendering gateway 1 via Ethernet.

3) Enterprise data centre and enterprise core network slides: The enterprise data centre slice formation is described here. The same principle applies to enterprise core network slices. There are two enterprise locations again labelled 1 and 2. They may be the same company in different locations. So like the bank case, the two enterprise entities use an OTN CPE. Enterprise 1 (E1) data is mapped into a brown OSU, while Enterprise 2(E2) data is mapped into a yellow OSU. E1's OSU (brown) is carried to the edge cross-connect node 2 in an OTU0, and E2's OSU (yellow) is carried to the edge cross-connect node 1 in an OTU0. In edge cross-connect node 2, E1 OSU (brown) is multiplexed into an ODU0 and carried to node 4 via an OTU2. In edge cross-connect node 1, E2 OSU (yellow) is multiplexed into an ODU0 and carried to node 3 via an OTU2. In node 3, E2 OSU (yellow) is multiplexed into an ODU0 and carried to node 5 via an OTU4. In node 4, E1 OSU (brown) is multiplexed into an ODU0 and carried to node 5 via an OTU4. In node 5 E1, and E2 OSUs are multiplexed into the same ODU0 and carried to node 7 via an OTU2. In node 7, the brown and yellow OSUs are terminated and demapped into Ethernet and forwarded to the DC-GW.

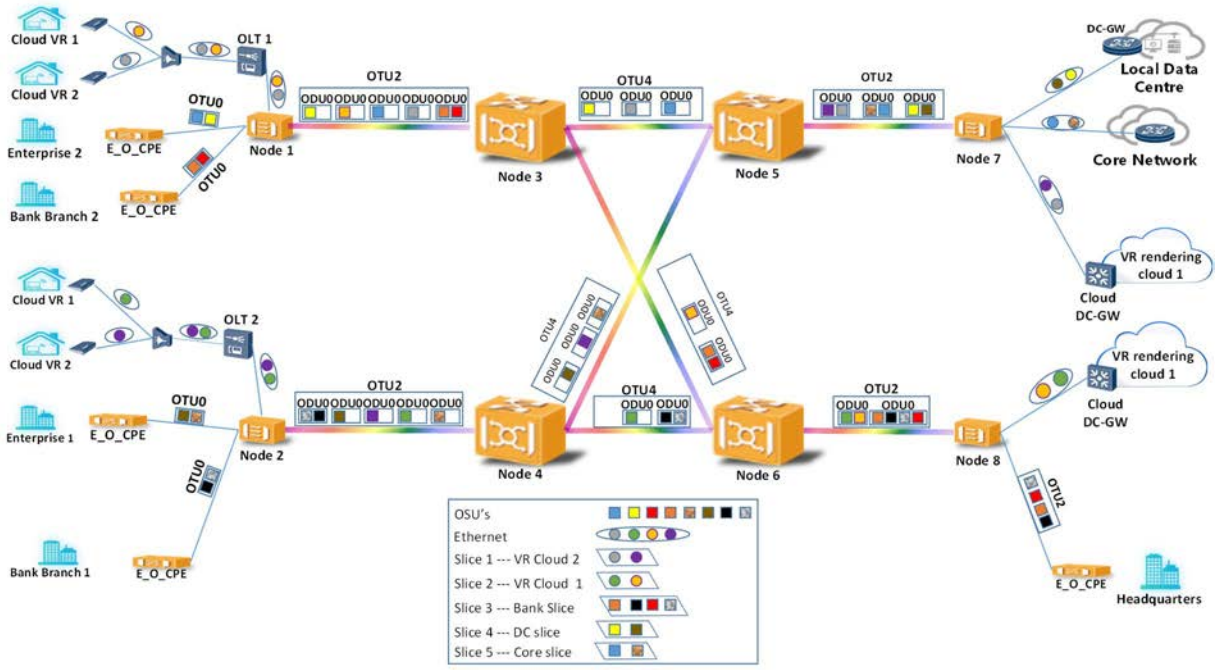


Figure 18: An example illustrating different OTN slices

5.4.1.11 IP AggN Slicing

In the present clause, the F5G application area for IP networking is the aggregation network segment implemented by an IP fabric. The SMP on the access network directs traffic to the IP fabric, which needs to support F5G end-to-end slicing.

IETF is currently working on network slicing for IETF networks, which are mainly IP networks. For example the IETF network slicing framework is currently under study by draft-ietf-teas-ietf-network-slices [i.5]. Meanwhile, there are several on-going activities in IETF to study how to implement slicing in IP network, for example draft-ietf-teas-enhanced-vpn [i.9] and draft-ietf-teas-ns-ip-mpls [i.10].

Today's IP Networks are evolving and adopting IPv6 technology. IPv6 continues to evolve to meet the new requirements such as end-to-end Network Slicing (see ETSI GR IPE 005 [i.11]).

IP AggN Slicing is defined to meet the connectivity and performance requirements of different end-to-end services running over a shared AggN IP fabric. An IP network slice may span multiple IP network domains.

As mentioned, the IETF is working on enhanced VPNs [i.9] as a solution for IP network slicing. The purpose is to support the needs for new applications by utilizing an approach that is based on existing VPN and Traffic Engineering (TE) technologies and adds characteristics that specific services require beyond those provided by traditional VPNs.

The requirements of an Enhanced VPN service over the IP fabric are:

- Performance Guarantees.
- Isolation between different Enhanced VPN connections.
- Dynamic Changes, VPNs need to be created, modified, and removed from the network according to service demands.
- Customized Control and Management of the IP fabric.

There are several candidate data plane technologies that provide the required IP isolation and guarantees, and they are:

- Deterministic Networking: Deterministic Networking (DetNet), described in IETF RFC 8655 [i.12], is a technique developed in the IETF to enhance the ability of Layer-3 networks to deliver packets more reliably and with greater control over the delay.

- MPLS Traffic Engineering (MPLS-TE): MPLS-TE, described in IETF RFC 2702 [i.13] and IETF RFC 3209 [i.14], introduces the concept of reserving end-to-end bandwidth for a TE-LSP, which can be used to provide a point-to-point Virtual Transport Path (VTP) across the underlay network to support VPNs.

- Segment Routing: Segment Routing (SR), described in IETF RFC 8402 [5], is a method that prepends instructions to packets at the head-end of a path. These instructions specify the nodes and links to be traversed and allow the packets to be routed on paths other than the shortest path. With SR, it is possible to introduce such fine-grained packet steering by specifying the queues and resources through an SR instruction list. With Segment Routing, the SR instruction list could be used to build a point-to-point path, and a group of SR SIDs (Segment Identifier) could also be used to represent a P2MP or MP2MP network. Thus, the SR based mechanism could be used to provide both a Virtual Transport Path (VTP) and a Virtual Transport Network (VTN) for enhanced VPN services.

Segment Routing is the preferred technology for implementing slicing in the aggregation network. Indeed, SR enables easy end-to-end per-flow SR policies, allows fine granularity, introduces scalability properties as it reduces the amount of state information and supports services like Traffic Engineering and Virtual Private Networks.

For Segment Routing, it is possible to define the resource-aware SIDs (draft-ietf-spring-resource-aware-segments [i.15]) that retain their original forwarding semantics, but with the additional semantics to identify the set of network resources available for the packet processing action. The resource-aware SIDs can therefore be used to build SR paths or virtual networks with a set of reserved network resources. The proposed mechanism is applicable to both segment routing with MPLS data plane (SR-MPLS) and segment routing with IPv6 data plane (SRv6).

SRv6 takes advantage of the native end-to-end IPv6 connectivity and introduces the network programmability (IETF RFC 8986 [6]), enabling Service Function Chaining. This function is specifically for the transport of traffic to different Service Processing Points (SPP). Additional details can be found in ETSI GR IPE 005 [i.11] that reports the main SRv6 concepts.

5.4.2 Traffic Steering

5.4.2.1 Overview

From the network layer perspective, the traffic of different tenants is distinguished by some labels in the service flows. The most commonly used label is a VLAN tag, where different tenants may have different VLAN tags or can use the same VLAN tags in case of deterministic networks which are fully isolated. The Service Mapping Point (SMP), typically located in the Access Node, needs to map the traffic with a given label to the bearer connection matching the service requirements. In the network, the traffic is processed based on forwarding rules including QoS processing. For example, a video enthusiast tenant focuses on the bandwidth, latency and packet loss rate of the service links and a production enterprise tenants focuses on link latency, reliability and isolation for privacy.

Nodes connecting to the Service Access Point (SAP) need to be capable of identifying available slice types and marking the traffic with the appropriate label such that the SMP can appropriately divert the traffic to the network slice instance that matches the deterministic network requirements. In addition, the traffic needs to be identified and authenticated to be allowed to use a particular service characteristic or service class.

The control and management system authenticates and authorizes the access to an end-to-end slice instance and configures the traffic mapping function to the appropriate network slice instance. The automated mapping function is for further study.

5.4.2.2 Traffic Steering Architecture

5.4.2.2.1 High-level Framework

In the present clause, the focus is on the traffic steering functionalities. However, traffic steering has a relationship with and interacts with other functions.

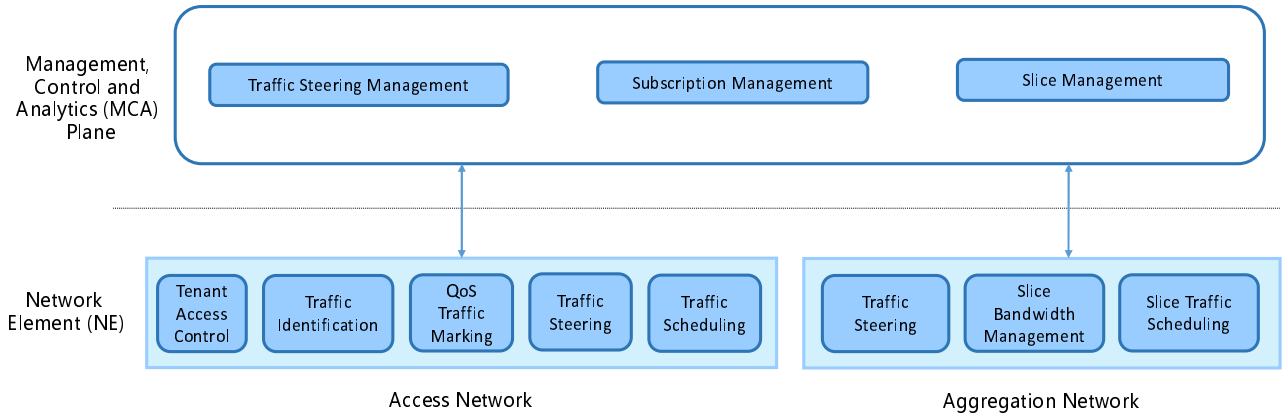


Figure 19: Traffic Steering Functional Overview

Figure 19 shows the functions related to traffic steering in the F5G architecture. Traffic steering consists of two parts: First, the Management, Control and Analytics (MCA) plane, which consists of traffic steering related functions, which interact with each other and with domain-specific MCA functions. Second, the Network Elements (NEs) are sub-divided into functions in the Access Network domain and the Aggregation Network domain. In the Access and the Aggregation Network Elements (NEs), there are functionalities associated with the Underlay Plane and other functionalities associated with the Service Plane. The functions are described in the following clauses.

5.4.2.2.2 Management Control and Analytics (MCA) functions

The MCA functions are integrated into management, control and analytics systems and further specified in the E2E Management document, ETSI GS F5G 006 [20]. The details on what management components have what function are for further study. The management has both technical and business aspects. For example, the MCA uses intent-based and autonomous management. The separation of functionality into different management systems is for further study.

- Traffic Steering Management:
  - Various functions are needed to manage traffic steering. The decisions to be made are based on the tenant, the slice instance, the operator's policies, and the terminating SPP at the AggN edge instance. The traffic steering management function maintains the data for the mapping of such traffic, as well as the requested capabilities. It also interacts with the slice management function in the case of slice update requests or optimizations, and it may expose an interface to other entities being involved in traffic steering decisions. Additionally, it interacts with the subscription management function in terms of authorization, service subscriptions, charging such that relevant actions can be taken.
  - The configuration of network elements for traffic steering is static. The assumption is that the decisions on what traffic is steered to what location over what underlay fabric is static and depend on operator policies and network design choices. Dynamic versions of traffic steering are for further study.
- Subscription Management:
  - The subscription management function manages all the functions associated with the subscriptions of tenants and users. It is used in the authentication and authorization processes of tenants and users. It also contains information about service level, slice type, service characteristics, which a tenant is using or is allowed to use and charging functionality for the tenant or the service user. Finally, the subscription management function handles the business and policy aspects of service requests and is responsible for issuing the resource policies.
- Slice Management:
  - The slice management function consists of the slice template design and rollout functionality, the slice types offered by the operator at a particular location. It manages the entire lifecycle of the slice instances, including the creation, monitoring, optimization, adaptation, and release of slice instances. The decision is based on the tenant's service characteristic requirements, the operator policies, and the availability of networking resources. The decision about whether a slice is needed is an operator decision.

5.4.2.2.3 Access Network Element Based Functions

- Tenant Access Control:
  - A tenant or user needs to get authorization to access a network service, which means the tenant or user and its devices need to be authenticated. Additionally the tenant needs to get authorization to use a particular service. In the case of a first-time connection of a tenant or its devices (CPEs, terminals, etc.) to the network and/or service, the authorization needs to be checked. There are cases where the tenant access control function needs to react when triggered by the first packet received indicating a new connection. In the case of dynamic service requests, the tenant access control function may receive access requests to the network service. In the static case, an a priori configuration is needed.
  - Additional information used in the interaction with the subscription management component and traffic steering management component are elements such as Line-ID, and other logical access information, such as VLAN ID, GEM Port ID, ONU Serial Number, CPE MAC address, IP addresses or IP 5-tuples, etc.
  - There are several possible scenarios, which eventually need different authentication mechanisms and different security measures depending on the service to be accessed.

NOTE 1: The security aspects are not addresses here and are for further study.

- Traffic Identification:
  - When a tenant is authorized, the tenant's traffic needs to be identified in order for the traffic to be handled according to the service characteristics specified. The identification policies for Access Nodes could, for example, be based on tenant VLAN IDs or tenant IP addresses.
  - The information used for identification may be elements such as Line-ID, or other logical Access Network information, such as VLAN ID, GEM Port ID, ONU Serial Number, CPE MAC address, IP addresses, IP 5-tuples, etc.

NOTE 2: There are scenarios and use cases, where traffic identification is based on application identification. This is for further study.

- QoS Traffic Marking:
  - The QoS Traffic Marking function marks the incoming traffic according to the specific traffic policies and rules such that it can be handled in the processing stage. In case the marking is needed for QoS, the marking needs to be transported across interface boundaries, which means protocol support for it is required. Typically protocol fields for that function are the Ethernet priority field or IP TOS/DSCP for QoS oriented marking.
- Traffic Steering:
  - The traffic steering function steers the traffic towards the appropriate underlay technology. That is the main function of the Service Mapping Point (SMP). Either the function steers the traffic to the appropriate bearer connection for the traffic with specific characteristics, or it sends the traffic over the appropriate fabric without bearer connections being used. The decisions depend on the service requested or the tenant subscription.
- Traffic Scheduling:
  - Depending on the configuration and dimensioning of the underlay networking technology, traffic from different tenants or different slices can be merged into the same bearer connection, in which cases traffic scheduling is needed to manage the congestion cases.

5.4.2.2.4 Aggregation Network Element Based Functions

- Traffic Steering:
  - The traffic steering function steers the traffic towards the appropriate underlay technology. That is the main function of the Service Mapping Point (SMP). Either the function steers the traffic to the appropriate bearer connection for the traffic with specific characteristics, or it sends the traffic over the appropriate fabric without bearer connections being used. The decisions depend on the service requested or the tenant subscription.
- Slice Bandwidth Management:
  - Depending on the traffic carried in the slice, the slice bandwidth might need to be adjusted to satisfy the requirements of the traffic in a particular slice.
- Slice Traffic Scheduling:
  - In cases where non-deterministic underlay technologies like packet-based technologies is used, each node in the Underlay Plane needs to schedule the traffic according to its required service level.

5.4.2.3 Example for Traffic Steering

Figure 20 shows an example of traffic steering, and it is shown in the context of an overall F5G architecture. The example uses the concepts described above and simplifies many aspects, which are further detailed in other sections. Several tenants are accessing network services that require different service characteristics. The figure shows the logical Service Plane connection in dashed lines. Figure 20 shows 4 different service examples, a best effort service, a better than best-effort service, a guaranteed service and a premium service.

The traffic is transported in the Underlay Plane, chosen based on the tenant and the particular service characteristics. In the Underlay Plane, the traffic is either sent over a bearer connection to guarantee appropriate service characteristics, or the technology can be used natively without any guarantees (for example, using native IP).

NOTE 1: The SAP, SPP and SMP are concepts and processes, which are independent of the underlay technology used.

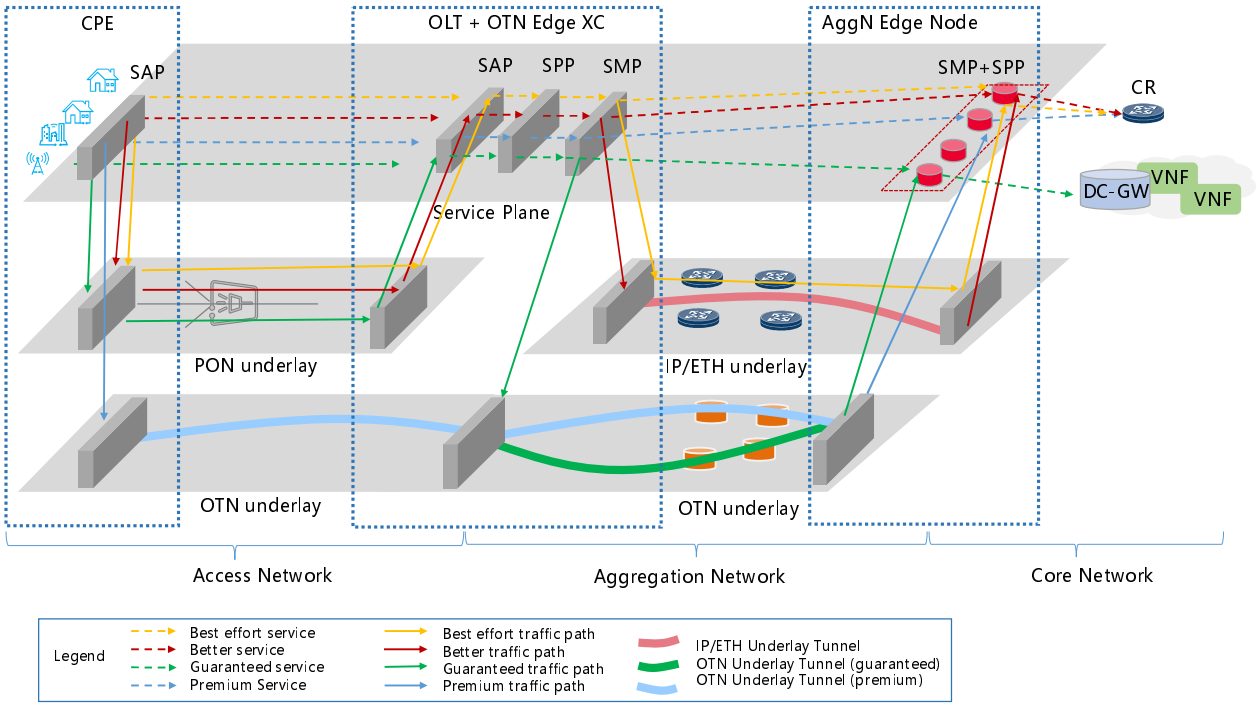


Figure 20: Example Traffic Steering Scenarios

The slice management function creates a bearer connection in the appropriate underlay fabric. Those bearer connections are statically pre-configured. The decision is based on the operator's service class, slice type definitions and network service offered. In Figure 20, there is one bearer connection in the IP/Ethernet underlay fabric, and two bearer connections in the OTN underlay fabric, all of which have been pre-configured.

"Best effort service" (yellow in Figure 20) is using the PON underlay to transport the traffic in the Access Network. The Aggregation Network transports the traffic to the Aggregation Network Edge using best effort. The yellow arrow shown in the IP/Ethernet underlay is for this case where no bearer connection and no guarantees are needed, and the underlay technology is used natively.

"Better service" (red in Figure 20) uses PON with higher quality in the underlay and is steered by the SMP to a bearer connection with higher quality characteristics in the SRv6/IP/ETH network.

"Guaranteed service" (green in Figure 20) uses PON as underlay with guaranteed service characteristics. The SMP steers this traffic to an OTN-based path in the underlay, which has pre-configured guaranteed characteristics.

"Premium service" (blue in Figure 20) uses OTN in the underlay and is transported based on the pre-configured path with guarantees through the OTN Access and Aggregation networks.

NOTE 2: This example shows a static, a priori configuration of bearer connections in the underlay. More dynamic cases are for further study.

NOTE 3: Depending on the scenario in the CPN, there might be some traffic steering functionalities being involved before traffic is mapped to the PON underlay or OTN based underlay network to be handled according to the service characteristics requested.

A tenant requesting service access from the network connects to the Service Access Point (SAP), which handles the entire access authentication, and interacts with the subscription management for authorization of that access. The Service Processing Point (SPP) handles traffic, for example, QoS marking. The Service Mapping Point (SMP) function steers the traffic to the appropriate underlay fabric and the right bearer connections.

The traffic is transported in the Underlay Plane to the right location, where it is forwarded to the SPP/SMP at the Aggregation Network Edge for further handling. The SPP in the Aggregation Network Edge is making further decisions on what traffic handling is required and SMP steers the traffic towards the core network (shown as Core Router (CR)) or towards the local Data Centre for accessing special compute intense services.

NOTE 4: The assumption in these examples is that the traffic is steered to the SPP/SMP at the Aggregation Network Edge to be further processed. SPP/SMP at the Aggregation Network Edge needs to be known in advance for setting up the bearer connections appropriately.

NOTE 5: The opposite direction is not shown in these examples, but the mechanisms needed are similar.

NOTE 6: These examples require a set of management interactions and processes. These management interactions and processes are not shown for simplicity reasons.

5.4.3 Separation of Services Plane and Underlay Plane

5.4.3.1 Introduction

5.4.3.1.1 Purpose of service and network separation

- Reduces the network specifications required by a large number of service connections:
  - Fabric nodes are unaware of services and provide only large-granularity device-to-device bearer connections. (If stateless bearer connections are used, fabric nodes do not need to know the bearer connection specification.)
- New business agility:
  - Services are only processed on Access Node and Aggregation Edge. The coupling between the networks and the services are reduced.

- Elastic scaling of the Aggregation Network:
  - The entire Aggregation Network is similar to a group of distributed switching nodes. The fabric part functions as a switching network and provides only large-capacity interconnection switching without service processing. Additional nodes can be added to establish a new fabric or to expand the capacity of additional nodes added to established fabrics.
- On-demand service selection and flexibility:
  - Services are configured only on edge nodes and are mapped to preconfigured underlay bearer connections based on SLA requirements.

5.4.3.1.2 Implementation of separation between service and network

In F5G architecture, the data plane is comprised of a Service Plane and an Underlay Plane, where the service identification and processing are separated from network traffic forwarding and routing. Traffic is distinguished on the Service Plane by application type, SLA, etc. The services are processed in the Service Plane and may be mapped to bearer connections in the Underlay network according to SLA. The Underlay Plane is comprised of bearer connections with different SLAs.

VLAN and EVPN [7] shall be used for the connection on the Service Plane. SRv6 shall be used as the bearer connection on the IP/Ethernet fabric Underlay Plane, while for the OTN fabric, OSU [i.8]/ODUk [2] shall be used as the bearer connection on the Underlay Plane.

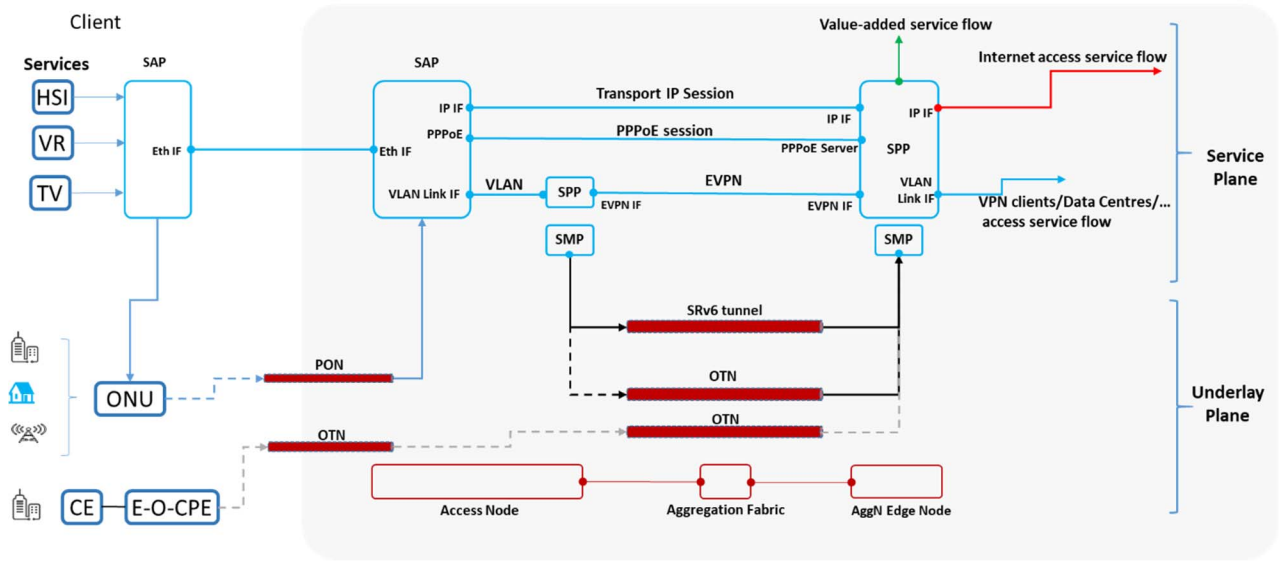


Figure 21: Example of Service-Network Separation for F5G

Figure 21 is an example of traffic forwarding from the user through the Service Plane to the Underlay Plane. There are two preconfigured bearer connection types shown, one in the IP/Ethernet fabric and the other in the OTN Fabric. These bearer connections are configured and maintained by the management and control system. The Service Mapping Process (SMP) directs the traffic flows to the appropriate bearer connection according to the Service Process Point (SPP) steering guidance. These are the black coloured flows in Figure 21. Not all traffic is directed to the preconfigured bearer connection. Only traffic that requires specific SLA is directed to corresponding bearer connections. Other traffic will traverse the Aggregation Network as normal IP/Ethernet or OTN traffic in the Underlay Plane. These are the blue coloured flows in the IP/Ethernet fabric and the grey coloured flows in the OTN Fabric in Figure 21.

5.4.3.2 The Underlay Plane

5.4.3.2.1 Introduction

The choice of technologies for the Underlay Plane will directly affects the quality of service in the Service Plane above. To ensure the quality and security of services carried on the Underlay Plane, the following aspects shall be considered:

1) Powerful service capabilities and smooth evolution capability:

   - SLA requirements of various services need to be met, and strong service evolution and expansion capabilities need to be provided to maximize investment protection on the live network.

2) Network slicing:

   - In F5G various services have different requirements on the networks. E2E network slicing is required to ensure differentiated service quality. One network carries traffic from a wide range of different industries. Many new industries require network slicing to isolate internal services from each other. This reduces the impact of new services on the entire network and minimizes trial and error.

3) High reliability:

   - Provides comprehensive node-level and network-level fault detection, redundancy protection, restoration, and fault self-healing mechanisms.

4) Data security:

   - This feature ensures the reliability, integrity, and confidentiality of services carried on the Underlay Plane.

5) Operable and manageable:

   - Provides comprehensive fault localization, isolation and troubleshooting functions, which provide the basis for routine network maintenance & management and network optimization. The simplified Underlay Plane protocol greatly improves network operation and management efficiency.

   - The Underlay Plane has two technology approaches:

     a) Packet switching, such as IP/SRv6/Multiprotocol Label Switching (MPLS); and

     b) TDM switching such as Optical Transport Network (OTN).

The statistical multiplexing capability of packet switching matches the traffic characteristics of data services to achieve high network utilization. The TDM switching technology features reliable transport and bearing capabilities, flexible add/drop multiplexing, powerful protection and restoration functions, and carrier-level maintenance and management capabilities. The TDM switching technology guarantees timing transparency, which is unavailable in packet switching. The two technical approaches collaborate during the evolution process and together form a reliable, flexible infrastructure for the F5G Underlay Plane network.

The Underlay Plane is fundamentally a physical network plane comprised of physical network nodes. The Underlay Plane provides connections and dynamically configurable paths under the control of the F5G controller in the MCA Plane. The network switching capacity shall be scalable without interfering with the Service Plane.

As shown in Figure 22, the Underlay Plane has four segments, the Customer Premises Network (CPN), the Access Network (AN), the Aggregation Network and the Core Network. In the CPN segment, various technologies are used, which will depend on the user and their functional requirements. For example, the Home Access, Wi-Fi® 6 and FTTR can be introduced as new technologies, while SME type Enterprise Access can benefit from POL to gain easy deployment and high bandwidth. For private line Enterprise Access, OTN can be deployed for customers requiring high-quality VPN services. The Access Network segment is mainly composed of the ODN and the OLT. The ODN shall be based on XGS-PON technology and point to point OTN connections for high-quality VPN services. The OLT will be the access termination point for PON and the traffic steering entity that directs traffic towards the aggregation segment. The other entity in the Access Network is the MS-OTN function which terminates the point to point OTN traffic for the high-quality private line Enterprise connections. It can also provide high-quality connections in the OTN aggregation network for customers accessed via PON, for example, VR Cloud services. Traffic from the PON infrastructure may be steered by the OLT to the IP/Ethernet fabric or to the OTN fabric, depending on customer types and services delivered. The Aggregation Network segment comprises two parallel fabrics, an IP/Ethernet fabric and an OTN fabric. The IP/Ethernet fabric comprises spine switches that may be interconnected via Ethernet links. The OTN fabric is comprised of OTN nodes, which perform ODUk/OSU switching on a hop by hop bases. For actual IP/Ethernet and OTN fabric deployment, there could be multiple physical fabrics of the same type co-existing in one network. Both fabrics have an Aggregation Network Edge as the handover point to the Core Network segment. The Aggregation Network Edge is comprised of routers, and OTN nodes that are co-located. There might be multiple bearer connections between Access Network and Aggregation Network Edge, which go over either the IP/Ethernet fabric or the OTN fabric. There may be multiple paths through different nodes for differentiated SLA bearer connection instances in one fabric. Typically, there is only one bearer connection instance for a certain SLA level.

The Underlay plane shall support an End-to-End slicing with different characteristics supporting different SLAs over either the IP/Ethernet fabric or the OTN fabric. The Underlay plane is unaware of the SLA but only focuses on the physical connectivity. The fabrics only provide large-capacity switching without service processing. The path of the traffic is configured by the Aggregation Network management.

The user data traffic is carried by Ethernet frames and transported to the access equipment either by PON or via OTN encapsulation. The access equipment identifies the route to take either via an IP/Ethernet fabric or an OTN fabric.

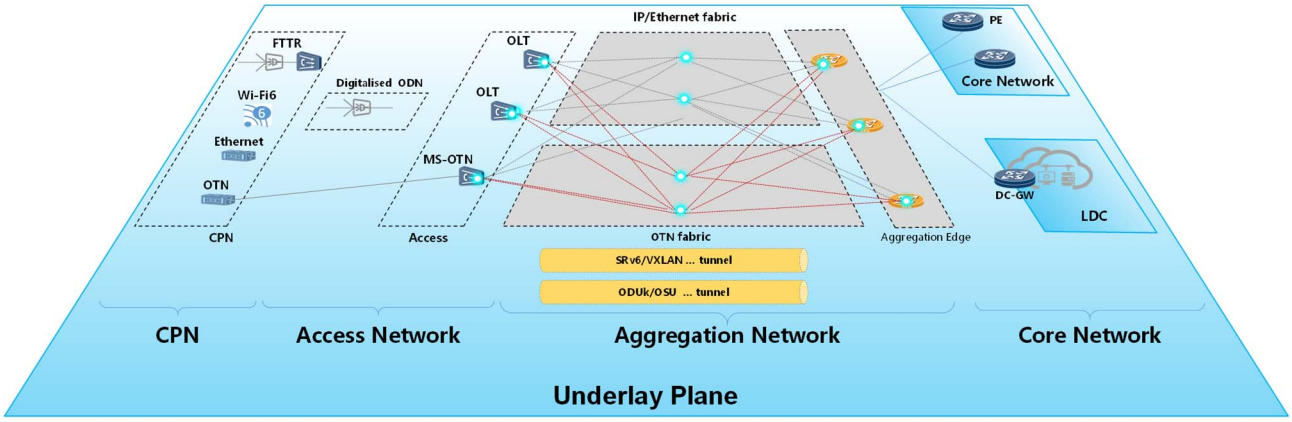


Figure 22: The functional blocks of the Underlay plane for F5G

5.4.3.2.2 Bearer Technologies

- PON Technology Analysis:
  - PON is a Point-to-MultiPoint (P2MP) single-fibre bidirectional optical access network technology. The PON system consists of the Optical Line Terminal (OLT), Optical Distribution Network (ODN) and user-side Optical Network Unit (ONU). In the downstream direction (from the OLT to the ONU), the signals, which are sent by the OLT, reach each ONU through the ODN. In the upstream direction (from the ONU to the OLT), the signals sent by the ONU only reach the OLT but do not reach other ONUs. To avoid data conflicts and improve network efficiency, the TDMA multiple access mode is used in the upstream direction, and data transmission of each ONU is managed. The ODN provides optical channels between the OLT and the ONU.

Figure 23: The PON stack

- OTN Technical Analysis:

  - The OTN technology migrates the powerful OAM&P concept and functions of SDH to the WDM optical network, which effectively makes up for the shortcomings of the existing WDM system in terms of performance monitoring and maintenance management. OTN technology supports the transparent transmission of client signals, high-bandwidth multiplexing, switching, configuration, powerful overhead support, and powerful OAM functions. Supports multi-layer nested Tandem Connection Monitoring (TCM) and Forward Error Correction (FEC) support. Currently, the OTN technology standardization is developing a small-granularity OTN technology, which can flexibly carry multiple small-granularity bandwidth signals, further expanding the OTN technology's application space.

Figure 24: The OTN stack

- Ethernet Technical Analysis:

  - The Ethernet concept was first proposed by Xerox Corporation in 1972 and gradually improved based on Carrier Sense Multiple Access/Collision Detection (CSMA/CD) technology. Since the 1980s, Ethernet has been developed in compliance with the standard architecture defined by IEEE 802.3.1 [18]. It has been driven by industry technologies and service requirements. Ethernet has become the most widely used L2 interconnection technology and the most complete ecosystem in the IT industry.

  - With the wide application of the Ethernet interface technology, the carrier Ethernet technology of the MAN and WAN has been developed and improved since the 2000s. Carrier Ethernet is developed by organizations such as the MEF and IEEE to meet the requirements of carrier networks for high reliability, operation, and maintenance. Carrier Ethernet provides carrier-class functions such as OAM, protection switching, high-performance clock, and QoS/QoE assurance. It is widely used in MAN, WAN, mobile bearer networks, and leased line access scenarios.

Figure 25: The Ethernet stack

- IP Technology Analysis:
  - Legacy MPLS technologies face the following challenges:
    1) Tunnelling protocols, including extensions for traffic engineering like Resource Reservation Protocol-Traffic Engineering (RSVP-TE) and Label Distribution Protocol (LDP), become more and more complex with increasing functions.
    2) The MPLS forwarding plane is designed based on specific entries, which are inflexible and difficult to expand.
    3) In a connection-oriented tunnel, each node in a network needs to maintain a status of a TE tunnel and an LSP (Link State Protocol) tunnel. This limits the number of tunnels on the entire network.

With the development of SDN, traditional MPLS technologies cannot meet the requirements for a more agile network, and therefore SR (Segment Routing) has been developed. SR enables smarter network edges and simpler cores, simplifying network design and management.

SRv6 protocol is designed based on source routing to forward IPv6 packets on a network. SRv6 adds a Segment Routing Header (SRH) to an IPv6 packet and adds an explicit IPv6 address stack to the SRH. In addition, the intermediate node continuously updates the destination address and offset address stack to complete hop-by-hop forwarding. QoS capabilities in SRv6 are provided by the well-known IP QoS management mechanisms.

SRv6 has the following benefits:

1) SRv6 is compatible with IPv6 routing and forwarding. It is easier to connect different network domains based on IP reachability and requires no extra signalling or network-wide upgrade as MPLS does.
2) SRv6 supports more types of encapsulation based on SRH, which can meet new diverse service requirements.
3) The synergy between SRv6 and IPv6 enables SRv6 to seamlessly integrate IP networks with IPv6-capable applications, bringing more potential value-added services to carriers through network awareness.

Simplified networking, integrated access, and programmability are the main development directions of the Underlay Plane. SRv6 can be used to implement differentiated bearer connections of multiple services in a simpler and more agile manner.

5.4.3.2.3 Summary and Analyses

Currently, the aggregation network is constructed based on the IP/Ethernet technology in many deployments. It mainly provides best-effort bearer connections, which have a set of QoS capabilities. The F5G aggregation network needs to provide differentiated bearer connection capabilities. It shall provide both high-quality bearer connections with committed bandwidth and latency and best-effort low-cost bearer connections.

For the F5G differentiated end-to-end services, a proper combination of IP/Ethernet bearer connection capability, high-quality fine-granular enhanced OTN hard pipe connection capabilities and enhancements of widely deployed PON access is essential.

5.4.3.3 The Service Plane

5.4.3.3.1 Introduction

The Service Plane provides connectivity for users' network services. It is where applications are identified, and network services are provided through specific processing and forwarding. Network services are Service Plane connections for user traffic, e.g. VoIP or IPTV connections for a certain user. The Service Plane is a logical plane running on top of the Underlay Plane. The Service Plane shall use Ethernet Virtual Private Network (EVPN) IETF RFC 7209 [7] and IETF RFC 8584 [8] for service connectivity. EVPN is regarded as an all-in-one VPN technology, which can simplify the network and greatly improve operational efficiency. By using a unified connection technology, the Service Plane traffic can easily be carried over an IP/Ethernet or an OTN fabric in the Underlay Plane.

The Service Plane functions are comprised of SAP, SPP and SMP. As depicted in Figure 26, these functional modules only reside on selected locations and nodes.

NOTE: The locations and nodes implementing those functions are flexible from an architectural perspective.

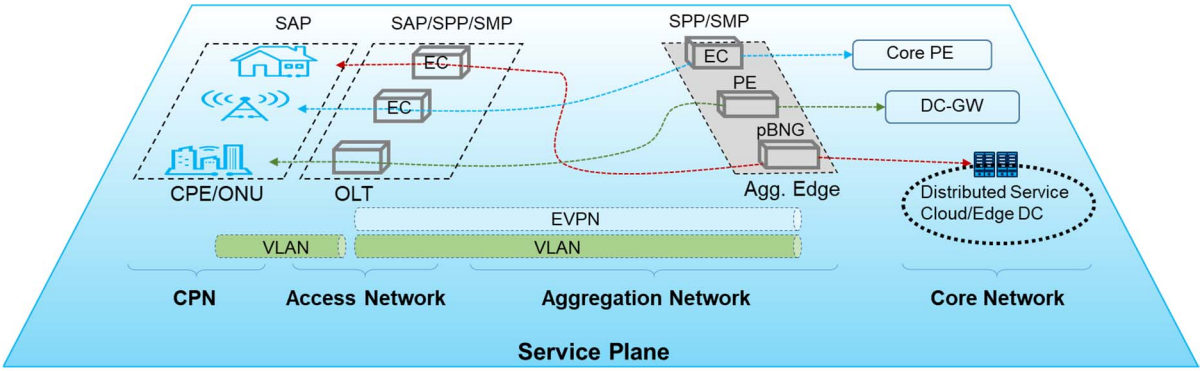


Figure 26: Functional blocks on the Service Plane for F5G

The SAP is the access point that identifies the user's application traffic and provides access to the operator's network. Typically, the SAP is located on the ONU/CPE/HGW or the OLT. Functionally, the SAP includes VLAN tagging for ingress and egress traffic, L2/L3 forwarding, QoS processing, and egress packet encapsulation, etc. On the OLT, another SAP might be used to identify scenarios, the application type and if an application is online/offline. This provides the necessary information for the SPP and SMP. The OLT has the functionality for identifying ONUs and verifying their subscription.

SPP is the point where service-specific processing of traffic is performed. Service processing refers to service tunnel identification for ingress traffic, L2-L7 traffic processing, including VLAN encapsulation conversion, PPPoE termination, L2 wholesale Gateway, virtual Firewall, egress encapsulation, etc. Based on the performance requirements, SPP typically resides on the OLT and/or the Aggregation Network Edge.

SMP is the point where service traffic is mapped into bearer connections on the Underlay Plane. Typical functions of SMP includes ingress service tunnel indication, QoS processing, service layer encapsulation, bearer connection selection and mapping, etc. SMP locates in the OLT and the Aggregation Network Edge. To map the traffic to the correct bearer connections on the Underlay Plane, SMP needs to have the bearer connection information for these bearer connections even though they are on the Underlay Plane. This information is provided and configured by the controller in the MCA plane. Also, in some scenarios, the SMP might be located in the CPE, specifically in the cases where OTN technology is used in the CPE, because it is there that the customer traffic needs to be mapped to the appropriate OTN bearer connections.

5.4.3.3.2 Traffic encapsulation for the Service Plane

Depending on the service, various encapsulation can be used for the Service Plane traffic. For example, the residential customer's traffic is indicated by S+C VLAN tags, which is encapsulated by SPP on the OLT and decapsulated by SPP on the BNG. For services like private line and mobile backhaul, a single VLAN tag is used from the CPE, and it is additionally encapsulated by OLT SPP and de-encapsulated by SPP on the PE of Aggregation Network Edge.

5.4.3.3.3 Signalling for the Service Plane

Multiprotocol BGP (MP-BGP) [9] is the signalling technology used for the Service Plane traffic carried by the IP/Ethernet Underlay Plane.

EVPN uses MP-BGP to carry IP/Ethernet routing control plane messages. It learns the local MAC/IP addresses and routes from the access side, learns the remote MAC addresses and routes from the core network and automatically discovers VPNs. Therefore, Layer 2 and Layer 3 packet forwarding entries are generated to guide packet transmission on the data plane. EVPN can provide a wide range of services, such as L2VPN (E-LAN, E-Line and E-Tree) and L3VPN, meeting the requirements for availability, scalability, bandwidth utilization and simplified O&M. It is applicable to multiple scenarios such as cross-public network enterprise interconnection, Data Centre (DC) interconnection and intra-DC overlay.

When the Service Plane traffic is carried by the OTN Underlay Plane, the MP-BGP cannot be used as the signalling protocol in its current form. Typically the OTN nodes are not configured with IP addresses for traffic forwarding. Therefore an appropriate protocol is required to run in the C2 and C2' interfaces, which has the equivalent functionality to MP-BGP. This protocol is for further study.

5.4.4 The Aggregation Network Fabric

5.4.4.1 IP/Ethernet Fabric

The IP/Ethernet fabric provides a simplified aggregation network architecture. As shown in Figure 27, the IP/Ethernet Fabric consists of integrated Access Leaf (AL), Aggregation Edge Leaf (AEL), and large-capacity and high-density interconnection Aggregation Fabric (AgF):

1) The AL provides large-capacity integrated service access. In F5G networks, the AL is typically part of the access node such as an OLT and has SAP and SMP functionality.

2) The AEL is the extraction and steering node which directs and connects the Aggregation Network traffic to the Core Network and DC-GWs and vice versa. In F5G, the AEL is typically part of the AggN Edge Node.

3) The AgF nodes provide large-capacity and high-density interfaces and multiple layers to implement full interconnection between AL and AEL nodes. The AgF nodes can be a large-scale Layer 3 switch or router. In addition, a centralized SDN controller can be introduced to provide programmable bearer connection paths and automatic O&M in the Underlay Plane. In F5G networks, the AgF is a particular choice of the aggregation fabric.

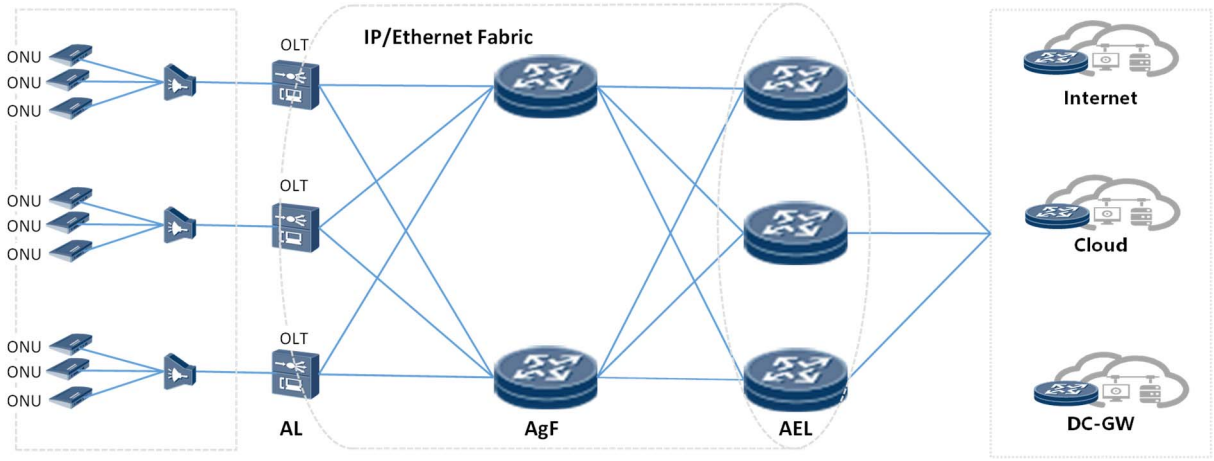


Figure 27: IP/Ethernet Fabric

The IP/Ethernet Fabric architecture uses this infrastructure to implement full connectivity. Based on the principle of decoupling the Underlay Plane from the Service Plane, the IP/Ethernet Fabric uses a simplified protocol stack to simplify the network layer and introduce SDN automation to achieve the following benefits:

1) Full-mesh:

   - A small number of links implement the full interconnection of the leaf nodes, meeting the growing trend of aggregation east-west traffic in the future.

2) Scale-out:

   - AgF nodes can be expanded horizontally or vertically on demand, and the leaf nodes are unaware of these changes.

3) Multi-path redundancy:

   - Multi-path protection: Multiple paths exist between a leaf node and another leaf node. The failure of a single node or link does not affect online services.

   - Programmable path: A path that carries service traffic can be dynamically selected based on SLA requirements and path load status.

   - Multi-path load balancing: Load balancing is used to distribute traffic to multiple links, achieve statistical multiplexing of the overall network capacity, and prevent imbalance between busy and idle links on a traditional tree network.

4) Centralized management and control (SDN):

   - Centralized management and control implement traffic prediction and supports accurate capacity expansion planning. Inter-domain and multi-vendor networks are centrally managed, and minutes-level end-to-end provisioning is enabled. Network topology and link status are monitored and analysed centrally to implement the programmability of bearer connection paths.

5) Protocol simplification:

   - Protocols are simplified and unified. The bearer connection is unified to SRv6, and the corresponding control protocol is converged to BGP, which greatly reduces learning complexity.

6) Stateless network:

   - The AgF nodes are unaware of the SRv6 tunnel status. Path changes should not affect the traffic characteristics of the tunnel. Tunnel specifications are scalable.

5.4.4.2 OTN Fabric

Traditionally the OTN aggregation network was based on ring networking topology. It was comprised of the Access ring, Aggregation ring, and Core ring converged on a single layer, and electrical cross-connections would multiplex/de-multiplex on a hop by hop basis. If the aggregation traffic load is light, the ring network topology is very efficient. With the onset of multi-service networking and higher bandwidth links, ring networking topology becomes a hindrance to service development. Therefore, the OTN networking topology needs to "break loops and form a tree" and move to a mesh network topology, which is termed an OTN fabric network. Figure 28 shows the migration or transformation of the network topology to a more mesh type topology. Now, if there are N nodes, each node needs to connect the N-1 nodes, ensuring all nodes can be connected with each other, but the links only carried the traffic required between each node and not that of the other nodes under normal operation.

An OTN fabric network consists of access leaf nodes, aggregation edge leaf nodes, and the OTN aggregation Fabric nodes:

1) Access leaf nodes perform the aggregation and appropriate access functionality for home broadband, leased line, and mobile base stations, and cover OLT, IP RAN, ASG and Multi-Service Optical Transport Network (MS-OTN) leased line access functions. In F5G networks, the access leaf node is usually collocated or part of the access node.

2) Aggregation edge leaf nodes extract the traffic and provide service connectivity to the Core Network and Data Centres. In F5G networks, the aggregation edge leaf nodes typically collocated or part of the AggN Edge Node.

3) OTN Fabric nodes provide full interconnection of Access leaf nodes with Aggregation edge leaf nodes. In F5G networks, the OTN fabric is a particular choice of the aggregation fabric.

NOTE: A mix of ring and mesh topologies can be used for migration to a new topology with the described benefits.

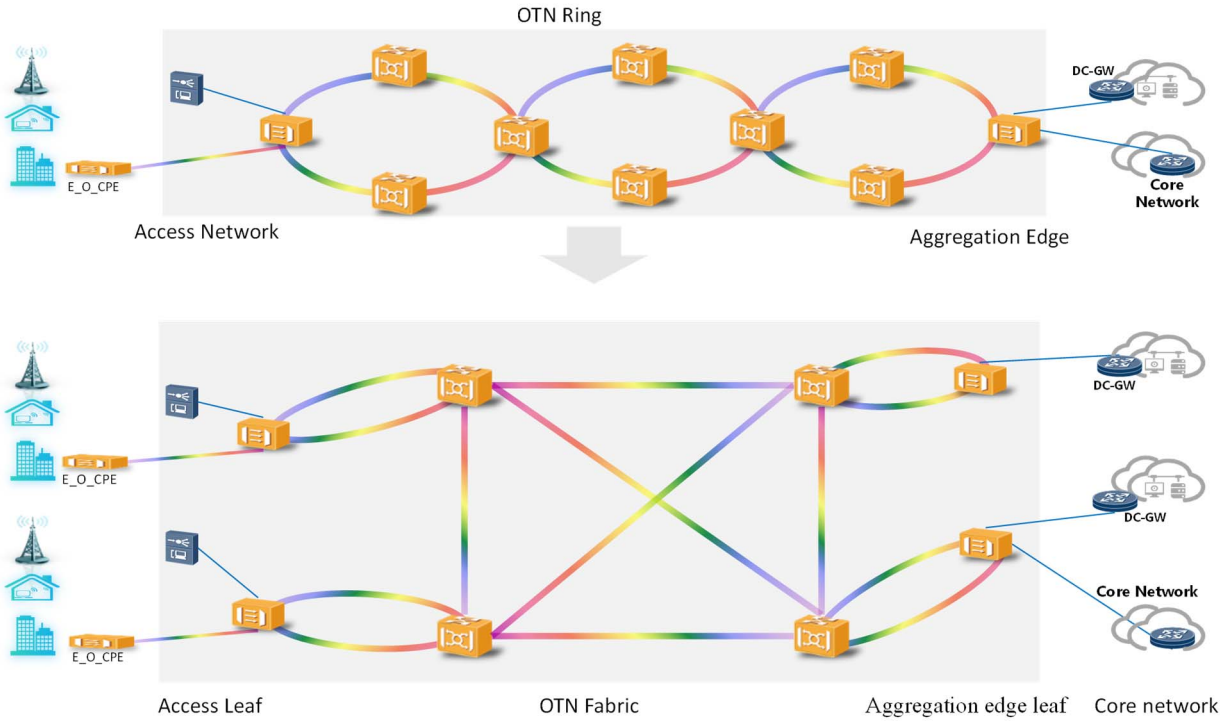


Figure 28: OTN Fabric

The OTN aggregation Fabric networking architecture has the following advantages:

1) Direct connection supports high-priority services:

   - If the nodes use electrical cross connects the direct electrical layer connection between leaf nodes may be implemented. If the nodes use Optical Cross-connect (OXC) switching, a direct optical layer connection between leaf nodes may be implemented. High-priority services that were identified in the Service Plane requiring extremely low latency can be steered to the OTN fabric in the Underlay Plane. The OTN fabric will then provide high-quality service transport. The OTN fabric nodes are unaware of the OTN bearer connection status. Path changes do not affect the services. The bearer connection specifications are scalable.

2) High reliability:

   - The ring network topology can support a single fibre cut failure condition, as traffic traverses the ring in both directions. However, this may induce higher latency. The fabric network has alternate paths. If there are N nodes, then there are N-1 alternate paths. The Network controller has at its disposal N-1 path to choose from, allowing it to choose the best alternate path that is best suited to the service characteristics of the failed link. The fabric network, therefore, provides higher reliability.

3) The overall bandwidth utilization is high:

   - Multi paths networking facilitates network traffic balancing and improves overall network bandwidth utilization.

4) Simplify the network:

   - Access Nodes, such as OLTs, function as optical leaf nodes and implement multi-service access for home broadband, leased line, and mobile bearer services. All-in-one simplifies Access Node types. All bearer connections use the leaf-fabric-leaf three-hop structure, simplifying the network layer. The fabric functions as a centralized forwarding node for traffic, facilitating traffic monitoring and scheduling.

5.5 Management, Control and Analytics (MCA)

5.5.1 Overview

The MCA Plane, as shown in Figure 29, is managing the Underlay Plane as well as the Service Plane. The MCA Plane may have different interfaces to a variety of IT systems for various purposes. The integration of the MCA Plane into surrounding IT systems through its northbound interfaces is for further study.

The AI analyser performs analytics tasks based on the information in the digital twin. The result of that analyses is either visualized or used for reasoning about the current status and eventual changes needed in the network. The AI analyser may be trained based on historic data or use unsupervised learning for performing its functionality. Example functions are:

1) Predictive maintenance: the AI analyser predicts future issues based on the current data and status of the network.

2) Smart traffic steering: the AI analyser can find out what traffic is flowing in the F5G network, and can find out whether there are service affecting issues, and eventually recommend that traffic is steered differently.

The Autonomous Management and Control (Autonomous M&C in Figure 29)) performs network configuration, service deployment, and network operation functions.

The digital twin is the real-time status of the F5G network.

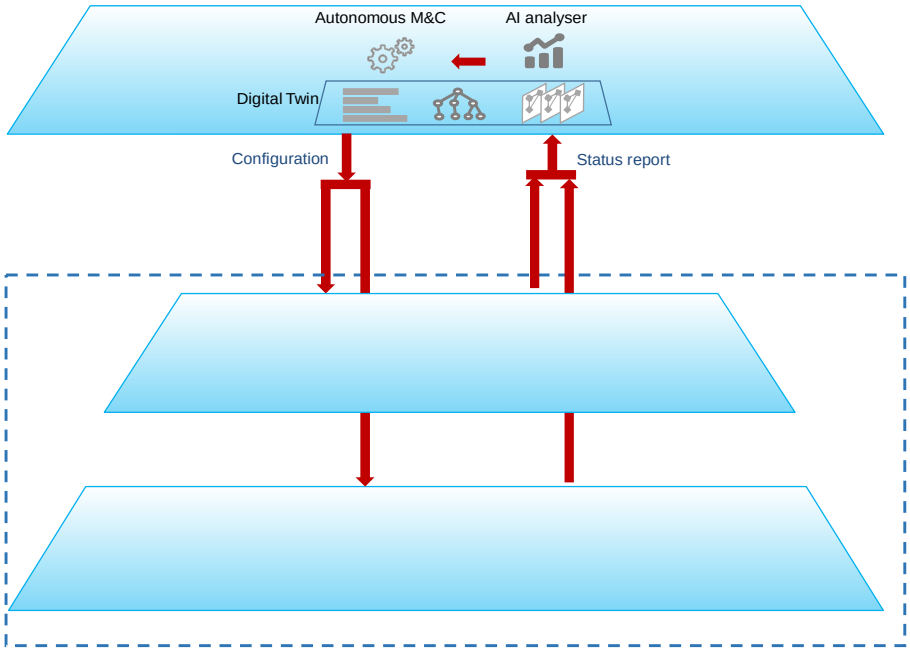


Figure 29: The MCA plane

5.5.2 Autonomous Management and Control

The autonomous management and control functionalities are the main tasks for network configuration, service deployment, and network operation. It contains autonomous engines in the E2E Orchestrator and in the domain controllers, depending on the need of the level of knowledge and data to perform that functionality.

The interfaces and functionalities specified in ETSI GS F5G 006 [20] shall be used and the requirements specified in ETSI GS F5G 006 [20] shall apply.

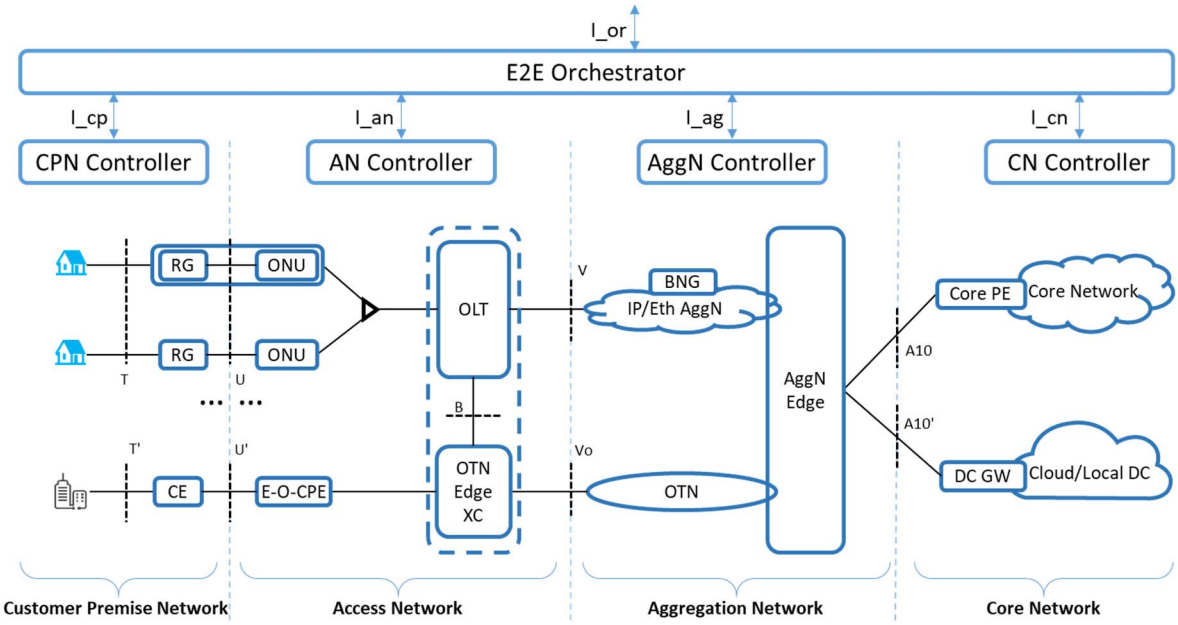


Figure 30: E2E Management and Control Architecture (from ETSI GS F5G 006 [20])

The interfaces of the E2E Management and Control Architecture should be using the intent-driven approach as much as possible and wherever it has its benefits. For further information about intend-driven approaches and interface specifications refer to ETSI GS F5G 006 [20].

5.5.3 Digital Twin and Telemetry

The digital twin of the F5G network contains several data structures including all network information and the current real-time status of the network. Naturally there is a trade-off between the accuracy of the digital twin information and the number of updates from the network required.

In order to receive timely information, two types of interfaces are defined per network domain. The telemetry interface is used to send telemetry data to a collector function. The configuration interface is used to configure telemetry tasks.

For the access network domain, the telemetry shall use the interfaces as defined in ETSI GS F5G 011 [21] and the requirements as defined in ETSI GS F5G 011 [21] shall apply.

For the other network domains, the telemetry interfaces are for further study.

5.5.4 Network Abstraction and Model-driven Design

The F5G network has domain controllers for each of the network segments. The domain controllers perform the network abstraction function to provide a concise view of the network segment resources, without too many detailed technology-specific information (see clause 6.3.2.4 of ETSI GS F5G 006 [20]). This aids the E2E Orchestrator to orchestrate different network domains with different technologies and different types of network elements.

To enable the network and service programming, a set of common standard APIs are required on the northbound interfaces of the domain controllers, which are designed as model-driven interfaces. The YANG data modelling language [24] shall be used to model the data for the network management and control (e.g. configuration data and state data).

ETSI GS F5G 006 [20] specifies the key parameters for the management and control of the F5G network segments. These parameters shall be modelled using the YANG data modelling language. The data models for F5G management, control and analytics are for further study.

Network management protocols defined by IETF such as NETCONF [25] and RESTCONF [26], can be used to transmit the modelled data for the F5G network management and control.

5.6 Security

The F5G security architecture is derived from various aspects and is detailed in ETSI GS F5G 012 [22]. The F5G security architecture overlays and extends the core connectivity architecture shown in Figure 1. Each plane shall define a set of security authorities such as the authentication authority, authorization authority, and a trust manager. The network element software integrity shall be managed using Roots of Trust (RoT) and there may be function specific RoTs per plane. The secure interaction between the underlay and service plane shall be typically go through the MCA plane, since each plane is regarded as a separate trust domain.

The MCA plane takes an important role and can implement various security related functions for the overall end-to-end security management in the F5G network. The MCA plane acts as the overall RoT for a particular F5G network operator and established the different trust domains for that operator.

6 Network devices/equipment requirements

6.1 Customer Premises Network requirements

[R-1] Residential Gateway and Customer Equipment in the CPN shall support Wi-Fi® 6 [10] and mesh mode.

[R-2] Residential Gateway and Customer Equipment in the CPN shall support IPv6.

[R-3] Residential Gateway and Customer Equipment in the CPN shall support VLAN tag processing.

[R-4] Residential Gateway shall support traffic classification based on Ethernet priority, IP address, and IP TOS/DSCP fields for both upstream and downstream traffic.

[R-5] Customer Equipment for enterprise shall support L3 routing and L2 switching mode.

[R-6] Customer Equipment for enterprise shall support traffic management.

[R-7] Customer Equipment for enterprise shall support IPSec.

[R-8] Customer Equipment for enterprise shall support NAT.

[R-9] Customer Equipment for enterprise should support VxLAN.

[R-10] The E-O-CPE shall support both Ethernet PCS transparent and Ethernet MAC transparent mapping.

[R-11] The E-O-CPE shall support the transparent mapping of PDH payload.

[R-12] The E-O-CPE shall support the transparent mapping of SDH payload.

[R-13] The E-O-CPE shall support OTN containers with 2 Mbit/s and above to efficiently match the bandwidth requirements.

[R-14] The E-O-CPE shall support hitless bandwidth resizing of OTN containers.

[R-15] The E-O-CPE shall support redundant OTN links.

[R-16] The E-O-CPE shall support the use of OTUk for k = 0 to 4 for its access connection.

6.2 Optical Access Network requirements

6.2.1 Access Network System Requirements

[R-17] The Access Network system shall support XG(S)-PON per Recommendation ITU-T G.9807.1 [11].

[R-18] The Access Network system shall have the capability to create, change, and delete service slice templates.

[R-19] The Access Network system shall have the capability to manage application lists and the mapping of applications to slice types or slice instances.

[R-20] The Access Network system shall have the capability to import and export the applications list.

[R-21] The Access Network system shall have the capability to add, change, and delete application list entries.

[R-22] The Access Network system shall support slice instance management, specifically adjusting the slice instance based on service requirements.

[R-23] The Access Network system shall support service slicing, where the service is identified by VLAN, ONU, ONU LAN port, or application Destination IP.

[R-24] The Access Network system shall support a northbound interface to the MCA plane to manage applications and services.

6.2.2 ONU Requirements

6.2.2.1 Functional Requirements

[R-25] The ONU shall be capable of classifying application traffic and mapping it to the appropriate GEM port or VLAN.

[R-26] The ONU shall have the capability to set or modify the service priority by changing the appropriate fields in the traffic (such as the Ethernet priority or IP TOS/DSCP fields).

[R-27] The ONU shall support traffic scheduling per T-CONT based on the service priority.

[R-28] When processing upstream and downstream services, the ONU shall support mapping the services to different priority queues based on the Priority code point (PCP) defined in IEEE 802.1Q [19]) and performing queue scheduling.

[R-29] The ONU, when combined with a residential gateway, shall support Wi-Fi® 6 [29].

[R-30] The ONU, when combined with a residential gateway, should support Wi-Fi® 6 slice separation based on RU.

[R-31] The ONU, when combined with a residential gateway, should ensure the bandwidth of each slice through the RU division.

[R-32] The ONU, when combined with a residential gateway, should support static reservation of RU resources based on service SLAs.

[R-33] The ONU shall support the traffic information collection to generate statistics for the sent, received, and lost packets per slice.

[R-34] The ONU shall support the reception of slice configuration from the OLT through OMCI.

6.2.3 OLT Requirements

6.2.3.1 Functional Requirements

[R-35] The OLT shall support D-Nets on the PON link.

[R-36] The OLT shall support ONUs on the same PON port belonging to different D-Nets.

[R-37] The OLT shall support the functionality to allocate upstream bandwidth in PON of all the T-CONT of the same tenant.

[R-38] The OLT shall support the isolation of one tenant's traffic from other tenants' traffic.

[R-39] The OLT shall support VLANs of different tenants with the same VLAN tag on the same PON port.

[R-40] The OLT shall support equivalent VLAN tags for different tenants when they are on different uplink interfaces.

[R-41] The OLT shall support sharing the OLT uplink port among different D-Nets and different service-oriented slice instances.

[R-42] The OLT shall support per D-Net traffic isolation of the uplink ports.

[R-43] The OLT shall support per D-Net traffic shaping on the uplink ports.

[R-44] The OLT shall support independent forwarding domains for each D-Net.

[R-45] The OLT shall support that forwarding domain that are isolated from each other.

[R-46] The OLT shall support hierarchical QoS scheduling for separating different services of the same tenant for the PON ports.

[R-47] The OLT shall support hierarchical QoS scheduling for separating different services of the same tenant for the uplink ports.

[R-48] The OLT shall support different queuing disciplines.

[R-49] The OLT shall support high-priority traffic even under congestion conditions.

[R-50] The OLT shall support user group slicing per ONU and OLT uplink port.

[R-51] The OLT shall support the traffic classification for different application services. The classification shall be based on GEM Port-ID and VLAN tag on the PON ports.

[R-52] The OLT shall support the traffic classification based on a service priority identifier, such as the Ethernet priority field and may use the TOS/DSCP field of the IP packet header.

[R-53] The OLT shall support the configuration of ONUs for slicing features.

[R-54] The OLT shall support slicing per VLAN, SRv6 and OTN on the uplink port(s).

[R-55] The OLT shall support modifying upstream and downstream service priority identifiers (the Ethernet priority field or TOS/DSCP field).

[R-56] The OLT shall support copying C-VLAN to S-VLAN for the traffic flows.

[R-57] The OLT shall provide H-QoS and traffic shaping based on the PON port.

[R-58] The OLT shall support Default Forwarding, Expedited Forwarding, and Assured Forwarding for downstream service slices.

[R-59] The OLT shall support H-QoS and traffic shaping based on uplink Ethernet ports.

[R-60] The OLT shall support Default Forwarding, Expedited Forwarding, and Assured Forwarding for uplink service slices on the Ethernet port.

[R-61] The OLT shall support isolating queue resources between service slices.

[R-62] The OLT shall support mapping different priority queues based on the Priority Code Point as defined in IEEE 802.1Q [19].

[R-63] The OLT shall support alarm reporting per network slice instance.

6.2.3.2 Interface Requirements

[R-64] The OLT shall support a management interface, which includes telemetry functionality.

[R-65] The OLT management interface shall support network slice instance configuration.

6.3 Optical Transport Network requirements

The Optical Transport Network (OTN) comprises the OTN edge cross-connect nodes, the OTN aggregation network nodes, and the OTN aggregation edge nodes, among other OTN network elements. These individual network elements will not be referred to except in requirements specific to them.

[R-66] The OTN network node shall adhere to Recommendation ITU-T G.709 [2] for framing and mapping.

[R-67] The OTN network node shall adhere to Recommendation ITU-T G.709.1 [3] for short reach FlexO transport.

[R-68] The OTN network node shall adhere to Recommendation ITU-T G.709.3 [4] for long reach FlexO transport.

[R-69] The OTN network node functionality shall comply with the equipment functional requirements of Recommendation ITU-T G.798 [12].

[R-70] The OTN network node shall comply with the Protection switching requirements of Recommendations ITU-T G.873.1 [13], G.873.2 [14] and G.873.3 [15].

[R-71] The OTN network node shall comply with Recommendation ITU-T G.8251 [16] for jitter and wander requirements.

[R-72] The OTN network node shall comply with Recommendation ITU-T G.8201 [17] for error performance.

[R-73] The OTN network shall support the establishment, configuration and tear down of OTN paths under the control of the Network Management System (NMS).

[R-74] The OTN network shall support the establishment, configuration and tear down of appropriate traffic characteristic bearer connections under the control of the NMS.

[R-75] The OTN network shall support fine-granular allocation of bandwidth of 2 Mbit/s and above by NMS.

[R-76] The OTN network shall support hitless bandwidth adjustment by NMS. The OTN network shall support on-demand connection provisioning and configuration by the NMS.

[R-77] The OTN network shall support five nines availability.

[R-78] The OTN network shall support deterministic low latency independent of traffic load.

[R-79] The OTN edge cross-connect shall support both Ethernet PCS transparent and Ethernet MAC Transparent mapping.

[R-80] The OTN edge cross-connect shall support the transparent mapping of PDH payload.

[R-81] The OTN edge cross connect shall support the transparent mapping of SDH payload.

[R-82] The OTN edge cross-connect shall support OTN containers with 2 Mbit/s and above to efficiently match the bandwidth requirements.

[R-83] The OTN aggregation network nodes shall support OTN connectivity between OTN Edge cross-connect nodes and OTN aggregation edge nodes under the control of the NMS.

[R-84] The OTN aggregation edge nodes shall support OTN bearer connection termination and appropriate traffic steering to local data centres and Cloud services.

[R-85] The OTN aggregation edge nodes shall support dedicated OTN connection to local Data Centres.

[R-86] The OTN aggregation edge nodes shall support dedicated OTN connection to Cloud services.

6.4 IP Network requirements

[R-87] The IP Network shall support EVPN.

[R-88] The IP Network shall support an MP-BGP control plane.

[R-89] The IP Network shall support SRv6 Best Effort (BE).

[R-90] The IP Network should support SRv6 Traffic Engineering (TE).

[R-91] The IP Network shall support congestion-free and high-availability deployments.

[R-92] The IP Network shall support low and deterministic latency.

[R-93] The IP Network shall support slicing.

[R-94] The IP Network shall support an automated O&M system.

[R-95] The IP Network shall support either Dual IP Stack to support the IPv6 transition or translation of IPv4 traffic into IPv6 for transport of IPv4 over the IPv6 network.

6.5 F5G Security requirements

The security requirements are organized according to the network management domain, transport network domain, and the F5G network domain.

[R-96] The provisions defined in ETSI TS 103 924 [23] shall apply.

[R-97] For the network management security domain requirements, the provisions in clause 6.2 of ETSI GS F5G 012 [22] shall apply.

NOTE 1: The provisions deal with the overall RoT, the integration of Service Plane and Underlay Plane elements into the F5G network, and interfaces between the Service Plane, Underlay Plane, and the MCA plane.

[R-98] For the underlay plane security requirements, the provisions in clause 6.3 of ETSI GS F5G 012 [22] shall apply.

NOTE 2: The provisions deal with the connections between Underlay Plane network elements and their integrity and addition to the trust domain.

[R-99] The security associations as shown in Table 6.1 of clause 6.3 of ETSI GS F5G 012 [22] shall be defined.

7 Network migration

The migration to an F5G architecture has several aspects to be considered. The migration is heavily dependent on the system currently in operation, which one intends to migrate from. This clause discusses some aspects of migrating to an F5G architecture from a conceptual and architectural perspective. For details on particular technologies, refer to the appropriate technology standards.

Why migrating to F5G

F5G provides the mechanisms for implementing a wider range of applications with a variety of requirements. Therefore F5G provides the technologies to increase the bandwidth, specifically in the access network, to increase the QoE through mechanisms for guaranteed services through dual aggregation network technologies (packet and OTN) and evolve OTN for finer granularity premium private line services to multiple clouds. All these features increase the value to the customers.

On the Underlay plane, providing both IP/Ethernet and OTN networks, F5G gives a choice to transport traffic over the appropriate network fabric to match the required quality of service.

On the Service plane, the OLT functions as the edge mapping/steering point for services and the bearer connections enables differentiated service slicing and edge intelligence. The OLTs and ONUs jointly identify applications and service types, and the OLT directs service flows to appropriate slices based on differentiated SLA requirements.

On the Management, Control, and Analytics plane, service-triggered request for E2E path establishment and selection for service traffic is provided. Compared with segmented management of a network, F5G network cross domain controllers are orchestrated to deliver dynamic E2E path for SLA guaranteed services.

Easy Migration

The evolution from the existing network architectures to the F5G architecture is relatively moderate. The possible steps are as follows:

1) For the use of the packet aggregation network, the OLT software is upgraded to support the SRv6 as Underlay Plane protocol. The OLT hardware expansion supports the forwarding plane hard slicing and OTN upstream transmission. The OLT is connected to the OTN network seamlessly.

2) Upgrading of the network management system to include the traffic steering and slicing control functions and interconnect with the cross-domain orchestrator.

3) The configuration management of the IP network is extended to the OLT as the edge of the IP network. When SRv6 Traffic Engineering (TE) is enabled, the OLT needs to interconnect with the TE path computation controller in the IP domain.

4) OTN deployment at the Access Network is needed, where there is a business requirement for premium services.

5) Replace ONUs when necessary to increase bandwidth (GPON to XG(S)-PON) and to enable applications and services identification, marking and scheduling, depending on service requirements. Note that the migration from copper is not in scope for the present document.

Compatibility with existing ODNs

The existing fibre infrastructure for the ODN can be re-used and is in most cases compatible with F5G, and therefore no changes are needed on existing ODNs.

Re-use of ONU and CPN equipment

Existing ONUs and CPN equipment can be re-used, however, without benefiting from the new F5G capabilities. The majority of existing packet-based CPNs are compatible with the F5G architecture.

Upgrading the CPN for F5G

To receive the full F5G benefits, an upgrade of the CPN components is required. The upgrade of CPN elements to Wi-Fi® 6 capabilities in the residential and enterprise gateways is necessary to provide higher bandwidth. For differentiated services capabilities, the CPN needs traffic differentiation and isolation capabilities. Depending on the technologies, such capabilities like CPN slicing, Wi-Fi® 6 slicing, Wi-Fi® mesh, etc. with different migration paths can be foreseen.

For even higher bandwidth and a future proof fixed network, fibre-based CPNs are proposed and should be planed and deployed to fully benefit from F5G potential. Long-term planning for migrating to fibre-based CPNs needs to be in place, since that will take some time. Specifically for new buildings or replacement of in-house installations, the fibre connections need to be available.

Also, for end-to-end QoE, including the CPN segment, the traffic needs to be identifiable in the network to receive the appropriate provisioning along the end-to-end path. Therefore, new software or new devices are required. For example, the new Cloud VR terminal needs to be F5G compatible.

Migrating to dual aggregation networks for higher QoE

The OTN network is connected to the Access Network, and the OLT is directly connected to the OTN network. From the perspective of service transport, OTN becomes a viable optical underlay network, which is at the same layer as the IP network and provides higher QoE than other technologies.

The deployment of OTN in the OLT or in the Access Network is largely a business decision depending on the service quality provided to the customers. And the deployment can be done gradually.

Gradual migration

Due to the flexibility and separation on different planes in the F5G architecture, the migration can evolve gradually depending on what benefits are best suited for the market segments and service offerings at a given time. However, gradual migration will not achieve the full F5G benefits quickly.

Upgrading and Migrating in the Future

Through the separation of Service Plane and Underlay Plane, the future upgrading or adaptation of the network capacity is simplified. First, the capacity of the Underlay Plane can be expanded or contracted transparent and independent of the Service Plane. Second, the Underlay Plane is unaware of the addition, reduction, and migration of Service Access Points (SAPs) and Service Processing Points (SPPs) in the Service Plane. The service access points and service processing nodes can implement horizontal scale-up/down.

Migration to IPv6/SRv6

The IPv6 transition is key for the evolution of the IP network. The initial stage is to implement Dual Stack for the IPv6 transition. Any IPv6 transition would need an update of the IP Network Management Systems because many carriers already have some level of automation, and some configurations would have different parameters for IPv6.

Annex A (informative): How the F5G Architecture addresses the Gaps

The F5G technology landscape requirements and gap analysis document [27] has listed several gaps based on the requirements of each use case. The F5G architecture addresses some of those gaps. Table A.1 is an assessment of F5G architecture as shown in the present document with regards to whether those gaps are addressed. Gaps which are not addressed are for further study. Note that this is at the time of publication of the present document and will change over time.

NOTE: Also some of the gaps are addressed from an architectural perspective, but the baseline technologies might still need to be defined in the SDOs, which define the used technology baseline.

Table A.1: Gaps address in the F5G architecture

Suggested actions	Relevant gaps	F5G architecture addressing gaps
Define a high quality slicing mechanism.	Gap03-3, Gap15-3, Gap15-13	The F5G architecture defines slicing end-to-end and with different (on service or user oriented) and different quality levels.
Define the mechanisms for a large number of different parallel slices.	Gap15-4	From an architectural perspective a high number of slices are supported. On the data plane all technologies on an end-to-end path need also be able to support high number of slices.
Define hard slicing for Wi-Fi®, CPE and PON.	Gap03-4	Hard isolation in general is supported in the F5G architecture, the mechanisms for hard slicing per technology is out of scope for the ISG F5G.
Define AI based traffic and application type identification.	Gap03-5, Gap10-2	The identification of traffic and applications is handled in the MCA plane of F5G, whether AI technologies are used is an implementation choice.
Define E2E slicing management including management and control function requirements and network resource allocation.	Gap03-6, Gap01-11, Gap01-18	End-to-end slice management is support.
Define slice management APIs for applications to request and release network slices.	Gap15-6, Gap15-10	The slice management interface is defined and is reusing data models from other SDOs.
Define interface between telco network and cloud network for guaranteed services.	Gap03-8	The interface A10' is defined in the F5G architecture.
Define Time-of-day based SLA management interface and data models for commercial customers.	Gap03-10	SLA management interfaces are defined in the end-to-end management of F5G. The time-of-day based data models are for further study.
Define mechanism of fast provisioning of private line service.	Gap03-12, Gap23-5	The private line provisioning is defined.
Define management interfaces to coordinate end-to-end path setup and release.	Gap18-3	End-to-end path setup is defined.
Define mechanism of automatic and fast fault detection, localization, demarcation, isolation and correction/recovery.	Gap03-13, Gap32-4, Gap32-5, Gap32-6	Fault management functionality is defined.
Specify management tools and action lists of fault and service degradation issues.	Gap32-7	Fault management is defined in the F5G management architecture, however tools and mechanism are implementation oriented and do not need standardization.
Define visualized network operation SLA indicators.	Gap03-14	The support of getting data to be visualized is supported. The details on how to visualize are implementation specific.
Define service level slicing for OTN.	Gap02-2	OTN slicing is defined on the data paths, however, the management and control of OTN slices if for further study.
Specify on-demand ordering capability for CPE and Edge node.	Gap02-3	The interface for on-demand ordering is supported.
Define E2E slicing mechanism with consistent SLA on multiple network segments with different physical technologies, including slice granularity.	Gap06-1, Gap10-4, Gap01-16	End-to-end slicing is a core feature supported by the F5G architecture.
Specify interworking of PON and TSN.	Gap06-3	TSN performance requirements can be implemented in F5G, however, detailed interwork is for further study.

Suggested actions	Relevant gaps	F5G architecture addressing gaps
Specify Industrial PON ONU with industrial interfaces and protocol interpreting functions.	Gap06-4, Gap06-5	The client side industrial interfaces of ONUs is for further study.
Specify PON telemetry requirements.	Gap06-9	The telemetry for the F5G access network is specified.
Define automatic network resource allocation and configuration enabled by AI based functions within the PON system.	Gap06-9, Gap30-2, Gap30-3	The F5G Access network controller in the F5G architecture specifies this functionality.
Define support for F5G network protection switching times better than 30ms (e.g. dual-homing with Type-C in PON).	Gap24-2	Dual-homing with Type-C in PON is supported, however, the high performance switching time is needed for certain use cases, and therefore the current specifications are not good enough and therefore this is for further study.
Define standards for edge/cloud computing integrated with optical F5G networks.	Gap15-11, Gap15-12	Edge computing is loosely defined. The functionality is supported at the AggN edge node and over the A10 and A10' interfaces. Edge computing at the F5G Access Network Node (OLT or OTN Edge XC) is for further study.
Define a mechanism for on-demand allocation of compute resources for optimized multi-party latency optimization	Gap18-5	The interface for on-demand compute allocation is for further study.
Define Industrial PON system with computing power metric for edge computing platforms.	Gap06-12	The aspects of Industrial PON beyond the traditional use of PON and the integration with compute are for further study.
Define application type identification mechanism.	Gap10-1	Application type identification is supported through the MCA plane.
Specify method of dynamic establishment and updates of application feature database using Big Data and Machine Learning mechanisms.	Gap10-3	The functionality is available in the MCA plane, however the detailed mechanisms are implementation specific.
Define mechanisms to identify network usage of applications, which have potential acceleration demands.	Gap10-8	The interface to detect those usages is defined, however, the mechanisms are implementation specific.
Define mechanisms for near real-time non-intrusive monitoring of F5G network resource utilization, delay, and health status.	Gap10-10, Gap23-6, Gap25-9, Gap30-3	The interfaces for monitoring are defined.
Specify a light-weight Telemetry technology for Access Network.	Gap11-1	Telemetry interfaces are defined.
Develop and specify a dedicate data model for performance monitoring and data collection for Access Network.	Gap11-2, Gap26-3, Gap26-5, Gap32-2	The data model for F5G access network telemetry is specified.
Define OLT device with OTN capabilities.	Gap01-7	The architecture defines OLT devices with OTN capabilities.
Define a mechanism for transport network resource allocation and adjustment for services like Cloud VR.	Gap01-12, Gap01-13, Gap 01-14, Gap01-17	The interfaces for transport network resource allocation is defined.
Define a simple mechanism for bandwidth demand changing.	Gap01-15	The interface with the demand for on-demand bandwidth change is defined.
Specify interfaces for applications to detect service capabilities supported by the F5G network.	Gap15-2	The detection of service capability detection is for further study.
Define mechanisms and APIs to exchange QoE related metrics between application and network	Gap15-7	The definition of the API is for further study.
Specify access management mechanisms to prevent over-requesting resources from the F5G network, which are not used by the application.	Gap15-17	The feature is part of the MCA plane having the oversight of the resource allocations and usage.
Define a mechanism to learn the client and cloud side of the F5G networks addressing and building up the mapping tables (in the SMP) automatically.	Gap16-1, Gap17-1, Gap17-2	The interfaces with that functionality are specified.
Specify YANG models for the request for network connectivity to the cloud.	Gap16-2, Gap17-3	The YANG models are reused from other SDOs.
Specify YANG models for OTN slice management.	Gap16-8, Gap17-11	The YANG models are reused from other SDOs.
Specify YANG models for optical predicted and real failure information reporting.	Gap31-5	The YANG models are reused from other SDOs.

Suggested actions	Relevant gaps	F5G architecture addressing gaps
Specify OTN signalling protocols for large scale OTN connections (plenty of OTN connections).	Gap16-9, Gap16-12, Gap17-5, Gap17-16, Gap17-12	The interface for signalling protocols is specified.
Define a Ethernet/TSN translation and mapping function to run on ONUs and OLTs.	Gap19-5	The translation of TSN to F5G is for further study.
Specify TSN-like features for industrial automation.	Gap21-1, Gap22-4	TSN-like features are in general supported due to the low latency, high bandwidth characteristics of F5G.
Specify support of native industrial Ethernet protocols (functional and performance).	Gap21-6, Gap21-7	This is for further study.
Specify functional model for photonic automatic cross-connects.	Gap25-6	The functional model of a photonic cross-connect is for further study.
Specify the P2MP aggregation network architecture.	Gap28-2	P2MP aggregation is for further study.
Specify the P2MP aggregation network control and management interface and mechanisms.	Gap28-6, Gap28-7	This gap is for further study.
Specify privacy conserving mechanisms for the F5G network.	Gap30-4, Gap10-9, Gap15-15	Various security aspects are defined by the security architecture.
Define evaluation schemes for QoE of specific applications.	Gap10-6	The evaluation schemes for QoE is described in the QoE document [28]. The F5G architecture has the mechanisms and functionality to improve QoE and QoS for the users.

History

Document history		
V1.1.1	May 2023	Publication