ETSI GS F5G 006 V1.1.1 (2022-09)

Fifth Generation Fixed Network (F5G); End-to-End Management and Control; Release #1

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-006_E2E_MGMT

Keywords
F5G, management

ETSI

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

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

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

Contents

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

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

Foreword

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

Modal verbs terminology

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

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

1 Scope

The present document focuses on the management and control aspects of the F5G End-to-End network architecture ETSI GS F5G 004 [1]. The present document specifies the End-to-End management and control architecture and its related interfaces, including:

- The technical requirements and functional blocks of the domain controllers and the E2E orchestrator in the F5G networks (Customer Premises Network (CPN), Access Network and Aggregation Network);
- The technical requirements and interface parameters of the northbound interfaces of the domain controllers of the Customer Premises Network (CPN), the Access Network, the Aggregation Network, the Core Network, and the E2E orchestrator.

NOTE: The technical requirements and functional blocks of the Core Network Controller is out of scope of the present document. However, it is part of the management architecture and interface.

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] ETSI GS F5G 004 (V1.1.1): "Fifth Generation Fixed Network (F5G); F5G Network Architecture".

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

[3] ETSI GS ZSM 002 (V1.1.1): "Zero-touch network and Service Management (ZSM); Reference Architecture".

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

[5] IETF RFC 8346: "A YANG Data Model for Layer 3 Topologies".

[6] IETF RFC 8944: "A YANG Data Model for Layer 2 Network Topologies".

[7] IETF RFC 8299: "YANG Data Model for L3VPN Service Delivery".

[8] IETF RFC 8466: "A YANG Data Model for Layer 2 Virtual Private Network (L2VPN) Service Delivery".

2.2 Informative references

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

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

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] TM Forum IG1230 (V1.1.0): "Autonomous Networks Technical Architecture".

[i.2] TM Forum IG1218 (V2.1.0): "Autonomous Networks - Business requirements & architecture".

[i.3] TM Forum IG1251 (V1.0.0): "Autonomous Networks - Reference Architecture".

[i.4] ETSI GR F5G 008 (V1.1.1): "Fifth Generation Fixed Network (F5G); F5G Use Cases Release #2".

[i.5] IETF RFC 7926: "Problem Statement and Architecture for Information Exchange between Interconnected Traffic-Engineered Networks".

[i.6] ETSI GR F5G 010 (V1.1.1): "Fifth Generation Fixed Network (F5G); Security; Threat Vulnerability Risk Analysis and countermeasure recommendations for F5G".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI GS F5G 004 [1] and the following apply:

alarm propagation relationship: logical association of a set of correlated alarms

NOTE: The logical association of a set of correlated alarms includes but not limit to derivative association, causal association and time association.

autonomous domains: basic logical business entities to expose network resources/functionalities as services/capabilities in support E2E lifecycle of automated intelligent network/ICT services

NOTE: The definition of this term comes from TM Forum IG1218 [i.2].

autonomous network: system of networks and software platforms that are capable of sensing its environment and adapting its behaviour accordingly with little or no human input

NOTE: The definition of this term comes from TM Forum IG1230 [i.1].

domain: logical collection of network nodes and interconnecting links, including their management and control system. A domain may be further divided into multiple sub-domains

NOTE: In F5G, a domain is a network segment with its domain controller.

event source: the network components where the root alarm event is generated

NOTE: The network components could be a network element or a port.

incident: set of correlated events

intent: formal specification of the expectations, including requirements, goals, and constraints, given to a technical system

NOTE: The definition of this term comes from TM Forum IG1230 [i.1].

network segment: logical collection of network nodes and interconnecting links, grouped based on network technologies or for administration purposes

NOTE: In F5G networks, there are four types of network segments: the Customer Premises Network (CPN), Access Network (AN), Aggregation Network (AggN) and the Core Network (CN).

root alarm event: primary event of the original alarm event(s) that is triggered by the root cause of an incident

root cause: original cause or the critical factor(s) which leads to an incident

3.2 Symbols

Void.

3.3 Abbreviations

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

10G-EPON	10 Gbit/s Ethernet Passive Optical Network
ACTN	Abstraction and Control of TE Networks
AggN	Aggregation Network
AI	Artificial Intelligence
AN	Access Network
API	Application Programming Interface
BOM	Bill Of Materials
CMI	CNC-MDSC Interface
CN	Core Network
CPE	Customer Premise Equipment
CPN	Customer Premises Network
CSN	Commit Sequence Number
DC	Data Centre
E2E	End-to-End
E-O-CPE	Enterprise-OTN-Customer Premise Equipment
EPON	Ethernet Passive Optical Network
FTTR	Fibre To The Room
GEM	GPON encapsulation mode
GOSNR	Generalized Optical Signal-to-Noise Ratio
GPON	Gigabit Passive Optical Network
GRE	Guaranteed Reliable Experience
HGU	Home Gateway Unit
HSI	High Speed Internet
ID	Identifier
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPTV	Internet Protocol Television
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISG	Industry Specification Group
LTP	Link Termination Point

NOTE: See section 3.5 of IETF RFC 8795 [2] for the definition of LTP.

MAC	Media Access Control
MCA	Management, Control & Analytics
MDSC	Multi-Domain Service Coordinator
MDU	Multi-Dwelling Unit
MP2MP	Multi-Point to Multi-Point
MPI	MDSC-PNC Interface
MTU	Maximum Transmission Unit
NBI	Northbound Interface
ODN	Optical Distribution Network
ODU	Optical Data Unit
OLT	Optical Line Terminal
OMCI	ONU Management and Control Interface
ONU	Optical Network Unit
OSNR	Optical Signal-to-Noise Ratio
OTN	Optical Transport Network
OTU	Optical Transport Unit
PNC	Provisioning Network Controller
POL	Passive Optical LAN
PON	Passive Optical Network

QoS	Quality of Service
RFC	Requests for Comments
SAP	Service Access Point
SFU	Single Family Unit
SLA	Service Level Agreement
SME	Small and Medium Enterprises
SMP	Service Mapping Point
SPP	Service Processing Point
TE	Traffic Engineering
TM	Telecommunication Management Forum
TPN	Tributary Port Number
TTP	Tunnel Termination Point

NOTE: See section 3.6 of IETF RFC 8795 [2] for the definition of TTP.

UUID	Universally Unique Identifier
VLAN	Virtual Local Area Network
VOD	Video On Demand
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VR	Virtual Reality
VxLAN	Virtual extensible Local Area Network
WTR	Wait-To-Restore
XC	Cross-Connect
XG-PON	10-Gigabit-capable Passive Optical Network
XGS-PON	10-Gigabit-capable Symmetric Passive Optical Network
YANG	Yet Another Next Generation data modelling language
ZSM	Zero-touch network and Service Management

4 Requirements for E2E management and control of F5G networks

4.1 Motivation

Guaranteed Reliable Experience (GRE) is one of the key dimensions of a F5G network, which enables the business demand of highly sensitive services, high reliability and high availability communication, and high operational efficiency.

To meet the requirements of GRE, the Management, Control & Analytics (MCA) Plane is introduced in the F5G architecture, which is responsible for the management, control and analytics of the E2E F5G networks covering the CPN, AN, AggN and CN.

The present document defines the F5G E2E management and control architecture as a subset of the overall F5G MCA Plane as defined in ETSI GS F5G 004 [1].

4.2 General requirements and management aspects

In the following a general set of management aspects of the F5G E2E management and control system are described.

- E2E service provisioning:

  The F5G network supports a rich set of applications and services traversing multiple network segments. The F5G E2E management and control system shall support the instantiation, configuration and maintenance of these F5G E2E services, including their creation, modification and termination, and supporting the automation of the corresponding workflows.

- Efficient network operation:

  The F5G network improves the efficiency of the network operation by an intelligent E2E management and control system. The key requirements of this intelligent E2E management and control system include:

  - Network resource visibility: The F5G E2E management and control system shall support the necessary functionality to provide the F5G network resource information to the network administrators. This improves the efficiency for the network operators to operate and manage their networks. Additionally, the system should support the visualization of the information at a high-level of abstraction for administrators to see important system aspects.

  - Intelligent fault management: The F5G E2E management and control system shall support intelligent root cause analysis and alarm correlation analysis, which provides effective guidance to the network operators for accurate troubleshooting. The management and control E2E management and control system shall also support proactive fault management to identify and eliminate potential risks in advance.

- Interoperability:

  In the F5G network, different network segments may be from different vendors. The F5G E2E management and control system shall support the collaboration and orchestration of the domain controllers for different network segments. This is achieved through open interfaces between the E2E orchestrator and each domain controller.

5 Architecture of E2E management and control of F5G network

5.1 Design principles

TM Forum IG1251 [i.3] defines the methodology, general principles, and the high-level business and technical architecture of Autonomous Networks. The present document specifies he E2E management and control architecture as an "Autonomous F5G Network", which enables the self-configuration, self-healing, self-optimizing and self-evolving of F5G resources and services with less human intervention.

The design principles for this management and control architecture include:

- Autonomous domain:

  Each of the F5G domains, the CPN, the AN and the AggN (together with the management and control system of that domain) are considered an autonomous domain. This enables the support of F5G E2E services.

- Intent-driven:

  Intent defines what is expected to be achieved but leaves the details of how the network is deployed and operated to the autonomous domain. In the F5G E2E management and control system, the interfaces exposing to the E2E Orchestrator the resources/functionalities of each autonomous domain shall be designed in an "intent" style. In this way, each F5G autonomous domain could be treated as a whole, and the E2E management and control system does not need to be aware of the detailed information of each domain.

  The F5G E2E management and control system shall focus on the interaction and orchestration of different autonomous domains through their intent-driven interfaces.

- Closed-loop control:

  Based on the autonomous domain and intent-driven interfaces, it is possible to design the resource and service control closed-loops in the F5G E2E management and control system. The service control closed-loop enables the full lifecycle service operation, while the resource control closed-loop enables the full lifecycle cross-domain and cross-layer resource orchestration.

- Simplicity:

  The concept of "simplicity" is a fundamental principle of network design. For management and control aspects, it means fewer layers, interfaces, and protocols. Intelligent and automatic mechanisms enable simplicity. In the F5G network, the E2E management and control system shall be designed hierarchically and includes intelligent components to simplify the architecture.

5.2 Hierarchy architecture overview

5.2.1 F5G E2E management and control architecture

ETSI GS ZSM 002 [3] defines the End-to-End network and service management framework for multi-domain, multi-technology and multi-layer networks with hierarchical service management domains. The management and control of F5G networks is an instance of the ZSM architecture applied to optical communication networks.

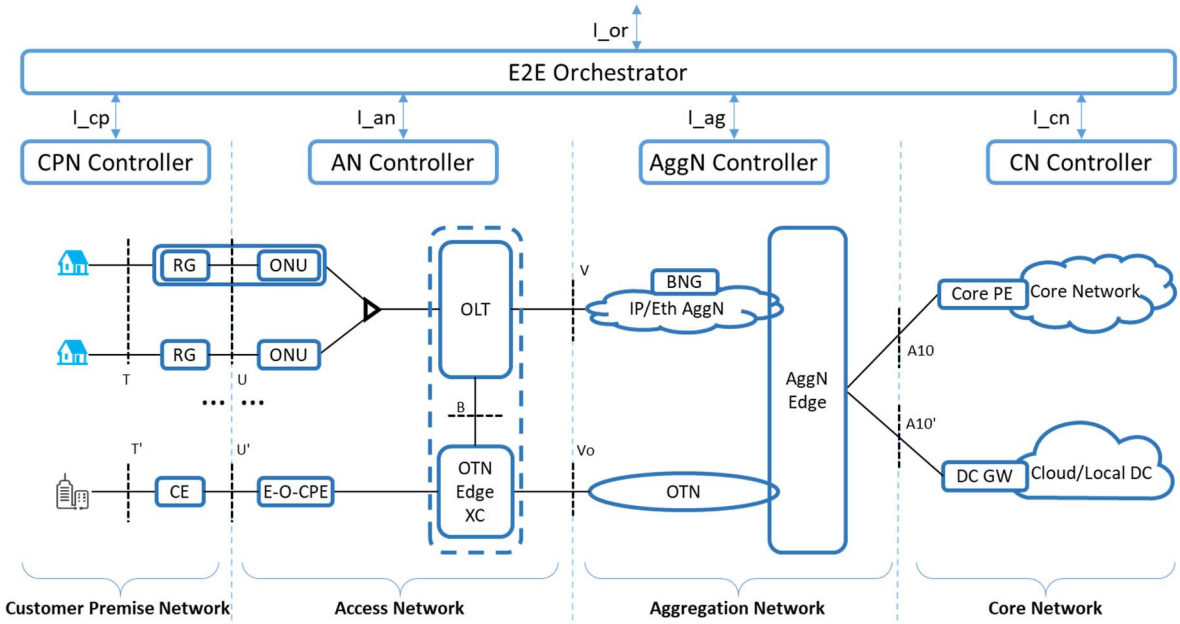

Figure 1: F5G E2E management and control architecture

Figure 1 shows the F5G E2E management and control system architecture, which adds hierarchical controllers and an orchestrator to the F5G network topology defined in ETSI GS F5G 004 [1]. Note that all the controllers and the orchestrator in this architecture are logical functional blocks, which are not necessarily physical controllers in the network.

A domain controller is introduced for each F5G network segment:

- Customer Premises Network Controller (CPN Controller): Used to manage and control the CPN. The CPN Controller could be deployed within the CPN or in a remote location. In the remote deployment case, the management and control of the CPN is the responsibility of the network operator.

- Access Network Controller (AN Controller): Used to manage and control the Access Network, including OLTs, ODNs and associated ONUs. The AN Controller function includes management and control of the Underlay Plane (PON network) and the SAP, SPP and SMP in the Service Plane of the Access Network.

- Aggregation Network Controller (AggN Controller): In F5G, both IP/Ethernet network and OTN are possible options for the Aggregation Network, and both types of Aggregation Networks can co-exist. The AggN Controller is used to control different types of Aggregation Networks, and provides the resource and services orchestration function for both IP/Ethernet and OTN.

- Core Network Controller (CN Controller): The CN Controller controls the Core Network and may or may not control the Cloud/Local Data Centre. The CN Controller is outside the scope of the present document, but the interface I_cn on the northbound interface of the CN Controller is still in the scope, which is needed for E2E service provisioning.

The E2E Orchestrator interacts with each domain controller through the I_cp, I_an, I_ag and I_cn interfaces and performs the resource and service orchestration functions as follows:

- E2E resource orchestration function: this function mainly focuses on the orchestration of the F5G Underlay Plane. This function includes collecting the (abstracted) topology, resource and status information, triggering the creation of tunnels in each network segment, resource optimization across multiple network domains, identification and location of network failures, analysis of status change and prediction of failures.

- E2E service provisioning function: mainly focusing on the management and control of the F5G Service Plane. The E2E Orchestrator configures the SAP, SPP, and SMP for service access, service processing, and service mapping into respective tunnels to automatically enable the creation, activation, modification, and deletion of services. The E2E Orchestrator monitors the performance of the services, and takes necessary actions when service degradation occurs, according to the SLAs of the services.

5.2.2 Relationship with ZSM architecture

Figure 2 illustrates the mapping relationship between the F5G management and control architecture and the ZSM architecture defined in ETSI GS ZSM 002 [3].

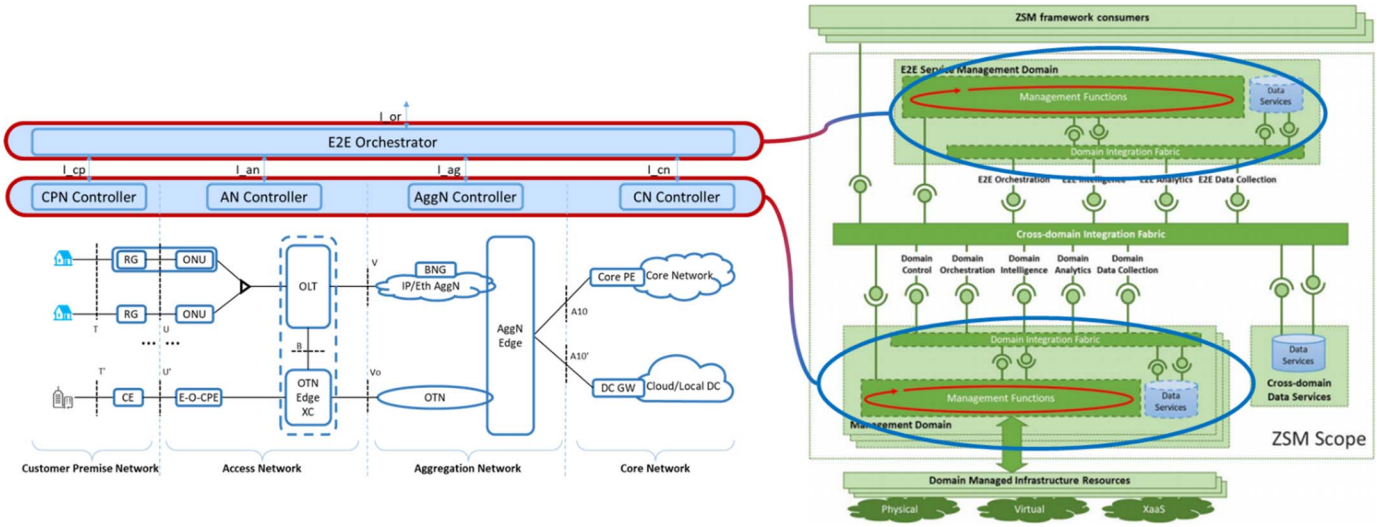

Figure 2: Relationship between the F5G E2E management and control architecture and the ZSM architecture

In ZSM architecture (ETSI GS ZSM 002 [3]), each management domain manages one or more entities, such as infrastructure resources and/or resource-facing services associated with the management domain. The F5G domain controllers, the CPN Controller, the AN Controller, the AggN Controller and the CN Controller, are equivalent to the entities of the ZSM Management Domains.

The E2E service management domain is a special management domain that provides End-to-End management of customer-facing services, composed from the customer-facing or resource-facing services provided by one or more management domains. The F5G E2E Orchestrator is an equivalent to an instance of the ZSM E2E Service Management Domain, which manages the F5G E2E services across multiple domains.

The management functions of the F5G E2E Orchestrator and the domain controllers are described in clause 6 of the present document.

5.3 Service Management Processes

5.3.1 Overview

The ETSI ISG ZSM architecture defines the general processes of cross-domain E2E service lifecycle management (covering the fulfilment and assurance processes) and describes the interactions between the E2E service management domain and the underlying management domains during these processes. This clause specifies the processes of service fulfilment and service assurance in the context of F5G.

Note that the error conditions of the service provisioning processes are not included below and are for further study.

5.3.2 F5G service fulfilment

5.3.2.1 Overview

The fulfilment of F5G services includes the processes of service instantiation, service activation, service modification, service deactivation and service decommissioning.

5.3.2.2 Service instantiation:

a) The E2E Orchestrator receives the E2E service instantiation request from the customer management system.

b) The E2E Orchestrator determines the performance requirements of the service and the policies to instantiate the service.

c) The E2E Orchestrator communicates with each domain controller associated with the service instantiation to perform a feasibility check. The feasibility check evaluates whether the service performance can be satisfied based on the current state of its domain network.

d) The E2E Orchestrator communicates with each domain controller associated with the service to instantiate the service instances in their respective domain networks. Depending on the service instantiation policies and the current network state, one of the following steps may be executed for each domain:

- To create a new service instance in a domain. That domain controller allocates the resource for the service instance in its domain. The path segment for the service instance of that domain in the Underlay Plane may be created at this stage or later when activating the service instance.

- To re-use an existing path segment instance in the domain shared by multiple E2E service instances. An existing path segment instance may be re-configured to increase its capacity for the new service request. For example, in the OTN AggN domain, an OTN container carries multiple E2E service instances from different CPNs. In the case of a new service request, an existing OTN container needs to be reconfigured.

e) Each domain controller communicates its updated topology/inventory information to the E2E Orchestrator.

f) The E2E Orchestrator creates a service instance in its database.

NOTE: The action f) may occur in at any stage in the aforementioned sequence.

5.3.2.3 Service activation

a) The E2E Orchestrator receives the service activation request from the customer management system.

b) The E2E Orchestrator communicates with each domain controller associated with the service to activate the service instance within its domain. The domain controller may activate the path of the service instance within its domain in the Underlay Plane, if it has not already been activated. The domain controllers at both ends of the path for this service instance may also configure the admission control in the Service Plane, to allow the customer's traffic to be adapted and carried by the service instance.

c) Each domain controller communicates its updated topology/inventory information to the E2E Orchestrator.

d) The E2E Orchestrator changes the state of activation of the E2E service instances in its database where the state of the E2E service instances are maintained, if all related domain controllers succeed in activating the service instances within its domains.

Note that service instantiation and activation processes may be merged, which means that the service is activated immediately when it is instantiated.

5.3.2.4 Service Modification

a) The E2E Orchestrator receives the service modification request (e.g. a request to change the Service Level Agreement (SLA) of the E2E service) from the customer management system.

b) The E2E Orchestrator may communicate with each domain controller associated with the service to perform a feasibility check. The feasibility check evaluates whether the service modification can be fulfilled based on the current state of its network domain.

c) The E2E Orchestrator communicates with each domain controller associated with the service to modify the service instance within its domain. For example, to modify the bandwidth, the route or the recovery scheme of the service instance.

d) Each domain controller communicates its updated topology/inventory information to the E2E Orchestrator after modifying its service instance.

e) The E2E Orchestrator updates the service instance in its database.

5.3.2.5 Service Deactivation

a) The E2E Orchestrator receives the service deactivation request from the customer management system.

b) The E2E Orchestrator communicates with each domain controller associated with the service to deactivate the service instance within its domain. When the domain controllers are deactivating this E2E service, it should not raise any unnecessary alarms in the E2E Orchestrator.

c) Each domain controller deactivates the service instance in its Service Plane. In the Underlay Plane, if the service instance's path was shared with other services, the domain controller shall keep it active. Otherwise, the domain controller may deactivate it in its Underlay Plane at the same time.

d) Each domain controller communicates its updated topology/inventory information to the E2E Orchestrator.

e) The E2E Orchestrator deactivates the E2E service instance in its database, where the state of the E2E service instances is maintained.

5.3.2.6 Service Decommissioning

a) The E2E Orchestrator receives the service decommissioning request from the customer management system.

b) The E2E Orchestrator communicates with each domain controller associated with the service to decommission the service instance. Depending on the service instantiation policies and the current state of its domain network, one of the following steps may be executed for each domain:

- To release the resource allocated to the service instance in its domain and tear down this service instance;
- Decommissioning this service instance in its domain, which was shared with other E2E service instances, the overall capacity maybe decreased.

c) Each domain controller communicates its updated topology/inventory information to the E2E Orchestrator.

d) The E2E Orchestrator deletes the service instance in its database.

Note that the decommissioning of an activated service is allowed, which implies that the processes of service deactivating and decommissioning are merged and executed simultaneously.

5.3.3 F5G service assurance

5.3.3.1 Overview

Service assurance is performed during the lifecycle of the service. It includes performance management and fault management.

For the following clauses, the assumption is that the domain controllers are service-aware.

5.3.3.2 Performance management

a) Once an E2E service is provisioned, the performance of the service shall be monitored. Note that basically the network performance parameters are monitored and is associated with the E2E service. The E2E services performance needs to be assured. A service performance monitoring channel is created between the E2E Orchestrator and each domain controller associated with the service.

b) Each domain controller associated with the service reports the service performance information to the E2E Orchestrator. There are several methods:

- Event notification: The domain controllers report the information about the changes of service performance to the E2E Orchestrator in an event-triggering manner.
- Static subscription: The domain controllers provides service performance information regularly streamed to the E2E Orchestrator. The types of service performance information to be reported are statically configured in advance.
- Dynamic subscription: The E2E Orchestrator dynamically initiates a request for specific service performance information. The domain controllers stream the requested service performance information to the E2E Orchestrator after the subscription.

c) The E2E Orchestrator performs a service performance analysis based on the received service performance information. If a performance issue is detected, the E2E Orchestrator may attempt to resolve the issue by reconfiguring the service (see the process of "service modification" in clause 5.3.2). If the E2E Orchestrator fails to resolve the issue, it may notify the customer management system of a service quality degradation.

5.3.3.3 Fault management

When failure occurs in a given network domain affecting a set of services, the network equipment in that network domain shall trigger a recovery process in its domain, if the recovery scheme is configured and enabled in advance. For example, 1+1/1:1 protection or rerouting in the OTN, and Type B or Type C protection in the PON. This is the fastest way to recover the services from network failure.

If a network domain fails to recover the services, its domain controller reports the failure information to the E2E Orchestrator. The E2E Orchestrator may attempt to reconfigure a set of related domain controllers (may be different from the set of domain controllers related to the original service) to recover the E2E service. If the E2E Orchestrator still fails to recover the E2E service, it may send a service failure notification to the customer management system.

6 Domain Controllers and E2E orchestrator

6.1 Customer Premises Network Controller

Various technologies can be adopted in the CPN, depending on the end-user requirements. For example, Wi-Fi 6 and FTTR can be used for home broadband users, POL can be used in business areas or campus to support high bandwidth business services, and OTN technology can be used in the CPE for enterprises requiring high-quality private line or VPN services.

The CPN Controller is a logical functional block used to manage and control the various types of CPN. The detailed technical requirements and functions of the CPN Controller are for further study.

6.2 Access Network Controller

6.2.1 Overview of PON Access Network Controller

The Access Network Controller is used to manage and control the Access Network, including the OLT, the ODN and the ONU. Figure 3 shows an overview of the Access Network Controller.

In the present document, the assumption is that the Access Network is PON, and therefore the Access Network Controller is PON specific.

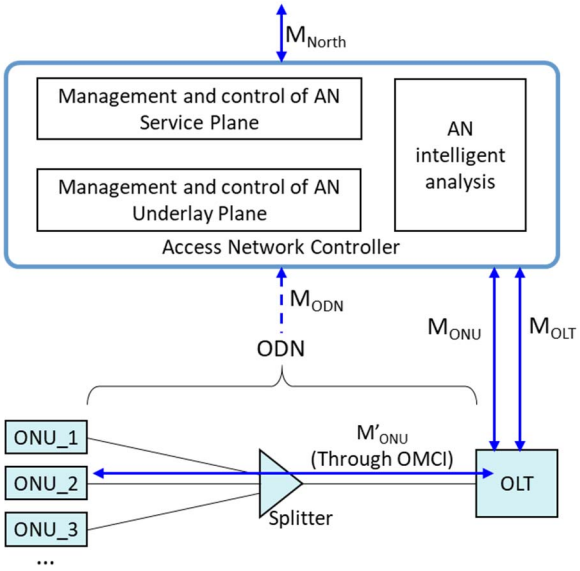

Figure 3: Overview of the PON Access Network Controller

The Access Network Controller shall support the interaction with the Access Network equipment and the E2E Orchestrator, for the management and control purposes. Such interactions include:

- M_{OLT}: The management interface to the OLT, which manages the OLT directly.
- M_{ONU} and M'_{ONU}: The management interface to the ONU. Since the ONU is located in the CPN, the Access Network Controller will indirectly manage and control the ONUs through the corresponding OLT (M_{ONU}) and the ONU Management and Control Interface (OMCI) between the OLT and the ONU (M'_{ONU}).
- M_{ODN}: The indirect management interface to the ODN. Since the ODN is passive, there is no direct management communication channel between the ODN and the Access Network Controller. The Access Network Controller shall obtain the ODN information (information from ODN deployment and information derived from ODN measurements), via other sources. The digitalized ODN as described in ETSI GR F5G 008 [i.4] may be deployed to enable the management of the ODN by the Access Network Controller.
- M_{North}: The management interface for the PON access network. The Access Network Controller interacts with the E2E Orchestrator, to enable the E2E network and service management and control.

NOTE: M_{North} is the PON access network specific interface, for other access network technologies an equivalent to M_{North} does exist. I_an is the interface between the E2E orchestrator and all the Access Network Controllers. M_{North} is a subset of the I_an.

The Access Network Controller is responsible for:

- Management and control of the Access Network Underlay Plane:
  - Maintaining the topology and the inventory of the Underlay Plane of the Access Network, including the OLT, the ODN and the ONU.
  - Configuration of the OLT and the ONU for the provisioning of broadband connections and PON slices.

- Management and control of the Access Network Service Plane:
  - Lifecycle management of the service-oriented slices.
  - Lifecycle management of the broadband application services within the Access Network.
- The Access Network Controller performs the Access Network intelligent analysis based on the network information (e.g. topology and resource information, network and service status information, and network configuration information) collected from the Access Network dynamically. The Access Network intelligent analysis includes:
  - Fault monitoring and troubleshooting.
  - Service performance monitoring and optimization.
  - Identification of potential high-value services.

The key functions of the Access Network Controller are described in the following clauses.

6.2.2 ODN management

The Access Network Controller plays an important role in the enabling of the management and control of the ODN topology and resources.

Digitalized ODN is one of the F5G use cases described in ETSI GR F5G 008 [i.4], which allows the network operators to identify and accurately record the ODN resources and manage the ODN. The Access Network Controller shall support the following functions if a digitalized ODN is deployed:

- Receiving the scanned digital label and the related location information.
- Automatically identifying and maintaining the ODN topology and the fibre resources based on the received digital label and location information.
- Displaying the ODN topology and the fibre resource usage information for the purposes of visibility and manageability.
- Reporting the ODN topology and fibre resource usage information to the E2E Orchestrator.
- Performing user service provisioning based on the fibre resource usage information.

For compatibility consideration, the Access Network Controller shall support importing the ODN information from the ODN databases that are maintained by the network operator, if the digitalized ODN is not supported.

6.2.3 Access Network slice management

ETSI GR F5G 008 [i.4] describes the scenario based broadband use case, including the home broadband applications (e.g. gaming, education and home office) and the small and medium enterprise broadband applications (e.g. PON leased line). Different broadband applications may require different network performances. E2E network slicing is one of the key technologies to ensure the experience of those high-value broadband applications.

The Access Network Controller is used to manage and control Access Network slicing, as a part of the E2E network slicing. It shall support the following functions:

- Access Network slice planning: The Access Network Controller plans the Access Network slices (e.g. resource allocation and resource isolation/sharing policies among different Access Network slices), or it imports the planning result from network planning tools.
- Creation of an Access Network slice instance:
  - Providing the E2E Orchestrator with an interface for the creation of an Access Network slice instance. An intent-driven API may be used in this interface.

  - Assigning bandwidth resources on both the OLT PON ports and the OLT uplink interfaces for an Access Network slice instance. For example, the traffic mapping on the PON port may be identified by VLAN IDs, and the traffic of the uplink interface may be identified by a VLAN ID or a VxLAN ID, or be an ODU ID, depending on the network type used in the AggN.
  - The ONU PON slice configuration is managed and controlled by the Access Network Controller.
  - Configuring the bandwidth resources on both the PON ports (on both ONU and OLT) and the uplink interfaces for the Access Network slice instance.

- Service activation for the users in the Access Network slice:
  - Providing the E2E Orchestrator with an interface for the provisioning of broadband application. An intent-driven API may be used in this interface.
  - Configuring the application traffic profiles on the ONU, so that the traffic of different broadband applications can be identified.
  - Configuring the mapping of the application traffic into the Access Network slice, e.g. by assigning a VLAN ID and a GPON Encapsulation Mode (GEM) port on the ONU and OLT port, so that the identified application traffic can be steered to the right Access Network slice instance.

NOTE: The Access Network Controller cannot configure the ONU directly, but will configure the OLT through the M_{ONU} interface and then the OLT configures the ONUs through the M'_{ONU} interface (e.g. OMCI).

- Access Network slice maintenance, monitoring and optimization:
  - Maintaining and displaying the information of the created Access Network slice instances, and the status of the services carried by the corresponding Access Network slice instances, for the purposes of visibility and manageability.
  - Reporting the status of the Access Network slice and services carried by the Access Network slice to the E2E Orchestrator, so that the E2E Orchestrator can manage the E2E network slices and services carried by the corresponding Access Network slice.
  - Monitoring the performance of the services in the Access Network slice, and optimizing the resource allocation of the Access Network slice when necessary, to satisfy the qualities of the services.
- Service deactivation in the Access Network slice: when a service is terminated, the Access Network Controller may configure the Access Network slice to deactivate the service.
- Access Network slice decommissioning: the Access Network Controller removes an empty Access Network slice.

6.2.4 Fault monitoring and troubleshooting

In a purely alarm-based fault monitoring and troubleshooting approach, without the support of the alarm correlation analysis and root cause analysis, a single fault in the access network may result in a large number of alarms reported. The administrators cannot accurately dispatch trouble tickets and handle network faults in a timely fashion.

In an incident-based fault monitoring and troubleshooting approach, a set of correlated events are defined as an "incident". The correlated events include alarms, performance indicator statistics, and configuration change. The events are correlated when they occur synchronously or sequentially within a certain period of time or with other correlation mechanisms. Incidents are relevant if they affect the E2E services or network performance. This significantly reduces the number of the incidents to handle, and can guide the operators to accurately locate and repair the network faults.

Note that, a fault that has occurred or a potential fault (that has not occurred yet) may generate an incident. This allows the Access Network Controller to perform fault analysis and prediction, which enables proactive fault management.

To evolve towards an autonomous access network, the Access Network Controller shall support the incident-based fault monitoring and troubleshooting, including the following functions:

- Collecting the network event information (e.g. equipment and network fault information, and service performance information) from the access network equipment. Telemetry or other methods may be used for this collection.

- Identifying an incident (may be a fault or a potential fault) from a set of received network events:
  - Determine the faults
  - Predict potential faults
- Fault analysis and diagnosis:
  - Analyse the event source(s)
  - Analyse the root cause of event source(s)
  - Analyse which access network components or services have been or may be affected by the incident
- Recovery procedure: Provide the identified fault information to the network operator to recover from the fault, or to prevent a potential fault. Such fault information includes:
  - Fault type, such as fibre degradation, hardware failure, or software error
  - Fault (measured or estimated) occurrence time
  - Fault severity

AI technologies may be used by the Access Network Controller to perform incident identification, fault prediction, fault analysis and diagnosis.

In the example shown in Figure 4, the Access Network Controller receives multiple alarm events and optical performance information from the OLT, and determines that the source of the alarm events is Port_2 of the OLT. The Access Network Controller further determines that the root cause of the fault is on the fibre between Splitter_2 and Splitter_2.2 (e.g. fibre damaged or fibre connectors disconnected). As illustrated in Figure 4, it will affect the user traffic on ONU_9 to ONU_16. The Access Network Controller then advices the network operator to check and repair the related fibre and fibre connectors.

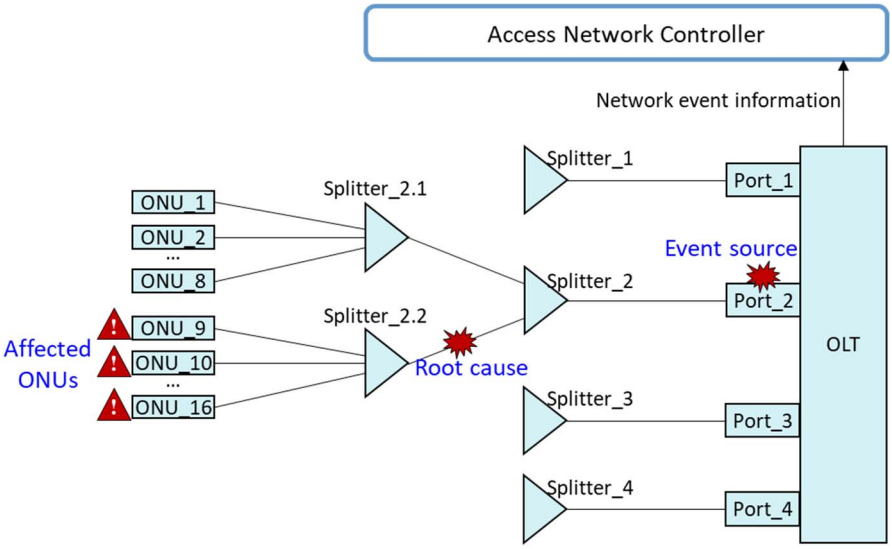

Figure 4: Example of incident-based fault monitoring and troubleshooting

6.3 Aggregation Network Controller

6.3.1 Overview of Aggregation Network Controller

In F5G, the aggregation network is composed of IP/Ethernet network and OTN. F5G services are carried over either technology in the aggregation network. The technology choice is up to the network operator and its service requirements.

The Aggregation Network Controller may be an IP/Ethernet Controller, or an Optical Transport Controller, or both depending on the type of network deployed in the Underlay Plane.

6.3.2 Optical Transport Controller

6.3.2.1 Overview of Optical Transport Controller

The Optical Transport Controller is used to manage and control the OTN network elements within the OTN AggN. The OTN Edge XC may be managed and controlled by the Optical Transport Controller or by the Access Network Controller, depending on the deployment of the OTN Edge XC. The Optical Transport Controller and the Access Network Controller coordinate via the E2E Orchestrator.

The Optical Transport Controller should be aware of the complete OTN AggN information, including the edge links connecting the OTN AggN to other network domains (via the interfaces Vo and A10', as shown in Figure 5). The Optical Transport Controller may also be aware of the OTN Edge XC and the interface B connecting the OTN Edge XC to the OLT.

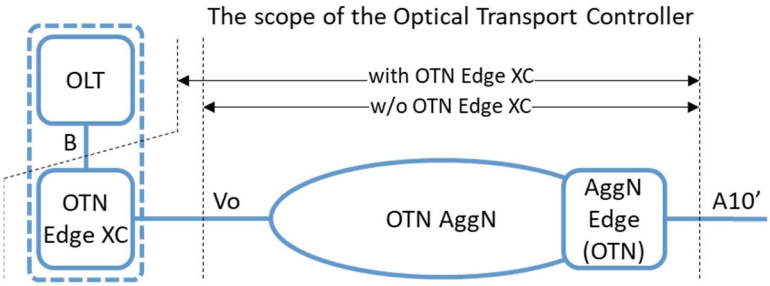

Figure 5: The scope of the Optical Transport Network

The Optical Transport Controller should manage and control the OTN network (which may or may not include the OTN Edge XC), including its Underlay Plane and Service Plane.

For different types of services, OTN connections may start and end at different nodes inside or outside the OTN AggN. There are three cases:

1) The OTN network connection starts and ends inside the OTN AggN.

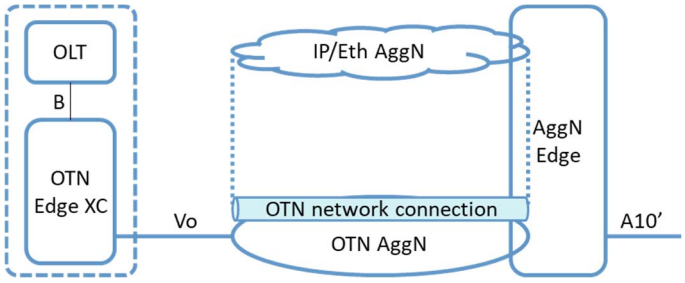

Figure 6: Case 1 - OTN connection inside OTN AggN

In this case, the service connections are carried by the IP/Ethernet flows, and one or multiple IP/Ethernet flows with the same source and destination in the IP/Ethernet AggN are aggregated and transparently carried by one or more OTN connection(s).

The Optical Transport Controller manages and controls the complete OTN connection(s) in the OTN AggN and interworks with the IP/Ethernet Controller for multi-layer network control across the OTN and the IP/Ethernet network. The Optical Transport Controller is unaware of the service connections in the IP/Ethernet flows in the Service Plane.

2) The OTN network connection is between the OTN Edge XC and the AggN Edge node.

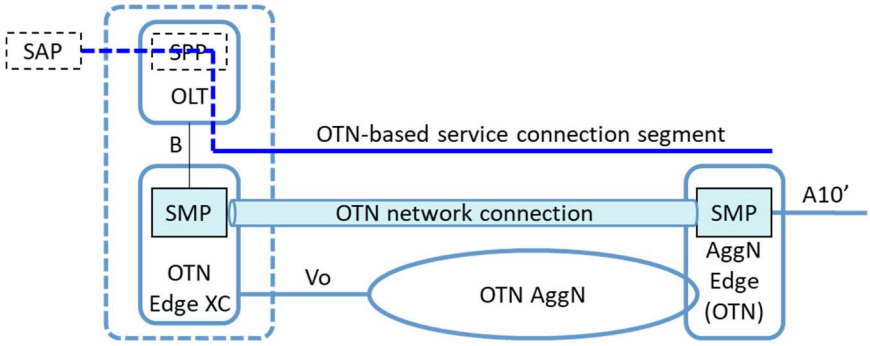

Figure 7: Case 2 - OTN connection between Access Network and AggN Edge

The use case for premium home broadband into multiple clouds (ETSI GR F5G 008 [i.4]) uses this approach. Multiple users' service connections from the same OLT going to the same AggN Edge may be aggregated at the OLT and may be mapped to different OTN connection(s) at the OTN Edge XC in the Access Network.

If the OTN Edge XC is managed and controlled by the Optical Transport Controller, the complete OTN connection(s) in the OTN AggN in the Underlay Plane, and the source and destination SMPs of the OTN-based service connection(s) in the Service Plane, are controlled directly by the Optical Transport Controller.

If the OTN Edge XC is managed and controlled by the Access Network Controller, which needs to interwork with the Optical Transport Controller (via the E2E Orchestrator) to manage and control the E2E connection in the Underlay Plane and the source and destination SMPs of the service connection in the Service Plane. The Optical Transport Controller is used to manage and control the OTN connection segment inside the OTN AggN in the Underlay Plane, as well as the OTN-based service connection segment inside the OTN AggN in the Service Plane.

3) The OTN connection starts at the CPN node (e.g. at the E-O-CPE in the Premium Private Line scenario (ETSI GR F5G 008 [i.4]) and ends at the AggN Edge node.

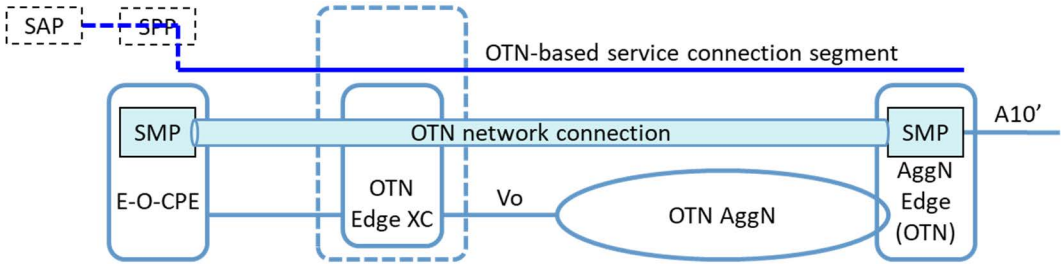

Figure 8: Case 3 - OTN connection between CPE and AggN Edge

For the Underlay Plane, the Optical Transport Controller is used to manage and control the OTN connection segments inside the OTN Access and AggN, and may interwork with the CPN Controller and Access Network Controller (via the E2E Orchestrator) to manage and control the E2E OTN connection.

For the Service Plane, the Optical Transport Controller is used to manage and control the OTN-based service connection segments inside the OTN Access and AggN, and may interwork with the CPN Controller (via the E2E Orchestrator) to manage and control the source and destination SMPs of the OTN-based service connection.

6.3.2.2 Multi-domain OTN AggN

The OTN AggN may be composed of multiple domains. One scenario is when, the user of the service and the Data Centre, which provides the service, may be located in two different cities. Therefore the OTN AggN contains at least three domains: the two Metro OTN domains where the user and the Data Centre are located, and the backbone OTN domain that connects the two Metro OTN domains. In this case, a multi-domain control system is used to control the multiple OTN domains. The multi-domain control system is treated as a logical Optical Transport Controller as illustrated in Figure 9. The internal multi-domain control procedures are out of the scope of the present document.

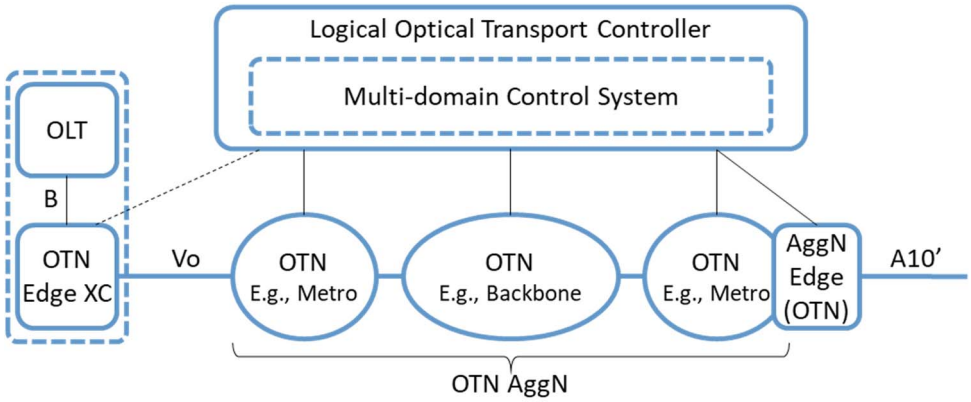

Figure 9: Logical Optical Transport Controller for multi-domain OTN network

6.3.2.3 Relationship with ACTN

In IETF, the ACTN architecture is defined in IETF RFC 8453 [4] for multi-domain, multi-technology network management and control, as illustrated in Figure 10.

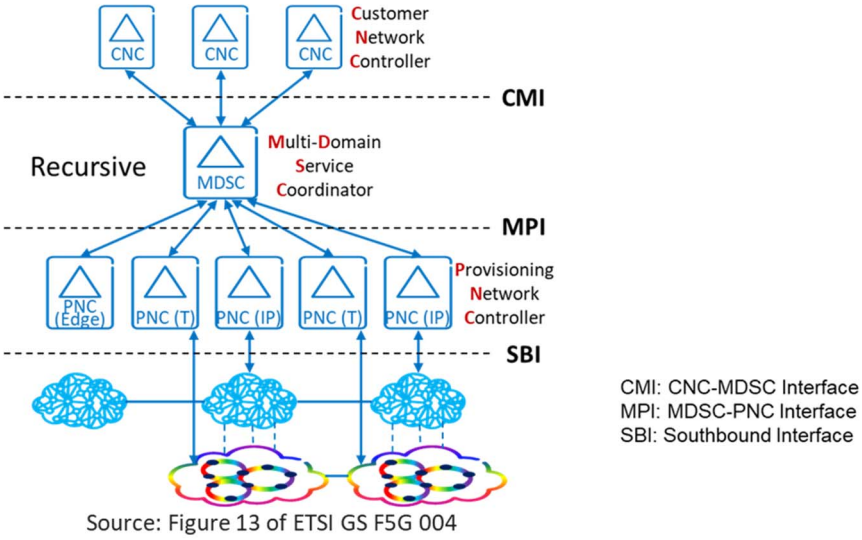

Figure 10: ACTN architecture

In the ACTN architecture, the Provisioning Network Controller (PNC) is introduced as a domain controller for different types of network domains, including the OTN domain. The Multi-Domain Service Coordinator (MDSC) is introduced for the coordination among different domains. The interface between the PNC and the MDSC is the MPI, and the MDSC northbound interface is the CMI. The ACTN architecture supports the management and control of OTN networks.

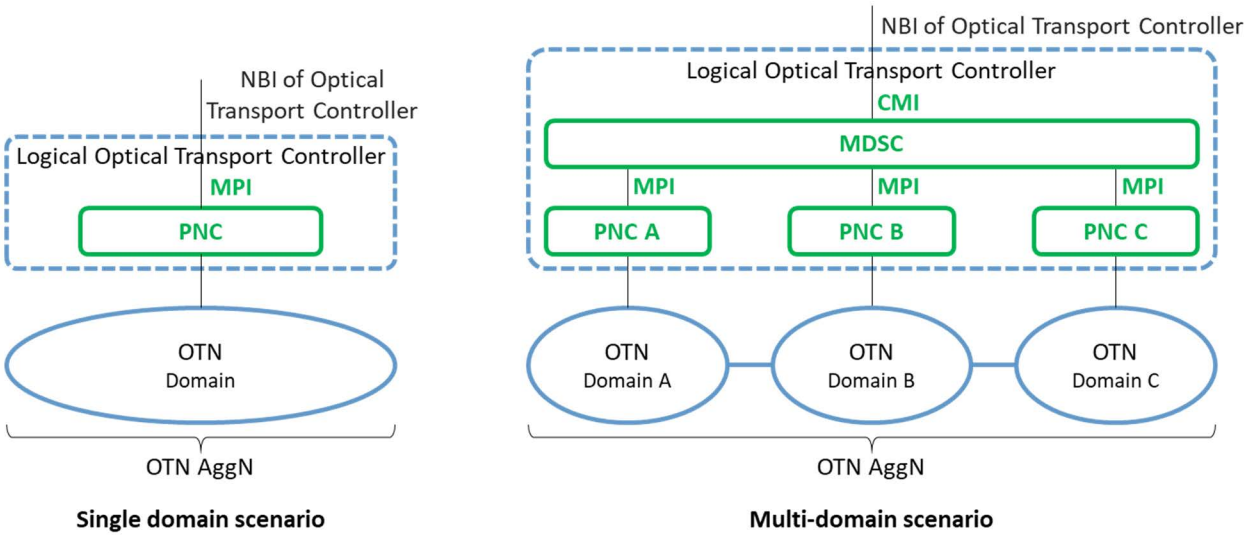

Figure 11: Relationship between the Optical Transport Controller and the ACTN architecture

Figure 11 shows the relationship between the Optical Transport Controller and the ACTN architecture in both single-domain and multi-domain scenarios.

In a single-domain scenario, the PNC performs the same functions as the Optical Transport Controller, which is used to control a single-domain OTN network. The MPI performs the same functions as the NBI of the Optical Transport Controller in F5G.

In the multi-domain scenarios, the MDSC is used to coordinate multiple OTN domains (each controlled by a PNC). The complete ACTN hierarchical controller system, including the MDSC and the PNCs, is treated as a logical Optical Transport Controller. The CMI performs same functions as the NBI of the Optical Transport Controller in F5G.

6.3.2.4 Management and control of the OTN Underlay Plane

In the Underlay Plane, the Optical Transport Controller should support the following functions:

1) Maintenance of the optical network topology information:

   The Optical Transport Controller should be able to collect and maintain the OTN network topology and update the topology information according to the changes of the network (e.g. due to network failures or creation/deletion of connections, etc.).

   The OTN AggN topology is maintained by the Optical Transport Controller including the OTN nodes, the links interconnecting the OTN nodes, and the edge links. The edge links are connections to other network nodes outside of the OTN AggN (The OTN Edge XC may or may not be included in the AggN). The edge links are either OTN or IP/Ethernet links. For example, the OTN AggN and the Access Network via the Vo interface is an OTN link and the link connecting the OTN AggN and the DC gateway via the A10' interface is an IP/Ethernet link.

   The OTN topology information includes:

   a) Basic node and link topology information.

   b) Traffic Engineering (TE) information, for example, the network resource information of each link.

   c) Performance information such as link latency information.

2) Control and Maintenance of OTN connections:

   The Optical Transport Controller creates, modifies or deletes OTN AggN connections or connection segments. The Optical Transport Controller creates, modifies, or deletes OTN cross-connections at each OTN node along the path. The Optical Transport Controller controls the nodes either in a centralized way or using an OTN distributed signalling mechanism.

The Optical Transport Controller should maintain the information of the connections or connection segments for the complete lifecycle of these connections or connection segments. The information about connections or connection segments include the connection identification, bandwidth information and performance information such as connection latency.

3) Path computation and evaluation:

The Optical Transport Controller performs the OTN path computation between a pair of OTN AggN nodes (may or may not include the OTN Edge XC) so that the E2E Orchestrator can perform the E2E Underlay Plane path computation across multiple network domains.

The Optical Transport Controller evaluates the performance (e.g. the latency) of the computed OTN path or segment. The E2E Orchestrator can evaluate whether the computed E2E Underlay Plane path can satisfy the SLA.

4) OTN AggN abstraction:

The Optical Transport Controller shall support the mechanism to provide an abstracted view of the OTN AggN to the E2E Orchestrator. According to the definition of abstraction in IETF RFC 7926 [i.5], the OTN AggN abstraction is the process of applying a policy to the available OTN-TE information to produce selective information. That makes it simpler for the E2E orchestrator to make connections across several networks. There may be different granularities of OTN AggN abstraction:

- No abstraction: all details of the OTN topology are presented to the E2E Orchestrator.
- Complete abstraction: the entire OTN AggN is abstracted as a single abstracted node. The access links of the OTN AggN are presented as the ports of the abstract node.
- Partial abstraction: a partial and incomplete view of the OTN AggN, and a finer granularity compared to complete abstraction. The OTN AggN contains multiple OTN AggN sub-domains, which are presented as individual abstracted nodes. The inter-sub-domain links are presented as the abstracted links between different pairs of abstracted nodes.

By performing the OTN abstraction, the E2E Orchestrator maintains a simplified OTN AggN information. Removing unnecessary data significantly reduces the compute and communication load during the information collection and network service planning and delivering. This allows the E2E Orchestrator to treat the OTN AggN as an autonomous domain and to manage the OTN AggN in an intent-based approach. This requires the northbound interface (I_ag) of the Optical Transport Controller to support an intent-based approach.

The Optical Transport Controller shall support the following functions:

- Provide the E2E Orchestrator with the information that represents the OTN topology in accordance with the abstraction policies of its administrator.
- Maintain the mapping relationship between the physical OTN AggN topology resources and the abstracted topology resources.
- Update the abstracted topology based on changes of the physical OTN AggN topology by adding, modifying, or deleting specific abstracted nodes or links and remapping their corresponding physical topology resources.

5) OTN AggN slicing:

The Optical Transport Controller shall create OTN AggN slices for different F5G services. An OTN slice is a logical network that serves specific service types (e.g. for industrial users) on a shared Underlay Plane infrastructure. Each slice can be flexibly defined with its logical topology to meet the differentiated requirement of the services, such as large bandwidth, ultra-low latency, and massive number of connections.

The Optical Transport Controllers shall interact with the E2E Orchestrator to support planning, deployment, maintenance and optimization of the different slices. Slice planning determines slice resources based on the client access points, bandwidth and delay requirements. Slice deployment creates virtual interfaces, virtual links, virtual nodes and tunnels to form the OTN slice. Slice maintenance includes traffic maintenance, link status and service quality in the OTN slice. Slice optimization is the process of adjusting the OTN slice's resources to optimizing the use of the physical OTN resources in the Underlay Plane.

6) OTN AggN analysis:

The Optical Transport Controller shall be able to monitor, analyse and diagnose the status of the OTN AggN to eliminate network faults, avoid security risks and improve the OTN performance, including the following aspects:

- Transmission performance analysis: The Optical Transport Controller shall monitor the performance indicators of the optical channels to perform the transmission performance analysis. The Optical Transport Controller adopts specific channel control strategies by analysing the performance indicators of the optical channels to ensure signal quality. Such performance indicators may include the Optical Signal-To-Noise Ratio (OSNR) or the Generalized OSNR (GOSNR).

- Network traffic analysis: The Optical Transport Controller shall monitor and analyse the traffic statistics, topology and bandwidth status of the OTN AggN to perform the network analysis. Telemetry and the traditional monitoring mechanisms may both be used to monitor the OTN network. The Optical Transport Controller adopts traffic control strategies based on the different needs of the E2E Orchestrator and the OTN AggN status. The control strategies include but are not limited to service (e.g. the SLA), path calculation, and survivability (e.g. the type and priority of service protection and restoration).

- Network fault analysis: The Optical Transport Controller shall analyse the services and resources related to alarms reported by the OTN AggN equipment to perform the network fault management. The Optical Transport Controller shall filter and process alarm notifications and analyse alarm correlation to diagnose and locate the OTN AggN faults.

To enable the OTN AggN analysis functions, the Optical Transport Controller may use Artificial Intelligence (AI) technologies to improve the efficiency and performance of the OTN AggN. AI technologies can be applied but not limited to the following aspects:

- The processing and filtering of the OTN AggN status data.

- The analysis and prediction of the OTN AggN resource and traffic changes.

- The implementation of the OTN AggN control strategies.

- The prediction and localization of the OTN AggN faults.

6.3.2.5 Management and control of Service Plane

In the Service Plane, the Optical Transport Controller shall support the following functions:

1) VPN configuration:

A customer may access the network from multiple access points and may need to connect to multiple destinations (for example, multiple Data Centres). In such cases, the service connection in the Service Plane will be a Multi-Point to Multi-Point (MP2MP) connection. VPN technologies can be used for such MP2MP services.

The Optical Transport Controller shall support the configuration of VPN information on the edge of the OTN AggN where the service is mapped/de-mapped to/from OTN. Such VPN configuration on the related edge OTN AggN nodes includes assigning and configuring a VPN ID for each service and assigning a set of physical or virtual ports to this VPN.

An example with two VPNs for two customers is shown in Figure 12. Customer A with 2 sites and customer B with a single site are connecting to two separate Core Networks 1 and 2.

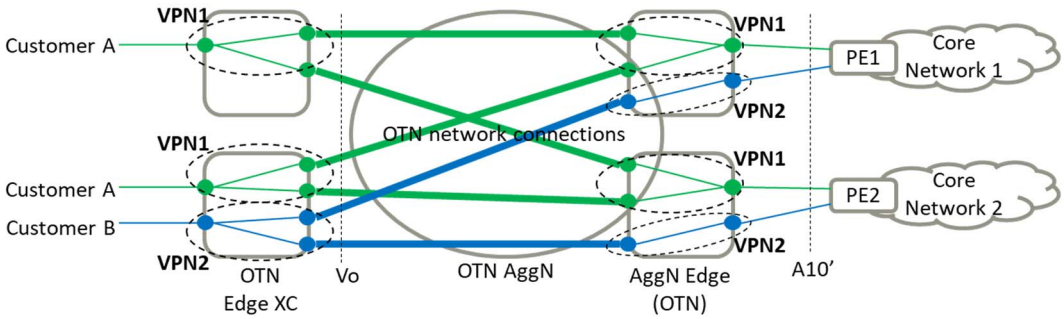

Figure 12: Example VPN configuration

The Optical Transport Controller shall support maintaining the VPN information for the lifecycle of the VPN service.

2) Creation and maintenance of service mapping relationship:

Different service connections are mapped into/de-mapped from different OTN AggN connections at the two ends of an OTN AggN path. This is processed by the SMPs located at the two ends of the OTN AggN path.

At the edge of the OTN AggN the data flow of the service connections shall at least support the identification by VLAN ID and IP/MAC address, but may also support other identifiers. The termination points of the OTN AggN connections are identified by the ODUs within OTU frames, together with the Tributary Port Numbers (TPN) within the OTN end-nodes. The mapping/de-mapping relationship in the SMP includes identifying the service connections, the identification of OTN AggN connections, and the mapping relationship between them.

Figure 13 shows an example where two service connections are mapped into two OTN AggN connections via the SMP functions. The two service connections might be part of a single application with the same service requirements or from different applications with different service requirements. In the latter case, the two OTN AggN connections need different network parameters.

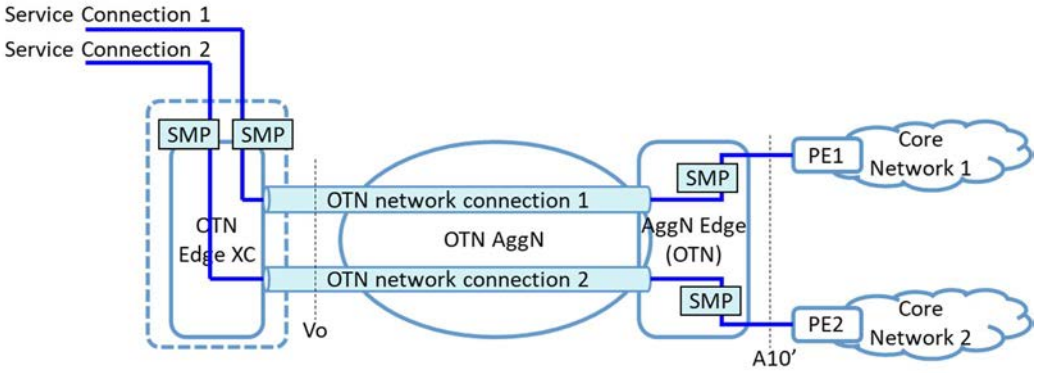

Figure 13: Examples of mapping service connections into OTN network connections

The Optical Transport Controller shall support the coordination with the C2 or C2' control interfaces (see ETSI GS F5G 004 [1]) in the Service Plane to automatically generate the mapping/de-mapping relationship of the SMPs at the two ends of the OTN AggN connections. The specification of the protocols on the C2/C2' interfaces for the mapping relationship creation is out of scope of the present document.

The E2E Orchestrator coordinates with the Optical Transport Controller and either the Access Network Controller or the CPN Controller to match the source and destination SMP configuration. This is because the source SMP may be located at the Access Network or CPN outside the OTN AggN. In contrast, the destination SMP is located at the AggN Edge node inside the OTN AggN.

The Optical Transport Controller shall maintain the mapping/de-mapping relationship between the service connections and the OTN AggN connections for the lifecycle of the service connections.

6.3.3 IP/Ethernet Controller

The IP/Ethernet Controller performs the management and control of the IP/Ethernet Aggregation Network. The key functions of the IP/Ethernet Controller include:

- Monitoring and analysing the network topology and link status.
- Inter-domain IP/Ethernet network management.
- Automatic provisioning of IP/Ethernet bearer tunnel paths.
- IP/Ethernet traffic prediction and accurate capacity expansion planning.

The detailed technical requirements and functions are for further study.

6.4 E2E Orchestrator

6.4.1 Overview of the E2E Orchestrator

The E2E Orchestrator performs the End-to-End orchestration across all F5G network domains. Network orchestration is a process related to the arrangement, coordination, and management of the network infrastructures to provide different services to customers. The E2E Orchestrator manages End-to-End service paths from users to destinations.

Figure 14 shows the E2E Orchestrator management and control system architecture. The E2E Orchestrator interacts with the domain network controllers to achieve the procedures such as service statistics, topology information collection, resource management, and End-to-End service provisioning.

The E2E Orchestrator shall support the following functions:

- Network service management: The E2E Orchestrator shall support the life cycle management of the network services, including but not limited to the creation, modification and deletion of the service templates, and the life cycle management of network service instances.
- Network resource management: The E2E Orchestrator shall maintain a view of the whole network topology and resources (may or may not be in an abstracted form), and perform the resource allocation, configuration, monitoring and releasing for a given service.
- General management: The E2E Orchestrator shall support the collaboration function of multi-domain controllers, and the management of the customer information.

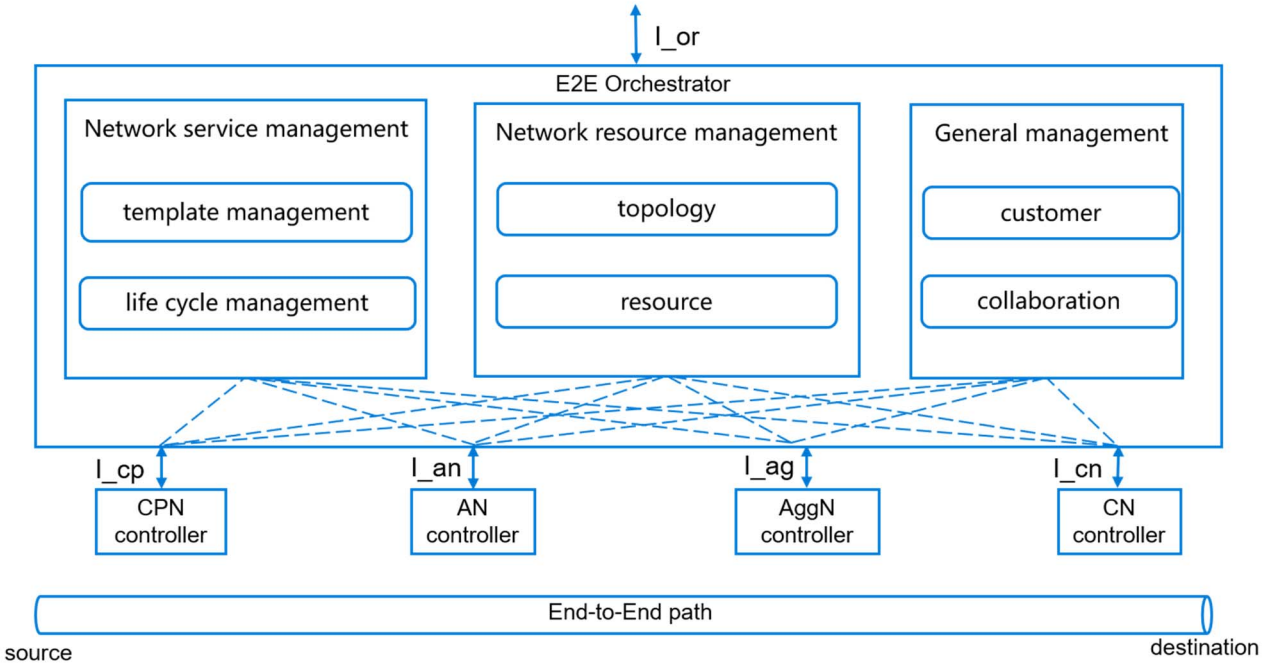

Figure 14: Overview of the E2E Orchestrator

6.4.2 Network service management

The E2E Orchestrator shall support the following functions related to the network service management:

1) Service template management

   The service template is used to parameterize the service information for a certain type of service. A service template contains a customer-facing part and a resource-facing part. The customer-facing part defines a set of parameters with their defined value ranges, which allows the customers to request a service. The resource-facing part maps the customer-facing parameters to the network resource configuration parameters used for network service provisioning.

   The E2E Orchestrator may support the importation, modification and deletion of a service template. The E2E Orchestrator may also support the validation of the customer's service request, and the translation of the customer's service request into the network resource request, according to the related service template.

2) Service life cycle management

   The E2E Orchestrator shall support the full life cycle management of network services, and provide functions for instantiation, activation, modification, deactivation and decommissioning of services. See clause 5.3.2 of the present document.

   The E2E Orchestrator shall support the information collection of the E2E network services from associated domain controllers, and analyse the qualities of the services according to their SLA requirements. See clause 5.3.3 of the present document.

6.4.3 Network resource management

The E2E Orchestrator collaborates and orchestrates with the domain controllers for the E2E network resource management in the F5G Underlay Plane.

1) The E2E Orchestrator shall collect the (abstracted) topology, resource and status information, from each domain controller.

2) The E2E Orchestrator shall instruct each domain controller to create network paths in each network domain.

3) The E2E Orchestrator shall collect the incident information from each domain controller, to evaluate the End-to-End network health status.

4) The E2E Orchestrator shall monitor and analyse the network performance (e.g. traffic load) of each network domain, and may perform resource optimization across multiple network domains.

6.4.4 General management

The E2E Orchestrator shall support the following functions with respect to the general management of the F5G network:

1) Collaborating and communicating with the different domain controllers

   The E2E Orchestrator shall be aware of the capabilities and the status of the each domain controller, and shall maintain the communication channels with each domain controller. This allows the E2E Orchestrator to collaborate with the corresponding domain controllers to perform the network resource and service management.

2) Managing customer information

   The E2E Orchestrator shall maintain the information of the F5G customers (e.g. creation, deletion, and modification of customer information), and shall associate the customer information with the network services and resources.

7 Interface requirements and parameters

7.1 Interface overview

7.1.1 Overview

The I_cp, I_an, I_ag and I_cn interfaces are the Northbound Interfaces (NBIs) of the CPN Controller, the AN Controller, the AggN Controller and the CN Controller, respectively.

Clause 7 of the present document specifies the technical requirements and the key parameters of the technology-specific NBIs of the CPN Controller, the AN Controller, the AggN Controller and the CN Controller, which are used to manage and control the technology-specific network segments (e.g. PON access network, OTN and IP/Ethernet AggN). Each technology-specific NBI is a subset of the I_cp, I_an, I_ag and I_cn.

Clause 7 of the present document also specifies the technical requirements and the key parameters of the I_or interface, which is the NBI of the E2E Orchestrator.

7.1.2 Intent-driven NBIs

The F5G E2E management and control architecture adopts the intent-based management approach on the northbound interfaces of the domain controllers and the E2E Orchestrator. This enables the definition of an autonomous F5G network, which is composed of several autonomous domains.

As defined in TM Forum IG1230 [i.1], the intent-based management approach is the formal specification of the expectation, including requirements, goals and constraints, given to a technical system. The intent needs to be communicated to the F5G network domains through an intent-driven interface. This interface enables the request of an expected behaviour in a set of simplified declarative policies, which is also known as "goal-policies". The essential difference between the intent-driven interface and traditional imperative interface is, the intent-driven interface declares WHAT is wanted, rather than HOW to do it.

Figure 15 shows a high-level intent framework. Through the intent-driven interface, the intent owner can send requests in a declarative form. The detailed actions to achieve the goals are not included in the request, but are deduced and determined automatically by the inner control loop of the intent handler. In this way, the design, deployment and implementation of the inner control loop of the intent owner could be significantly simplified.

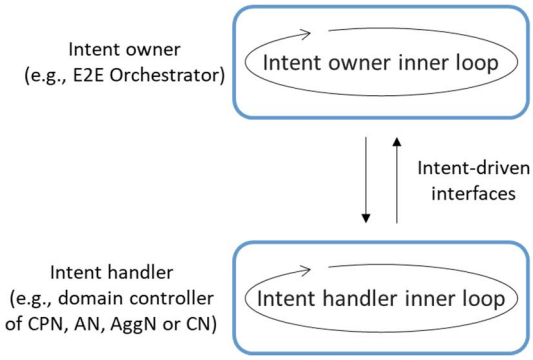

Figure 15: High-level intent framework

An intent-driven interface shall carry the following information:

- Intent Identification: the identifier and the name of the intent.
- Intent category: the category of the intent.
- Intent specification:
  - Intent expectation target: the target to be achieved by the intent.
  - Intent expectation context: the constraints and the policies applying to the intent when achieving the intent target.
  - Intent expectation object: the object that the intent is applied to.

The benefits of intent-driven interfaces in F5G include:

- Simplicity: In an intent control loop, the intent owner (e.g. the E2E Orchestrator or its customers) does not need to be aware of the technical details of the physical network. This simplifies the design of the intent owner.
- Agility: Since the control loop in the intent owner (e.g. the E2E Orchestrator or its customers in Figure 15) is technology agnostic, it simplifies the development and deployment of the intent owner to support new functions, e.g. development and deployment of new types of services.

Note that not all the northbound interfaces of the F5G domain controllers and E2E orchestrator need to be intent-driven. Traditional imperative interfaces may still be used in certain circumstances.

For each function defined in the following clauses of the present document, it will be stated whether it is an intent-driven interface or a traditional interface.

7.2 NBI of the Customer Premises Network Controller

The requirements and parameters of the NBI of the Customer Premises Network Controller are for further study.

7.3 NBI of the Access Network Controller

7.3.1 Interface for Access Network topology and inventory report

7.3.1.1 Functional requirements

For visibility and maintenance of the Access Network, the E2E Orchestrator shall be aware of the information with regard to the topology and inventory of the Access Network, which is collected from the Access Network Controller. Figure 16 shows the topology and inventory information to be reported by the Access Network Controller to the E2E Orchestrator.

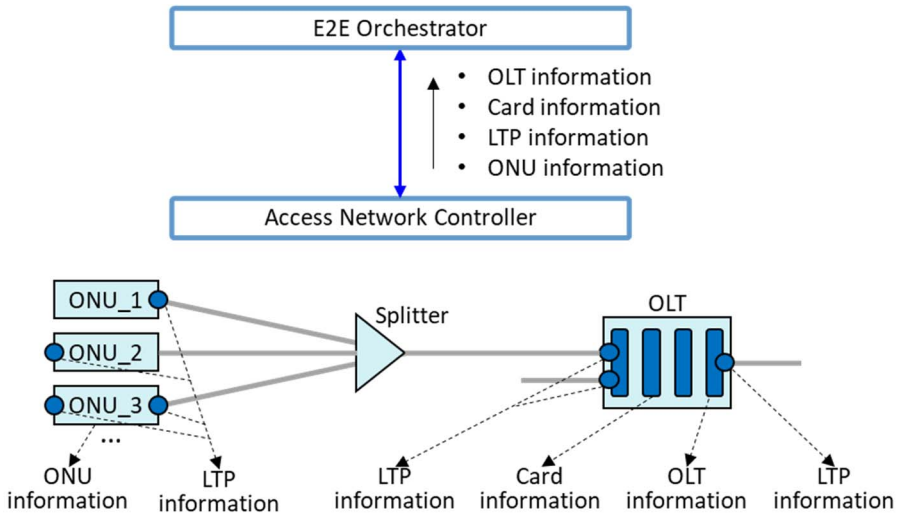

Figure 16: Report of Access Network topology and inventory information

In Figure 16 the following information is defined. See the tables below for more detailed explanation of the information:

- OLT information: The OLT information shall include the OLT identifier, the OLT equipment information, address information and state information.
- OLT Card information: The card information installed in the OLT shall include the card identifier, card type, the card location information (within the chassis), product information and state information.
- LTP information: The Link Termination Point (LTP) can be the PON port of the OLT, the uplink interface of the OLT, the PON port of the ONU, or the customer facing interface of the ONU. The LTP information shall include the LTP identifier, the LTP resource information, location information address information and the state information.
- ONU information: The ONU information shall include the ONU identifier, ONU type, the ONU position information, terminal device information, address information and state information.

Figure 17 shows the interface for Access Network topology and inventory report.

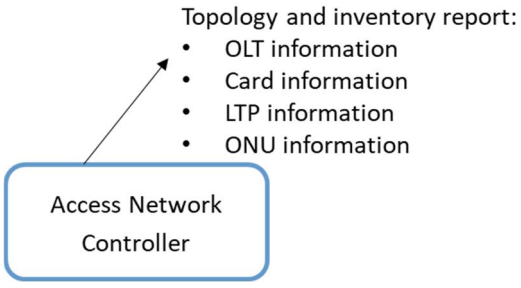

Figure 17: Interface for Access Network topology and inventory report

7.3.1.2 Key parameters

The interface shall include the key parameters of the OLT, card, LTP and ONU information, which are listed in Tables 1, 2, 3 and 4, respectively, unless otherwise stated.

Table 1: Key parameters of the OLT information

Types	Parameters	Description
OLT identifier	OLT ID	The Universally Unique Identifier (UUID) of the OLT.
	OLT name	The name(s) of the OLT equipment. Note that an OLT may have multiple names for manageability considerations. For example, the OLT vendor may provide an OLT equipment system name for each OLT, while the network operator may use another OLT name or Alias name to identify the OLT in the Access Network.
OLT Device information	Product name	The equipment model name of the OLT.
	Sequence Number	The Sequence Number of the OLT.
	Manufacturer	The manufacturer of the OLT.
	Manufacture date	The manufacture date of the OLT.
	Location	The geographic location information of the OLT.
	Software version	The software version of the OLT.
	Object creation time	The time when the OLT object was created in the Access Network Controller after the OLT was installed.
Address information	IP address	The management IP address of the OLT. IPv4 or IPv6 may be used.
	MAC address	The management MAC address of the OLT.
State information	Admin state	The administration state of the OLT, e.g. active, inactive, test or maintenance state.
	Operation state	The operation state of the OLT, e.g. normal operation state, or abnormal non-operation state.

Table 2: Key parameters of the OLT card information

Types	Parameters	Description
OLT Card identifier	Card ID	The identifier of the card.
	Card name	The name(s) of the card. Note that a card may have multiple names for manageability considerations.
Card Type	Card type	The type of the card.
Card location information	OLT ID	The identifier of the OLT that the card is located in.
	Frame number	The number of the frame where the card is installed.
	Slot number	The number of the slot where the card is installed.
	Sub-slot number	The number of the sub-slot where the card is installed (applicable only if the card is a sub-card).
Card product information	Product name	The product model name of the card.
	Serial Number	The Serial Number of the card.
	Manufacturer	The manufacturer of the card.
	Manufacture date	The manufacture date of the card.
	Software version	The software version of the card.
	BOM	The Bill Of Materials (BOM) of the card.
	Barcode	The barcode of the card.
	Object creation time	The time when the card object was created in the Access Network Controller after the card was installed.
State information	Admin state	The admin state information of whether the card is installed or not, and is active or inactive.
	Operation state	The operation state of the card, indicating whether the card is in-service or out-of-service; and for the latter state, it may further indicates the reasons, e.g. alarm or performance events, manually paused by external commands, or both.

Table 3: Key parameters of the LTP information

Types	Parameters	Description
LTP identifier	LTP ID	The UUID of the LTP.
	Port number	The LTP Port Number, which is unique among all LTPs on the same OLT.
	LTP name	The name(s) of the LTP. Note that an LTP may have multiple names for manageability considerations.
LTP resource information	LTP type	The type of the LTP. See note.
	Bandwidth	The total bandwidth of the port.
	MTU	The MTU (Maximum Transmission Unit) of the port (Applicable when the LTP is an Ethernet port).
	Ethernet working mode	The working mode of the Ethernet port, e.g. Auto-Negotiation, 100M-Half-Duplex, 100M-Full-Duplex, 1 000M-Half-Duplex, 1 000M-Full-Duplex, 2,5G or 10G.
	Access PON type	The PON type of the Access Network that the LTP belongs to. For example, GPON, EPON, XG-PON, XGS-PON or 10G-EPON.
	Optical module	The LTP optical module type, e.g. CLASS B+, CLASS C+, CLASS B, CLASS C++, GPON CLASS B+, EPON PX20+, GPON CLASS B or EPON PX20.
LTP location information	LTP location	Indicating whether the LTP is located on the OLT or the ONU.
	OLT ID	The identifier of the OLT that the LTP belongs to (applicable if the LTP is on an OLT).
	Frame number	The number of the frame that the LTP belongs to (applicable if the LTP is on an OLT).
	Slot number	The number of the slot that the LTP belongs to (applicable if the LTP is on an OLT).
	Card ID	The identifier of the card that the LTP belongs to (applicable if the LTP is on an OLT).
	Sub-slot number	The number of the sub-slot that the LTP belongs to (applicable only if the card that the LTP belongs to is a sub-card on an OLT).
	ONU ID	The identifier of the ONU that the LTP belongs to (applicable if the LTP is on an ONU).
Address information	MAC address	The MAC address of the LTP.
	IP address	The IP address of the LTP. IPv4 or IPv6 may be used.
State information	Admin state	The administration state of the LTP, e.g. active, inactive, test or maintenance state.
	Operation state	The operation state of the LTP, e.g. normal operation state, or abnormal non-operation state.
NOTE: In the Access Network, an LTP may be, for example, an Ethernet port or a PON port.		

Table 4: Key parameters of the ONU information

Types	Parameters	Description
ONU identifier	ONU UUID	The UUID of the ONU.
	ONU ID	The ONU identifier, which is unique among all ONUs under the same OLT.
	ONU name	The name(s) of the ONU. Note that an ONU may have multiple names for manageability considerations.
OLT relationship	Parent OLT	The OLT ID of the OLT that the ONU belongs to.
	Parent LTP	The LTP ID of the PON port on the OLT which the ONU belongs to.
ONU type	ONU class	Indicating the type of the ONU, depending on how the ONU is used, e.g. HGU, SFU, or MDU.
	ONU PON type	Indicating the type of the ONU, depending on the PON technology. E.g. GPON, EPON, XG-PON, XGS-PON or 10G-EPON. This parameter shall be used when the ONU PON port is not modelled as an LTP (see ONU 2 in Figure 16).
	PON bandwidth type	The upstream and downstream bandwidth of the ONU in its current working mode.
ONU terminal device information	Terminal type	The terminal product model type of the ONU.
	Sequence Number	The Sequence Number of the ONU.
	Soft version	The software version of the ONU.
	ONU authentication	The ONU authentication information used to authenticate the ONU.
	Object creation Time	The time when the ONU object was created in the Access Network Controller.
Address information	MAC Address	The MAC address of the ONU.
	IP Address	The IP address of the ONU (when assigned).
State information	Admin State	The administration state of the ONU, e.g. active or inactive state.
	Operation State	The operation state of the ONU, e.g. normal operation state, or abnormal non-operation state.

7.3.2 Interface for service fulfilment in the Access Network

7.3.2.1 Functional requirements

The Access Network may provide different types of services to the users, such as:

- Traditional home broadband services, such as HSI, VoIP, IPTV and VOD.
- Value-added home broadband services, such as online education and Cloud VR.
- PON leased line services for SMEs.

The E2E Orchestrator may use an intent-driven interface to request the Access Network Controller to perform service fulfilment.

Figure 18 shows the intent-driven service fulfilment interface in the Access Network, which shall at a minimum carry the following information:

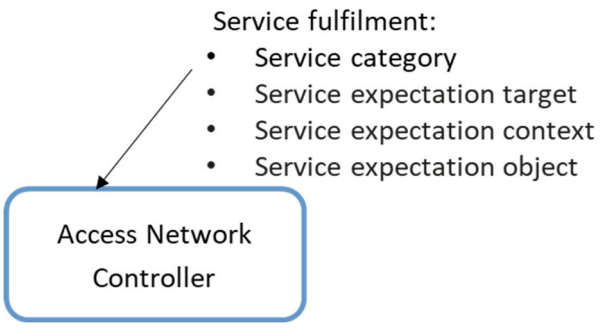

Figure 18: Interface for service fulfilment in Access Network

Intent-driven service fulfilment interface information shall be:

- Service category: Indicating the type of the Access Network service, e.g. HSI, IPTV, VOD or Cloud VR service.
- Service expectation target: The target SLA requirements of the specific type of the service, including the bandwidth requirements, latency and packet jitter, packet lost rate, and the service availability.
- Service expectation context: The constraints and the policies to be applied to the service.
- Service expectation object: Indicating the service instance to be fulfilled.

The detailed actions to fulfil the service in the Underlay Plane of the Access Network are deduced and determined automatically by the Access Network Controller.

7.3.2.2 Key parameters

The interface shall include the key service fulfilment parameters for the Access Network, which are listed in Table 5, unless otherwise stated.

Table 5: Key service fulfilment parameters for the Access Network

Types	Parameters	Description
Service category	Service category	The type of the Access Network service to be fulfilled.
Service expectation target	Expectation target	The target SLA of the service, including the bandwidth requirements, latency, packet jitter, and packet lost rate, and the service availability.
Service expectation context	Constraints	The constraints of the service fulfilment expectation. See note 1.
	Policies	The policies of the service expectation. See note 2.
Service expectation object	Service expectation object	The identification of the target object which is associated with the service expectation. In the context of service fulfilment, the identification of the expectation object is the identification of the service to be fulfilled.
NOTE 1: Examples of the service expectation context constraints are the service source end (e.g. the ONU) and the destination end (e.g. the OLT) identifiers. NOTE 2: Examples of service expectation context policies are the ONU authentication policies, and the QoS scheduling policies.		

7.3.3 Interface for fault monitoring and troubleshooting in the Access Network

7.3.3.1 Functional requirements

The mechanism for incident-based fault monitoring and troubleshooting is described in clause 6.2.4. The northbound interface of the Access Network Controller shall support the reporting of the incident information to the E2E Orchestrator, as shown in Figure 19.

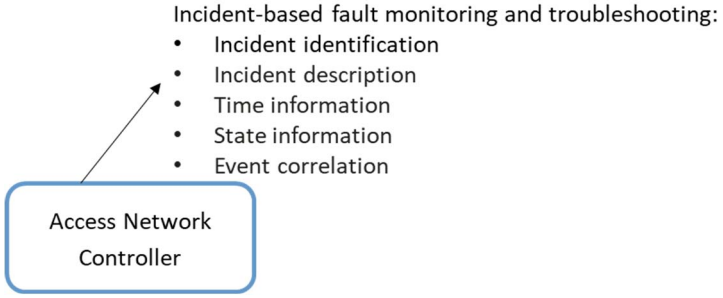

Figure 19: Interface for fault monitoring and troubleshooting in Access Network

Incident-based fault monitoring and troubleshooting information shall include:

- Incident identification: the identification and the category of the incident.
- Incident description: the detailed incident information includes the event source and the root cause of the incident, the components or services which have been or will be affected by the incident, the severity of the incident, and the repair advice to recover from the incident.
- Time information: the time when the incident is identified, updated, cleared and acknowledged by the network operator.
- State information: the state information of the incident.
- Event correlation: this information correlates the incident with the original alarm events in the traditional alarm-based system, and provides the detailed information about the alarm propagation relationship. This allows for the transition from the traditional alarm-based system to the new incident-based system, and provides guidance for accurate troubleshooting.

7.3.3.2 Key parameters

The interface shall include the key parameters for fault monitoring and troubleshooting in Access Network, which are listed in Table 6, unless otherwise stated.

Table 6: Key parameters for fault monitoring and troubleshooting in Access Network

Types	Parameters	Description
Incident identification	Commit Sequence Number (CSN)	The CSN of the incident when committed to the database.
	Incident name	The name of the incident.
	Category	The category of the incident. Examples of incident categories are: equipment hardware and software, power environment, line and protocol.
Incident description	Event source	Identifying the event source which causes the incident. The event source may be an equipment, a port or other Access Network components. See note.
	Root cause	Identifying the root cause, and the detailed description of the root cause. See note.
	Affected entities	Identifying the Access Network components or services which have been or will be affected by the incident. See note.
	Severity	The severity of the incident. It provides information for the network operator to determine the priority to handle the incident. As an example, the severity can be determined by two aspects: • Impact: how serious the users or services are impacted by the incident; • Urgency: how much time to recover from the incident that the users can tolerate, the shorter the more urgent.
	Repair Advice	The advice on how to repair the fault, or to prevent the potential fault.
Time information	Occurrence time	The time when the incident is firstly identified. If the incident is a potential fault, the Occurrence time is the time when the potential fault is firstly identified.
	Update time	The last time the state of the incident was updated.
	Clear time	The time when the incident is cleared.
	Ack time	The time when the incident is acknowledged by the network operator.
Status information	Incident acknowledgement	Indicate whether the incident has been acknowledged by the network operator.
	Incident status	Indicate whether the incident has been cleared or not.

Types	Parameters	Description
Event correlation	Root event CSNs	The CSNs of the root alarm events which are correlated to the incident. The detailed information of the root alarm events can be maintained in the traditional alarm-based fault monitoring and troubleshooting system.
	Event CSNs	The CSNs of all the original alarm events which are correlated to the incident. The detailed information of the original alarm events can be maintained in the traditional alarm-based fault monitoring and troubleshooting system.
	Link list	The alarm propagation relationship of the incident. A single fault may result in a large number of alarm events in different parts of the Access Network. This parameter provides the detailed propagation relationship of these alarm events, including the position of the root fault, the position of the fault symptom and the services which have been or will be affected by the incident.
NOTE: See the example described in clause 6.2.4.		

7.4 NBI of Aggregation Network Controller

7.4.1 NBI of Optical Transport Controller

7.4.1.1 General description

From the F5G E2E management and control perspective, the OTN AggN (including the Optical Transport Controller) acts as an autonomous domain. The Optical Transport Controller northbound interface shall be specified as an intent-driven interface for the OTN AggN (which may be a single-domain or multi-domain, see clause 6.3.2.2 of the present document). Through this intent-driven NBI, the Optical Transport Controller shall expose the abstracted OTN AggN resource information to the E2E Orchestrator so that the E2E Orchestrator can manage and control the OTN AggN in an intent-based approach, without perceiving the detailed OTN information.

IETF specifies the ACTN architecture (see clause 6.3.2.3 of the present document), and a set of YANG data models for the MPI and the CMI of OTN under the ACTN architecture. The NBI of the Optical Transport Controller shall be based on IETF RFC 8795 [2], which defines the YANG data models for general TE topology.

NOTE: The NBI of the Optical Transport Controller could adapt to additional YANG data models which are currently under development in IETF.

7.4.1.2 Interface for OTN topology report

7.4.1.2.1 Functional requirements

The NBI of the Optical Transport Controller shall present the abstracted OTN topology information to the E2E Orchestrator, including the general network topology information, link information, node information and Link Termination Point (LTP) and Tunnel Termination Point (TTP) information of OTN AggN, as shown in Figure 20.

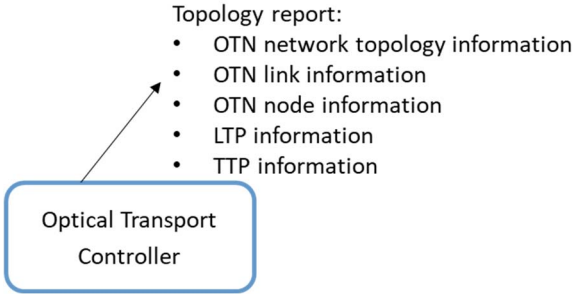

Figure 20: Interface for OTN topology report

Interface topology report information:

1) OTN AggN topology information: the general information of the OTN AggN topology. On the NBI of the Optical Transport Controller, the OTN AggN topology may be an abstracted network topology which is not necessary the same as the physical OTN AggN in the Underlay Plane. The topology ID uniquely identifies this abstracted OTN AggN topology, the provider ID indicating the provider of the OTN AggN topology, and the client ID indicating the client or the user of the OTN AggN topology.

2) OTN link information: an OTN link connects two OTN nodes within the same OTN AggN abstracted topology. The OTN link attributes include the link's source and destination information, the link bandwidth information, and the link latency information.

3) OTN node information: On the NBI of the Optical Transport Controller, an OTN node may be an abstract node that may represent one or several physical OTN nodes or a part thereof.

4) LTP information: an LTP is a termination point of a link at a node. In the OTN AggN, the LTP may be a termination point of an OTN link or a termination point of a link at the client-side of the OTN node, where the client signal of the OTN AggN will be mapped into the OTN connection. For the latter case, the client signals supported by the LTP need to be specified.

5) OTN TTP information: a Tunnel Termination Point (TTP) in an OTN AggN is a termination/adaptation point at an OTN node that can potentially terminate an OTN connection and adapt the client signal into the OTN connection. A given TTP in an OTN node is connected to the LTPs either originated or terminated by the OTN node. This depends on the internal constraints of the OTN node.

Figure 21 shows an example of an OTN AggN topology with OTN nodes, links, connections, LTPs (including OTN client LTPs and OTN LTPs) and TTPs.

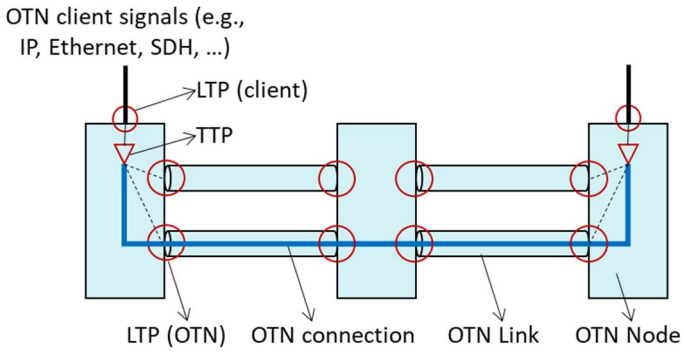

Figure 21: Example OTN network topology

7.4.1.2.2 Key parameters

The interface shall include the key parameters for the OTN topology, which are listed in Table 7, unless otherwise stated.

Table 7: Key parameters for the OTN topology

Types	Parameters	Description
Network	Network ID	The identifier of the native OTN AggN in the Underlay Plane.
	Network type	The type of the network topology. For OTN, the type is "OTN topology".
	Topology ID	The identifier of the abstracted OTN topology on the NBI of the Optical Transport Controller.
	Provider ID	The identifier to uniquely identify the provider (e.g. the Optical Transport Controller) who generates the abstracted OTN AggN topology. See IETF RFC 8795 [2] for the description of Provider ID.
	Client ID	The identifier to uniquely identify the client (i.e. the user) of the abstracted OTN AggN topology.
OTN Link	Link ID	The identifier for an OTN link in an OTN topology.
	Source	The logical source node and source LTP of an OTN link.
	Destination	The logical destination node and destination LTP of an OTN link.
	Operational state	The current operational state of an OTN link.
	Link bandwidth	The bandwidth of an OTN link.
	Unallocated bandwidth	The available bandwidth of an OTN link.
	Delay	The delay of an OTN Link, which is measured by the fibre length between two OTN nodes.
OTN Node	Node ID	The identifier for an OTN node in the native OTN AggN.
	TE-node ID	The identifier of an abstracted OTN node in the OTN TE topology.
	Operational state	The current operational state of an OTN node.
	Name	The name of an OTN node.
Link Termination Point (LTP)	LTP ID	The identifier for an LTP in the native OTN AggN.
	TE LTP ID	The identifier of an LTP in the OTN TE topology.
	Client-facing LTP	Indicates whether this LTP is a termination point of a link at the client-side of the OTN node.
	Client signals	Indicates the client signals supported by the LTP (only used when the LTP is a client-facing LTP).
	Operational state	The current operational state of the LTP.
	Name	The name of an LTP.
Tunnel Termination Point (TTP)	TTP ID	Tunnel termination point identifier.
	Operational state	The current operational state of the TTP.
	Name	The name of the tunnel termination point.

7.4.1.3 Interface for service provisioning in the OTN domain

7.4.1.3.1 Different ways for OTN domain service provisioning

There are two ways, an E2E Orchestrator can provision the service in the OTN domain:

1) Request for OTN connection provisioning:

   The E2E Orchestrator may directly request the Optical Transport Controller to create an OTN connection to carry the OTN domain service. In this case, the E2E Orchestrator shall at least be aware of the edge information of the OTN AggN and be able to decide where to create the OTN connection for the OTN domain service.

   The functional requirements and key parameters for the request of OTN connection provisioning are described in clause 7.4.1.3.2 and clause 7.4.1.3.3, respectively.

2) Request for transmitting the traffic of the OTN domain service:

   The E2E Orchestrator may use an intent-driven approach and request the Optical Transport Controller to transmit the client traffic of the OTN domain service through the OTN AggN without expressing the request of the OTN connection creation. In such cases, the Optical Transport Controller either determines how to create an OTN connection or uses a pre-created OTN connection to carry the traffic of the OTN domain service. Such determination may include:

   - The type and bandwidth of the OTN connection, based on the bandwidth requirements of the OTN domain service.

- The source and destination nodes and LTPs of the OTN connection.
- The route of the OTN connection, based on the performance constraints of the OTN domain service.
- The recovery scheme of the OTN connection is based on the availability requirements of the OTN domain service.

The functional requirements and key parameters for transmitting the OTN domain service traffic are described in clause 7.4.1.3.4 and clause 7.4.1.3.5, respectively.

7.4.1.3.2 Functional requirements for the request of OTN connection provisioning

The NBI of the Optical Transport Controller shall support the following information for OTN connection creation, activation, modification, deactivation and deletion:

1) Source and destination information: the identifiers of source and destination nodes, source and destination client-side link termination points, and the type of the client signal to be mapped into the OTN connection.
2) Bandwidth information: for the OTN AggN, it refers to the granularity of the OTN container of the OTN connection.
3) Recovery information: the protection and restoration type of the OTN connection to be created or modified, as well as the related configurations (e.g. Wait-To-Restore (WTR)).
4) Path constraint information: indicating the path constraint information of the OTN connection to be created or modified. It may include the optimization metric of the path calculation and the inclusion or exclusion of specific link(s) or node(s).
5) Administrative state: Indicating the target administrative state of the connection.

The NBI of the Optical Transport Controller shall also support the retrieval of the information of an existing OTN connection, including:

1) Actual path: presenting the actual path route information to the E2E Orchestrator.
2) Operational state: presenting the operational state of the OTN connection to the E2E Orchestrator.
3) Provisioning state: presenting the provisioning state of the OTN connection to the E2E Orchestrator.

Optionally, the NBI of the Optical Transport Controller may support the retrieval of the latency information of the OTN connection.

The interface for OTN connection provisioning is shown in Figure 22.

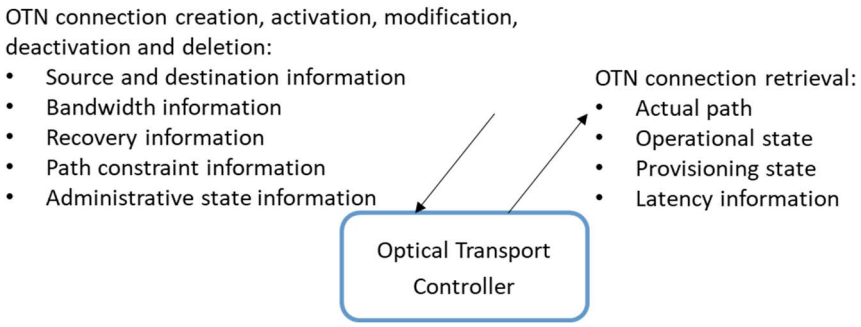

Figure 22: Interface for OTN connection provisioning

7.4.1.3.3 Key parameters for the request of OTN connection provisioning

The interface shall include the key parameters for the OTN connection creation, modification, deletion and retrieval, which are listed in Table 8 and Table 9, respectively, unless otherwise stated.

Table 8: Key parameters for the OTN connection creation, modification and deletion

Types	Parameters	Description
Source and destination	Source and destination nodes	Identifier of the source and destination nodes.
	Source and destination LTPs	Identifier of the source and destination client-side LTPs.
	Client signal	Identifying the client signal type associated with the access port.
Bandwidth	OTN Bandwidth	The bandwidth of the OTN connection.
Recovery	Protection/restoration type	Indicating the protection type and restoration type of the OTN connection, e.g. unprotected, 1+1 protection or full rerouting.
	Reversion	Reversion refers to returning the traffic to the working path after the working path has been repaired. This parameter indicates whether the reversion is enabled. And if it is enabled, it further indicates the WTR time.
Path constraints	Optimisation metric	The route calculation optimisation objective is used for calculating the route for the requested OTN connection, e.g. minimal hops, minimal latency or shortest distance.
	Route constraints	Inclusion or exclusion of specific link(s) or node(s).
Administrative state	Administrative state	Indicating the target administrative state of the connection, e.g. administrative-up (i.e. activate the OTN connection) or administrative-down (i.e. deactivate the OTN connection).

Table 9: Key parameters for the OTN connection retOptimizationrieval

Types	Parameters	Description
Actual Path	Actual Path	This parameter is used to retrieve the actual route of the OTN connection in the abstracted topology reported by the Optical Transport Controller. Note that the actual path in the abstracted topology is an abstracted view of the route of the physical OTN connection.
Operational state	Operational state	This parameter is used to retrieve the current operational state of the OTN connection.
Provisioning state	Provisioning state	This parameter is used to retrieve the current provisioning state of the OTN connection.
Latency	Latency	The latency of the OTN connection.

7.4.1.3.4 Functional requirements for the request of service traffic in the OTN domain

The NBI of the Optical Transport Controller shall support the request information of the client traffic of the service in the OTN domain, in an intent-driven approach:

1) Client source and destination information: The source and destination client nodes and client-side link termination point, and the client signal type.

2) Client signal bandwidth: the bandwidth requirement for the client signal.

3) Availability: the availability requirements of the OTN domain service. In an intent-driven approach, the detailed recovery scheme (e.g. 1+1 or 1:1 protection, or restoration) is not specified, but is automatically determined by the Optical Transport Controller based on the client signal's availability requirements.

4) Client signal constraints: technology-agnostic constraints of the client signal, e.g. latency and packet jitter constraints.

The NBI of the Optical Transport Controller shall support the reporting of the client traffic of the service in the OTN domain:

1) Operational state: presenting the operational state of the OTN client signal transmission to the E2E Orchestrator.

2) Provisioning state: presenting the provisioning state of the OTN client signal transmission to the E2E Orchestrator.

Optionally, the NBI of the Optical Transport Controller may support reporting the latency information of the OTN connection.

The interface for the request of OTN domain service transmission is shown in Figure 23.

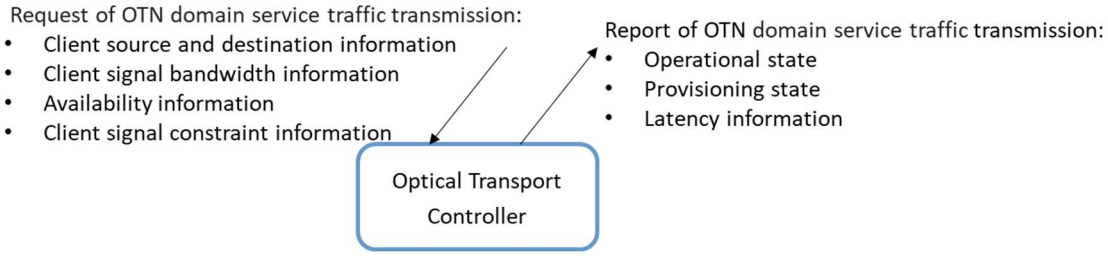

Figure 23: Interface for the request of OTN domain service traffic transmission

7.4.1.3.5 Key parameters for the request of OTN domain service traffic transmission

The interface shall include the key parameters for the request and report of the client traffic transmission of the OTN domain service, which are listed in Table 10 and Table 11, respectively, unless otherwise stated.

Table 10: Key parameters for the request of OTN domain service traffic transmission

Types	Parameters	Description
Client source and destination	Client source and destination nodes	Identifier of the source and destination nodes of the client-side.
	Client source and destination LTPs	Identifier of the source and destination client-side LTPs at the client-side nodes.
	Client signal	See the description in Table 8 in clause 7.4.1.3.3.
Client signal bandwidth	Client signal bandwidth	The bandwidth requirements for the client signal.
Availability	Availability	The availability requirements of the service, e.g. the maximum interruption time per year or the percentage of the service availability (e.g. 99,99 % or 99,999 %).
Client signal constraint	Latency/packet jitter	Either the latency or the packet jitter constraints of the client signal, or both.

Table 11: Key parameters for the report of OTN domain service traffic transmission

Types	Parameters	Description
Operational state	Operational state	This parameter is used to report the current operational state of the OTN client signal transmission.
Provisioning state	Provisioning state	This parameter is used to report the current provisioning state of the OTN client signal transmission.
Latency	Latency	See the description in Table 9 in clause 7.4.1.3.3.

7.4.1.4 Interface for the OTN connection calculation and evaluation

7.4.1.4.1 The functional requirements

To check the possibility of whether an E2E service could be created, the E2E Orchestrator may request each related domain controller to do a feasibility check in its domain before the provisioning of the E2E service.

For the OTN AggN, the E2E Orchestrator may request the Optical Transport Controller to evaluate whether the current state of the OTN AggN fulfils the performance requirements of a connection before requesting to create the connection. This is achieved by calculating the potential OTN path(s) for the requested OTN domain service and evaluating the OTN path(s) performance (e.g. latency, hop number and distance) by the Optical Transport Controller. Multiple candidate paths with their own performance information may be returned to the E2E Orchestrator. The E2E Orchestrator makes the final decision of which path to use according to its policies.

Note that the Optical Transport Controller only performs the path calculation and evaluation at this stage, without reserving any OTN resource for the path nor any configuration in the OTN.

The NBI of the Optical Transport Controller shall support communicating the following OTN path information for path calculation and evaluation purposes:

1) Source and destination information: the source and destination of the OTN path. See clause 7.4.1.3.2.

2) Bandwidth information: for the OTN AggN it refers to the granularity of the OTN container of the OTN connection.

3) Recovery information: the protection and restoration type of the OTN connection.

4) Path constraint information: the path constraint information of the OTN connection. See clause 7.4.1.3.2.

This interface shall support returning the path computation and evaluation result which, include:

1) Calculated paths: provides the calculated route information to the E2E Orchestrator. Note that the calculated path is an abstracted path in the abstracted OTN topology reported to the E2E Orchestrator, which may be different from its actual physical path in the Underlay Plane. Note also that multiple candidate calculated paths may be included.

2) Path characteristic data: provides the calculated path relevant characteristic data of each calculated path in response to the E2E Orchestrator request, e.g. latency, hop number and distance.

Figure 24 shows the interface for the OTN connection calculation and evaluation.

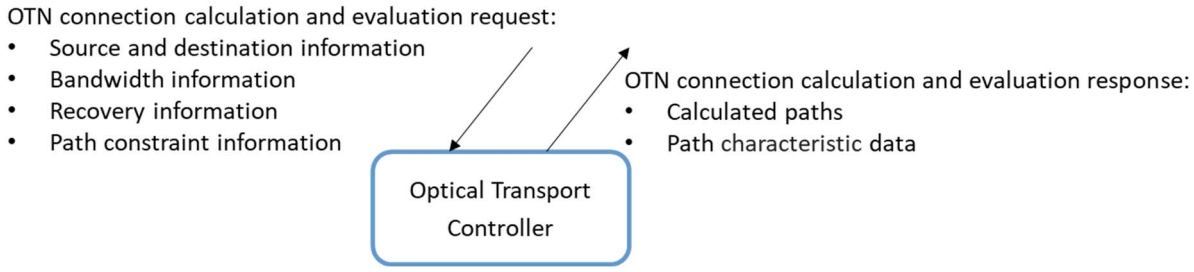

Figure 24: Interface for OTN connection calculation and evaluation

7.4.1.4.2 Key parameters

The interface shall include the key request and response parameters for the OTN connection calculation and evaluation, which are listed in Table 12 and Table 13, respectively, unless otherwise stated.

Table 12: Key request parameters for the OTN connection calculation and evaluation

Types	Parameters	Description
Source and destination	Source and destination nodes	See the description in Table 8 (see note).
	Source and destination LTPs	See the description in Table 8 (see note).
	Client signal	See the description in Table 8 (see note).
Bandwidth	OTN Bandwidth	See the description in Table 8 (see note).
Recovery	Protection/restoration type	See the description in Table 8 (see note).
Path constraint	Optimization metric	See the description in Table 8 (see note).
	Route constraints	See the description in Table 8 (see note).
NOTE: Table 8 in clause 7.4.1.3.3 contains more parameters than Table 12, and those parameters in Table 8, which are not in Table 12, are not applicable for path calculation and evaluation.		

Table 13: Key response parameters for the OTN connection calculation and evaluation

Types	Parameters	Description
Calculated paths	Calculated paths	The calculated route information.
Path characteristic data	Path properties	The relevant characteristic data of the calculated path, e.g. latency, hop number and distance.

7.4.1.5 The Interface for OTN service performance monitoring

7.4.1.5.1 The Functional requirements

After an OTN service is provisioned, the customer may request to monitor the service performance. In such a case, a performance monitoring task will be created between the E2E Orchestrator and the Optical Transport Controller. The Optical Transport Controller will report the performance data to the E2E Orchestrator under this performance monitoring task.

The NBI of the Optical Transport Controller shall support configuring (e.g. creating and deleting) a performance monitoring task and support retrieving the information of a created performance monitoring task. The information below shall be included in this NBI for performance monitoring configuration:

- Service identifier: the identifier of the OTN service to be monitored.
- Performance monitoring task switch status: used to control the opening, re-opening or closing of a performance monitoring task.
- Performance monitoring time granularity: the time period of the performance collection.
- Performance indicator: the list of the performance parameters to be monitored.
- Performance measurement mode: The measurement mode needs to be specified for some specific performance indicators.

After the performance monitoring task is created, the OTN service performance data generated on the Optical Transport Controller shall be reported to the E2E Orchestrator through the NBI of the Optical Transport Controller. The OTN service performance data shall include:

- Name of performance indicator: the parameter name of the performance data.
- Index: the index of the performance data.
- Performance parameter value: the parameter value of the performance data.
- Performance parameter unit: the parameter unit of the value of the performance data.
- Collect time: the start and end times of the performance data collection.

The interface for OTN service performance monitoring is shown in Figure 25.

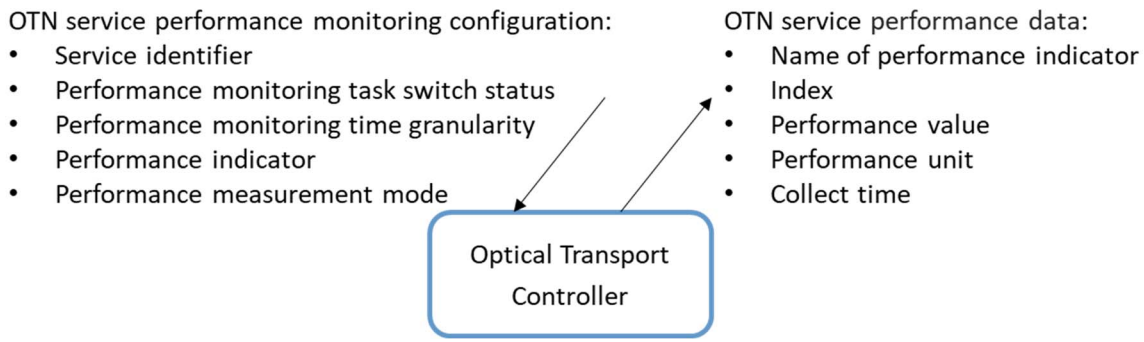

Figure 25: Interface for OTN service performance monitoring

7.4.1.5.2 Key parameters

The interface shall include the key parameters for OTN service performance monitoring, which are listed in Table 14, unless otherwise stated.

Table 14: Key OTN service performance monitoring parameters

Types	Parameters	Description
Performance monitoring configuration	Service identifier	The identifier of the OTN service to be monitored.
	Performance monitoring task switch status	A switch status used to control the opening, re-opening or closing of a performance monitoring task.
	Performance monitoring frequency	The frequency of the performance collection, e.g. 1 minute, 15 minutes or 24 hours.
	Performance indicator	The list of the performance parameters to be monitored includes latency, package received, and frame lost.
	Performance measurement mode	The measurement mode needs to be specified for some specific performance indicators, e.g. the loopback mode (remote or local).
Performance data	Name of performance indicator	The parameter name of the performance data, such as latency, package received, and frame lost.
	Index	The index of the performance data.
	Performance parameter value	The parameter value of the performance data.
	Performance parameter unit	The parameter unit of the value of the performance data.
	Collect time	The start time and the end time of the performance data collection.

7.4.2 NBI of IP/Ethernet Controller

The northbound interface of the IP/Ethernet Controller is used to manage and control the IP/Ethernet networks, including but not limited to, the network topology report, the VPN service provisioning, the traffic monitoring and the fault monitoring.

IETF defines a set of YANG data models for the management and control of the IP/Ethernet networks. The NBI of the IP/Ethernet Controller shall support the following YANG data models:

- IETF RFC 8346 [5] and IETF RFC 8944 [6], which define the YANG data models for layer 3 and layer 2 network topologies, respectively.
- IETF RFC 8299 [7] and IETF RFC 8466 [8], which define the YANG data models for the delivery of L3VPN and L2VPN, respectively.

7.5 NBI of Core Network Controller

The requirements and parameters of the NBI of the Core Network Controller are for further study.

7.6 NBI of E2E Orchestrator

The requirements and parameters of the NBI of the E2E Orchestrator are for further study.

8 Security consideration

The present document defines the technical requirements and key functions of the domain controllers, the orchestrator, and the interfaces of the F5G E2E management and control system. The security aspects of the server hardware should be considered when deploying the domain controllers and the orchestrator. The security aspects of interfaces between the F5G domain controllers and the E2E orchestrator should be considered.

Clause 5.10 of ETSI GR F5G 010 [i.6] identifies security threats to the F5G MCA plane. The countermeasures against these security threats are for further study.

History

Document history		
V1.1.1	September 2022	Publication