

TR-412

Test Cases for CloudCO Applications

Issue: 1
Issue Date: March 2021

Notice

The Broadband Forum is a non-profit corporation organized to create guidelines for broadband network system development and deployment. This Technical Report has been approved by members of the Forum. This Technical Report is subject to change. This Technical Report is owned and copyrighted by the Broadband Forum, and all rights are reserved. Portions of this Technical Report may be owned and/or copyrighted by Broadband Forum members.

Intellectual Property

Recipients of this Technical Report are requested to submit, with their comments, notification of any relevant patent claims or other intellectual property rights of which they may be aware that might be infringed by any implementation of this Technical Report, or use of any software code normatively referenced in this Technical Report, and to provide supporting documentation.

Terms of Use

1. License

Broadband Forum hereby grants you the right, without charge, on a perpetual, non-exclusive and worldwide basis, to utilize the Technical Report for the purpose of developing, making, having made, using, marketing, importing, offering to sell or license, and selling or licensing, and to otherwise distribute, products complying with the Technical Report, in all cases **subject to the conditions set forth in this notice and any relevant patent and other intellectual property rights of third parties (which may include members of Broadband Forum)**. This license grant does not include the right to sublicense, modify or create derivative works based upon the Technical Report except to the extent this Technical Report includes text implementable in computer code, in which case your right under this License to create and modify derivative works is limited to modifying and creating derivative works of such code. For the avoidance of doubt, except as qualified by the preceding sentence, products implementing this Technical Report are not deemed to be derivative works of the Technical Report.

2. NO WARRANTIES

THIS TECHNICAL REPORT IS BEING OFFERED WITHOUT ANY WARRANTY WHATSOEVER, AND IN PARTICULAR, ANY WARRANTY OF NONINFRINGEMENT AND ANY IMPLIED WARRANTIES ARE EXPRESSLY DISCLAIMED. ANY USE OF THIS TECHNICAL REPORT SHALL BE MADE ENTIRELY AT THE USER'S OR IMPLEMENTER'S OWN RISK, AND NEITHER THE BROADBAND FORUM, NOR ANY OF ITS MEMBERS OR SUBMITTERS, SHALL HAVE ANY LIABILITY WHATSOEVER TO ANY USER, IMPLEMENTER, OR THIRD PARTY FOR ANY DAMAGES OF ANY NATURE WHATSOEVER, DIRECTLY OR INDIRECTLY, ARISING FROM THE USE OF THIS TECHNICAL REPORT, INCLUDING BUT NOT LIMITED TO, ANY CONSEQUENTIAL, SPECIAL, PUNITIVE, INCIDENTAL, AND INDIRECT DAMAGES.

3. THIRD PARTY RIGHTS

Without limiting the generality of Section 2 above, BROADBAND FORUM ASSUMES NO RESPONSIBILITY TO COMPILE, CONFIRM, UPDATE OR MAKE PUBLIC ANY THIRD PARTY ASSERTIONS OF PATENT OR OTHER INTELLECTUAL PROPERTY RIGHTS THAT MIGHT NOW OR IN THE FUTURE BE INFRINGED BY AN IMPLEMENTATION OF THE TECHNICAL REPORT IN ITS CURRENT, OR IN ANY FUTURE FORM. IF ANY SUCH RIGHTS ARE DESCRIBED ON THE TECHNICAL REPORT, BROADBAND FORUM TAKES NO POSITION AS TO THE VALIDITY OR INVALIDITY OF SUCH ASSERTIONS, OR THAT ALL SUCH ASSERTIONS THAT HAVE OR MAY BE MADE ARE SO LISTED.

All copies of this Technical Report (or any portion hereof) must include the notices, legends, and other provisions set forth on this page.

Issue History

Issue Number	Approval Date	Publication Date	Issue Editor	Changes
1	5 March 2021	5 March 2021	DingHai ChinaUnicom Wei Lin, Huawei	Original

Comments or questions about this Broadband Forum Technical Report should be directed to info@broadband-forum.org.

Editor: Ding Hai, China Unicom
Wei Lin, Huawei

Work Area Director(s): George Dobrowski, Morris Creek Consulting
Bruno Cornaglia, Vodafone

Project Stream Leader(s): Yves Hertoghs, VMWare
Ning Zong, Huawei Technologies CO Ltd

Table of Contents

Executive Summary6

1 Purpose and Scope7

 1.1 Purpose7

 1.2 Scope7

2 References and Terminology8

 2.1 Conventions8

 2.2 References8

 2.3 Definitions8

 2.4 Abbreviations9

3 Technical Report Impact11

 3.1 Energy Efficiency11

 3.2 Security11

 3.3 Privacy11

4 Test Environment and Setup12

5 Reporting Requirements and Guidelines13

 5.1 Report content13

6 Functional Test Cases14

 6.1 General14

 6.2 Bootstrapping an NFVI to a Cloud Central Office14

 6.3 Establish High Speed Internet Access (HSIA) Service15

 6.3.1 *Create Resources and Control Plane for HSIA Services*15

 6.3.2 *Create HSIA Service for a User*18

 6.3.3 *Activate HSIA Service for a User (Authentication Successful)*19

 6.4 Virtual Access Node (vAN)-based FANS service20

 6.5 SDN-based FANS service24

 6.6 Converged-Core-as-a-Service (with PNF based User Plane)29

 6.7 Parental Control on NERG32

 6.8 Monitoring, Diagnostics, and Optimization in a Residential Broadband System.33

 6.9 ONAP Integration of Residential Broadband HSIA Service Use Case36

 6.9.1 *Create and Activate HSIA Service for ONAP Integration for Residential Broadband HSIA Service* 36

 6.9.2 *Zero-touch relocation of the ONT for ONAP Integration for Residential Broadband HSIA Service (Same OLT)*39

 6.9.3 *Zero-touch relocation of the ONT for ONAP Integration for Residential Broadband HSIA Service (Different OLT)*39

 6.10 NERG Overlay LSL with vG_MUX PNF40

 6.11 EasyMesh Cloud Controller42

Appendix I. Test Report Example46

 I.1 Overview46

 I.2 Devices under Test46

 I.3 Additional Components involved46

 I.4 Results46

 I.5 Configurations47

 I.6 Logs47

 I.7 Action Points47

Table of Figures

Figure 1 Generic Testing Setup.....12

Executive Summary

TR-412 defines the reference architectural infrastructure of the CloudCO, whose functionality can be accessed via its Northbound API, allowing the service providers to consume the functionality and build their own services. This infrastructure is fundamentally different in many ways from legacy broadband networks.

To instruct readers how to consume a CloudCO “service”, the BBF has developed Application Notes to describe the implementable use cases by using CloudCO functionality. These Application Notes are located [here](#).

This document provides a set of test cases to verify the Application Notes, and thus validate CloudCO functionality.

1 Purpose and Scope

1.1 Purpose

The purpose of this Technical Report is to provide a set of test cases to validate CloudCO functionality defined in TR-384 and uses of that functionality as documented in the various CloudCO applications notes (App Notes). The CloudCO functionality incorporates multiple CloudCO components, their behaviors and interactions.

Application Notes, describing the implementable use cases for CloudCO 'services', will provide inputs for the test cases to validate these CloudCO 'services'. However, the portfolio of test-cases should not have to map one to one with a certain AppNote. This will allow re-usability of test-cases across App Notes. For more information about the relationship between Application Notes and Test Cases, please refer [here](#).

These test cases will be consumed by the Open Broadband Labs (OBLabs) when they get approval. The OBLabs will provide the test beds, test results and corresponding test reports to AppNote users. The detailed outcome of the tested AppNote instance shouldn't be publicly posted, they are only shared between the AppNote users and the OBLab producing those results.

In summary, TR-412 provides:

- Detailed Test Cases (e.g., Purpose, Procedures, Metrics) applicable to one or more Application Notes
- Guidelines on reporting test outcomes, including requirements on documentation of the Application Note instance (hardware and software specifics)
- Guidelines on providing feedback from testing to the Broadband Forum projects relating to CloudCO
- Guidelines on providing feedback from testing to the Open Source Community

1.2 Scope

The test cases focus on the verifying the functionality of the implementation Application Notes, but do not include the sort of tests more commonly associated with commercial communication infrastructure, such as performance, resilience, scalability for example.

2 References and Terminology

2.1 Conventions

In this Technical Report, several words are used to signify the requirements of the specification. These words are always capitalized. More information can be found in RFC 2119.

MUST	This word, or the term “REQUIRED”, means that the definition is an absolute requirement of the specification.
MUST NOT	This phrase means that the definition is an absolute prohibition of the specification.
SHOULD	This word, or the term “RECOMMENDED”, means that there could exist valid reasons in particular circumstances to ignore this item, but the full implications need to be understood and carefully weighed before choosing a different course.
SHOULD NOT	This phrase, or the phrase "NOT RECOMMENDED" means that there could exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications need to be understood and the case carefully weighed before implementing any behavior described with this label.
MAY	This word, or the term “OPTIONAL”, means that this item is one of an allowed set of alternatives. An implementation that does not include this option MUST be prepared to inter-operate with another implementation that does include the option.

2.2 References

The following references are of relevance to this Technical Report. At the time of publication, the editions indicated were valid. All references are subject to revision; users of this Technical Report are therefore encouraged to investigate the possibility of applying the most recent edition of the references listed below.

A list of currently valid Broadband Forum Technical Reports is published at www.broadband-forum.org.

Document	Title	Source	Year
[1] TR-384	Cloud Central Office Reference Architectural Framework	BBF	2018
[2] TR-411	Definition of interfaces between CloudCO Functional Modules	BBF	2021
[3] TR-454	YANG Modules for Access Network Map & Equipment Inventory	BBF	2021
[4] TR-413	SDN Management and Control Interfaces for CloudCO Network Functions	BBF	2018
[5] TR-317	<i>Network Enhanced Residential Gateway</i>	BBF	2016
[6]	“Wi-Fi CERTIFIED EasyMesh™ Test Plan Version 2.0	Wi-Fi Alliance	2019

2.3 Definitions

The following terminology is used throughout this Technical Report.

Application Note	An AppNote is using the TR-384 framework to describe an implementable Use Case for a CloudCO 'application'.
CloudCO	Cloud Central Office
SDN M&C	Software Defined Networking Management and Control

2.4 Abbreviations

This Technical Report uses the following abbreviations:

AAA	Authentication, Authorization and Accounting
AN	Access Node
API	Application Programming Interface
AppNote	Application Note
BAA	Broadband Access Abstraction
BBF	Broadband Forum
BNG	Broadband Network Gateway
BRG	Bridged Residential Gateway
CCO	CloudCO
CCDO	CCO Domain Orchestrator
CO	Central Office
CDN	Content Delivery Network
CPE	Customer Premise Equipment
DC	Data Center
DHCP	Dynamic Host Configuration Protocol
IETF	Internet Engineering Task Force
I/O	Input/Output
IP	Internet Protocol
LAN	Local Area Network
LSL	Logical Subscriber Link
L2	Layer 2
MANO	Management and Network Orchestration
MEC	Mobile Edge Compute
MSBN	Multi Service Broadband Network
NERG	Network Enhanced Residential Gateway
NETCONF	Network Configuration (management protocol)
NFV	Network Function Virtualization
NFVI	NFV Infrastructure
OBLabs	Open Broadband Labs
OLT	Optical Line Termination
OSS	Operational Support System
PNF	Physical Network Function
RG	Residential Gateway
SDN	Software Defined Network
TR	Technical Report

VLAN	Virtual Local Area Network
vG	Virtual Gateway
vFW	Virtual Firewall
vG	Virtual Gateway
VIM	Virtualized Infrastructure Manager
VNF	Virtualized Network Function
YANG	Yet Another Next Generation (data modeling language)

3 Technical Report Impact

3.1 Energy Efficiency

This Technical Report may impact energy efficiency, as network functions can now be decoupled from existing standalone nodes. Use of generic hardware, as such not optimized for a specific network application, and migration of network functions to more distributed locations could lead to higher energy consumption. However, on-demand allocation of hardware resources and hardware sharing across multiple applications can produce energy gains. This Technical Report does not intend to quantify these opposite effects on energy efficiency.

Regulatory differences related to electrical power, Heating, Ventilation and Air Conditioning (HVAC) and fire protection between traditional COs and datacenters is out-of-scope for this document.

3.2 Security

Security provides "a form of protection where a separation is created between the assets and the threat." CloudCO enables the sharing of a common infrastructure between various use cases that may be operated by different departments (e.g., wireline and mobile) or different companies (other service providers, including other network service providers). CloudCO also provides an increased opportunity for Operators to dynamically control the network service behavior, with the use of APIs. In addition, it is expected that management and control plane interfaces are protected from security risks (CloudCO relies on an increased separation between the control plane and the forwarding plane).

It is noted that existing threats, safeguards, and enhancements remain applicable to CloudCO deployments, whether in the forwarding or management-control planes. This specification assumes a foundation of current security best practices that have been defined for the existing Multi Service Broadband Network (MSBN). However, some new or amplified concerns also appear and without appropriate precautions, the above conditions could impact a network's security.

3.3 Privacy

A multi-tenant CloudCO hosts functionality for a set of actors with potentially competing interests that the CloudCO will be required to isolate from each other. At the same time it is required to enable business interactions between the same set of actors requiring careful design of the points of contact.

A multi-tenant CloudCO is a system of sufficient complexity that it will expose new attack vectors to malicious parties that have access to the CloudCO system. For example, the "black box" steady state functionality of a virtualized system may be identical to a corresponding physical network function implementation, but the elasticity and dynamic behavior a virtualized system is capable of implies significantly different system responses to load will be possible, which can be exploited for malicious purposes if poorly designed or executed.

Privacy involves the need to ensure that information to, from and between customers can only be accessed by those who have the right to do so. Further, privacy requirements can vary by regulatory region. In general, two ways to ensure privacy is recognized:

- Preventing data, from being copied to a non-intended destination.
- Encrypting data, so that it cannot be understood even if it is intercepted.

This document does not define any specific mechanisms.

4 Test Environment and Setup

In the context of CloudCO, the test environment basically consists of an NFVI, a set of Access I/O and a set of Network I/O. The NFVI is sized according to need and includes compute and storage (not shown) nodes, as well as a leaf-spine fabric. In addition, the test environment contains the test devices to enable controlling the test execution, collecting the test measurements, and other assistant devices, like test PC to present the test results.

In a traditional test environment, the physical test device establishes a session with device under test (DUT) and exchanges traffic to assess the network functions and their performance. However, some network functions under test in the CloudCO environment are instantiated and executed as VNFs that are deployed on the general-purpose resources. To validate the VNFs, the test devices used in CloudCO test cases will not only include the traditional hardware-based tools, but also include the virtual tools running as software to execute the same testing work.

Figure 1 indicates a generic test setup providing an abstract framework within which any specific test cases can use. The generic testing architecture helps to provide a structure for the test cases later. In a specific test case, it may be required to define several specific functions under test to execute the whole testing and achieve the 'service' in the Application Note.

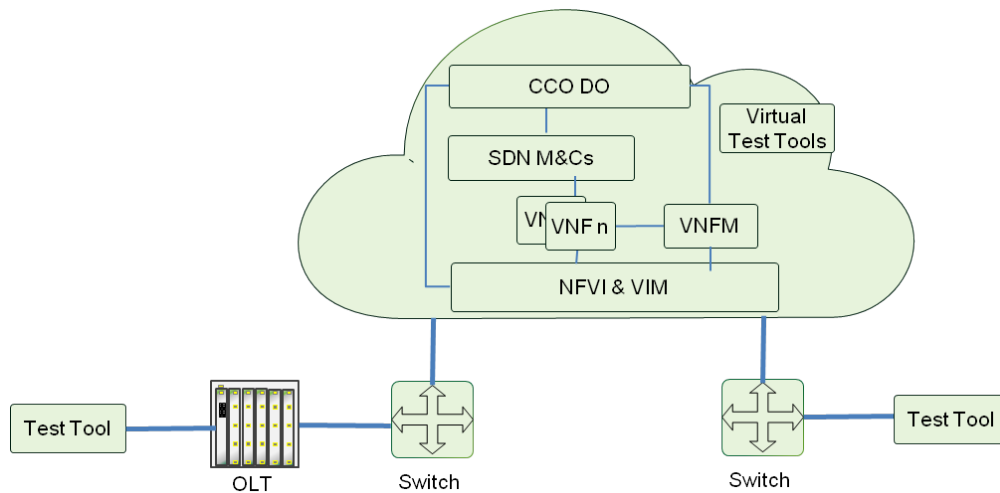


Figure 1 Generic Testing Setup

5 Reporting Requirements and Guidelines

5.1 Report content

The report must contain an overview/reference of what has been tested.

- Test case (+version, APP Notes)
- Involved environment (OBLab details)
- Devices Under Test (DUT) (vendor + version)
- Additional devices (Traffic generators, simulated Clients, Proxies)
- A short summary showing the passed/failed result steps
- Who performed the test
- When the test was performed
- Overall/final status (pass/fail)

The report should contain the details of each step.

- Step summary
- Expected result
- Actual result
- Status (pass/fail)

The report should contain further details as well:

- Configurations of DUT
- Optional comments (logs, why it failed, additional observations)

The report could contain.

- Further action points
 - Bug reports to open source projects
 - Errata to RFC
 - Improvements to APP Notes/drafts

6 Functional Test Cases

6.1 General

This section outlines a series of test cases to demonstrate the “services” depicted in the Application Notes. There are no test cases for the suspending or rejecting Application Notes and ensure each test case to cover at least one approved Application Note. Additionally, there are no high-performance test cases since validating functionality is the main objective of this document.

Each test case contains the following contents and test case template as below

Test Case ID	For example C1
Test Case Name	Bootstrapping an NFVI to a Cloud Central Office
Test Objective	State the purpose of the test
Test Case Reference	The directly involved AppNotes
Test Setup	Outlines the System Under Test (SUT) and the test tools
Pretest Conditions	A high level description of the state of SUT and pre-configurations
Test Procedure	A description of the procedure to be followed for the test
Expected results	A high level description of the behavior should the test succeed

6.2 Bootstrapping an NFVI to a Cloud Central Office

Test Case ID	6.2
Test Case Name	Bootstrapping an NFVI to a Cloud Central Office
Test Objective	Validate how the NFVI bootstrapping in a CloudCO domain is described
Test Case Reference	CloudCO-APPN-000
Test Setup	The test architecture provides a Network Function Virtualization Infrastructure (NFVI) with a corresponding Virtualized Infrastructure

	<p>Manager (VIM).</p> <p>The diagram illustrates a network architecture. A central cloud contains three main components: CCO DO at the top, SDN M&Cs in the middle, and NFVI & VIM at the bottom. A box labeled 'Virtual Test Tools' is positioned to the right of the cloud. Below the cloud, an OLT (Optical Line Terminal) is connected to a central Switch. This central Switch is connected to two other Switches, one on the left and one on the right. Blue lines indicate the connections between the cloud components and the physical network devices.</p>
<p>Pretest Conditions</p>	<ul style="list-style-type: none"> • The corresponding images/steps for the CloudCO DO and SDN M&C deployment have been prepared. • If external connectivity is required it needs to be provided as well. (Software Repositories, License servers, DNS)
<p>Test Procedure</p>	<p>Step1 : The VIM is instructed to create overlay networks to interconnect various elements of the CloudCO domain, such as VIM, CloudCO DO and SDN M&C.</p> <p>Step2 : The VIM is instructed to deploy the CCO DO and SDN controllers with access to the respective overlay networks.</p> <p>Step3 : The CloudCO DO NB API is used to trigger the creation of a new Service Provider tenant.</p>
<p>Expected results</p>	<ol style="list-style-type: none"> 1. Overlay networks have been created. 2. The CloudCO DO and SDN M&C are up and running. The devices can ping each other. 3. Service Provider tenant is created on the CloudCO DO. The CloudCO DO created a Service Provider tenant instance on the SDN M&C

6.3 Establish High Speed Internet Access (HSIA) Service

6.3.1 Create Resources and Control Plane for HSIA Services

<p>Test Case ID</p>	<p>6.3.1</p>
<p>Test Case Name</p>	<p>Create Resources and Control Plane for HSIA Services</p>

<p>Test Objective</p>	<p>This test case aims to validate the creation of the resources needed to deploy HSIA services within the CloudCO. The HSIA service is provided in the following scenario:</p> <p>Create HSIA Service. The HSIA service is created from CloudCO Access PNF NNI to the Edge resources.</p>
<p>Test Case Reference</p>	<p>CLOUDCO-APPN-001</p>
<p>Test Setup</p>	<p>The test architecture provides a Network Function Virtualization Infrastructure (NFVI) with associated management and control (DC SDN M&C, VIM), virtual network functions for the Edge (Edge SDN M&C, vAAA and vIPAM) and Access (Access SDN M&C, OB-BAA). It also provides for an instance of the CCO Domain Orchestrator, providing an API endpoint to instantiate the service instances and appropriate service attributes. These are all deployed as virtual workloads inside the NFVI, with the necessary virtual networks to interconnect those Orchestration, Management and Control, and Network functions, as per below diagram</p> <p>The diagram illustrates the Network Function Virtualization Infrastructure (NFVI) architecture. At the top, a user icon labeled 'GUI/API (REST)' connects to the 'CCO DO' (CCO Domain Orchestrator) within the NFVI. A central 'CCO Domain MGMT Network' connects the CCO DO to several management and control functions: 'BAA', 'Access SDN M&C', 'DC SDN M&C', and 'VIM'. Below these, an 'Access M&C Network' connects 'BAA' and 'Access SDN M&C' to an 'L3GW' (L3 Gateway) virtual function. An 'Edge M&C Network' connects 'Edge SDN M&C', 'IPAM VNF', and 'AAA VNF'. The 'L3GW' connects to a 'DPU / OLT' (Data Plane Unit / Optical Line Terminal) and a 'Fabric Switch'. The 'Fabric Switch' connects to a 'Core' network. An 'RG / ONT' (Residential Gateway / Optical Network Terminal) is also connected to the 'DPU / OLT'.</p>
<p>Pretest Conditions</p>	<p>In the figure above the various functions have been pre-established and provide the following:</p> <ul style="list-style-type: none"> • The CCO Domain Orchestrator is responsible for creating service instances and adding attributes to the service instance, through a UI or through a RESTful API. The CCO DO (e.g., ONAP, or similar) might be a set of different virtual workloads, but in this example, it is visualized as a single virtual workload. • CCO DO is able to communicate with the various Management, Infrastructure and Control Functions such as Access M&C, DC M&C, VIM and Edge M&C VNFs. In this example a single virtual network “CCO Domain Network” is leveraged to create this connectivity. • The OB-BAA VNF is connected to the Access SDN M&C VNF for management plane functionality. In addition, the OLTs connect via the management plane to the OB-BAA reference implementation. In this example a L3GW virtual function is used to route the physical

	<p>management VLAN of the OLT to the Access M&C Virtual Network inside the NFVI.</p> <ul style="list-style-type: none"> • VIM control of the NFVI to instantiate networks and virtual workloads is assumed and not shown on the diagram • DC SDN M&C control of the fabric is assumed and noted as a dotted black line on the diagram. • The AAA and IPAM VNFs can communicate with the relevant SDN M&C via the “CCO Domain Network” Virtual Network. • Physical Connectivity from the Customer Premises (RG/ONT) to the Central Office (OLT) is assumed, as well as physical connectivity between the OLTs and the Switch Fabric, physical connectivity between the NFVI and the switch fabric, as well as physical connectivity between the NFVI and the Core Network Infrastructure, (shown in Black on the diagram).
<p>Test Procedure</p>	<ol style="list-style-type: none"> 1. CCO DO receives a HSIA Service creation request via its REST API. 2. (Connectivity between Access SDN M&C and AAA and IPAM VNFs has been pre-established) 3. CCO DO requests the Access SDN M&C to create an S-VLAN on the OLT (through the BAA) for that HSIA Service; assign OLT UNIs to that S-VLAN and enable split-horizon forwarding on that S-VLAN. 4. CCO DO requests the Access SDN M&C Access SDN M&C to provision the OLT (via the BAA) to redirect 802.1x and DHCP packets within the context of that S-VLAN to it, while blocking all the rest. 5. CCO DO requests the DC SDN M&C to configure that S-VLAN on the switch attached to the Access PNF on all of its ports. 6. CCO DO requests the VIM to create two virtual networks (“access-facing-network” and “core-facing-network”) as well as a L2-gateway between said S-VLAN and the “access-facing-network” virtual network 7. CCO DO requests the VIM to deploy a vRouter VNF and connect it to the two virtual networks. (“access-facing-network” and “core-facing-network”). 8. CCO DO requests the VIM to deploy a L2-gateway or a L3-gateway between the core network and the “core-facing-network” virtual network. 9. CCDO requests the Edge SDN M&C to configure the vRouter interfaces and other configuration. 10. CCDO reports 'Service Ready' <p>This results in the following topology:</p>

	<p>The diagram illustrates the Network Function Virtualization (NFVI) architecture. At the top, a GUI/API (REST) interface connects to the CCO DO (CloudCO Domain Orchestrator). The CCO DO is connected to a CCO Domain MGMT Network, which manages several VNFs: BAA (Broadband Access Agent), Access SDN M&C (Management and Control), DC SDN M&C (Data Center SDN M&C), VIM (Virtualized Infrastructure Manager), Edge SDN M&C (Edge SDN M&C), IPAM VNF (IP Address Management), and AAA VNF (Authentication, Authorization, and Accounting). The BAA and Access SDN M&C are connected to an Access M&C Network, which includes an L3GW (Layer 3 Gateway). The Edge SDN M&C, IPAM VNF, and AAA VNF are connected to an Edge M&C Network, which includes an L2GW or L3GW (Layer 2 or 3 Gateway). The physical network consists of an RG/ONT (Residential Gateway/On-Net Terminal) connected to a DPU/OLT (Data Plane Unit/Optical Line Terminal), which is connected to a Fabric Switch. The Fabric Switch is connected to a vRouter VNF (Virtual Router) and an L2GW or L3GW. The vRouter VNF is connected to an Access-Facing Network, and the L2GW or L3GW is connected to a Core-Facing Network, which is connected to a Core network.</p>
<p>Expected results</p>	<ol style="list-style-type: none"> 1. CCO DO maintains the HSIA service request 2. Control plane packets (802.1x and DHCP) can be exchanged between the Premises' physical termination and Access SDN M&C, via the BAA. 3. Control plane packets (802.1x and DHCP) can be exchanged between the Premises PNF and the control plane VNFs. 4. Routed User Plane Connectivity is created, initially with no packet forwarding from the premises PNFs to the core network.

6.3.2 Create HSIA Service for a User

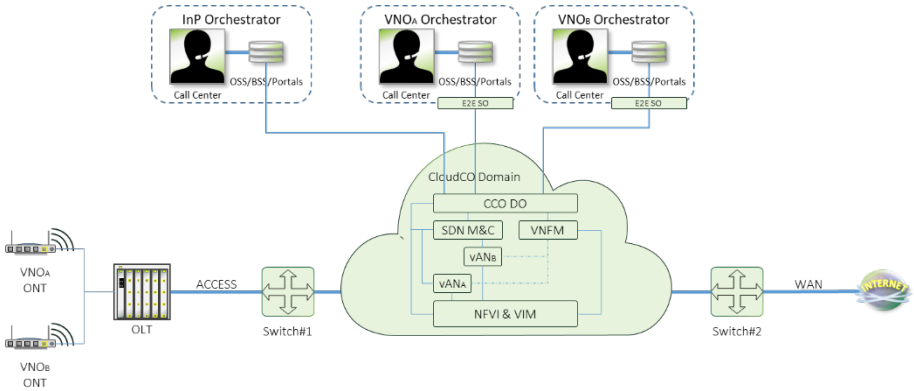
<p>Test Case ID</p>	<p>6.3.2</p>
<p>Test Case Name</p>	<p>Create HSIA Service for a User</p>
<p>Test Objective</p>	<p>This test case aims to validate the Residential Broadband HSIA Service for a subscriber within a CloudCO has been created but not yet activated. The HSIA service is provided in the following scenario:</p> <ul style="list-style-type: none"> • Create HSIA Service User
<p>Test Case Reference</p>	<p>CLOUDCO-APPN-001</p>
<p>Test Setup</p>	<p>Setup uses the Create Resources and Control Plane for HSIA Services test scenario.</p>
<p>Pretest Conditions</p>	<p>HSIA Service has been created. (See first test case)</p>
<p>Test Procedure</p>	<ol style="list-style-type: none"> 1. CCO DO receives a HSIA Service User creation request with end-user (tenant) information; rate/quality of service, type of protection, and user credentials. 2. CCO DO requests the Access SDN M&C to configure the OLT via the BAA layer the users C-VLAN and forwarding connectivity though the Access NNI's S-VLAN 3. CCO DO requests the Edge SDN M&C to configure the AAA VNF with the end-user (tenant) credentials.

	4. CCO DO requests the Edge SDN M&C to configure the IPAM VNF with the end-user (tenant) addresses and policies (rate/quality of service, type of protection)
Expected results	<ol style="list-style-type: none"> 1. HSIA Service User is created 2. AAA and IPAM VNFs are configured with the end-user (tenant) information 3. Still no packet forwarding from the premises PNFs to the core network.

6.3.3 Activate HSIA Service for a User (Authentication Successful)

Test Case ID	6.3.3
Test Case Name	Activate HSIA Service for a User
Test Objective	This test case aims to validate the Residential Broadband HSIA Service for a subscriber within a CloudCO has been activated and the user is provided access to the Internet after successful authentication.
Test Case Reference	CLOUDCO-APPN-001
Test Setup	Setup uses the Create Resources and Control Plane for HSIA Services test scenario.
Pretest Conditions	RG /ONT is generating 802.1x and DHCP request traffic.
Test Procedure	<ol style="list-style-type: none"> 1. User attaches the Premises PNF / RG /ONT to the Access Network 2. ONT/RG sends 802.1x packets upstream, which is redirected to the Access SDN M&C via the BAA. The Access M&C forwards the EAP information from the 802.1x packet toward the AAA VNF. The AAA VNF authenticates the end-user (tenant) and returns the response to the Access SDN M&C, which in turn responds back to the ONT/RG via the BAA. 3. Upon successful authentication, the Access SDN M&C reports a port activation to the BAA which reports it to OLT which establishes L2 connectivity between the end-user port and the OLT NNI via S-VLAN forwarding. 4. OLT relays, via the BAA and Access SDN M&C, the DHCP request to the IPAM VNF; IPAM VNF responds with the address information and policies for the end-user (tenant). 5. The DHCP response is sent downstream, via the Access SDN M&C and BAA, from the OLT to the Premises PNF/RG/ONT. 6. Access SDN M&C reports an end-user (tenant) activation to the CCO DO with the attachment point.
Expected results	<ol style="list-style-type: none"> 1. HSIA service is established for that user at the requested rate, quality of service and protection scheme.

6.4 Virtual Access Node (vAN)-based FANS service

Test Case ID	6.4
Test Case Name	Virtual Access Node (vAN)-based FANS service
Test Objective	This test case aims to verify the interactions described in CloudCO ApplicationNote-006, and thus validate CloudCO functionalities against a vAN-based FANS implementation.
Test Case Reference	CLOUDCO-APPN-006
Test Setup	<p>In the context of CloudCO, the generic test setup consists of a set of NFVI, Access PNFs and a set of Network I/O, a switch fabric and all the Management, Control and Orchestrations elements to implement a CloudCO asset tailored to this Access domain application.</p>  <p>Notes:</p> <ul style="list-style-type: none"> • The minimal server farm includes at least one compute server and one controller server if HA is not required in the CloudCO. • The test setup does show an NFVI and related MANO components. This is possible but not strictly necessary especially for a setup dedicated to tests. Software components like the CCO DO, the Access SDN M&C may run on compute hosts but not necessarily as VNFs with heavy lifecycle requirements within an NFVI.
Pretest Conditions	<p>The following pretest conditions are not necessarily prescriptive and some of them may be extended to widen the applicability of the APPNOTE:</p> <ul style="list-style-type: none"> • The InP CloudCO Domain Orchestrator instance and the SDN M&C are already fully bootstrapped. • A single VNF is deployed in the CloudCO and it is the solely responsible for instantiating the VNFs (vANs). • A VIM is installed in the COTS within the NFVI <p>Note: For ease of setup, it is assumed that the CloudCO DO, SDN M&C, VNF and VIM instances run locally over the compute host. This shall not</p>

	<p>considered as a restrictive choice with regard to a more realistic architecture with distribution of these functions at different locations (and hosts) in the network.</p> <ul style="list-style-type: none"> • The OLT is physically connected with switch fabric • The OLT is configured with a VLAN dedicated to management and control. Traffic over this VLAN is extended to across the switch connected to the OLT. The VLAN is also extended to the compute hosts that are connected to this switch • All the VNOs' ONTs terminate on the same OLT
<p>Test Procedure</p>	<p>The detailed interactions among CloudCO blocks and related ladder diagrams for AppNote-006 are documented at CloudCO-APPN-006: Virtual Access Node (vAN)-based FANS service.</p> <ul style="list-style-type: none"> • Interaction 1: VNO Network Creation <ol style="list-style-type: none"> 1. VNO MS sends a “VNO Network Creation” request to CCO DO 2. CCO DO expose a L2-based service interface and a network map of the OLTs (herein only one) to the VNO MS <p>Note: for these tests the list of OLTs exposed to the VNOs is exactly the same; in real deployment the lists are tailored based on InP-VNO agreements; such tailored lists are configurable only by the InP.</p> • Interaction 2: VNO L2 Service Creation <ol style="list-style-type: none"> 1. VNO MS sends a “VNO L2 Service” request to CCO DO. This request leads to two separated test cases: <ol style="list-style-type: none"> a. The request fulfills the constraints previously agreed with the InP (OK case) b. The request DOES NOT fulfill the constraints previously agreed with the InP (KO case) 2. For the case “1a”, the OLT NNI connectivity is properly up and the vAN instance of VNO is configured by the SDN M&C 3. For the case “1b”, VNO MS receives a negative notification to indicate that the request cannot be fulfilled <p>Note: The constraints are configurable by the InP via the Os-Ma-ccodo interface. The full list of Os-Ma-ccodo parameters are defined in the Table 2 of TR-411 [2]. As an example, the VNO MS request can contains the following parameters:</p>

	<ul style="list-style-type: none"> ▪ NNI-OVLAN-prof <ul style="list-style-type: none"> • # of O-VLANs Per VLAN: <ul style="list-style-type: none"> • DS-guarant-BW • DS-peak-BW • US-guarant-BW • US-peak-BW • priority • id 	<ul style="list-style-type: none"> ▪ NNI-SVLAN-prof <ul style="list-style-type: none"> • # of S-VLANs Per VLAN: <ul style="list-style-type: none"> • DS-guarant-BW • DS-peak-BW • US-guarant-BW • US-peak-BW • priority • id 	<ul style="list-style-type: none"> ▪ UNI-CVLAN-prof <ul style="list-style-type: none"> • # of C-VLANs Per VLAN: <ul style="list-style-type: none"> • DS-guarant-BW • DS-peak-BW • US-guarant-BW • US-peak-BW • priority • id 	
<ul style="list-style-type: none"> • Interaction 3: VNO ONT Pre-provisioning <ol style="list-style-type: none"> 1. VNO MS sends a “ONT Provisioning” request to CCO DO. This request leads to two separated test cases: <ol style="list-style-type: none"> a. The request fulfills the constraints previously agreed with the InP (OK case) b. The request DOES NOT fulfill the constraints previously agreed with the InP (KO case) 2. For the case “1a”, the ONT UNI connectivity is properly up and the ONT is pre-configured by the SDN M&C to the OLT in which it will be attached to 3. For the case “1b”, VNO MS receives a negative notification to indicate that the request cannot be fulfilled <p>Note: The constraints are configurable by the InP via the Os-Ma-ccodo interface. The full list of Os-Ma-ccodo parameters are defined in the Table 2 of TR-411 [2]. As an example, the VNO MS request can contains the following parameters:</p> <div style="border: 1px solid black; padding: 5px; margin: 10px auto; width: fit-content;"> <ul style="list-style-type: none"> ▪ UNI-CVLAN-prof <ul style="list-style-type: none"> • # of C-VLANs Per VLAN: <ul style="list-style-type: none"> • DS-guarant-BW • DS-peak-BW • US-guarant-BW • US-peak-BW • priority • id </div> • Interaction 4: VNO ONT Activation <ol style="list-style-type: none"> 1. The ONT is properly installed at VNO’s customer premise and a L1 connectivity with the OLT is established 				

	<p>2. VNO MS sends a “ONT Activation” request to CCO DO</p> <p>Note: it is assumed the ONT authentication mechanism is successfully completed.</p> <ul style="list-style-type: none"> • Interaction 5: VNO ONT L2 Performance Monitoring <ol style="list-style-type: none"> 1. VNO MS sends a “ONT L2 Performance Monitoring” request to CCO DO, to collect Performance Monitoring (PM) measures from the target ONT <p>Note: The full list of Os-Ma-ccodo parameters are defined in the Table 2 of TR-411 [2]. As an example, the VNO MS request can contains the following parameters:</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <ul style="list-style-type: none"> ▪ Target ONT ▪ L2 PM activation command <ul style="list-style-type: none"> • VLAN id • VLAN PM parameters to be collected • Collection Frequency </div> • Interaction 6: Handling a Customer Migration (VNO_A customer service to VNO_B) <ol style="list-style-type: none"> 1. VNO_A MS sends a “Customer-J release” request to CCO DO 2. VNO_B MS sends a “Customer-J activation” request to CCO DO 3. VNO_B MS sends a “VNO L2 Service Creation” request to CCO DO. This request leads to two separated test cases: <ol style="list-style-type: none"> a. The request fulfills the constraints previously agreed with the InP (OK case) b. The request DOES NOT fulfill the constraints previously agreed with the InP (KO case) 4. VNO_B MS sends a “ONT Provisioning” request to CCO DO 5. VNO_B MS sends a “ONT Activation” request to CCO DO <p>Note: <i>it</i> is assumed the ONT authentication mechanism is successfully completed</p>
<p>Expected results</p>	<ul style="list-style-type: none"> • Pass/Fail Criteria for Interaction 1: <ol style="list-style-type: none"> 1. VNOs can access to its OLTs network map according to the list agreed with the InP • Pass/Fail Criteria for Interaction 2: <ol style="list-style-type: none"> 1. L2 resources of the target OLT are configured and allocated per VNO request 2. InP’s full network view and VNO’s scoped network view are updated per the above configuration • Pass/Fail Criteria for Interaction 3: <ol style="list-style-type: none"> 1. L2 resources of the target ONT are configured and allocated per VNO request

	<p>2. InP's full network view and VNO's scoped network view are updated per the above configuration</p> <ul style="list-style-type: none"> • Pass/Fail Criteria for Interaction 4: <ol style="list-style-type: none"> 1. L1 and L2 connectivity is established between the ONT and the OLT's uplink interface 2. VNO is able to deliver the service to the end customer • Pass/Fail Criteria for Interaction 5: <ol style="list-style-type: none"> 1. L2 PM collection is carried out as configured 2. Collected L2 PM counters are reported and stored in the Access SDN M&C 3. Collected L2 PM counters are made available to the VNO Orchestrator • Pass/Fail Criteria for Interaction 6: <ol style="list-style-type: none"> 1. The customer termination is removed from the VNO_A's manageable resources 2. The customer migration is completed successfully, and the customer can access to connectivity and services through VNO_B network
--	--

6.5 SDN-based FANS service

Test Case ID	6.5
Test Case Name	SDN-based FANS service
Test Objective	This test case aims to verify the interactions described in CloudCO ApplicationNote-007, and thus validate CloudCO functionalities against an SDN-based FANS implementation.
Test Case Reference	CLOUDCO-APPN-007
Test Setup	In the context of CloudCO, the generic test setup consists of a set of Access PNFs and a set of Network I/O, a switch fabric and all the Management, Control and Orchestrations elements to implement a CloudCO asset tailored to this Access domain application.

	<p>Notes:</p> <ul style="list-style-type: none"> • For a CloudCO application like FANS, confined to the Access domain, the CCO DO and the Access SDN M&C blocks may possibly be merged together. • The test setup does show an NFVI and related MANO components. This is possible but not strictly necessary especially for a setup dedicated to tests. Software components like the CCO DO, the Access SDN M&C and the BAA layer may run on compute hosts but not necessarily as VNFs with heavy lifecycle requirements within an NFVI. • For a pure SDN-based FANS application this choice may apply also to real deployments.
<p>Pretest Conditions</p>	<p>The following pretest conditions are not necessarily prescriptive and some of them may be extended to widen the applicability of the AppNote:</p> <ul style="list-style-type: none"> • The InP CloudCO Domain instance is already fully bootstrapped. • The InP CloudCO Domain consists of access network resources (for simplicity physical OLTs operating on a PON based FTTH architecture). • The CCO DO exposes to the VNOs (Service Tenants) a NB API that fulfill the FANS framework as agreed between the InP and the Service Tenants. This is realized by giving to VNOs the ability to connect to the FANS NB API of the CCO per the following options: <ul style="list-style-type: none"> • segregated and secured VNO Management System (MS) instances provided by the InP and accessed via e.g., service-client applications • each VNO has its own flavour of MS in terms of FCAPS management and flow control • a mix of the above • Regardless of the source of the VNO MS, this element shall support the standard FANS NB API. • Each VNO MS instance is dedicated to a VNO (e.g., VNO_A) and accesses via the CCO NB API to:

	<ul style="list-style-type: none"> • a geographical map of the access network resources (i.e., mainly a map of the deployed OLTs and ODN PONs location - e.g., street address - and the number of uplink interfaces) • a L2-based service interface to configure and manage the OLTs logical resources • The CCO DO, exposes also its resources to the OSS layer of the InP. 			
<p>Test Procedure</p>	<p>The detailed interactions among CloudCO blocks and related ladder diagrams for AppNote-007 are documented at CloudCO-APPN-007 - SDN-based FANS service.</p> <ul style="list-style-type: none"> • Interaction 1: VNO Network Creation <ol style="list-style-type: none"> 1. VNO_A and VNO_B Management Systems request the list of OLTs defined on the network map 2. VNO_A and VNO_B Management Systems retrieve the information associated to an OLT selected from the list <p>Note: for these tests the list of OLTs exposed to the VNOs is exactly the same; in real deployment the lists are tailored based on InP-VNO agreements; such tailored lists are configurable only by the InP.</p> • Interaction 2: VNO OLT Uplink L2 Service Creation <ol style="list-style-type: none"> 1. VNOA MS sends two OLT Uplink L2 service requests (Request1 and Request2) as defined in the model of the Os-Ma-ccodo defined in Table 2 of TR-411 [2] to allocate and configure all relevant VLANs information (see below) for the NNI connectivity of the OLT, based on information contained in the Port Mapper. Request1 fulfills the constraints agreed with the InP. Request2 does not fulfill the constraints. Constraints are configurable by the InP via the Os-Ma-ccodo interface between the CCO DO and the InP OSS. Example of constraints: <ul style="list-style-type: none"> • total OLT uplink interface guaranteed bandwidth assigned to a single VNO <=20% of available L2 bandwidth <p>Some of the possible parameters contained in the request are:</p> <table border="1" data-bbox="599 1381 1427 1812"> <tr> <td data-bbox="599 1381 873 1812"> <ul style="list-style-type: none"> ▪ NNI-OVLAN-prof <ul style="list-style-type: none"> • # of O-VLANs Per VLAN: <ul style="list-style-type: none"> • DS-guarant-BW • DS-peak-BW • US-guarant-BW • US-peak-BW • priority • id </td> <td data-bbox="873 1381 1148 1812"> <ul style="list-style-type: none"> ▪ NNI-SVLAN-prof <ul style="list-style-type: none"> • # of S-VLANs Per VLAN: <ul style="list-style-type: none"> • DS-guarant-BW • DS-peak-BW • US-guarant-BW • US-peak-BW • priority • id </td> <td data-bbox="1148 1381 1427 1812"> <ul style="list-style-type: none"> ▪ UNI-CVLAN-prof <ul style="list-style-type: none"> • # of C-VLANs Per VLAN: <ul style="list-style-type: none"> • DS-guarant-BW • DS-peak-BW • US-guarant-BW • US-peak-BW • priority • id </td> </tr> </table> 	<ul style="list-style-type: none"> ▪ NNI-OVLAN-prof <ul style="list-style-type: none"> • # of O-VLANs Per VLAN: <ul style="list-style-type: none"> • DS-guarant-BW • DS-peak-BW • US-guarant-BW • US-peak-BW • priority • id 	<ul style="list-style-type: none"> ▪ NNI-SVLAN-prof <ul style="list-style-type: none"> • # of S-VLANs Per VLAN: <ul style="list-style-type: none"> • DS-guarant-BW • DS-peak-BW • US-guarant-BW • US-peak-BW • priority • id 	<ul style="list-style-type: none"> ▪ UNI-CVLAN-prof <ul style="list-style-type: none"> • # of C-VLANs Per VLAN: <ul style="list-style-type: none"> • DS-guarant-BW • DS-peak-BW • US-guarant-BW • US-peak-BW • priority • id
<ul style="list-style-type: none"> ▪ NNI-OVLAN-prof <ul style="list-style-type: none"> • # of O-VLANs Per VLAN: <ul style="list-style-type: none"> • DS-guarant-BW • DS-peak-BW • US-guarant-BW • US-peak-BW • priority • id 	<ul style="list-style-type: none"> ▪ NNI-SVLAN-prof <ul style="list-style-type: none"> • # of S-VLANs Per VLAN: <ul style="list-style-type: none"> • DS-guarant-BW • DS-peak-BW • US-guarant-BW • US-peak-BW • priority • id 	<ul style="list-style-type: none"> ▪ UNI-CVLAN-prof <ul style="list-style-type: none"> • # of C-VLANs Per VLAN: <ul style="list-style-type: none"> • DS-guarant-BW • DS-peak-BW • US-guarant-BW • US-peak-BW • priority • id 		

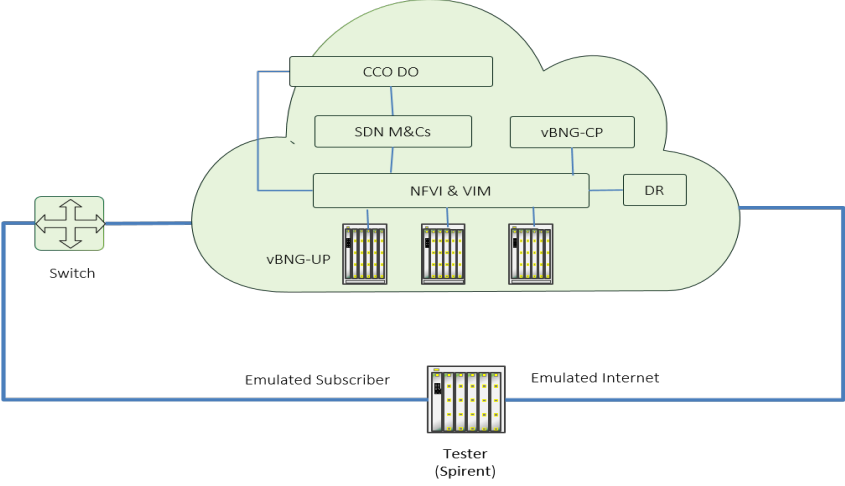
	<ul style="list-style-type: none"> • Interaction 3: VNO ONT L2 Service Creation <ol style="list-style-type: none"> 1. VNOA MS sends two ONT L2 service requests (Request3 and Request4) as defined in the model of the Os-Ma-ccodo defined in Table 2 of TR-411 [2] to allocate and configure all relevant VLANs information (see below) for the UNI connectivity of an ONT and cross-connection to the NNI, based on information contained in the Port Mapper. <p>Request3 fulfills the constraints agreed with the InP. Request4 does not fulfill the constraints. Constraints are configurable by the InP via the Os-Ma-ccodo interface between the CCO DO and the InP OSS. Example of constraints:</p> <ul style="list-style-type: none"> • maximum number of C-VLANs <= 3 • total guaranteed bandwidth <= x Mbit/s. <p>Some of the possible parameters contained in the request are:</p> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <ul style="list-style-type: none"> ▪ UNI-CVLAN-prof <ul style="list-style-type: none"> • # of C-VLANs Per VLAN: <ul style="list-style-type: none"> • DS-guarant-BW • DS-peak-BW • US-guarant-BW • US-peak-BW • priority • id </div> • Interaction 4: VNO ONT activation <ol style="list-style-type: none"> 1. Physical connection and switch-on of the ONT to the PON termination point at VNO_A's customer premises. Note: it is assumed the ONT authentication mechanism is positively finalised. • Interaction 5: VNO ONT L2 Performance Monitoring <ol style="list-style-type: none"> 2. VNOA MS sends a ONT L2 performance monitoring request as defined in the model of the Os-Ma-ccodo defined in Table 2 of TR-411 [2] <p>Some of the parameters contained in the request are:</p> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <ul style="list-style-type: none"> ▪ Target ONT ▪ L2 PM activation command <ul style="list-style-type: none"> • VLAN id • VLAN PM parameters to be collected • collection frequency </div> • Interaction 6: Handling a Customer Migration <ol style="list-style-type: none"> 1. VNO_A MS sends a Customer-J release to CCO DO
--	--

	<p>2. VNO_B MS sends a Customer-J activation to CCO DO</p> <p>3. VNO_B MS sends a ONT L2 Service Creation to CCO DO Note: this command is applicable only after the customer activation procedure has been finalised. Furthermore it is assumed the ONT authentication mechanism is again positively finalised.</p>
<p>Expected results</p>	<ul style="list-style-type: none"> • Pass/Fail Criteria for interaction 1 <ol style="list-style-type: none"> 1. CCO DO sends the list of OLTs to VNO_A and VNO_B MSes as defined in the Access Network Map (ANM) model of the Os-Ma-ccodo defined in Table 1 of TR-411 [2] and TR-454 [3] 2. CCO DO sends the requested OLT information to VNO_A and VNO_B MSes as defined in the Access Network Map (ANM) model of the Os-Ma-ccodo defined in Table 1 of TR-411 [2] and TR-454 [3] <p>More specifically the following information is reported:</p> <ul style="list-style-type: none"> • AN-geo-location • Access-netw-termination-point • AN-status <p>Note: the CCO DO may possibly retrieve the above information from the Access SDN Manager & Controller</p> • Pass/Fail Criteria for interaction 2 <ol style="list-style-type: none"> 1. CCO DO sends to VNO_A MS a positive notification about the fulfillment of Request1 and a negative notification about Request2 2. The information about the VLANs of the configured OLT Uplink L2 service is available on VNO_A MS upon retrieval from the related OLT representation on the network map <p>Optional</p> <ol style="list-style-type: none"> 3. The information about the total allocation of resources of the CloudCO Domain is available on InP OSS upon retrieval of the Port Mapper status. 4. The configurations of all network resources are stored in the Access SDN M&C and the BAA and available on InP OSS upon retrieval • Pass/Fail Criteria for interaction 3 <ol style="list-style-type: none"> 1. CCO DO sends to VNO_A MS a partially positive notification about the fulfillment of Request3 indicating that on the OLT the UNI resources have been allocated and that the ONT configuration has been acquired but that the physical ONT has not been configured accordingly because it is not connected. <p>CCO DO sends to VNO_A MS a negative notification about the fulfillment of Request4</p> <ol style="list-style-type: none"> 2. The information about the VLANs of the configured ONT L2 service is available on VNO_A MS upon retrieval from the related ONT representation on the network map. The ONT representation also indicates that the physical ONT <u>is not connected</u> <p>Optional</p>

	<p>3. The information about the total allocation of resources of the CloudCO Domain is available on InP OSS upon retrieval of the Port Mapper status.</p> <ul style="list-style-type: none"> • Pass/Fail Criteria for interaction 4 <ol style="list-style-type: none"> 1. CCO DO sends to the VNO_A MS a positive notification on the total fulfilment of the ONT L2 service request and connectivity to the NNI via the previously configured OLT Uplink L2 service. 2. The information about the VLANs of the configured ONT L2 service is available on VNO_A MS upon retrieval from the related ONT representation on the network map. The ONT representation also indicates that the physical ONT <u>is connected</u> 3. A PC host connected to the ONT is able to browse a web page from the Internet (assuming appropriate connectivity is in place from the OLT to the Internet) • Pass/Fail Criteria for interaction 5 <ol style="list-style-type: none"> 1. The CCO DO sends to the VNO_A MS the collected PM counters at the configured frequency. • Pass/Fail Criteria for interaction 6 <ol style="list-style-type: none"> 1. CCO DO sends a positive notification of the customer release command to VNO_A MS. VNO_A MS has no more access to the ONT representation corresponding to Customer-J. 2. CCO DO sends a positive notification of the customer activation command to VNO_B MS. VNO_B MS has access to the ONT representation corresponding to Customer-J. 3. The information that Customer-J's ONT is under VNO_B control is available on InP OSS upon retrieval of the Port Mapper status. 4. CCO DO sends to VNO_B MS a positive notification about fulfilment of the ONT L2 service request and connectivity to the NNI Note: it is assumed that an OLT Uplink L2 service has previously been configured from VNO_B MS. 5. The information about the VLANs of the configured ONT L2 service is available on VNO_B MS upon retrieval from the related ONT representation on the network map. The ONT representation also indicates that the physical ONT <u>is connected</u>. 6. A PC host connected to the ONT is able to browse a web page from the Internet (assuming appropriate connectivity is in place from the OLT to the Internet)
--	--

6.6 Converged-Core-as-a-Service (with PNF based User Plane)

Test Case ID	6.6
Test Case Name	Converged Core-as-a-Service (with PNF based User Plane)

<p>Test Objective</p>	<p>This test case aims to validate the service depicted the AppNote-441(Converged Core-as-a-Service (with PNF based User Plane), in which the Converged Core service is instantiated in a CloudCO domain. The Converged Core can serve both wireline and wireless services by providing the functionalities such as BNG, EPC and etc. In this test case, the Converged Core is only offering the BNG functionality</p>
<p>Test Case Reference</p>	<p>CLOUDCO-APPN-441</p>
<p>Test Setup</p>	<p>The Converged Core can serve both wireline and wireless services by providing the functionalities such as BNG, EPC and etc., as shown in below. In this test case, the Converged Core is only offering the BNG functionality</p>  <p>The diagram illustrates the test setup for BNG functionality. A central CloudCO Domain (CCO DO) contains several components: SDN M&Cs, vBNG-CP, NFVI & VIM, and DR. The CCO DO is connected to a Switch on the left. Below the CCO DO, there are three vBNG-UP components. An Emulated Subscriber, represented by a Tester (Spirent), is connected to the vBNG-UP components and also to an Emulated Internet on the right. The Switch is also connected to the Emulated Internet.</p>
<p>Pretest Conditions</p>	<ul style="list-style-type: none"> • The CloudCO Domain instance is already fully bootstrapped. • The BNG User Plane PNFs have been deployed to fulfill the BNG user plane. The BNG User Plane PNFs have IP addresses to communicate with Edge SDN M&C if BNG User Plane PNFs support the standard northbound Minf and Mfc interfaces. • The physical connectivity between Tester, Switch Fabric, BNG User Plane PNFs, and Network I/O has been established.
<p>Test Procedure</p>	<ul style="list-style-type: none"> • Interaction1- Create Converged Core Service <ol style="list-style-type: none"> 1. CCO DO receives a Converged Core Service creation request from the Service Provider tenant. 2. CCO DO requests VIM to deploy a Converged Core Control Plane VNF instance and establish the connectivity between the Converged Core Control Plane VNF and the Edge SDN M&C. the CC CP VNF includes multiple functional components, like DHCP Server, AAA, Service Control etc. Alternatively, above functions can be a set of independent VNFs. 3. CCO DO requests VNFM to manage the lifecycle of the Converged Core Control Plane VNF. 4. CCO DO requests Edge SDN M&C to configure the Converged Core Control Plane VNF. For example, configuring DHCP server with the available IP address pools, AAA with the RADIUS server information and Service Control with the policy server information.

	<ol style="list-style-type: none"> 5. CCO DO requests Edge SDN M&C to configure the Converged Core User Plane PNF assigned for the Service Provider tenant as well. For example, configuring User Plane to forward the subscriber access control related messages (e.g., PPPoE, IPoE, DHCP) to Control Plane. 6. CCO DO requests the VIM to establish L3 connectivity between the Converged Core Control Plane VNF and dedicated Converged Core User Plane PNF. 7. CCO DO reports 'Service Ready'. <ul style="list-style-type: none"> • Interaction 2: Create Converged Core Service User <ol style="list-style-type: none"> 1. CCO DO receives a Converged Core Service User request with end user information, e.g., the quality of service, user credentials. 2. CCO DO requests Edge SDN M&C to configure the Converged Core Control Plane VNF, including the AAA VNF component with the end user credentials, the IPAM VNF component with the end user IP address pool and Service Control VNF component with the end user policies, like bandwidth, QoS etc. • Interaction 3: Activate Converged Core Service <ol style="list-style-type: none"> 1. The Premises PNF (RG) sends a subscriber access control related message (e.g., IPoE or PPPoE request message). 2. Converged Core User Plane PNF intercepts the request message and forwards it to the Converged Core Control Plane VNF via the connectivity created in the step 6 of Interaction 1. 3. Converged Core Control Plane VNF handles the request with its components (AAA VNFC, IPAM VNFC, SC VNFC and etc) inside itself. 4. Upon the successful authentication, IP address allocation and policies enforcement, Converged Core Control Plane VNF sends a response downstream to the Converged Core User Plane PNF. 5. The Converged Core User Plane PNF forwards the response to the Premises PNF (RG). 6. Converged Core Control Plane VNF reports an end user activation to the CCO DO via the Edge SDN M&C • Interaction 4: Change Bandwidth Service based on CC <ol style="list-style-type: none"> 1. CCO DO receives a request to change the bandwidth for the end user. 2. CCO DO requests Edge SDN M&C to configure the Service Control VNF component of the Converged Core Control Plane VNF with the end-user's bandwidth on-demand. 3. Converged Core Control Plane VNF instructs the Converged Core User Plane PNF to enforce the bandwidth modification for the end user. 4. Converged Core Control Plane VNF reports a bandwidth change acknowledge to the CCO DO via the Edge SDN M&C
<p>Expected results</p>	<ul style="list-style-type: none"> • Pass/Fail Criteria for interaction 1 <ol style="list-style-type: none"> 1. Converged Core resources, i.e., VNF and PNF, have been allocated. • Pass/Fail Criteria for interaction 2 <ol style="list-style-type: none"> 1. Converged Core Service User is created. 2. AAA VNFC is configured with the end-user credentials.

	<ol style="list-style-type: none"> 3. IPAM VNFC is configured with the end-user IP address pool. 4. SC VNFC is configured with the end-user policies. <ul style="list-style-type: none"> • Pass/Fail Criteria for interaction 3 <ol style="list-style-type: none"> 1. Converged Core Service is established for the end-user. <ul style="list-style-type: none"> • Pass/Fail Criteria for interaction 4 <ol style="list-style-type: none"> 1. The bandwidth of the end user has been changed on demand
--	--

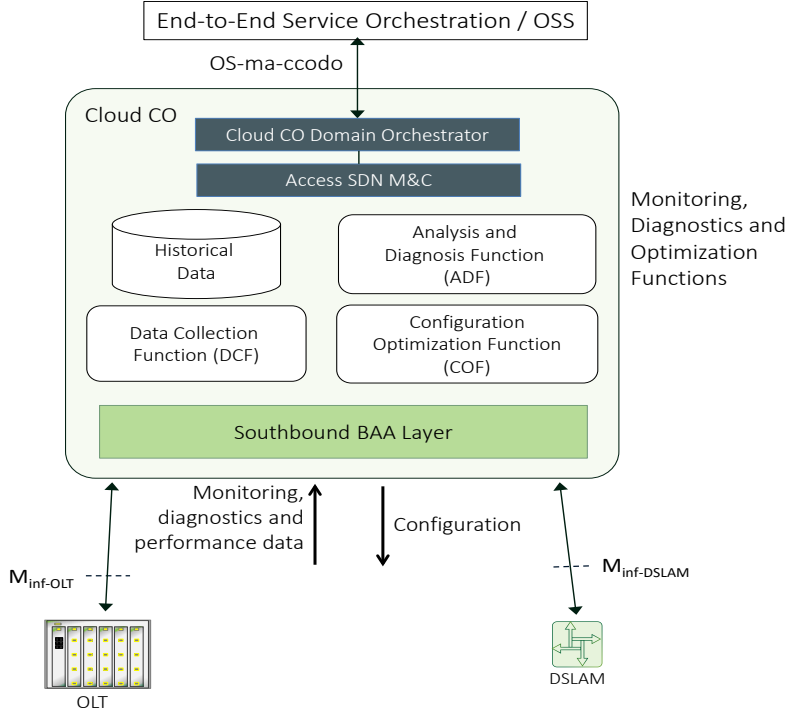
6.7 Parental Control on NERG

Test Case ID	6.7
Test Case Name	Parental Control on NERG
Test Objective	This test case aims to validate how the Parental Control Value Added Service is instantiated in a CloudCO domain
Test Case Reference	CLOUDCO-APPN-442
Test Setup	<p>The test architecture provides a Network Function Virtualization Infrastructure (NFVI) with a corresponding Virtualized Infrastructure Manager (VIM). The NFVI architecture also allows the connection to external devices.</p>
Pretest Conditions	<ul style="list-style-type: none"> • The CloudCO Domain instance is already fully bootstrapped. • The NERG service is already successfully instantiated in the CloudCO Domain. • The filtering policies of this service for tenants are executed by a multi-tenant Firewall VNF. This VNF is managed through the Ms reference point by the Edge SDN M&C.
Test Procedure	<ul style="list-style-type: none"> • Interaction 1 <ol style="list-style-type: none"> 1. CCO DO receives a Parental Control Service creation request. 2. CCO DO requests VIM to deploy and instantiate a multi-tenant Firewall VNF inside the CloudCO Domain. This VNF is managed by the Edge SDN M&C via the Ms reference point.

	<p>3. CCO DO requests VIM to create a virtual network to connect the vG VNF and the Firewall VNF.</p> <ul style="list-style-type: none"> • Interaction 2 <ol style="list-style-type: none"> 1. CCO DO receives a Parental Control Service User creation request with tenant filtering policies. 2. CCO DO requests the Edge SDN M&C to configure the vG VNF to forward the traffic of the tenant to the vFW, rather than forwarding to the Distributed Router directly. 3. CCO DO requests the Edge SDN M&C to configure the vFW with the tenant filtering policies. • Interaction 3 <ol style="list-style-type: none"> 1. The service user visits the web site blocked by the tenant filtering policies 2. The vG VNF forwards the user plane traffic to the vFW via the virtual network between them. <p>The vFW blocks the traffic based on the filtering rules.</p>
<p>Expected results</p>	<ul style="list-style-type: none"> • Pass/Fail Criteria for interaction 1 <ol style="list-style-type: none"> 1. The Firewall VNF is successfully deployed and instantiated in CCO. 2. The virtual network between vG VNF and Firewall VNF has been setup. 3. The virtual network between Edge SDN M&C and Firewall VNF has been setup • Pass/Fail Criteria for interaction 2 <ol style="list-style-type: none"> 1. vG VNF is configured to forward the traffic of the tenant to Firewall VNF. 2. Firewall VNF is configured with the filtering policies of the tenant. • Pass/Fail Criteria for interaction 3: <ol style="list-style-type: none"> 1. The service user cannot access the web site blocked by the tenant filtering policies.

6.8 Monitoring, Diagnostics, and Optimization in a Residential Broadband System.

Test Case ID	6.8
Test Case Name	Monitoring, Diagnostics, and Optimization in a Residential Broadband System
Test Objective	This test is to instantiate and test three Network Services for residential broadband: Monitoring, Diagnostics, and Optimization. The basic functionality of the VNFs composing these Network Services, and the Network Services

	<p>themselves, are tested. Tests are not exhaustive, and no accuracies are tested.</p>
<p>Test Case Reference</p>	<p>CLOUDCO-APPN-445</p>
<p>Test Setup</p>	<p>The test bed includes an OLT and DSLAM connected to a minimal server farm as required in Section 7.1 of TR-384. The minimal server farm includes at least one compute server and one controller server. The test architecture is built in an Open Broadband Laboratory (OBLabs), which provides the test bed and conducts the test procedures</p> <p>The test architecture provides a Network Function Virtualization Infrastructure (NFVI) with a corresponding Virtualized Infrastructure Manager (VIM). The NFVI architecture also allows the connection to external devices.</p>  <p>The diagram illustrates the test architecture. At the top is the 'End-to-End Service Orchestration / OSS' block, which connects to the 'Cloud CO' block via the 'OS-ma-ccodo' interface. The 'Cloud CO' block contains several components: 'Cloud CO Domain Orchestrator' and 'Access SDN M&C' at the top; 'Historical Data' (represented by a cylinder) and 'Data Collection Function (DCF)' (represented by a rounded rectangle) on the left; 'Analysis and Diagnosis Function (ADF)' and 'Configuration Optimization Function (COF)' (both represented by rounded rectangles) on the right; and a 'Southbound BAA Layer' (represented by a green bar) at the bottom. To the right of the Cloud CO block is the text 'Monitoring, Diagnostics and Optimization Functions'. Below the Cloud CO block, the 'Southbound BAA Layer' connects to two external devices: an 'OLT' (represented by a rack of servers) and a 'DSLAM' (represented by a network switch). Bidirectional arrows labeled 'Monitoring, diagnostics and performance data' connect the BAA Layer to both the OLT and DSLAM. A downward arrow labeled 'Configuration' points from the BAA Layer to the DSLAM. Dashed lines labeled $M_{Inf-OLT}$ and $M_{Inf-DSLAM}$ indicate monitoring links from the OLT and DSLAM back to the BAA Layer.</p>
<p>Pretest Conditions</p>	<ul style="list-style-type: none"> • The CloudCO and the End to End Orchestrator are already fully bootstrapped. • A single VIM is deployed in the CloudCO and it is the solely responsible for instantiating the VNFs. • The VIM is installed in the COTS within the NFVI <p>Note: For ease of setup, it is assumed that the End to End Orchestrator and VIM instances run locally over the compute host. This shall not considered as a restrictive choice with regard to a more realistic architecture with distribution of these functions at different locations (and hosts) in the network.</p> <ul style="list-style-type: none"> • There are an OLT and a DSLAM, both having connections to the Southbound BAA layer. • The VIM instantiates DCF VNF, ADF VNF and COF VNF. • End-to-End Service Orchestrator / OSS provides equipment identification and addresses to the BAA through the CloudCO Domain Orchestrator and Access SDN M&C so that the BAA can connect to the access equipment. The BAA creates Southbound interface(s) (SBI) to the

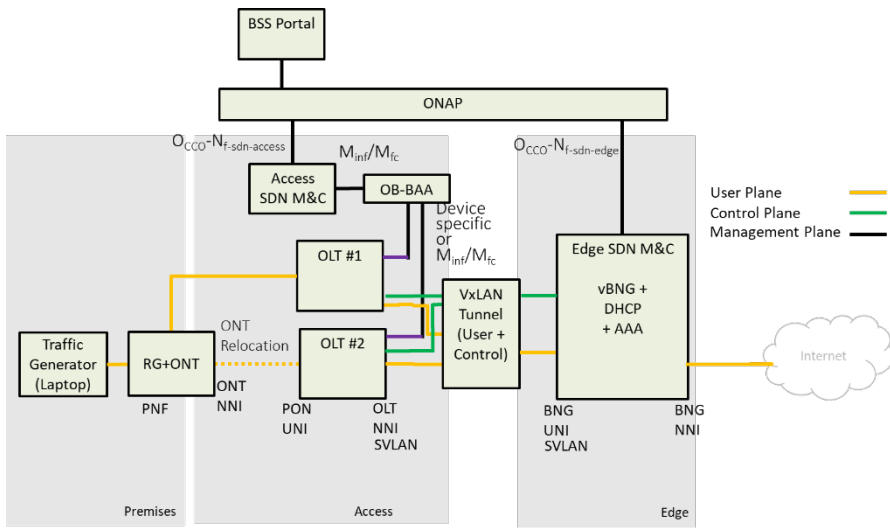
	<p>equipment, including legacy and or CloudCO NETCONF/YANG interfaces. SBIs are the Minf-OLT and Minf-DSLAM interfaces to the two access nodes.</p> <ul style="list-style-type: none"> • CloudCO Domain Orchestrator and Access SDN M&C instantiates the network services: <ul style="list-style-type: none"> • CloudCO Domain Orchestrator instantiates the Monitoring network service instance by chaining DCF and ADF. • CloudCO Domain Orchestrator instantiates the Diagnostics network service instance by chaining DCF and ADF. • CloudCO Domain Orchestrator instantiates the Optimization network service instance by chaining DCF, ADF and COF.
<p>Test Procedure</p>	<ul style="list-style-type: none"> • Interaction 1 – Monitoring End-to-End Service Orchestrator / OSS provides a request for monitoring broadband node(s)/line(s) which is passed through the CloudCO Domain Orchestrator and Access SDN M&C to the Monitoring network service. The request specifies that Layer 1 (L1) monitoring data (e.g., equipment status, performance monitoring counters, physical layer parameters) is to be periodically received. The request for periodically receiving monitoring data is sent from the ADF to the equipment through the DCF to the Southbound BAA layer. Monitoring data are sent from the equipment over the L1 M_{inf-OLT} and M_{inf-DSLAM} interfaces through the Southbound BAA layer through the DCF and received by the ADF. The monitoring data are read out and verified. • Interaction 2 – Diagnostics End-to-End Service Orchestrator / OSS provides a request for diagnosing broadband node(s)/line(s) which is passed through the CloudCO Domain Orchestrator and Access SDN M&C to the Diagnostics network service. The request specifies that L1 diagnostics data (e.g., equipment status, performance monitoring counters, physical layer parameters) is to be received. The request for diagnostic is sent from the ADF through the DCF and the BAA to the equipment through the Southbound BAA layer. L1 diagnostics data are sent from the equipment over the M_{inf-OLT} and M_{inf-DSLAM} interfaces, through the Southbound BAA layer through the DCF and received by the ADF. The Diagnostics data are read out and verified. • Interaction 3 – Optimization End-to-End Service Orchestrator / OSS provides a request for optimizing the configuration of broadband node(s)/line(s) which is passed through the CloudCO Domain Orchestrator and Access SDN M&C to the Optimization network service. Diagnostic data is received as described in Interaction 2. COF analyzes the received diagnostics data as well as network state and configuration data, and optionally additional data in a historical database. The COF then determines the new optimization configuration(s), writes these new configuration(s) through the ADF, DCF and Southbound BAA layer to the equipment over the M_{inf-OLT} and M_{inf-DSLAM} interfaces.

	The new optimization configuration is also optionally stored in the historical database. The new optimization configuration is verified to have been received by the equipment.
Expected results	Monitoring and Diagnostics data are to be received in the CloudCO. Optimized configurations are to be written from the CloudCO to the equipment.

6.9 ONAP Integration of Residential Broadband HSIA Service Use Case

6.9.1 Create and Activate HSIA Service for ONAP Integration for Residential Broadband HSIA Service

Test Case ID	6.9.1
Test Case Name	Create and Activate HSIA Service for ONAP Integration for Residential Broadband HSIA Service
Test Objective	<p>This test case aims to validate the Residential Broadband HSIA Service for a subscriber within a CloudCO using ONAP as the CloudCO Domain Orchestrator. The HSIA service is provided in the following scenario:</p> <ul style="list-style-type: none"> Zero-touch creation and activation of the customer facing HSIA service for residential Broadband subscribers. The CPE used is an ONT that contains the residential gateway functionality.
Test Case Reference	CLOUDCO-APPN-446
Test Setup	The test architecture provides a Network Function Virtualization Infrastructure (NFVI), virtual network functions for the Edge (Edge SDN M&C) and Access (Access SDN M&C, OB-BAA) and physical network functions for Access (OLT, ONT). The service is verified using a Laptop to browse the Internet. The Internet can be emulated through a host server.

	 <p>In the figure above the:</p> <ul style="list-style-type: none"> • Edge SDN M&C is a reference VNF that performs the functions of the vBNG, AAA and DHCP. It has connectivity to OLTs via VxLAN tunnels for the control plane and user plane as well as connectivity to an Internet point (which can be a host server for browsing from the traffic generator) and the ONAP NFVI. • The OLTs are connected to a device that can tunnel the user and control plane traffic to the Edge vBNG function. In addition, the OLTs connect via the management plane to the OB-BAA reference implementation. • The OB-BAA VNF is connected to the Access SDN M&C VNF for management plane functionality. • The Access SDN M&C is connected to the ONAP NFVI. • The ONT is originally attached to one OLT and then moved to the other OLT during the ONT relocation scenario. • The traffic generator is connected to the ONT to determine success criteria of the interactions. • BSS Portal is used to view status and trigger actions within the ONAP instance via north bound ONAP APIs, it may be emulated (e.g., not a fully featured BSS system).
<p>Pretest Conditions</p>	<p>ONAP provides the E2E Service Orchestration, CloudCO Domain Orchestration and management and control of the NFVI functionality (VIM, DC SDN M&C) and is fully bootstrapped.</p> <p>While the ONAP BBS Use Case places the Edge functionality in the service provider's centralized Data Center, this application note places the Edge functionality within the CloudCO's NFVI infrastructure.</p> <p>The following HSIA Infrastructure Services have been established:</p> <ul style="list-style-type: none"> • The VNFs are already deployed and running; ONAP is not used to deploy the VNFs. • OLT is onboarded to the Access BAA layer and Access SDN M&C and communicating with the BAA layer

	<ul style="list-style-type: none"> • Management plane connectivity exists between the BAA layer and the Access SDN M&C • Management plane connectivity exists between ONAP and the Access SDN M&C • Management plane connectivity exists between ONAP and the Edge SDN M&C • User plane connectivity between the OLT and Edge over a VxLAN tunnel • ONT is preconfigured for the HSIA service • ONT has ODN connectivity to OLT #1 and OLT #2
<p>Test Procedure</p>	<ol style="list-style-type: none"> 1. BSS Portal sends a CFS HSIA service instance creation request to ONAP External API including BSS's external ID for the new service instance, service type ID in ONAP catalog, HSIA and CPE attributes 2. ONAP registers the ONT and awaits activation. 3. ONT is attached to PON port on OLT #1 and is powered on. 4. OLT#1 detects a new ONT and initiates the ONT registration process 5. Access SDN M&C reports the ONT registration event to ONAP using the PNF registration VES event message that includes additional fields, such as PON UNI (OLT attachment port) and Remote-ID 6. ONAP continues with the provisioning of the CFS HSIA service by triggering the: <ul style="list-style-type: none"> • Creation of the RFS Access Connectivity, which will configure the ONT and the OLT via the Access SDN M&C • Creation/configuration of the RFS Internet Profile (e.g., customer's speed profile) 7. ONT becomes online and initiates the CFS HSIA activation procedure within the Edge SDN M&C using the information in the DHCP request 8. The Edge SDN M&C authenticates the ONT and sends the Authentication event result to ONAP using the CPE Authentication VES event message 9. ONAP reports the status of the CPE Authentication to the BSS portal.
<p>Expected results</p>	<ol style="list-style-type: none"> 1. The CFS HSIA order is successfully completed. 2. ONT receives a routable address that can reach the server that is acting as the "Internet" 3. ONT/RG is successfully authenticated 4. The customer gets Internet access with the requested rate

6.9.2 Zero-touch relocation of the ONT for ONAP Integration for Residential Broadband HSIA Service (Same OLT)

Test Case ID	6.9.2
Test Case Name	Zero-touch relocation of the ONT for ONAP Integration for Residential Broadband HSIA Service (Same OLT)
Test Objective	<p>This test case aims to validate the Residential Broadband HSIA Service for a subscriber within a CloudCO using ONAP as the CloudCO Domain Orchestrator. The HSIA service is provided in the following scenario:</p> <ul style="list-style-type: none"> Zero-touch relocation of the ONT within the same OLT that results in a change of the ONT's PON attachment point and results in the subscribers HSIA service being moved to the subscriber's new locations. This is called the Nomadic ONT scenario in the ONAP BBS use case.
Test Case Reference	CLOUDCO-APPN-446
Test Setup	<p>Setup is the same as the Create and Activate HSIA Service for ONAP Integration for Residential Broadband HSIA Service test scenario.</p> <p>OLT#2 is not needed for this scenario.</p>
Pretest Conditions	HSIA service has been activated via the Create and Activate HSIA Service for ONAP Integration for Residential Broadband HSIA Service test scenario.
Test Procedure	<ol style="list-style-type: none"> User moves the ONT from OLT #1 PON port #1 to OLT #1 PON port #2
Expected results	<ol style="list-style-type: none"> The CFS HSIA is automatically reconfigured after user moves and plugs ONT in a new location. Reconfiguration includes: <ol style="list-style-type: none"> Deletion of the Access RFS connectivity in OLT #1 PON port #1 Creation of the Access RFS connectivity in OLT #1 PON port #2 Reassignment of the routable address that can reach the server that is acting as the "Internet" Authentication of the ONT The HSIA service is established for that user at the requested rate

6.9.3 Zero-touch relocation of the ONT for ONAP Integration for Residential Broadband HSIA Service (Different OLT)

Test Case ID	6.9.3
Test Case Name	Zero-touch relocation of the ONT for ONAP Integration for Residential Broadband HSIA Service (Different OLT)

Test Objective	<p>This test case aims to validate the Residential Broadband HSIA Service for a subscriber within a CloudCO using ONAP as the CloudCO Domain Orchestrator. The HSIA service is provided in the following scenario:</p> <ul style="list-style-type: none"> • Zero-touch relocation of the ONT on a different OLT that results in a change of the ONT's PON attachment point and results in the subscribers HSIA service being moved to the subscriber's new locations. This is called the Nomadic ONT scenario in the ONAP BBS use case.
Test Case Reference	CLOUDCO-APPN-446
Test Setup	Setup is the same as the Create and Activate HSIA Service for ONAP Integration for Residential Broadband HSIA Service test scenario.
Pretest Conditions	HSIA service has been activated via the Create and Activate HSIA Service for ONAP Integration for Residential Broadband HSIA Service.
Test Procedure	<ol style="list-style-type: none"> 1. User moves the ONT to a PON port in OLT #1 to PON port on OLT #2
Expected results	<ol style="list-style-type: none"> 1. The CFS HSIA is automatically reconfigured after user moves and plugs ONT in a new location. Reconfiguration includes: <ol style="list-style-type: none"> a. Deletion of the Access RFS connectivity in OLT #1 b. Creation of the Access RFS connectivity in OLT #2 c. Reassignment of the routeable address that can reach the server that is acting as the "Internet" d. Authentication of the ONT 2. The HSIA service is established for that user at the requested rate

6.10 NERG Overlay LSL with vG_MUX PNF

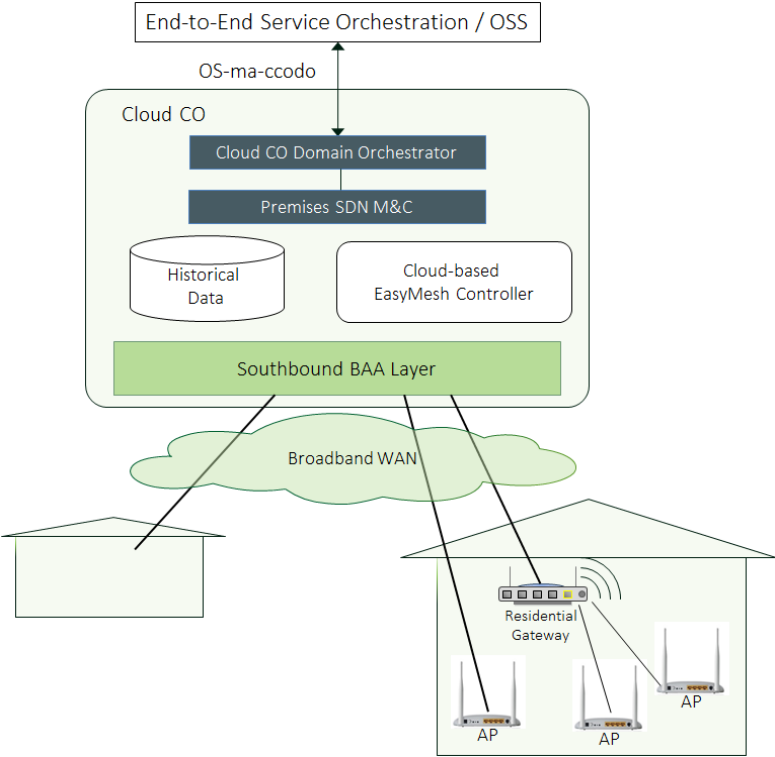
Test Case ID	6.10
Test Case Name	NERG Overlay LSL with vG_MUX PNF
Test Objective	This test case aims to validate how the NERG service is instantiated in a CloudCO domain. In this test case, the vG_MUX function is executed as a PNF on a L3 switch rather than a VNF running on the COTS
Test Case Reference	CloudCO-APPN-447
Test Setup	The test architecture provides a Network Function Virtualization Infrastructure (NFVI) with a corresponding Virtualized Infrastructure Manager (VIM). The NFVI architecture also allows the connection to external devices.

<p>Pretest Conditions</p>	<ul style="list-style-type: none"> • The COTS and OLT are physically connected with switch fabric. • The VIM is installed in the COTS. • The OLT is configured with a VLAN and this VLAN is extended to across the switch connected to the OLT. The VLAN is also extended to the compute hosts that are connected to this switch.
<p>Test Procedure</p>	<ul style="list-style-type: none"> • Interaction 1 <ol style="list-style-type: none"> 1. CCO DO requests VIM to create a Distributed Router across the NFVI through the VIM, associated with a pool of public IP addresses. 2. CCO DO requests VIM to create a overlay network to connect the uplink of Distributed Router, 3. DC SDN M&C sets up a bridge on the switch#2 to connect the overlay network to a pre-created S-VLAN configured on the switch#2 . The switch#2 is a L3 switch and supports VTEP function of the overlay network. 4. The switch#2 is connected to the video server via above pre-created S-VLAN. 5. vG_MUX function is supported on the switch#1, it is pre-configured with reachable IP address. 6. CCO DO requests VIM to create a new overlay network inside the NFVI and connect this overlay network between the vG_MUX and the Edge SDN M&C. The vG_MUX is managed by the Edge SDN M&C via this overlay network. • Interaction 2 <ol style="list-style-type: none"> 1. CCO DO requests VIM to deploy an IPAM VNF inside the CloudCO Domain. 2. CCO DO requests VIM to establish the connectivity between the Access SDN M&C and the IPAM VNF. 3. CCO DO requests Access SDN M&C to configure an S-VLAN on the Access PNF, as well as assigning Access UNIs to that S-VLAN. 4. CCO DO requests DC SDN M&C to configure the S-VLAN on the switch#1 attached to the Access PNF on all of its ports. • Interaction 3 <ol style="list-style-type: none"> 1. CCO DO requests the Edge SDN M&C to configure the IPAM VNF with the end user's addresses. • Interaction 4 <ol style="list-style-type: none"> 1. BRG attaches to the Access Network, the Access PNF relays the DHCP request to the IPAM VNF.

	<ol style="list-style-type: none"> 2. IPAM VNF responds with the address information, the tunnel information (vG_MUX's address) for the end user (tenant). 3. The Access SDN M&C reports a end user(tenant) activation to the CCO DO with the attachment point. 4. CCO DO requests VIM to deploy a vG instance and create a new overlay network inside the NFVI and connect this overlay network between the vG and the Edge SDN M&C. The vG is managed by the Edge SDN M&C via this overlay network. 5. The vG_MUX is configured with the mapping information between the BRG and the vG. 6. CCO DO requests VIM to create one new overlay network inside the NFIV and connect this overlay network between the WAN facing interface of the vG_MUX and the LAN facing interface of the vG to establish the user-plane connectivity between them. <p>CCO DO requests VIM to create another new overlay network inside the NFVI and connect this overlay network between the WAN facing interface of the vG and the Distributed Router to establish the user-plane connectivity between them.</p>
<p>Expected results</p>	<ul style="list-style-type: none"> • Pass/Fail Criteria for interaction 1 <ol style="list-style-type: none"> 1. Distributed Router is created. 2. Routed User Plane Connectivity is created, from the Distributed Router to switch#2 to the video server. 3. vG_MUX function is set up on the switch#1 with reachable IP address. • Pass/Fail Criteria for interaction 2 <ol style="list-style-type: none"> 4. IPAM VNF is created. 5. Management and control plane is established between the Premise PNF (BRG) and the IPAM VNF. • Pass/Fail Criteria for interaction 3 <ol style="list-style-type: none"> 1. IPAM VNF is configured with IP address pool. • Pass/Fail Criteria for interaction 4 <ol style="list-style-type: none"> 1. BRG gets its WAN IP address information and tunnel information 2. The vG VNF is created. 3. The user plane connectivity between the BRG, vG_MUX, vG and Distributed Router is established. 4. The Service User behind the BRG accesses the video service

6.11 EasyMesh Cloud Controller

Test Case ID	6.11
Test Case Name	EasyMesh Cloud Controller

<p>Test Objective</p>	<p>This test is to instantiate and test a Network Service that implements a Wi-Fi CERTIFIED EasyMesh™ controller in the CloudCO. The instantiation of a cloud-based EasyMesh controller service is tested, and the basic functioning of the Wi-Fi EasyMesh cloud controller is tested. However, this is not a certification test and many of the tests specified in the Multi-AP Test Plan [6] are not mandated here.</p>
<p>Test Case Reference</p>	<p>CLOUDCO-APPN-463</p>
<p>Test Setup</p>	<p>The test bed includes a Wi-Fi Access Point (AP) which runs a Wi-Fi EasyMesh agent, connected to a minimal server farm as required in Section 7.1 of TR-384.</p> <p>The minimal server farm includes at least one compute server and one controller server. The test architecture is built in an Open Broadband Laboratory (OBLabs), which provides the test bed and conducts the test procedures</p> <p>The test architecture provides a Network Function Virtualization Infrastructure (NFVI) with a corresponding Virtualized Infrastructure Manager (VIM). The NFVI architecture also allows the connection to external devices.</p> 
<p>Pretest Conditions</p>	<ul style="list-style-type: none"> • The CloudCO, the CloudCO Domain Orchestrator (CCO DO) and the Premises SDN M&C are already fully bootstrapped. • A single VIM is deployed in the CloudCO and it is the solely responsible for instantiating the VNFs. • The VIM is installed in the COTS within the NFVI <p>Note: For ease of setup, it is assumed that the CCO DO, the Premises SDN M&C, and the VIM instances run locally over the compute host. This shall not be considered as a restrictive choice with regard to a more realistic architecture with distribution of these functions at different locations (and hosts) in the network.</p>

	<ul style="list-style-type: none"> • There is a PNF, which is the Wi-Fi Multi-Access Point Under Test (MAUT). The MAUT hosts a Wi-Fi EasyMesh Agent which has a connection to the Southbound BAA layer. • The CloudCO Domain Orchestrator, Premises SDN M&C, and VIM instantiate the Wi-Fi EasyMesh cloud controller network service. • There are two different WAN transport options for Wi-Fi EasyMesh messages: <ul style="list-style-type: none"> • Transport local MAP Ethernet TLVs directly through a layer-2 tunnel (e.g., using VLANs, GRE, or VXLAN), or • Convert MAP Ethernet TLV parameters into messages sent via a Message Transfer Protocol (MTP). The high-level API, data model, or similar represents the MAP data which is transported across the WAN with an MTP such as TR-369/USP. <p>The WAN transport method is not yet defined, so testing here verifies that the functionality of the WAN transport method which is used on the G-interface in this case.</p>
	<ul style="list-style-type: none"> • Interaction 1: Instantiate cloud-based EasyMesh service • The CCO DO receives a request for cloud-based Wi-Fi control from external orchestration / OSS. <ul style="list-style-type: none"> a. The request identifies and contains addresses to communicate to the Multi-AP Under Test (MAUT). b. This request is passed from CCO DO to the Premises SDN M&C. • CCO DO/Premises SDN M&C requests the VIM to instantiate the cloud-based EasyMesh controller VNF. <ul style="list-style-type: none"> a. The VIM instantiates the cloud-based EasyMesh controller service. • CCO DO/Premises SDN M&C provides equipment identification/addresses to the BAA so the BAA can connect to the MAUT. • The BAA creates a Southbound Interface (SBI) to the MAUT across the G-interface or via a layer-2 tunnel. <ul style="list-style-type: none"> a. BAA is now enabled to receive a Northbound API call for a certain action from the cloud-based EasyMesh controller and translate this into the proper messages which are sent on its Southbound interface. For example, messages from the cloud-based EasyMesh controller issue instructions to the APs. b. CCO DO and Premises SDN M&C are notified that messaging is established. • Interaction 2 – Control the in-premises multi-AP Wi-Fi network with the cloud-based EasyMesh controller <p>Interaction 1 is conducted before this test.</p>

	<p>This test verifies that the cloud-based Multi-AP Controller Under Test (MCUT) includes appropriate TLVs and field values in a Channel Preference Query message and a Channel Selection Request message. The text assures that the MCUT can submit a query to a Multi-AP Under Test (MAUT), then formulate a command to control the MAUT, and properly issue that command.</p> <p>The test is run as specified in [6], Clause 5.5.1, MCUT §8 Channel Preference Query and Channel Selection Request Message test.</p>
<p>Expected results</p>	<p>The cloud-based EasyMesh service is instantiated and connects to the Multi-AP Under Test (MAUT). Test conditions PASS, as specified in [6], Clause 5.5.1, MCUT §8 Channel Preference Query and Channel Selection Request Message test.</p>

Appendix I. Test Report Example

The following report is a sample to provide a starting point.

I.1 Overview

Testcase: Bootstrapping an NFVI to a Cloud Central Office
 Source: TR-412
 Test date & time: August 16, 2019 11:00 UTC
 Location: OBL Berlin (EANTC AG, Salzufer 14, 10587 Berlin, Germany)
 Executor: Karsten Elfenbein (EANTC)
 overall result: PASS

I.2 Devices under Test

Role	Vendor	Device	Version	Comment
CloudCO DO	BIG Ltd.	Orchestrator	1.2	
OLT	Little AG	Spiderport-64	17.3	
SDN M&C	Smart Ltd	Super SDN	13.1.123	Running in Docker on Ubuntu 18.04.3

I.3 Additional Components involved

The VMware POD at the OBL Berlin was used to execute the tests.

Role	Vendor	Device	Version	Comment
NFVI	VMware	ESXI	6.7 build 123456	
VIM	VMware	VIO		
HV server	Dell	R730		2x CPU, 512GB RAM, SSD
Switch	Dell	S4048T-ON	9.10	
Traffic Generator	Canonical	Ubuntu	18.04.3	Ping only

I.4 Results

Step ¹	Expected result	Actual result	Result	Comment
VIM creates the overlay networks to interconnect the various elements of CloudCO Domain, such as CCO DO, VIM	x networks created	x networks created	PASS	

¹ Steps according to TR-412

and SDN Controllers.				
VIM deploys the CCO DO and SDN controllers.	CCO and SDN M&C deployed	CCO and SDN M&C deployed	PASS	
CCO DO interconnects VIM and SDN controllers via the overlay networks.	Components interconnected	Components already interconnected	FAIL	A connection could not be established.
Operator uses CCO NB API to create a Service Provider tenant.	CCO is instructed to create Service Provider tenant	Service provider tenant created on CCO DO Service provider tenant created on SDN M&C	INCONCLUSIVE	This could not be tested due to previous errors.
CCO DO creates a Service Provider tenant instances on the SDN Controllers.	Service Provider instance created on SDN M&C	SP instance already resent on SDN M&C	INCONCLUSIVE	This could not be tested due to previous errors.

I.5 Configurations

The ZIP archive with the device configurations is attached from before and after the test execution.

I.6 Logs

The logs of the devices and OpenStack are attached in a ZIP archive.

I.7 Action Points

The CloudCO DO needs a vendor fix to the connection issue. The tester opened a support request to the vendor.

End of Broadband Forum Technical Report TR-412