ETSI GS F5G 018 V1.1.1 (2024-10)

Fifth Generation Fixed Network (F5G); Architecture of Optical Cloud Networks

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-0018

Keywords

cloud, F5G, optical, service

ETSI

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

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

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

Contents

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

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

Foreword

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

Modal verbs terminology

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

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

Introduction

In F5G and beyond, there is a trend that more and more services will be deployed in the Cloud Data Centres (DCs), which requires high quality, high performance, high reliability, high security network transmission between the users and the Cloud DCs. ETSI GR F5G 008 [i.1] has already described several use cases that are related to such cloud services.

1 Scope

The present document specifies the architecture and the technical requirements of the Optical Cloud Network (OCN), including its underlay Optical Transport Network (OTN) infrastructure and the control interfaces used for the control of the optical services and connections. The present document also specifies the key functions of the Optical Service Protocols (OSP) which are running on the control interfaces of the OCN.

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 3209: "RSVP-TE: Extensions to RSVP for LSP Tunnels".

[2] IETF RFC 4920: "Crankback Signaling Extensions for MPLS and GMPLS RSVP-TE".

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

[4] IETF RFC 8776: "Common YANG Data Types for Traffic Engineering".

[5] Recommendation ITU-T G.808 (2016): "Terms and definitions for network protection and restoration".

[6] ETSI GS F5G 024 (V1.1.1): "Fifth Generation Fixed Network (F5G); F5G Advanced Network Architecture Release 3".

[7] Recommendation ITU-T G.709/Y.1331 (2020) Amd.3 (03/2024): "Interfaces for the optical transport network".

[8] Recommendation ITU-T G.709.20 (04/2024): "Overview of fine grain OTN".

[9] Recommendation ITU-T G.7044/Y.1347 (10/2011): "Hitless adjustment of ODUflex(GFP)".

[10] Recommendation ITU-T G.7701 (04/2022): "Common control aspects".

[11] Recommendation ITU-T G.7703 (2021) Amendment 1 (11/2022): "Architecture for the automatically switched optical network".

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

[13] Recommendation ITU-T G.873.1 (2017) Amendment 1 (02/2022): "Optical transport network: Linear protection".

[14] IETF RFC 8345: "A YANG Data Model for Network Topologies".

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

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".

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

connection ID: combination of the source and destination node IP addresses of a connection, and an index that remains constant over the life of the connection

NOTE: A connection ID is unique in a network, and is identical to the LSP_TUNNEL Session object in RSVP-TE (IETF RFC 3209 [1]).

crankback: mechanism allowing new path setup attempts to be made to bypass the blocked resources

NOTE: The blocked resource information is retrieved from the failure points in the previous path setup attempts, as defined in IETF RFC 4920 [2].

make-before-break: mechanism whereby an original path is still active while a new path is being set up in the connection restoration procedure

NOTE: The make-before-break mechanism avoids double reservation of resources by the original and new paths, as defined in IETF RFC 3209 [1] and IETF RFC 3945 [3].

node ID: node identification used in a Traffic Engineering (TE) topology

NOTE: A node ID is unique in a topology, as defined in IETF RFC 8776 [4].

protection group: combination of source and destination node functions, 1+1 or 1:n normal traffic signals, an extra traffic signal in the 1:n case if any, 1+1 or 1:n working paths, and 1+1 or 1:n protection path

NOTE: The 1+1 or 1:n protection path provides extra reliability for the transport of normal traffic signals, as defined in Recommendation ITU-T G.808 [5].

switching time: time between the initialization of the protection switching and the moment the traffic is selected from the protection path

NOTE: As defined in Recommendation ITU-T G.808 [5].

3.2 Symbols

Void.

3.3 Abbreviations

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

(fg)O-CPE	fgOTN Customer Premise Equipment
ASON	Automatically Switched Optical Network
BGP	Border Gateway Protocol
CBR	Constant Bit Rate
CDC	Central Data Centre
CE	Customer Edge
CPE	Customer Premise Equipment
CVLAN	Client Virtual Local Area Network
DC	Data Centre
E2E	End-to-End
F5G	Fifth Generation Fixed Network
F5G-A	Fifth Generation Fixed Network - Advanced
fgOTN	fine grain Optical Transport Network
GFP	Generic Framing Procedure
GW	GateWay
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
LDC	Local Data Centre
MAC	Media Access Control
MCA	Management, Control, and Analytics
MD-ROADM	Multi-Degree Reconfigurable Optical Add/Drop Multiplexer
MP2MP	Multi-Point-to-Multi-Point
NBI	NorthBound Interface
OCN	Optical Cloud Network
ODU	Optical Data Unit
ODUk	Optical Data Unit-k
OE	(fg)OTN Edge
OLT	Optical Line Terminal
OSP	Optical Service Protocols
OTN	Optical Transport Network
P2MP	Point-to-Multi-Point
PON	Passive Optical Network
QoE	Quality of Experience
QoS	Quality of Service
ROADM	Reconfigurable Optical Add/Drop Multiplexer
SAT	Service Address Table
SLA	Service Level Agreement
SMCC	Service Mapping Control Component
SME	Small and Medium Enterprise
SMP	Service Mapping Point
SMT	Service Mapping Table
SRLG	Shared Risk Link Group
SVLAN	Service Virtual Local Area Network
TDM	Time Division Multiplexing
TE	Traffic Engineering
UNI	User Network Interface
UNI-C	User Network Interface - Client
UNI-N	User Network Interface - Network
VBR	Variable Bit Rate
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VR	Virtual Reality
WDM	Wavelength Division Multiplexing
XC	Cross-Connect

4 Motivation

4.1 Overview of cloud access scenarios

With the rapid development of network technologies, more and more new services are emerging in the F5G era. There are two important trends for these services:

1) More and more services are deployed in the Cloud DCs, to take full advantage of shared cloud infrastructure.

NOTE: Cloud DCs can be placed at various locations. In ETSI GS F5G 024 [6], there are Local Data Centres (LDCs) co-located with the Aggregation Network Edge Nodes and the Central Data Centres (CDCs) located in the core network.

2) The requirements on those cloud service shall cover a wide range of network characteristic including those that satisfy the highest quality service experience. These highest quality cloud services are increasing significantly.

For convenience, such services that are deployed in the Cloud DCs are called "cloud services" in the present document.

ETSI GR F5G 008 [i.1] introduces 32 F5G use cases which are enabled by the F5G network, some of which are related to cloud service provisioning. For example:

- Use case #1: Cloud Virtual Reality. Cloud computing and cloud rendering technologies for VR services are introduced. Cloud VR content data are stored, read, rendered, coded compressed and transmitted to user terminals through the network.
- Use case #2: High Quality Private Line. Government institutions, financial organizations and medical organizations require high quality private lines for cloud access. Examples are medical cloud, cloud desktop and financial cloud.
- Use case #3: High quality low cost private line for small and medium enterprises. Small and Medium Enterprises (SMEs) may need cloud services such as cloud desktop and cloud storage.
- Use case #16: Enterprise private line connectivity to multiple Clouds. Enterprises are gradually migrating their applications to different clouds. Meanwhile, an enterprise may have multiple branches requiring access to the cloud applications. This requires the Multi-Point-to-Multi-Point (MP2MP) cloud access.

- Use case #17: Premium home broadband connectivity to multiple Clouds. There is an increasing demand for premium home broadband Cloud-based services such as Cloud VR education, Cloud VR gaming, and Cloud gaming. Since different cloud applications are deployed in different Cloud DCs, this use case also requires the Multi-Point-to-Multi-Point (MP2MP) cloud access from different OLTs.

In these use cases, there is an increasing number of mission critical services, which require stable and highest quality network transmission. OTN is a recommended technology for these services, because it naturally has the characteristics of guaranteed bandwidth, low deterministic latency and low packet jitter, high availability and traffic isolation.

4.2 Requirements from the Use Cases

In general, the cloud service related F5G use cases can be categorized into two types:

- PON access network case: Users (including residential broadband users and SMEs) access the network via a PON network;
- OTN access network case: Users (including large enterprises) access the network via an OTN equipment (including fgOTN Customer Premise Equipment ((fg)O-CPE)).

Figure 1 shows the general F5G network topology which uses the OTN AggN for the high-quality cloud services. Both PON access and OTN access use cases are covered in figure 1.

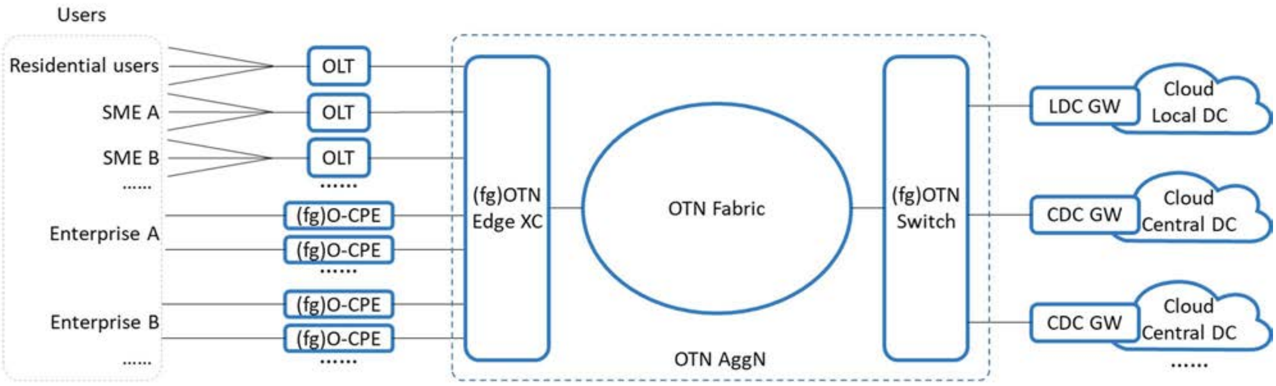

Figure 1: OTN-based general network topology for cloud services

NOTE 1: An enterprise may have multiple sites which are connected to the network using different technologies like PON or (fg)O-CPE. See the example enterprise A and B in Figure 1.

NOTE 2: Both the residential users and SME/large enterprise customers are called "users" for simplicity in the present document.

The key requirements of the cloud service related use cases shall include:

- Multi-user access: For the PON access case, multiple residential users or SMEs are accessing the OTN AggN via different OLTs. For the OTN access case, an enterprise has multiple branches, which access the OTN AggN via different (fg)O-CPEs and CPEs (Ethernet based).

- Isolation between users: The isolation between different users are required, for the consideration of manageability, QoE assurance and security. The isolation shall include address isolation and traffic isolation.

- Multi-cloud access: Users of cloud services may run different cloud applications which are deployed in different Cloud DCs. Furthermore, a user may connect to two or more Cloud DCs at the same time for backup and disaster recovery consideration.

- Automatic OTN connection provisioning: Considering the MP2MP connectivity from multiple user sites to multiple clouds, the OTN AggN needs to support on-demand resource scheduling and connection provisioning between any pair of edge OTN nodes, driven by the requests of the MP2MP connectivity services.

5 OCN architecture

5.1 Design principle

To provide high quality enterprise private line as well as Residential and SME broadband connectivity to multiple clouds services, the OCN architecture shall support the following network features:

1) Automation: Network automation technologies via control protocols shall be introduced in OCN for the automatic Cloud DC selection and service connection provisioning, to reduce the manual processes to a minimum. This will reduce the service enabling time, improves the users' experience, and reduce the configuration errors caused by human mistakes.

2) Bandwidth Flexibility: Different cloud application services may require very different bandwidths ranging from tens of Mbps to several Gbps. Furthermore, a user may have different bandwidth requirements at different times of the day. The OCN architecture shall be designed to support flexible OTN containers with hitless bandwidth adjustment, to match the above service bandwidth requirements.

3) Traffic Isolation: The OCN architecture shall be designed to support user service traffic isolation. Each user data to and from the clouds needs to be isolated from other user traffic, without affecting other traffic or being affected by other's traffic.

4) Connection Scalability: The OCN architecture shall be designed to provide scalable connection control and management, to support the increasing number of connections.

5) Reliability and Availability: The OCN architecture shall be designed to support at least 99,999 % service availability in the presence of one or multiple network failures within the OTN, with deterministic connection recovery performance.

6) Simplicity: The OCN architecture shall be designed to support minimal network layers, interfaces and protocols. Fewer network layers means higher resource utilization and easier network operation and maintenance. The interface protocols shall be designed so as to minimize their complexity, and shall support backwards compatible.

5.2 Overview of OCN architecture

In current Virtual Private Networks (VPNs), the OTN connection is used as a transparent pipe to transport the packet flows (including IP and Ethernet flows), without recognizing the users' service traffics within the packet flows. Therefore current OTN connections are not service aware, making it difficult to satisfy the VPN Service Level Agreement (SLA) requirements.

To guarantee network characteristics including assured flexible bandwidth, low deterministic latency, low packet jitter, high availability and traffic isolation for cloud services additional processes are necessary. The OCN shall directly support the transport of the highest quality cloud services and control and manage the service traffic.

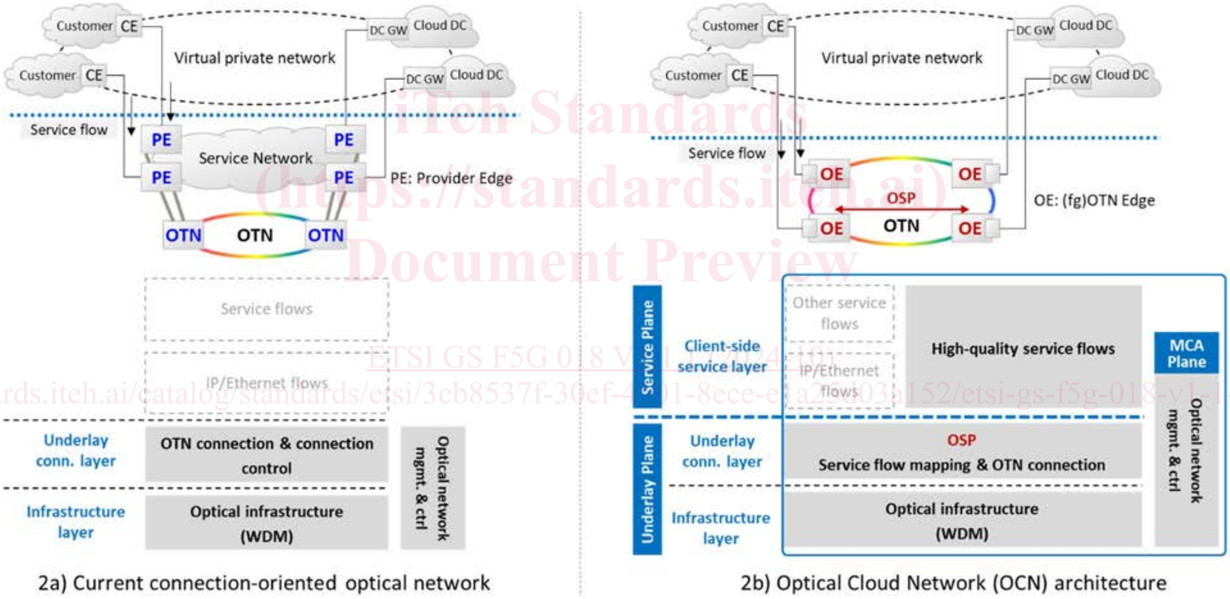

Figure 2: Evolving to the OCN architecture

NOTE 1: The (fg)OTN Edges (OEs) in Figure 2 is the edge nodes of the (fg)OTN domain, including the (fg)O-CPE, the (fg)OTN Edge XC in the Access Node, and the (fg)OTN Switch in the AggN Edge.

Figure 2 shows a comparison between the current connections oriented optical network (2a in Figure 2) and the OCN architecture (2b in Figure 2).

Comparing the current connection-oriented optical network (as shown in 2a) of Figure 2), the most distinct change is that the OTN connections are services aware, and carry the services directly over OTN connections. This reduces and simplifies the network layers, and ensures service quality. The two major improvements of OCN are:

- Current OTN transports IP/Ethernet packet flows transparently, without recognizing the users' service traffics within the packet flows, and therefore cannot guarantee the service latency, bandwidth, and hard isolation. With the support of the Optical Service Protocols (OSP), the OCN supports recognizing the service request information (including the service bandwidth, service source and destination and SLA requirements), and support service differentiation and transmission with assurance.

- In current OTN, most of the network connections are provisioned manually and are not dynamic. In OCN, with the support of OSP, a large number of network connections shall be dynamically provisioned, triggered by the users' service requests. Hitless bandwidth adjustment of OTN connection shall also be supported, based on the changing service bandwidth requirements.

The OCN architecture contains three network layers see 2b) in Figure 2:

1) Infrastructure layer: The Wavelength Division Multiplexing (WDM) technology is used as the OCN optical infrastructure. This is unchanged from the current connection-oriented optical network.

2) Underlay connection layer: The OTN connections (ODUk/fgODU connection) are used to carry the client-side services. In addition, to enable automatic provisioning the services orientated OTN connections, the Optical Service Protocols (OSP) are deployed in the underlay connection layer, with the two main control functions:

    - Service flow mapping control: The edge OTN nodes (Access Node and AggN Edge node) interact with the client-side overlay protocol and map the service flows to the OTN connections.

    - OTN connection control: Enhances the performance of the OTN signalling mechanisms to support dynamic control of a larger number of connections.

3) Client-side service layer: High-quality services cloud services are the main services to be carried directly by the OTN connections. Note that IP/Ethernet flows (which may be identified by existing technologies such as VLAN) can still be carried by the OTN network in the OCN architecture.

NOTE 2: It is important to note that the OCN architecture does not change the data plane interfaces and protocols on the customer equipment.

5.3 Integration of OCN into the F5G-A network architecture

ETSI GS F5G 024 [6] specifies the overall F5G-A architecture and its network topology. The OCN architecture is a sub-set of the overall end-to-end F5G-A architecture.

As part of the F5G-A architecture, the OCN architecture mainly focuses on the use of OTN (including fgOTN, referring to as (fg)OTN in the present document) in the CPE, the Access node of the Access network and the Aggregation Network (including the AggN Edge node) for high-quality services between the users (including, residential, SME users, and enterprise private line customers) and the cloud DCs.

Figure 3 shows the relationship between the overall F5G-A network topology and the scope of OCN architecture.