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

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

Disclaimer

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

Reference
DGS/F5G-0018

Keywords
cloud, F5G, optical, service

ETSI

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

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

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

Contents

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

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

Foreword

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

Modal verbs terminology

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

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

Introduction

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

1 Scope

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

2 References

2.1 Normative references

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.2 Informative references

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

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

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

[i.1] ETSI GR F5G 008 (V1.1.1): "Fifth Generation Fixed Network (F5G); F5G Use Cases Release #2".

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

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

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

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

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

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

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

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

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

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

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

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

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

3.2 Symbols

Void.

3.3 Abbreviations

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

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

4 Motivation

4.1 Overview of cloud access scenarios

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

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

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

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

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

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

- Use case #1: Cloud Virtual Reality. Cloud computing and cloud rendering technologies for VR services are introduced. Cloud VR content data are stored, read, rendered, coded compressed and transmitted to user terminals through the network.
- Use case #2: High Quality Private Line. Government institutions, financial organizations and medical organizations require high quality private lines for cloud access. Examples are medical cloud, cloud desktop and financial cloud.
- Use case #3: High quality low cost private line for small and medium enterprises. Small and Medium Enterprises (SMEs) may need cloud services such as cloud desktop and cloud storage.
- Use case #16: Enterprise private line connectivity to multiple Clouds. Enterprises are gradually migrating their applications to different clouds. Meanwhile, an enterprise may have multiple branches requiring access to the cloud applications. This requires the Multi-Point-to-Multi-Point (MP2MP) cloud access.
- Use case #17: Premium home broadband connectivity to multiple Clouds. There is an increasing demand for premium home broadband Cloud-based services such as Cloud VR education, Cloud VR gaming, and Cloud gaming. Since different cloud applications are deployed in different Cloud DCs, this use case also requires the Multi-Point-to-Multi-Point (MP2MP) cloud access from different OLTs.

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

4.2 Requirements from the Use Cases

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

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

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

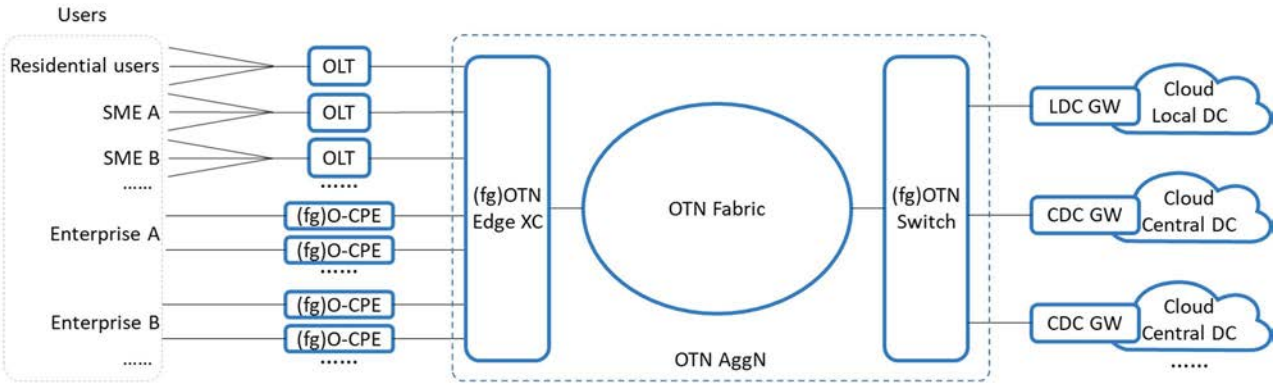

Figure 1: OTN-based general network topology for cloud services

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

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

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

- Multi-user access: For the PON access case, multiple residential users or SMEs are accessing the OTN AggN via different OLTs. For the OTN access case, an enterprise has multiple branches, which access the OTN AggN via different (fg)O-CPEs and CPEs (Ethernet based).
- Isolation between users: The isolation between different users are required, for the consideration of manageability, QoE assurance and security. The isolation shall include address isolation and traffic isolation.
- Multi-cloud access: Users of cloud services may run different cloud applications which are deployed in different Cloud DCs. Furthermore, a user may connect to two or more Cloud DCs at the same time for backup and disaster recovery consideration.
- Automatic OTN connection provisioning: Considering the MP2MP connectivity from multiple user sites to multiple clouds, the OTN AggN needs to support on-demand resource scheduling and connection provisioning between any pair of edge OTN nodes, driven by the requests of the MP2MP connectivity services.

5 OCN architecture

5.1 Design principle

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

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

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

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

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

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

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

5.2 Overview of OCN architecture

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

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

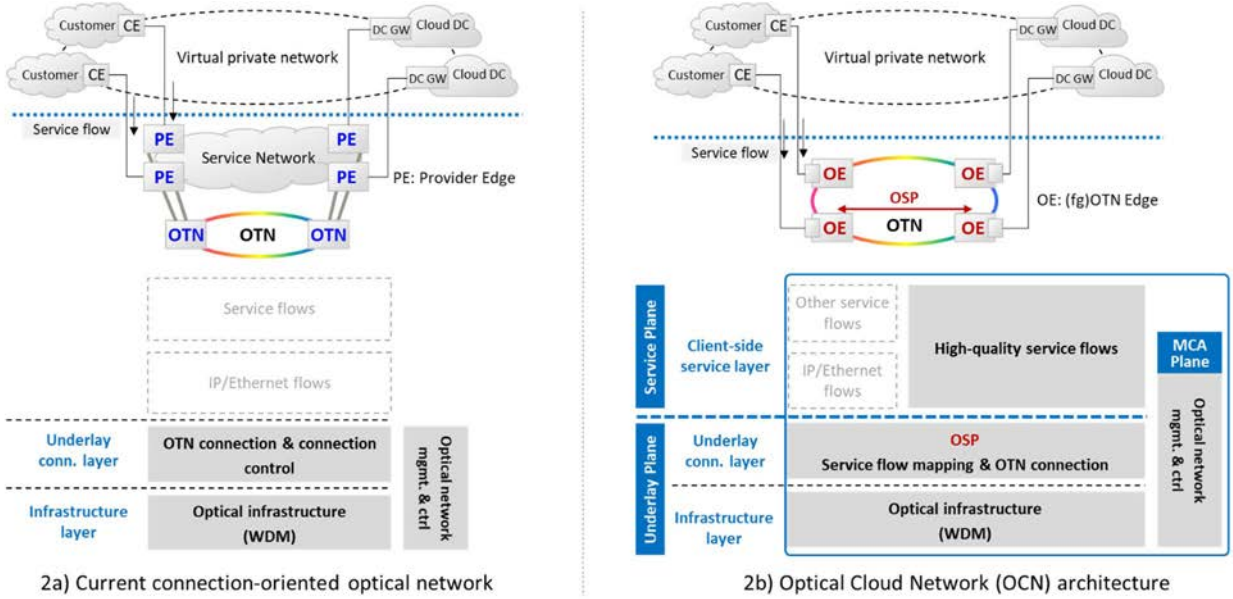

Figure 2: Evolving to the OCN architecture

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

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

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

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

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

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

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

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

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

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

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

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

5.3 Integration of OCN into the F5G-A network architecture

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

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

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

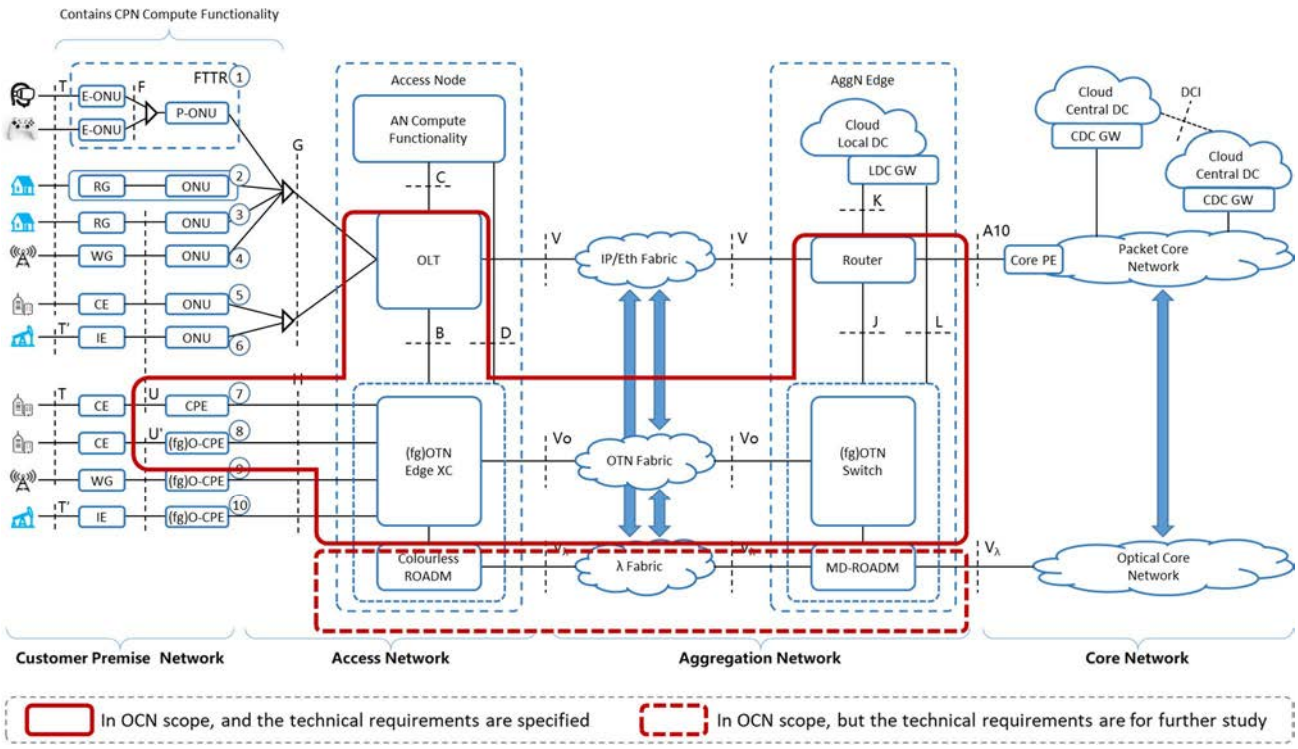

Figure 3: OCN in the F5G-A network topology

In the OCN architecture, the high-quality cloud services from the OLT (including residential and SME services) are carried by the OTN or Ethernet through the interface B in the F5G-A architecture, while the enterprise private line or private network services are carried by the OTN or Ethernet through the interface H in the F5G-A architecture.

The OCN architecture also covers the WDM layer (including the Colourless ROADM, MD-ROADM and the λ fabric) in the Aggregation Network as its infrastructure layer. The detail technical requirements of the WDM network in the OCN architecture are for further study.

NOTE: Traditional service flows can still be carried by the IP/Ethernet network in the F5G-A architecture, which is out of scope of the present document.

In the AggN Edge node, a router may be used to interconnect the OTN and the cloud DCs, which is for further study.

In the F5G-Aarchitecture the control plane, clauses 5.3.3 and 5.3.4 of ETSI GS F5G 024 [6] define the near real-time control topology as well as its control interfaces. Specifically, clause 5.3.4.7 of ETSI GS F5G 024 [6] specifies the C1 and C2/C2' (fg)OTN control interfaces.

The OCN architecture includes two types of control interfaces: the connection control interface(C1) and the service control interface (C2/C2'). In clause 7.1 of the present document there is a more detail description of these interfaces.

5.4 Key capabilities of OCN

To ensure the transmission quality of the high-quality cloud services which requires assured bandwidth, low latency and high availability, the OCN architecture shall have the following capabilities:

1) Service agility: The OCN architecture shall provide agile service provisioning capability for Cloud DC services. It shall support identifying different cloud-side and user-side (including CPE and PON) service flows, and supports mapping these service flows into different OTN connections based on the service destinations. In this way, the OCN architecture provides automatic provisioning of Point-to-Multi-Point (P2MP) and Multi-Point-to-Multi-Point (MP2MP) service access to multiple Cloud DCs.

2) Service adaptation: The OCN architecture shall be aware of the service SLA requirements (including the bandwidth requirement), and provide fast and hitless bandwidth adjustment to the OTN connections, based on the variable service bandwidth requirements. This enables the OTN to adapt to service bandwidth changes on demand, and improves the OTN resource utilization.

3) Service slicing: The OCN architecture shall support service-oriented OTN slicing, to serve different service requests, and to ensure service isolation from each other service traffic. In addition, enterprises may use their own private addresses (IP addresses) for their private network services. To ensure private address conflict is avoided between different enterprises, private address isolation shall be supported for enterprise service transmission.

4) Service assurance: Cloud services including cloud VR and cloud gaming are more sensitive to latency and bandwidth. The service transport network needs to evolve from best effort to deterministic transmission. The OCN architecture shall provide secure service connection and guaranteed service bandwidth to ensure the service quality and the user experience. The service traffic traverses a variety of heterogeneous networks including Access Network, Aggregation Network and Core Network where Cloud DCs reside. Therefore, the OCN architecture shall support collaborating and integrating various network technologies to enable effective resource scheduling and reduce the E2E network processing delay.

5) Service capacity: OCN architecture shall support thousand-level OTN containers per 100 Gbps ODU link supporting increasing number of services, and OTN containers with bandwidth ranging from 10 Mbps to 100 Gbps, to adapt to various cloud services and to improve the OTN resource utilization.

6) Service availability: The reliability of the service carrier network is extremely important for the high-quality cloud services. The OCN architecture shall support self-monitoring, self-healing, and self-optimization, and be capable of detecting network failures (and in some cases, predict potential network failures) In addition the OCN architecture shall provide various protection and restoration mechanisms in the presence of single or multiple failures within the OTN, and between the OTN and the Cloud DCs.

6 OCN Data Plane technical requirements

The (fg)OTN is the data plane in the OCN architecture, to transport the high-quality cloud services. The key technical requirements for the OTN Data Plane include:

1) The (fg)OTN shall support the provisioning of connections with guaranteed bandwidth matching the transmission quality requirements of the cloud services, providing very low and deterministic latency and minimal packet jitter for packet service flows.

   The (fg)OTN is a Time-Division Multiplexing (TDM) technology, where different services are carried in dedicated time slots (called tributary slots in Recommendation ITU-T G.709 [7]). Unlike the packet forwarding technologies, OTN does not support store and forward, statistical multiplexing, oversubscription, queuing and buffering techniques are not necessary when performing OTN switching and transport. Therefore, OTN supports dedicated connections with guaranteed bandwidth, low deterministic latency and minimal packet jitter for packet services carried by the connection.

   As per Recommendation ITU-T G.709 [7], (fg)OTN supports both CBR and VBR client signals. OCN shall support both CBR and VBR-based services.

2) The (fg)OTN shall support both ODUk and fgODUflex matching the bandwidth requirements of the different cloud services.

   Different cloud services may require very different bandwidths from tens of Mbps to several Gbps. To improve the resource utilization of the OTN carrier network, the bandwidth per OTN connection shall match the bandwidth requirements of the cloud services.

   Recommendations ITU-T G.709 [7] and G.709.20 [8] define both ODUk (k = 0, 1, 2, 3, 4, flex) and fgODUflex containers which support bandwidths of N × 10 Mbps (N = 1 to 119) for sub-1G services, and the ODUflex containers which support bandwidths of N × 1,25 Gbps (N = 1 to the total number of 1,25 Gbps tributary slots of the ODUk that the ODUflex is multiplexed into) for higher bandwidth services.

3) The (fg)OTN shall support dynamic and hitless bandwidth adjustment of a connection to match the bandwidth changes of the cloud services.

   The high-quality cloud services might require different bandwidths in different time periods. To improve the resource utilization, the OTN connections shall support hitless bandwidth adjustment (increasing or decreasing) according to the change of the service bandwidth. When adjusting the bandwidth of the OTN connection, the existing service traffic shall not be affected.

The current OTN supports hitless adjustment of ODUflex(GFP) defined in Recommendation ITU-T G.7044/Y.1347 [9], and fgOTN defined in and Recommendation ITU-T G.709 [7].

7 OCN connection control and service control technical requirements

7.1 Overview

7.1.1 Introduction to the OCN control interfaces and protocols

The (fg)OTN control plane, which is separated from (fg)OTN data plane, is used for connection-oriented (fg)OTN control (including, OTN link and topology discovery, and (fg)OTN connection control). To further enable the automatic service-oriented control, the (fg)OTN control plane needs to be enhanced.

In the F5G-A Architecture (ETSI GS F5G 024 [6]), the (fg)OTN control interfaces C1 and C2/C2' reside in the (fg)OTN Access and (fg)OTN Aggregation Network, as shown in Figure 4:

- The C1 interface is used to control the (fg)OTN network connections.
- The C2 and C2' interfaces are used to control the (fg)OTN-based service connections.

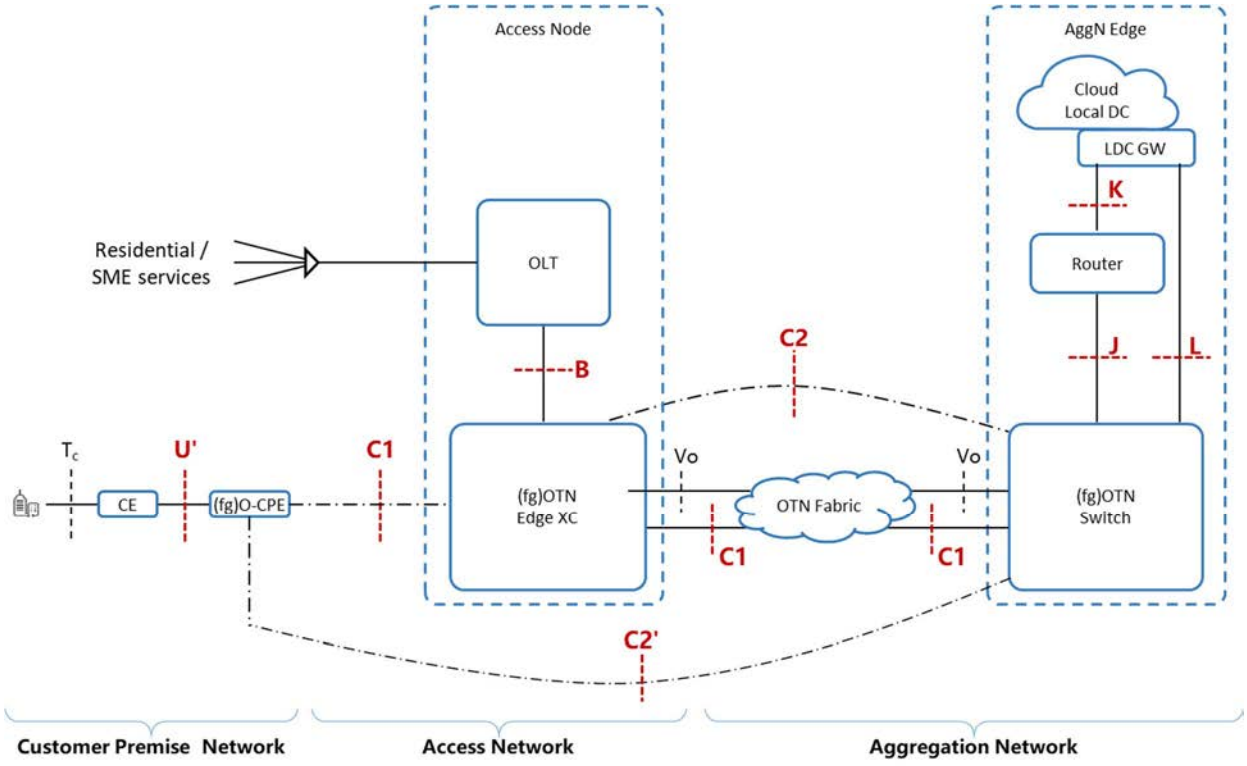

Figure 4: F5G-A interfaces (Interface names in red are related to OCN)

Based on the common control aspects of the transport network defined in Recommendation ITU-T G.7701 [10], the domain is used to express different administrative and/or managerial responsibilities including, trust relationships, addressing schemes, infrastructure capabilities, survivability techniques, and distributions of control functionality. The control plane supports the establishment of services through the automatic provisioning of end-to-end transport connections across one or more domains. The User Network Interface (UNI) is an inherent part of the Automatically Switched Optical Network (ASON) architecture in Recommendation ITU-T G.7703 [11]. The reference point between a user and a provider domain is the UNI, which represents a user-provider service demarcation point. From the OTN perspective, the provider domain is OTN and user domain is the OLT, CE and DC GW.

From the OCN perspective, UNIs are control reference points where the data plane interfaces B, U', J, K and L are specified in the (fg)OTN architecture as shown in Figure 5.

NOTE: As per F5G-A architecture [6], the (fg)OTN Switch may connect to the Cloud DC directly, or through a Router. In the former case, the UNI is the control reference point of interface L. In the latter case, if the Router and the (fg)OTN Switch within the AggN Edge are in the same physical equipment and the interface J is an internal interface, the UNI is the control reference point of interface K; If they are separated, the UNI is the control reference point of interface J. Figure 5 only shows the former case for simplicity.

In the use case "Premium home broadband connectivity to multiple Clouds" (see clause 7.3 of ETSI GR F5G 008 [i.1]), the OLT is in the user-side client network and supports the UNI-Client (UNI-C) functions while the OTN Edge XC is in provider-side OTN network and supports the UNI-Network (UNI-N) functions. In the use case of "Enterprise private line connectivity to multiple Clouds" (see clause 7.2 of ETSI GR F5G 008 [i.1]), the CE is in the user-side client network and supports the UNI-C functions while the (fg)O-CPE is in provider-side OTN network and supports the UNI-N functions. The (L)DC GW in the cloud-side client network and supports the UNI-C functions while the OTN AggN Edge is in provider-side OTN and supports the UNI-N functions. See Figure 5.

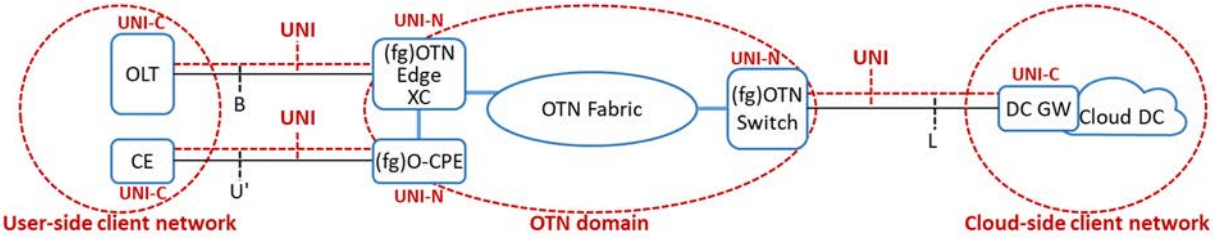

Figure 5: OTN UNIs and client networks

7.1.2 OCN control interfaces and protocols

The C1 interface is the control plane handover point between two (fg)OTN nodes (including the (fg)O-CPE, the (fg)OTN Edge XC and the (fg)OTN switch in the AggN Edge node) which are interconnected by OTN link.

In the OCN architecture, the OSP connection control is implemented on the C1 interface, to exchange the signalling information to control the (fg)OTN connections across the different network segments. The functions of the OSP connection control shall include:

- Configuration function: Automatic creation, modification and deletion of (fg)OTN connections.
- Bandwidth adjustment function: Hitless bandwidth adjustment of the (fg)OTN connections.
- Recovery function: (fg)OTN connection recovery from a network failure, satisfying the service recovery performance requirements.

The C2 and C2' interfaces are the control plane handover points between the two (fg)OTN endpoint connections, where the service traffic is mapped into or de-mapped from an (fg)OTN connection.

In the OCN architecture, the OSP service control is implemented on the C2 and C2' interfaces, to exchange service mapping information between the (fg)OTN endpoints (i.e. the OEs).

Since there are multiple OEs, each of which communicates with each other to exchange the service mapping information. This results in a large volume of information being exchanged between the different OEs. See the left-hand side of Figure 6 and the large number of interconnecting dotted lines between OEs.

To reduce the complexity of the C2/C2' interfaces and improve the scalability, a Service Mapping Control Component (SMCC) is introduced, which communicates with all the OEs via the C2/C2' interfaces within the same control plane, as shown on the right-hand side in Figure 6. The OEs only connect to the SMCC, significantly reducing the interconnect complexity.

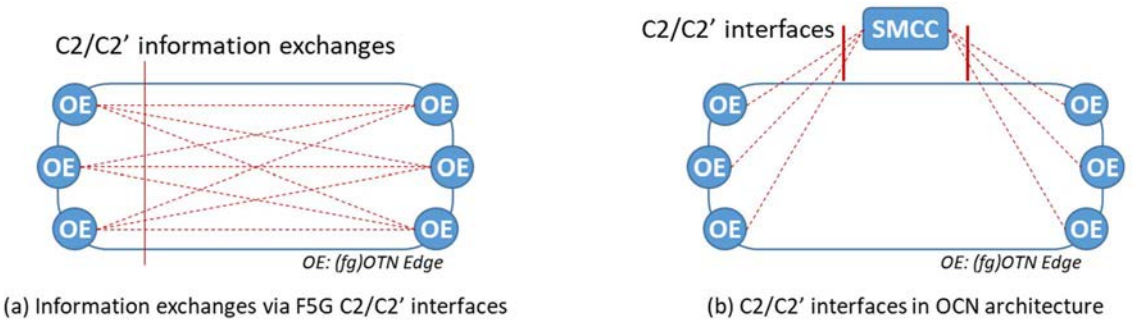

Figure 6: Introduction of C2/C2' interfaces

The SMCC runs the OSP service control to communicate with (fg)OTN edge nodes via the C2/C2' interfaces. The SMCC functions shall include:

- Collection of the Ethernet MAC addresses and/or IPv4/IPv6 addresses or prefixes of the user-side and cloud-side client network nodes from the (fg)OTN edge nodes (the (fg)O-CPE, the (fg)OTN Edge XC and the (fg)OTN Switch).
- Generation and maintenance of the service mapping rules.
- Configuration of the service mapping rules on the (fg)OTN edge nodes.

The SMCC functions are performed per Virtual Private Network (VPN) or per network slice instance. In the F5G-A Architecture (ETSI GS F5G 024 [6]), a network slice is defined as a logical network that achieves specific service requirements. There are two types of E2E slices in F5G: one is slicing the network into dedicated network resources according to SLA requirements for various tenants or operators, and the other is service-oriented slicing, where one network can be shared for different services with isolation and guaranteed QoS. VPN can be seen as a network slicing mechanism, as it provides different groups of users with logically isolated access to a common network.

A network slice or VPN topology includes a set of VPN nodes, each of which can have one or multiple VPN network accesses that represent the client-side ports associated with it. In the OCN architecture, a VPN node is an abstracted node on an (fg)OTN edge node, with one or multiple VPN network accesses, which means one or multiple physical client-side ports or a virtual client-side ports (with VLAN identifiers associated with a physical client-side port) on it.

The SMCC generates and configures the service mapping rules for each network slice or VPN.

The network slice or VPN information can be manually configured on the (fg)OTN edge nodes, this approach is out of scope of the present document.

The SMCC is a logical functional entity, which may be deployed in the MCA Plane of the F5G-A architecture (in the Optical Transport Controller) or in an (fg)OTN physical network element which has sufficient computing power to support the SMCC functions. This assumes that the SMCC residing on a given (fg)OTN physical network element communicates with all other (fg)OTN physical edge network elements.

7.2 OSP service control

7.2.1 Overview of service mapping control requirements

The following requirements shall be supported to enable the service flow mapping control:

1) Service attributes identification: To map services to the appropriated (fg)OTN connection and carry the services end-to-end, the(fg)OTN edge nodes shall recognize and learn the service attributes (including Layer 2/Layer 3 address information and VLAN identifiers. See clause 7.2.2) when the (fg)OTN edge nodes receive service flows from the client network.

2) Service/client node address report: To compute the appropriate (fg)OTN path to transport the services and automatically map or de-map the service traffic into/from the appropriated (fg)OTN connections, the SMCC shall collect the service/node addresses (see clause 7.2.3) from all (fg)OTN edge nodes.

3) Service mapping rules generation and maintenance: The SMCC shall generate and maintain the service mapping rules, and configure (fg)OTN edge nodes with the service mapping.

4) Service mapping and de-mapping: The (fg)OTN edge nodes shall support mapping of the service flows into the appropriate (fg)OTN connection based on the service mapping rules, and support de-mapping of the service flows from the (fg)OTN connection and forwarding the service flows to the corresponding client networks.

7.2.2 Service attributes identification

The (fg)OTN edge nodes shall recognize the following service attributes from the service packet headers to report service addresses and map services to the appropriated (fg)OTN connection:

- VLAN Identifier (SVLAN and/or CVLAN).
- Source and Destination Ethernet MAC addresses.
- Source and Destination IPv4 or IPv6 addresses.

Additional service attributes are for future study.

7.2.3 Client node addresses report

There are two approaches acquiring the service and client node addresses, as follows:

a) Pre-provisioning approach:

Each (fg)OTN edge node, which connects to a client network (user-side or cloud-side client network), shall report the addresses of the nodes in the client network to the SMCC before a service flow arrives, including:

- Ethernet MAC addresses of the nodes in the client network.
- IPv4 or IPv6 addresses of the nodes or prefixes in the client network.

NOTE 1: The (fg)OTN edge nodes may acquire the address information of the nodes in the client network by manual configuration (i.e. static route configuration for a VPN network access), or by using existing IP/Ethernet related protocols (including BGP). How the (fg)OTN edge nodes acquire the address of the nodes in the client network is out of scope of the present document.

b) Dynamic provisioning approach:

In this approach, the client node address information is collected from the service packets after a service flow arrives. Each (fg)OTN edge node shall learn the service address attributes and report them to the SMCC after a service flow arrives, including:

- Source and Destination Ethernet MAC addresses.
- Source and Destination IPv4 or IPv6 addresses.

NOTE 2: The source and destination MAC / IP addresses (i.e. the service address attributes) in the service packet headers are the addresses of the service source and destination nodes which are located on the user-side and on the cloud-side client networks.

For both pre-previsioning and dynamic provisioning approaches, the addresses of the nodes in the client networks are reported to the SMCC.

The SMCC shall collect all the client node addresses reported from all (fg)OTN edge nodes in the network and generate a Service Address Table (SAT), see Figure 7.

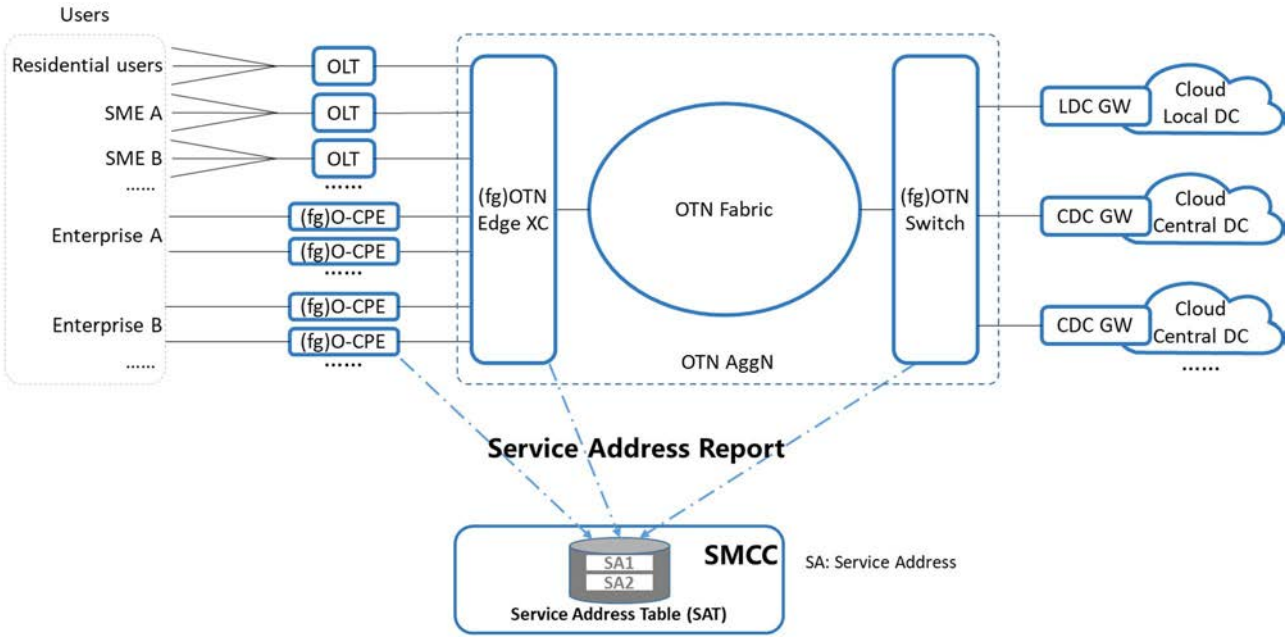

Figure 7: Collecting service addresses by the SMCC

The Service Address Table shall include the following attributes:

- The (fg)OTN edge node Identifiers.
- Identifiers of the client-side ports of the (fg)OTN edge nodes.
- Service/client node addresses (the MAC addresses, or IP addresses or prefixes of the client network nodes).

and the SAT may include:

- Other service attributes carried in the service packet headers, which is for future study.

7.2.4 Service mapping rules generating and maintaining

The service mapping rule includes the source service address, destination service address and the corresponding (fg)OTN connection identifier.

The SMCC shall generate and maintain the service mapping rules, as follows:

1) In the pre-provisioning approach (see clause 7.2.3 of the present document), for each pair of (source service address, destination service address), the SMCC determines the source and destination OTN edge nodes and the associated client-side ports on which the client service flow will be received from or sent to, according to the SAT. In the dynamic provisioning approach (see clause 7.2.3 of the present document), with the received source and destination service addresses information from the source OTN edge node, the SMCC determines the client-side port of the source (fg)OTN edge node on which the client service flows are received from, then determines the destination (fg)OTN edge node and its client-side port which matches the destination service address, by searching the SAT.

2) Based on the source and destination service addresses, the SMCC calculates the corresponding (fg)OTN connection between the client-side ports of the source and the destination (fg)OTN edge nodes, and generates the (fg)OTN connection identifier. This forms the bases for the SMCC to generate the service mapping rules.

3) The SMCC sends the service mapping rules to the source and destination (fg)OTN edge nodes, so that the client service flows can be transported by the corresponding (fg)OTN connections.

The SMCC shall also support dynamic updating of the service mapping rules based on changes of the client service attributes.

7.2.5 Service mapping

On receiving the service mapping rules, the (fg)OTN edge node shall generate the Service Mapping Table (SMT) in its data plane. Table 1 shows the information contained in the SMT.

Table 1: (fg)OTN edge node Service Mapping Table (SMT)

Service Attributes (Matching)	(fg)OTN Connection
SVLAN	(fg)OTN Connection Identifier
CVLAN	
Source service address (MAC address)	
Destination service address (MAC address)	
Source service address (IP address or address prefix)	
Destination service address (IP address or address prefix)	

The SMT provides the (fg)OTN edge node with the necessary information to transmit the service flows between service source and destination nodes (located in the user-side and cloud-side client networks) through the (fg)OTN connection. If one or more the service flow service attributes match those in the SMT, the (fg)OTN edge node shall automatically map the service flows to the corresponding (fg)OTN connection specified in the SMT, and de-map the service flows from the (fg)OTN connection. Figure 8 shows a simple example of service mapping and de-mapping.

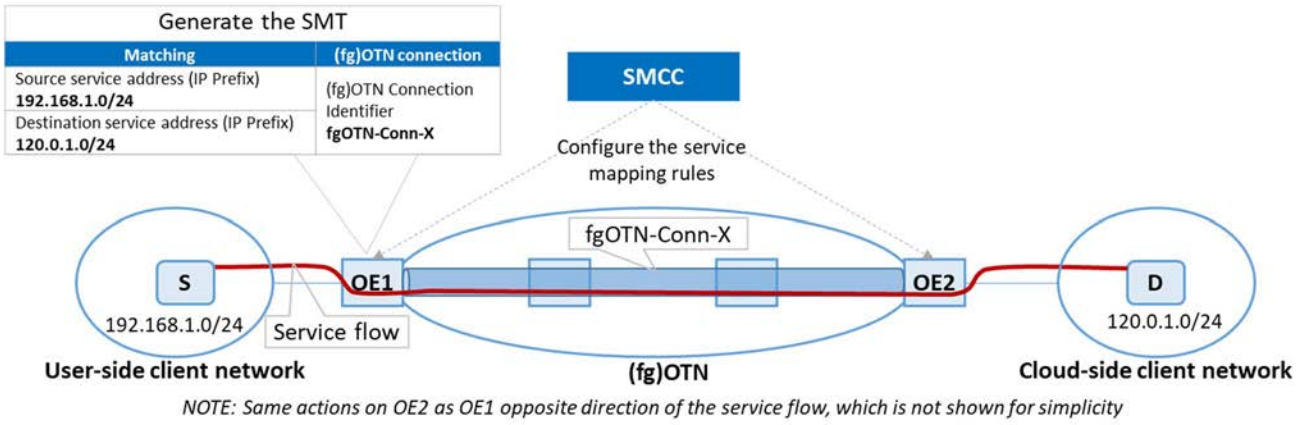

Figure 8: Example of service mapping and de-mapping process

7.2.6 OCN service control protocol messages

The present document gives a basic concept of the OSP service control messages for the C2/C2' interfaces for communication between SMCC and the (fg)OTN edge nodes. There are two messages types:

- Service/client node Address Report.
- Service Mapping Update.

NOTE: The detailed OSP service control message format is not defined in the present document and is for further study.

The Service/client node Address Report message is used to report the service/client node addresses from the (fg)OTN edge nodes to the SMCC (see clause 7.2.3). This message has the following parameters:

- Network slice/VPN identifier (see clause 7.1.2).
- (fg)OTN edge node identifier.
- Identifiers of the client-side ports of the (fg)OTN edge nodes.
- Service/client node addresses.

The Service Mapping Update message is sent by the SMCC to the (fg)OTN edge nodes, to update the SMT (see clause 7.2.5). This message has the following parameters:

- Network slice/VPN identifier (see clause 7.1.2).
- Service/client node addresses.
- (fg)OTN connection attributes:
  - Source (fg)OTN edge node identifier.
  - Destination (fg)OTN edge node identifier.
  - (fg)OTN connection identifier.

Figure 9 illustrates the message flow of a Service/client node Address Report message from the (fg)OTN edge node OE1 to the SMCC and a Service Mapping Update message from the SMCC to the (fg)OTN edge node OE2, and vice versa.

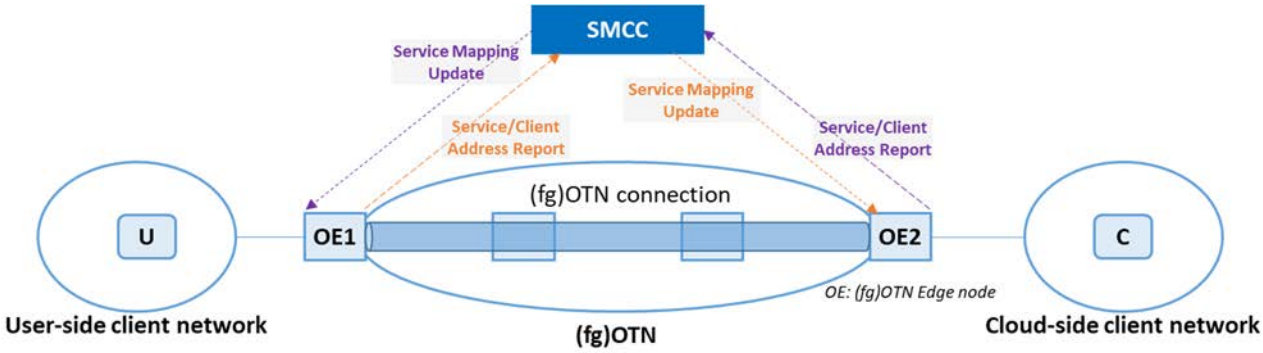

Figure 9: Service control messages

7.3 OSP connection control

7.3.1 Connection provisioning

7.3.1.1 Overview of connection provisioning

The following functional requirements shall be supported for OCN connection control:

1) E2E (fg)OTN connection creation: To automatically create (fg)OTN connections through transmitting signalling information.

2) Hitless bandwidth adjustment of the (fg)OTN connections: To perform hitless bandwidth adjustment of the (fg)OTN connections, triggered by the service demands.

NOTE: An (fg)OTN connection may be used to transport multiple services. The bandwidth adjustment of an (fg)OTN connection may be based on, for example, a change in the number of services, service's bandwidth adaptation needs, or a shift in service/application bandwidth needs.

3) E2E (fg)OTN connection deletion: To automatically delete (fg)OTN connections through transmitting signalling information.

4) Scalability: Scalable connection control for increasing the number of (fg)OTN connections, especially for fgOTN connections.

7.3.1.2 (fg)OTN connection creation

The (fg)OTN connection creation may be initiated by the users through the management and control system, or by a UNI-side service request. Therefore, there are two implementation approaches for the (fg)OTN connection creation:

Controller-driven approach.

UNI-driven approach:

a) Controller-driven approach

The management and control system sends the control information to the source node of the (fg)OTN connection, and then the source node sends the control information to other (fg)OTN nodes on the connection path through the OCN control plane OSP connection control signalling, to establish the (fg)OTN connection.

The control information from the management and control system to the source node shall include the following (fg)OTN connection information:

- Connection ID.
- Protection Type.
- Path Type, working path, protection path or restoration path.
- Connection Bandwidth.
- A list of Route Hops:
  - Node ID.
  - Ingress interface and ingress label.
  - Egress interface and egress label.

NOTE 1: The ingress and egress labels represent the resources in the ingress and egress interfaces used to form the connection. The label is technology specific. For example, in the OTN electrical layer, the label could be the tributary slots used to form the ODU connection. In a WDM photonic network, the label could be the wavelength used to form the optical connection.

Each (fg)OTN node on the connection path allocates the bandwidth resources and creates the (fg)OTN cross-connection between ingress interface/label and egress interface/label.

If the (fg)OTN connection creation fails for any reason (including unavailable resources), the (fg)OTN connection state shall be rolled back in the (fg)OTN nodes as well as in the management and control system, ensuring data plane and control plane consistency. The management and control system may compute a new path around the blocked link or node and initiate the connection creation again.

The signalling mechanism shall support the concurrent provisioning of multiple connections, meaning a single message may contain multiple connection information.

There are two methods for the source node to send the control signalling information to other nodes to establish the (fg)OTN connection:

- Hop-by-hop signalling method.
- Parallel signalling method:

1) Hop-by-hop signalling method: The control signalling is sent hop by hop from the source node to the destination node along the connection path to trigger the cross-connection creation on each node. After the cross-connection is created successfully on the destination node, an acknowledgement signalling message is then sent back hop by hop from the destination node to the source node to confirm the successful cross-connection creation. Figure 10 shows the process.

The signalling shall include the following (fg)OTN connection information:

- Connection ID.

- Protection Type.
- Path Type (working path, protection path or restoration path).
- Connection Bandwidth.
- A list of Route Hops:
  - Node ID.
  - Egress interface and egress label.

Wherein the "A list of Route Hops" may further include the ingress interface and ingress label information.

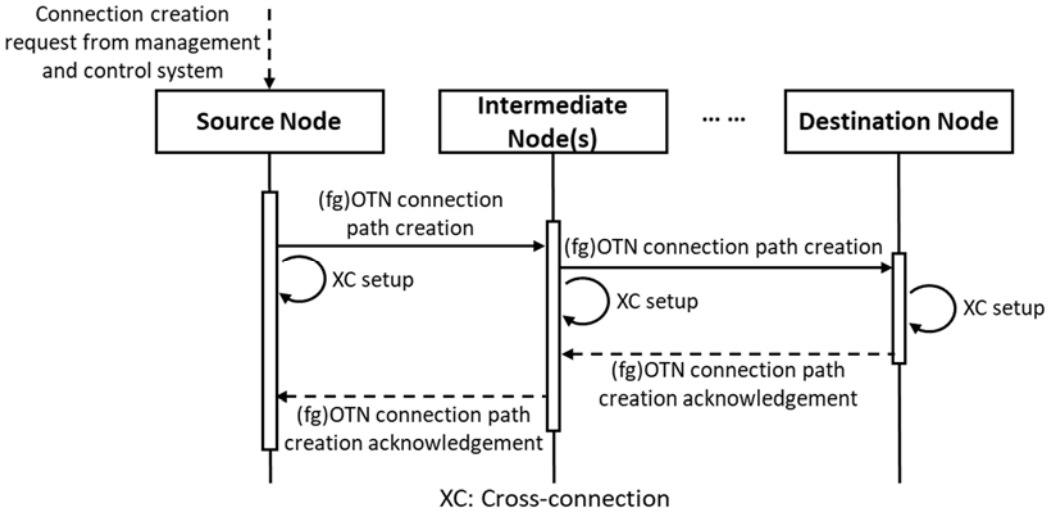

Figure 10: Hop-by-hop signalling method for (fg)OTN connection creation

NOTE 2: The source node may create the cross-connection before or after it sends the control signalling to all the downstream nodes.

2) Parallel signalling method: The control signalling is sent directly from the source node to other nodes on the connection path in parallel. After the cross-connection is created successfully, each node sends the acknowledgement signalling back directly to the source node to confirm the successful cross-connection creation. Figure 11 shows the process.

The signalling shall include the following (fg)OTN connection information:

- Connection ID.
- Connection Bandwidth.
- Cross-connection information:
  - Ingress interface and ingress label.
  - Egress interface and egress label.

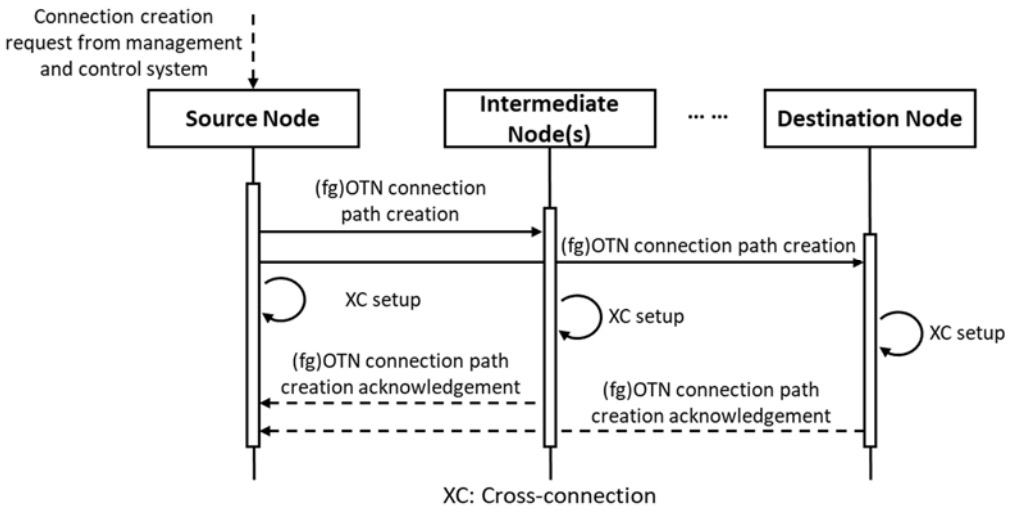

Figure 11: Parallel signalling method for (fg)OTN connection creation

NOTE 3: The source node may create the cross-connection before or after it sends the control signalling to all the downstream nodes.

b) UNI-driven approach

The UNI-C initiates the service creation process. After receiving the service creation request from the client network through the UNI, the (fg)OTN edge node (i.e. the (fg)OTN source node) starts the (fg)OTN connection establishment within the (fg)OTN by using the control plane OSP connection control signalling. Both hop-by-hop and parallel signalling methods are applicable for the source node to create the connection in the (fg)OTN, which is the same as that in a) in this clause.

Figure12 shows a simple example where hop-by-hop method is used.

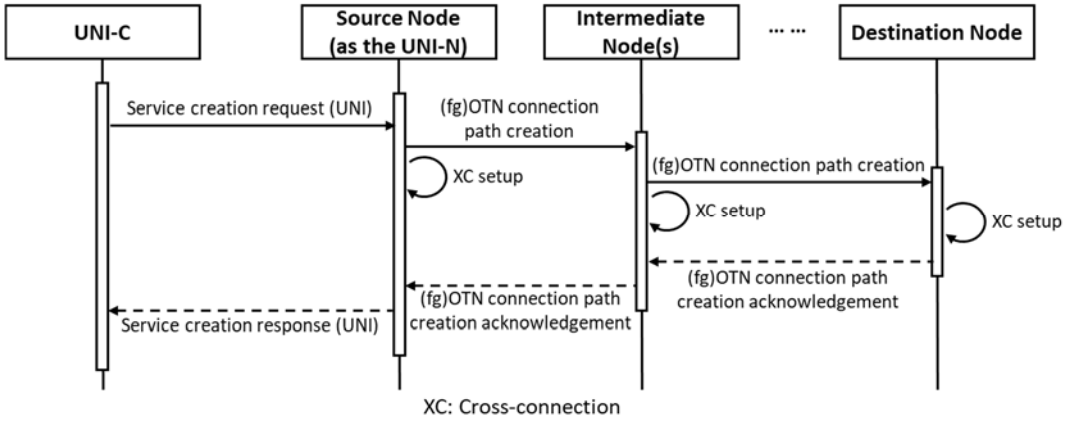

Figure 12: UNI-driven approach for (fg)OTN connection creation (using hop-by-hop signalling method)

NOTE 4: The source node may create the cross-connection before or after it sends the control signalling to all the downstream nodes.

The (fg)OTN shall provide an appropriate mechanism to ensure accurate and authorized usage of network resources as well as an appropriate mechanism to ensure UNI client accountability. Collectively, these mechanisms are often referred to as policy control. Policy-based criteria are applied in addition to resource availability considerations when deciding whether a connection creation request can be accommodated within the (fg)OTN. The details of policy control mechanisms are for future studies.

7.3.1.3 (fg)OTN connection bandwidth adjustment

The (fg)OTN connection bandwidth adjustment may be initiated by the users through the management and control system, or by UNI-side service requests.

The (fg)OTN data plane bandwidth adjustment mechanisms include hitless adjustment of ODUflex(GFP) defined in Recommendation ITU-T G.7044/Y.1347 [9] and fgOTN defined in Recommendations ITU-T G.7044/Y.1347 [9] and G.709 [7].

If the (fg)OTN connection bandwidth adjustment fails in the data plane, the (fg)OTN connection states shall be rolled back in the (fg)OTN nodes as well as in the management and control system, ensuring data plane consistency.

There are two approaches for E2E (fg)OTN connection bandwidth adjustment:

Controller-driven approach.

UNI-driven approach:

a) Controller-driven approach

The management and control system sends the control information to the source node of the (fg)OTN connection, and then the source node initiates the bandwidth adjustment process which follows the Recommendations ITU-T G.7044/Y.1347 [9] (for ODUflex(GFP) connections) and G.709 [7] (for fgOTN connections). The process is shown in Figure 13.

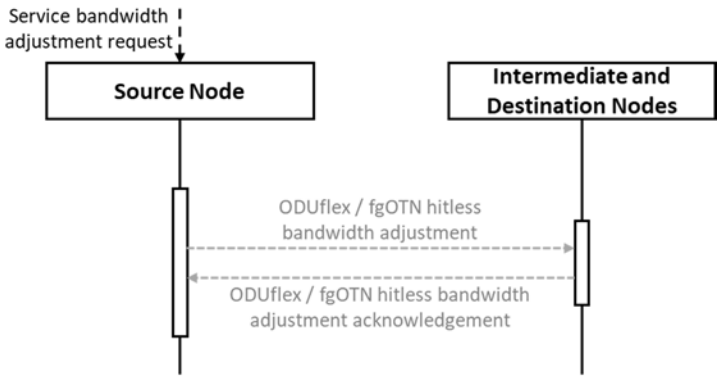

Figure 13: Controller-driven approach for (fg)OTN connection bandwidth adjustment

The control information from the management and control system to the source node shall include the following (fg)OTN connection information:

- Connection ID.
- Target bandwidth.
- Original bandwidth.

The control information may also include:

- A list of Route Hops:
  - Node ID.
  - Ingress interface and ingress label.
  - Egress interface and egress label.

b) UNI-driven approach

The UNI-C initiates the service bandwidth adjustment. After receiving the service bandwidth adjustment request from the client network through the UNI, the (fg)OTN edge source node starts the (fg)OTN connection bandwidth adjustment within the (fg)OTN carrier network. The connection bandwidth adjustment process within the OTN is the same as the process in a) in this clause. Once the bandwidth adjustment process is finished, the OTN source node shall report the bandwidth adjustment result to the management and control system.

The (fg)OTN shall provide an appropriate mechanism to ensure accurate and authorized usage of network resources as well as an appropriate mechanism to ensure UNI client accountability. Collectively, these mechanisms are referred to as policy control. Policy-based criteria are applied in addition to resource availability considerations when deciding whether a connection bandwidth adjustment request can be accommodated within the (fg)OTN. The details of policy control mechanisms are for future studies.

The bandwidth adjustment policies, including service flow rate threshold, may be configured on the (fg)OTN edge nodes UNI-N from network management and control system. When the client service rate exceeds the threshold on a client-side port of an (fg)OTN edge node the (fg)OTN connection bandwidth adjustment process will be automatically triggered.

NOTE: When the client service rate exceeds the threshold on a client-side port of an (fg)OTN edge node, both the threshold and the current client service rate need to be below the current (fg)OTN connection bandwidth to allow hitless service transmission. The UNI-driven bandwidth adjustment process is shown in Figure 14.

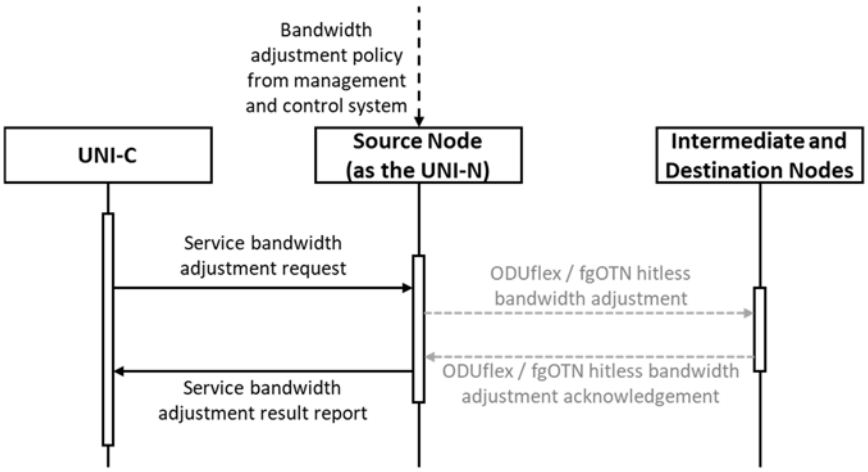

Figure 14: UNI-driven approach for (fg)OTN connection bandwidth adjustment

7.3.1.4 (fg)OTN connection deletion

The (fg)OTN connection deletion may be initiated by the users through the management and control plane, or by UNI-side service requests. Therefore, there are two approaches for (fg)OTN connection deletion:

Controller-driven approach.

UNI-driven approach:

a) Controller-driven approach

The management and control system sends the control information to the source node of the (fg)OTN connection, and then the source node sends the control information to other (fg)OTN nodes on the connection path through the control plane connection control signalling, to delete the (fg)OTN connection.

The control information from the management and control system to the source node shall include the following (fg)OTN connection information:

- Connection ID.

The control information may also include:

- Protection Type.
- Path Type (working path, protection path or restoration path).
- Connection Bandwidth.
- A list of Route Hops:
  - Node ID.
  - Ingress interface and ingress label.
  - Egress interface and egress label.

Each (fg)OTN node on the connection path releases the bandwidth and deletes the (fg)OTN cross-connection between ingress interface/label and egress interface/label.

If the (fg)OTN connection deletion fails for any reason, the (fg)OTN connection state shall be rolled back in the (fg)OTN nodes as well as in the management and control system, ensuring data plane and control plane consistency.

The signalling mechanism shall support the concurrent deletion of multiple (fg)OTN connections, meaning a single message may contain multiple delete connection information.

There are two methods for the source node to send the control signalling information to other nodes to delete the (fg)OTN connection:

- Hop-by-hop signalling method.
- Parallel signalling method.

1) Hop-by-hop signalling method: The control signalling is sent hop by hop from the source node to the destination node along the connection path to trigger the cross-connection deletion on each node. After the cross-connection is deleted successfully on the destination node, an acknowledgement signalling is then sent back hop by hop from the destination node to the source node to confirm the successful cross-connection deletion. Figure 15 shows the process.

   The signalling shall include the following (fg)OTN connection information:

   - Reason for deletion.
   - Connection ID.

   The signalling may also include:

   - A list of Route Hops:
     - Node ID.
     - Ingress interface and ingress label.
     - Egress interface and egress label.

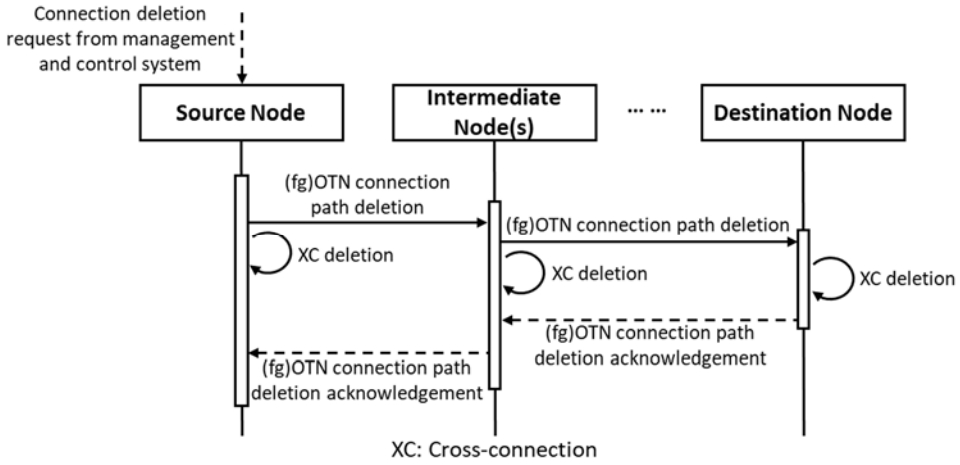

Figure 15: Hop-by-hop signalling method for (fg)OTN connection deletion

NOTE 1: The source node and each intermediate node may delete the cross-connection before or after it sends the control signalling to its downstream node.

2) Parallel signalling method: The control signalling is sent directly from the source node to all the other nodes on the connection path in parallel. After the cross-connection is deleted successfully, each node sends the acknowledgement signalling back directly to the source node to confirm the successful cross-connection deletion. Figure 16 shows the process.

The signalling shall include the following (fg)OTN connection information:

- Reason for deletion.
- Connection ID.

The signalling may also include:

- Cross-connection information:
  - Ingress interface and ingress label.
  - Egress interface and egress label.

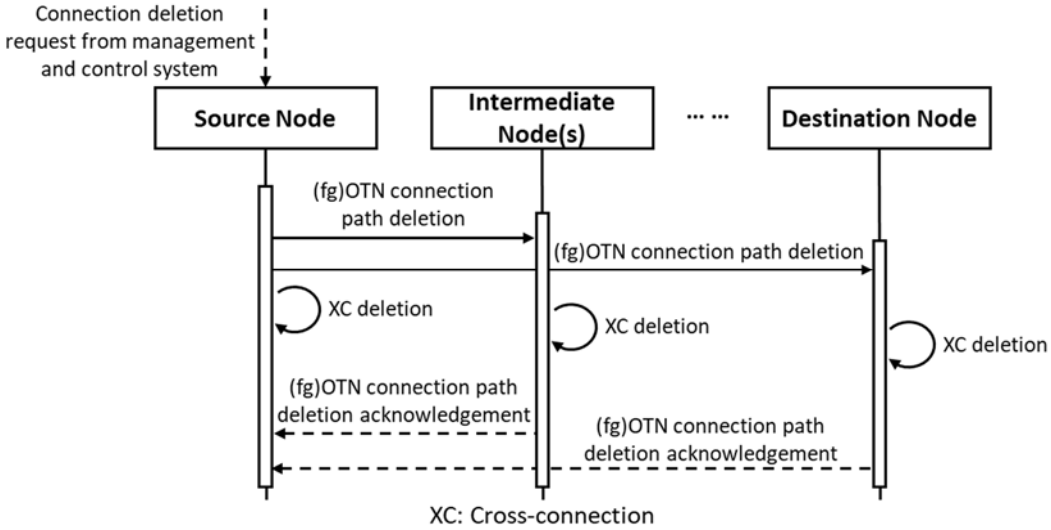

Figure 16: Parallel signalling method for (fg)OTN connection deletion

NOTE 2: The source node may delete the cross-connection before or after it sends the control signalling to all the downstream nodes.

b) UNI-driven approach

The UNI-C initiates the connection deletion process. After receiving the service deletion request from the client network through the UNI, the (fg)OTN edge source node starts the (fg)OTN connection deletion within the (fg)OTN carrier network by using the control plane connection control signalling. Both hop-by-hop and parallel signalling methods are applicable for the source node to delete the connection in the (fg)OTN, which is the same as that in a) in this clause.

Figure 17 shows a simple example where hop-by-hop method is used.

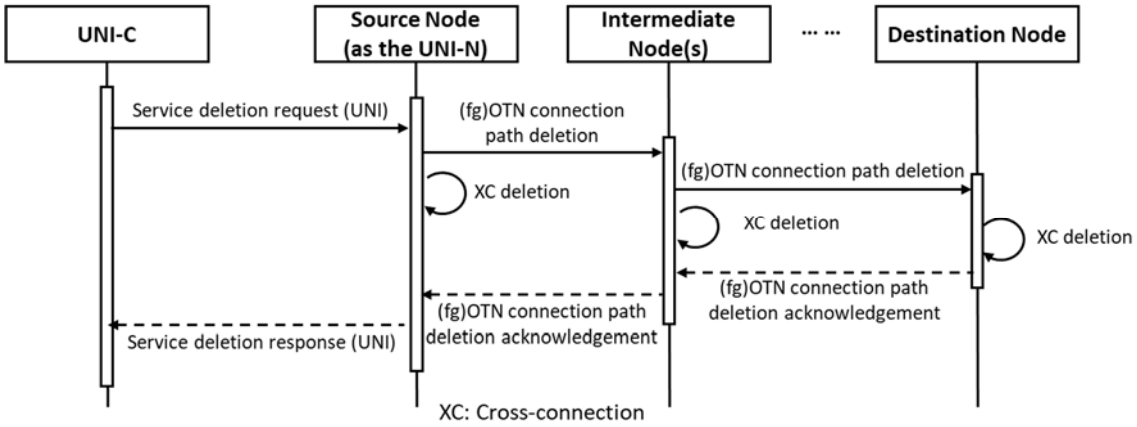

Figure 17: UNI-driven approach for (fg)OTN connection deletion (using hop-by-hop signalling method)

NOTE 3: The source node and each intermediate node may delete the cross-connection before or after it sends the control signalling to its downstream node.

The OTN network shall provide an appropriate mechanism to ensure accurate and authorized usage of network resources and an appropriate mechanism to ensure the UNI client accountability. Collectively, these mechanisms are often referred to as policy control. Policy-based criteria are applied in addition to resource availability considerations when deciding whether a connection deletion request can be accommodated within the (fg)OTN transport network. The details of policy control mechanisms are for future studies.

7.3.2 Connection recovery

7.3.2.1 Overview of connection recovery

The reliability of the (fg)OTN carrier network connecting the service user and the Cloud DCs is extremely important. The recovery of (fg)OTN connections following network failure(s) is essential to improve the availability of the services. Protection (1+1 protection), restoration (rerouting) mechanisms or a combination of them shall be used.

The (fg)OTN connection control shall satisfy the following functional requirements for end-to-end (fg)OTN connection recovery:

1) Support the following protection and restoration mechanisms, and a combination of them:

- (fg)OTN 1+1 protection: The protection switching time shall be less than 50 ms.
- (fg)OTN restoration: In the event of an (fg)OTN connection failure, a new restoration connection (the route of the restoration path may be pre-calculated or calculated in real-time) is established for recovery.
- Combination of (fg)OTN 1+1 protection and restoration: Initially, a working path and a protection path are created to form a 1+1 protection group. In the event of the first failure on the working path, the service is recovered by 1+1 protection switch to the protection path, with the protection switching time less than 50 ms. In the event of the second failure, the restoration mechanism is used for recovery.

- (fg)OTN permanent 1+1 protection: Initially, a working path and a protection path are created to form a 1+1 protection group. Whenever one of the paths in the protection group is failed, a new path will be created to replace the failed path, and then the new 1+1 protection group will be formed, provided that there are sufficient resources in the network. The protection switching time shall be less than 50 ms.

2) Support reversion mechanism, i.e. after the service is switched to the protection or restoration path, if the working path is recovered, the service will be switched back to the working path. It shall be configurable to enable or disable the reversion mechanism.

3) Support "make-before-break" connection restoration mechanism, where the resources of the failed working path will not be released until the restoration path is fully established. In such case, the resources of the failed working path can be reused by the restoration path.

4) Support the crankback mechanism. When the restoration path setup is blocked (because a link or node along the path has insufficient resources), the crankback mechanism allows the new restoration path setup to detour around the location of the failure. The number of crankback retry times shall be configurable.

5) Support a large number of (fg)OTN connection restoration for one or multiple network failures, with deterministic connection restoration performance.

6) Support dual-homing protection (Optional): Both user-side and cloud-side dual-homing protection mechanisms may be supported. Clauses 4.14 and 4.15 of ETSI GS F5G 013 [12] provide the technical requirements on the dual-homing protection for both enterprise private line and premium home broadband connectivity services. Figure 18 shows two examples of OTN dual-homing protection, which are from ETSI GS F5G 013 [12]. The details of dual-homing protection mechanisms are for future studies.

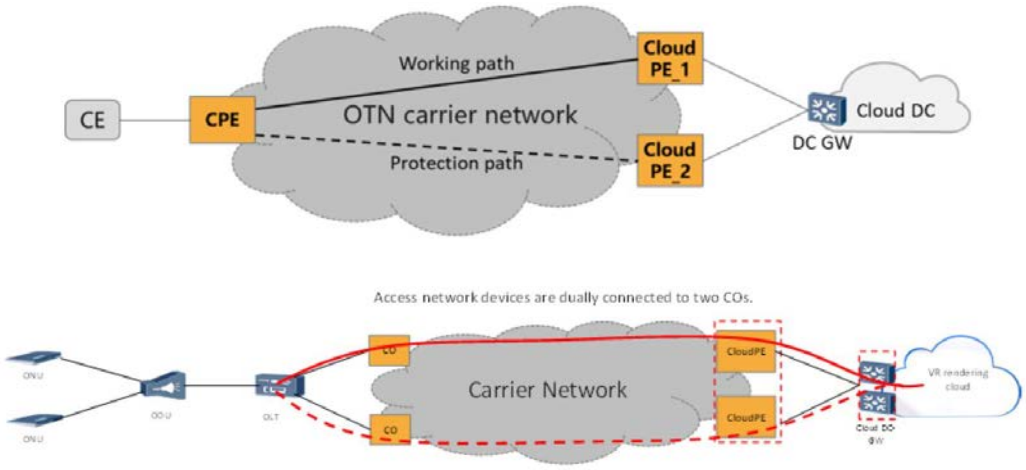

Figure 18: Examples of OTN dual-homing protection (Source: ETSI GS F5G 013 [12])

NOTE: The present document focuses on linear protection and restoration. Other protection types (including Ring protection) are for further study.

7.3.2.2 1+1 Protection function requirements

The management and control system shall support the provisioning of OTN working and protection paths to form a 1+1 protection group, in both 1+1 protection and permanent 1+1 protection scenarios.

A dedicated, resource-disjoint protection path is pre-established to protect the working path. Traffic is simultaneously sent on both paths; under normal conditions, the traffic from the working path is received by source node and destination node. See clause 7.3.1.2 of the present document for more detail on the OTN connection path creation process.

There are two recovery switching modes for 1+1 protection scheme, as shown in Figure 19. More details are defined in Recommendation ITU-T G.873.1 [13].

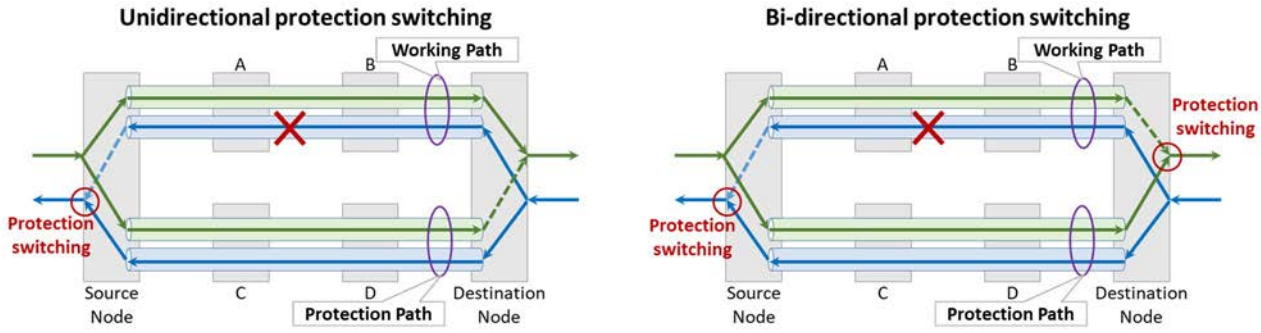

Figure 19: Unidirectional and bi-directional protection switching

a) Unidirectional protection switching

A unidirectional protection switching recovery switching mode is one in which, for a unidirectional fault (a fault affecting only one direction of transmission), only the normal traffic transported in the affected direction of the working path is switched to the protection path see left-hand side of Figure 19. A failure affecting the working path results in the receiving end node (either source node or destination node) selecting the traffic from the protection path in the respective direction.

There is no explicit signalling involved with this mode of protection.

b) Bi-directional protection switching

A bidirectional protection switching recovery switching mode is one in which, for a unidirectional fault, the normal traffic in both directions of the working path, including the affected direction and the unaffected direction, are switched to the protection path. A failure affecting the working path results in both source node and destination node selecting the traffic from the protection path in the respective directions.

This requires coordination between source node and destination node to switch to the protection path. The signalling mechanisms may be used to report the connection path failure alarm, as well as the switchover request and response.

7.3.2.3 Restoration function requirements

Restoration refers to the mechanism in which the protection path is only fully created after the working path has failed. In this way, the restoration resource for different working paths (which do not share the same risk of link/node failure) may be shared for the restoration paths pre-computation before failure happens. This could improve the resource utilization, compared with the 1+1 protection mechanism.

The present document focuses on the end-to-end restoration mechanisms where the working and restoration paths have the same source and destination nodes. Segment restoration cases are for further study.

Restoration mechanism shall support bi-directional switching mode, and it is optional to support uni-directional switching.

Three approaches to restoring an (fg)OTN connection shall be supported.

NOTE: Different approaches may be chosen for different (fg)OTN connections in the network, depending on the network operator's policies and users' service requirements.

a) Dynamic restoration

In the event of an (fg)OTN connection failure, the (fg)OTN connection source node is notified of the connection failure alarm and then the source node reports the connection failure to the management and control system. The management and control system calculates the restoration path in real time based on the available network resources, and triggers the restoration path creation process. After the connections are rerouted, the source node shall report to the management and control system the connection restoration event. The dynamic restoration process is shown in Figure 20.

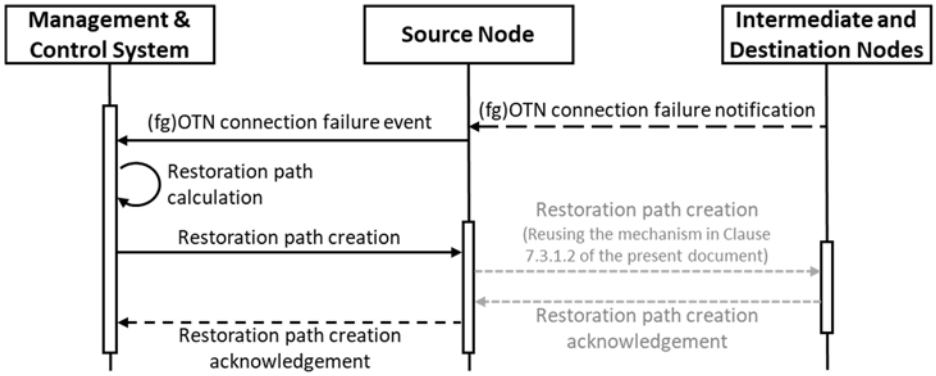

Figure 20: Dynamic restoration

The (fg)OTN connection failure notification signalling shall include the following information:

- Connection ID.
- Node ID of the node detecting the failure.

The (fg)OTN connection failure notification signalling may further include:

- Failure link/port ID.

The source node sends the signalling messages along the restoration path to create the path, the process of which is the same as that of a normal (fg)OTN connection creation. See clause 7.3.1.2 of the present document for more detail on the path creation process and control signalling information.

The signalling mechanism shall support the concurrent provisioning of multiple connection restoration paths, meaning a single message shall contain multiple connection restoration path information.

The mechanism "Make-before-break" may be used in the dynamic restoration approach. The restoration path may reuse some resources of the previous working path under failure condition and may also include additional intermediate nodes.

b) Pre-calculation of restoration path

The management and control system calculates the restoration path of the (fg)OTN connections in advance, and pre-configured the calculated route on the source node. Once the (fg)OTN connection failure occurs, the source node creates the restoration path based on the pre-calculated route. After the connections are rerouted, the source node shall report to the management and control system the restoration event. The whole restoration process is shown in Figure 21.

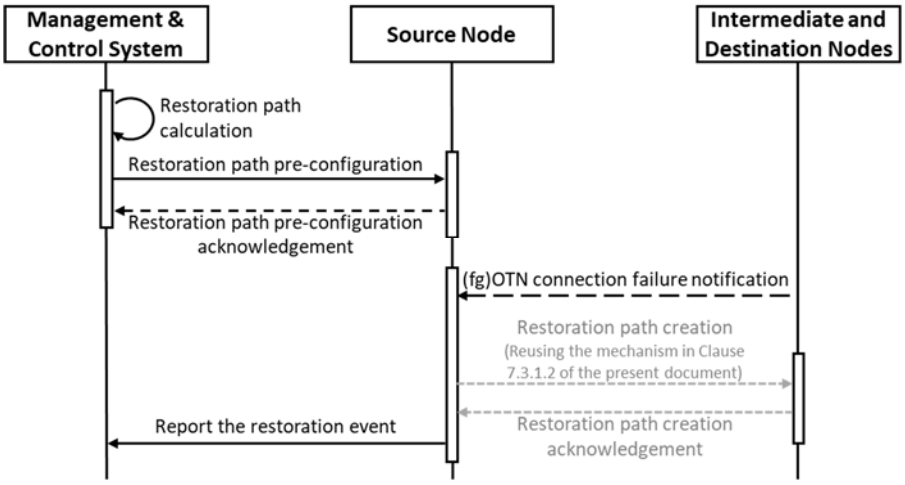

Figure 21: Pre-calculation of restoration path

The (fg)OTN connection failure notification signalling shall include the following information:

- Connection ID.
- Node ID of the node detecting the failure.

The (fg)OTN connection failure notification signalling may include:

- Failure link/port ID.

The source node sends the signalling messages along the restoration path to create the path, the process of which is the same as that of a normal (fg)OTN connection creation. See clause 7.3.1.2 of the present document for more detail on the path creation process and control signalling information.

The signalling mechanism shall support the concurrent provisioning of multiple connection restoration paths, meaning a single message shall contain multiple connection restoration paths information.

Multiple restoration paths are allowed to share common link and node resources. In this case, the protection capacity is typically shared only amongst (fg)OTN connections whose working paths are physically diverse, meaning these working paths that do not share the same risk of link/node failure.

c) Pre-configuration of restoration resource on each node

The management and control system calculates the restoration path of the (fg)OTN connections in advance, and pre-configure the restoration resource on each node along the restoration path.

Once the (fg)OTN connection failure occurs, the source node triggers the activation of the pre-configured restoration resources on each node along the restoration path.

The general restoration process is shown in Figure 22.

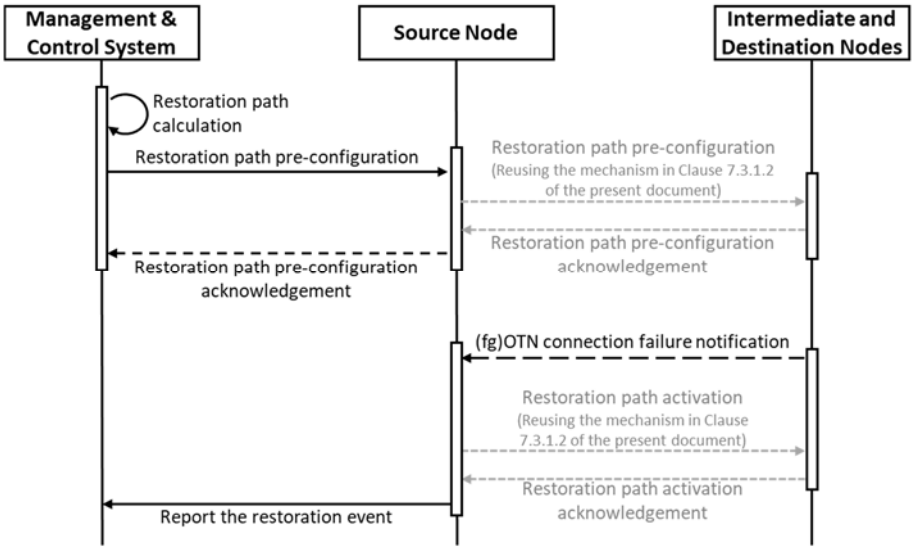

Figure 22: Pre-configuration of restoration resources on each node

When pre-configuring the restoration path before failure occurs, the cross-connection in each intermediate node along the restoration path can be created in advance, which pre-occupies the protection bandwidth X that is configurable and is much smaller than the target bandwidth that will be needed for the restoration path to transmit the service after failure occurs. In a typical example, in the fgOTN context, the pre-occupied protection bandwidth could be approximatively 10 Mbps, i.e. the minimum fgOTN connection bandwidth.

The source node sends the signalling messages along the restoration path to pre-configure the path, the process of which is the same as that of a normal (fg)OTN connection creation, except that the connection bandwidth information needs to include both the pre-occupied protection bandwidth (before failure occurs) and the target bandwidth (after failure occurs). See clause 7.3.1.2 of the present document for more detail on the path creation process and control signalling information.

Since the restoration path is created in advance and only occupies small protection bandwidth, most of the protection resource for different working paths which do not share the same risk can still be shared.

In the event of an (fg)OTN connection failure, the (fg)OTN connection source node is notified of the connection failure alarm. The (fg)OTN connection failure notification signalling shall include the following information:

- Connection ID.
- Node ID of the node detecting the failure.

The (fg)OTN connection failure notification signalling may include:

- Failure link/port ID.

When the source node receives the working connection failure notification, it generates and sends a bandwidth activation message along the restoration path, to trigger each intermediate node to increase the bandwidth of the restoration path, meaning from the pre-occupied protection bandwidth to the target bandwidth that is needed for the restoration path to transmit the service. The process of increasing the restoration path bandwidth is similar to one described in clause 7.3.1.3 of the present document. The only difference is that the hitless adjustment is not required here.

Figure 23 shows a restoration example where restoration path is created in advance with small protection bandwidth.

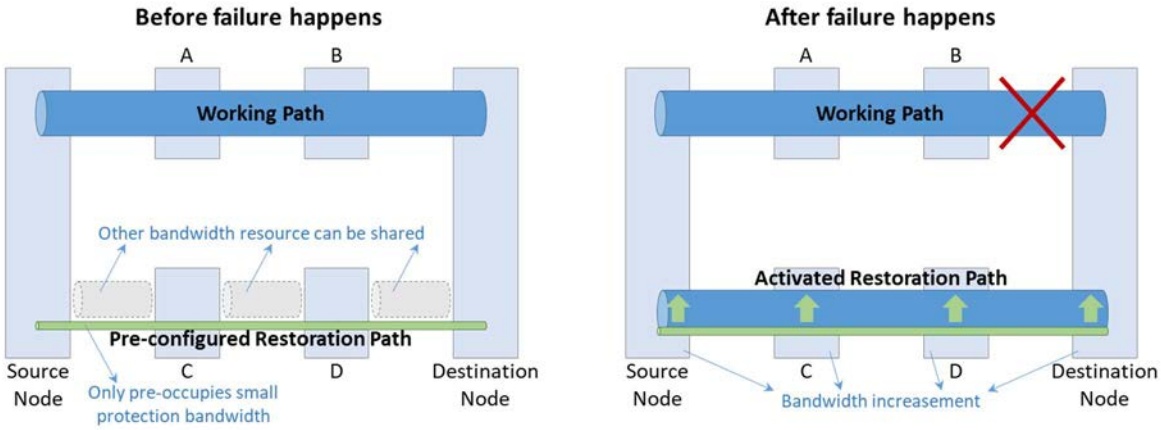

Figure 23: Example of pre-configuration of restoration resource on each node

Since the cross-connections in the restoration path has been created in advance, and only bandwidth increasement process is needed when activating the restoration path, the service could be recovered in a much shorter time.

8 OCN management and control technical requirements

8.1 Overview

The (fg)OTN network is used to transport high-quality cloud services in the OCN architecture. The service traffic flows are mapped into/de-mapped from an (fg)OTN connection (see Recommendation ITU-T G.709 [7]) at the (fg)OTN end-points. The (fg)OTN connection end-points are located on the (fg)O-CPE, the (fg)OTN Edge XC and the (fg)OTN switch in the AggN Edge node, which are shown in Figure 3 in clause 5.3 of the present document.

The technical requirements of OCN management and control includes:

1) Management and control of the service flow mapping.

2) Management and control of the (fg)OTN.

8.2 Technical requirements for management and control of service flow mapping

8.2.1 Configuration and maintenance of network slices and Virtual Private Networks (VPNs)

The management and control system shall support the configuration of network slices or VPNs on the (fg)OTN edge nodes where the service flows are mapped/de-mapped to/from (fg)OTN. The network slice or VPN configuration on the edge (fg)OTN nodes includes:

1) Assigning and configuring a network slice or VPN ID for each service.

2) Assigning a set of physical or virtual client-side interfaces (with VLAN identifiers associated with a physical client-side interface) to each network slices or VPNs.

The management and control system shall support maintaining network slices or VPNs configuration for the lifecycle of the associated high-quality cloud services.

8.2.2 Creation and maintenance of service flow mapping rules

Different service flows are mapped into/de-mapped from different (fg)OTN connections at the (fg)OTN path end-points. This is processed by the SMPs located at the end-points of the (fg)OTN path, Figure 8 in clause 7.2.5 of the present document shows more details.

The management and control system shall automatically generate and create the service flow mapping rules (see clause 7.2.4 of the present document for more details) for each network slice or VPN via the C2 and C2' interfaces (see clause 5.3 of the present document).

The management and control system shall maintain the mapping rules between the service flows and the (fg)OTN connections for the lifecycle of the associated services.

8.3 Technical requirements for management and control of the (fg)OTN

8.3.1 Maintenance of the OTN network topology information

The management and control system shall collect and maintain the OTN network topology and update the topology information based on the network state changes. The OTN topology includes the (fg)OTN nodes, and the OTN links interconnecting the (fg)OTN nodes.

IETF RFC 8345 [14] specifies network topology including node, termination point and link, and IETF RFC 8795 [15] specifies Traffic Engineering (TE) extensions to network topology including node, termination point and link.

The OTN topology information shall include:

a) (fg)OTN node information:

- Node ID (The identifier for an (fg)OTN node in the network).
- Node operational state.
- Node switch capabilities.
- A list of termination points (see IETF RFC 8345 [14]).

b) OTN link information:

- Link ID.
- Source node and source termination point.
- Destination node and destination termination point.
- Link operational state.
- Maximum bandwidth (total bandwidth of the OTN link, see IETF RFC 8795 [15]).
- Unallocated bandwidth (available bandwidth of the OTN link, see IETF RFC 8795 [15]).
- Shared Risk Link Groups (SRLGs).
- Latency.
- TE default metric (Typically it is assigned by a network administrator for traffic engineering purposes, see IETF RFC 8795 [15]).

8.3.2 (fg)OTN path computation

The management and control system shall support (fg)OTN path computation upon receiving a request, which could either be from either the E2E Orchestrator through North Bound Interface (NBI) or from an (fg)OTN node in the network.

NOTE 1: An (fg)OTN path is a sequence of (fg)OTN nodes and links, the first (fg)OTN node is called source node and the last (fg)OTN node is destination node.

The path computation request information shall include:

- Source and destination (fg)OTN nodes (Identifier of the source and destination (fg)OTN nodes).
- The type of the client signal.
- Required Bandwidth (see IETF RFC 8795 [15]).
- The protection and restoration type of the (fg)OTN connection and the related configurations.

The path computation request information may include:

- Routing policy.
- Path computational constraints.

The following routing policy shall be supported for (fg)OTN path computation:

a) Minimum number of hops: The path shall traverse a minimum number of (fg)OTN nodes.

b) Latency: The path latency (the sum of latency of all nodes and links traversed by the path) shall meet the E2E requirement.

c) Load distribution: Both TE default metric and link bandwidth utilization are taken into consideration for path selection.

NOTE 2: Since the default routing policy (Minimum number of hops) usually aims to select one or a group of hops with the "shortest" path, it is easy to cause some link bandwidth to be fully allocated when additional new connections are set up. This may result in a congested network, and eventually blocks new connections or connection restoration paths creation. With the load distribution policy, the (fg)OTN connections are distributed evenly over the links in the network so that the network resource utilization is optimized.

The following constraints may be supported for (fg)OTN path computation:

a) Inclusion of specific network resources (nodes or links): The specified node or link shall be included in the computed path.

b) Exclusion of specific network resources (nodes or links): The specified node or link shall be excluded from the computed path.

The following protection and restoration mechanisms shall be supported for (fg)OTN path computation:

a) Unprotected: Only the working path is computed.

b) 1+1 protection: A pair of resource disjoined working and protection paths are computed at the same time. The resource of the protection path is dedicated and not shared with other connection paths.

c) Restoration (path pre-calculation): The restoration path of an (fg)OTN connection is calculated in advance. Multiple restoration paths are allowed to share common link and node resources for different working paths which do not have the same SRLGs.

8.3.3 Control and maintenance of (fg)OTN connections

The management and control system shall support creation, activation, modification, deactivation and deletion of (fg)OTN connections. The management and control system creates, modifies, or deletes (fg)OTN cross-connections at each (fg)OTN node along the connection path.

The (fg)OTN connection provisioning information shall include:

- Source and destination (fg)OTN node (Identifier of the source and destination (fg)OTN nodes).
- The type of the client signal.
- Requested Bandwidth (see IETF RFC 8795 [15]).
- The protection and restoration type of the (fg)OTN connection and the related configurations.
- Administrative state (target administrative state of the connection).

The (fg)OTN connection provisioning information may include:

- Routing policy (see clause 8.3.2 of the present document).
- Path computational constraints (see clause 8.3.2 of the present document).

The management and control system shall maintain the (fg)OTN connection information for the full lifecycle of these connections. The information about (fg)OTN connection includes:

a) Connection identification.

b) Bandwidth.

c) Protection type.

d) Actual connection path route hops.

e) Operational state.

f) Latency of the connection.

History

Document history		
V1.1.1	October 2024	Publication