TECHNICAL REPORT

TR-416
CloudCO Use Cases and Scenarios

Issue: 1
Issue Date: April 2018

© The Broadband Forum. All rights reserved.

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 copyrighted by the Broadband Forum, and all rights are reserved. Portions of this Technical Report may be 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 IS EXPRESSLY DISCLAIMED. ANY USE OF THIS TECHNICAL REPORT SHALL BE MADE ENTIRELY AT THE IMPLEMENTER'S OWN RISK, AND NEITHER THE BROADBAND FORUM, NOR ANY OF ITS MEMBERS OR SUBMITTERS, SHALL HAVE ANY LIABILITY WHATSOEVER TO ANY IMPLEMENTER OR THIRD PARTY FOR ANY DAMAGES OF ANY NATURE WHATSOEVER, DIRECTLY OR INDIRECTLY, ARISING FROM THE USE OF THIS TECHNICAL REPORT.

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.

The text of this notice must be included in all copies of this Technical Report.

Issue History

Issue Number	Approval Date	Publication Date	Issue Editor	Changes
1	9 April 2018	14 May 2018	Georgios Karagiannis, Huawei Technologies	Original

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

Editors:
Georgios Karagiannis, Huawei Technologies
Ding Hai, China Unicom

SDN and NFV Work Area Director(s):
George Dobrowski, Huawei Technologies
Chris Croot, BT

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

Table of Contents

© The Broadband Forum. All rights reserved

List of Figures

© The Broadband Forum. All rights reserved

List of Tables

© The Broadband Forum. All rights reserved

Executive Summary

This Cloud-based Central Office (CloudCO) Use Cases and deployment Scenarios document complements the CloudCO architectural framework specified in TR-384, and helps drive a key element of the BBF's strategy in enabling new revenue generating-services articulated in the Forum's Broadband 20/20 vision. It encompasses the existing Multi Service Broadband Network service scenarios supported by the CloudCO architectural framework design, and elaborates a range of cloud based applications/Use Cases, how a broadband subscriber would access cloud services offered by a broadband cloud service provider, and how data centers as computing resources would be interconnected within a broadband network using this CloudCO architectural framework.

1 Purpose and Scope

1.1 Purpose

1.1.1 Overview

The application of Network Function Virtualization (NFV) and Software Defined Networking (SDN) techniques dramatically change the way broadband networks can be designed and deployed. It enables service providers to evolve to an Information Technology (IT) driven paradigm of service delivery where service providers gain unprecedented programmability and openness, automation, and network control to build highly scalable and flexible networks. Many of these benefits also extend to the end user/subscriber, and over time will lead to new services and applications that do not yet exist.

1.1.2 Purpose of this document

Cloud Central Office (CloudCO) based broadband networking is in the early stages and this specification encompasses examples of Existing Broadband Scenarios (Multi Service Broadband Network (MSBN) services) that are supported by the CloudCO architectural framework design and as well Use Cases that can be established using the TR-384 [5] CloudCO architectural framework.

1.2 Relationship to other industry work

There are several projects in the Broadband Forum (BBF) that are related to SDN and virtualization in MSBN. The project that encompasses this Technical Report and the CloudCO architectural framework specified in TR-384 [5] will consider inputs, where they make sense, from TR-317 (Networked Enhanced Residential Gateway) [19], TR-328 (Virtual Business Gateway) [25], TR-345 (Broadband Network Gateway and Network Function Virtualization) [21] , TR-359 (Framework for Virtualization) [24] and TR-370 (Fixed Access Network Sharing - Architecture and Nodal Requirements) [26], when architecting the CloudCO.

TR-370 [26] provides use cases for the CloudCO and at the same time the CloudCO can be an enabler to implement the Fixed Access Network Sharing (FANS) approach.

TR-317 [19] and TR-328 [25] decomposition of Customer Premises Equipment (CPE) functionality is expected to be supported on a CloudCO architecture naturally, where the virtual Gateway (vG) (TR-317) and virtual Business Gateway (vBG) (TR-328) will run as virtual network functions. Connectivity to the customer located entities in TR-317 [19] and TR-328 [25] is enabled through a combination of SDN techniques to set up connectivity state in physical devices on the one hand, and network virtualization to set up connectivity state between virtual functions on the other hand.

TR-345 [21] is essentially an extension of the legacy TR-178 [13] style architecture, where hierarchical Broadband Network Gateways (BNGs) are deployed as virtual network functions inside an NFV Infrastructure (NFVI). TR-359 defines the framework for NFV on the legacy TR-178 [13] style architecture. SDN and NFV enable new models of functional distribution that support simplifying TR-345 [21] and TR-178 [13] into fewer, simpler elements directed from one or more controllers.

Significant work on SDN and NFV-based architectures is ongoing in industry outside the Broadband Forum (BBF). European Telecommunications Standards Institute's (ETSI's) NFV Industry Specification Group (ISG) has generated a great deal of material on NFV from which this document draws. A large number of Open Source software projects are under development to provide both SDN and NFV components and systems for integration into networks.

1.3 Scope

This document was developed in parallel with, and to complement the CloudCO architectural framework specified in TR-384 [5]. It was essential that CloudCO based broadband networking continue to support the Existing Broadband Scenarios as well as enable new Use Cases that are established using the CloudCO architectural framework capabilities. This approach helped identify entities in existing MSBN and virtualized functions which need to be augmented with new reference points that are described in BBF architectural framework reports TR-359 [24] and TR-384 [5].

The CloudCO's functionality can be accessed through a Northbound Application Programming Interface (NB API), allowing Operators, or 3rd parties, to consume its functionality, while hiding how the functionality is achieved from the API consumer. In order to achieve this, SDN and NFV techniques have been leveraged, running on a cloud-like infrastructure deployed at Central Offices. In this way the NB API offers a Platform-as-a-Service (PaaS) style API. 'Cloud-like' means that the CloudCO architecture would typically leverage Data Center style equipment i.e., generalized network switches and generalized Compute Nodes. These switches, which can be seen as Physical Network Functions (PNFs), enable traffic forwarding at Layer 2 (L2) or Layer 3 (L3) from access functions (where the subscriber line terminates) towards virtualized network functions and/or towards the Broadband Core Network.

2 References and Terminology

2.1 Conventions

There are no requirements in this document which provide an architectural framework.
The reference figures and associated text describe the key elements expected to be part of the CloudCO implementations.

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 21.905 V14.1.1	*Vocabulary for 3GPP Specifications*	3GPP	2017
[2]	RFC1812	*Requirements for IP Version 4 Routers*	IETF	1995
[3]	RFC 4601	*Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)*	IETF	2006
[4]	RFC 4306	*Internet Key Exchange (IKEv2) Protocol*	IETF	2005
[5]	BBF TR-384	*Cloud Central Office Reference Architectural Framework*	BBF	2017
[6]	BBF TR-101 Issue 2	*Migration to Ethernet-Based Broadband Aggregation*	BBF	2011
[7]	BBF TR-069, Amendment 5	*CPE WAN Management Protocol, Amendment 5*	BBF	2013
[8]	BBF TR 101, Issue 2	*Migration to Ethernet-Based Broadband Aggregation; Issue 2*	BBF	2011
[9]	BBF TR-134	*Broadband Policy Control Framework (BPCF), Issue 1, Corrigendum 1*	BBF	2013
[10]	BBF TR-146 Issue 1	*Subscriber Sessions*	BBF	2013
[11]	BBF TR-156, Issue 3	*Using PON Access in the context of TR-101, Issue 3*	BBF	2012
[12]	BBF TR-167, Issue 2	*PON-fed TR-101 Ethernet Access Node, Issue 2*	BBF	2010

[13]	BBF TR-178 Issue 1	*Multi-service Broadband Network Architecture and Nodal Requirements*	BBF	2014
[14]	BBF TR-197, Issue 2	*DQS: DSL Quality Management Techniques and Nomenclature, Issue 2*	BBF	2014
[15]	BBF TR-198, Issue 2	*DQS: DQM systems functional architecture and requirements, Issue 2*	BBF	2012
[16]	BBF TR-203, Issue 1	*Interworking between Next Generation Fixed and 3GPP Wireless Networks*	BBF	2012
[17]	BBF TR-291, Issue 1	*Nodal Requirements for Interworking between Next Generation Fixed and 3GPP Wireless Access*	BBF	2014
[18]	BBF TR-301, Issue 1	*TR-301 Architecture and Requirements for Fiber to the Distribution Point Issue 1*	BBF	2015
[19]	BBF TR-317	*Network Enhanced Residential Gateway*	BBF	2016
[20]	BBF TR-321	*Public Wi-Fi Access in Multi-service Broadband Networks*	BBF	2015
[21]	BBF TR-345	*Broadband Network Gateway and Network Function Virtualization*	BBF	2016
[22]	BBF TR-348	*Hybrid Access Broadband Network Architecture*	BBF	2016
[23]	BBF TR-355	*YANG Modules for FTTdp Management*	BBF	2016
[24]	BBF TR-359, Issue 1	*A Framework for Virtualization, Issue 1*	BBF	2016
[25]	BBF TR-328	*Virtual Business Gateway (vBG)*	BBF	2017
[26]	BBF TR-370	*Fixed Access Network Sharing - Architecture and Nodal Requirements*	BBF	2017
[27]	TS 23.002 V14.0.0	*Network architecture*	3GPP	2016
[28]	TS23.401 v14.0.0	*Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access*	3GPP	2016
[29]	TS23.402 v14.0.0	*Architecture enhancements for non-3GPP accesses*	3GPP	2016
[30]	RFC 7365	*Framework for Data Center (DC) Network Virtualization*	IETF	2014
[31]	ETSI GS NFV-MAN 001	*Network Functions Virtualisation (NFV); Management and Orchestration*	ETSI ISG NFV	2014

2.3 Definitions

The following terminology is used throughout this Technical Report.

CloudCO

Central Office (CO) Domain that is (1) leveraging SDN and NFV techniques, (2) running on a cloud-like infrastructure deployed at Central Offices and (3) that is accessed through a Northbound API, allowing Operators, or 3rd parties, to consume its functionality, while hiding how the functionality is achieved from the API consumer.

CloudCO Domain

One or more CloudCO Macro-Nodes, orchestrated by a single CloudCO Domain Orchestrator and sharing a common, uniquely addressable CloudCO Northbound Interface.

CloudCO Domain Orchestrator

Manages, controls and orchestrates each CloudCO Domain.

DC SDN Manager & Controller

Directly accesses the Network Function Virtualization Infrastructure (NFVI) networking resources to implement functions (e.g., L3 routes in the switch fabric), via configuration of the underlying physical network infrastructure.

CloudCO Macro-Node

The ensemble of network, compute, storage, and application components that work together to deliver networking services, located in a single network site (this may comprise remotely located access functions whose backhauling is terminated on that site).

Container

An instance of operating-system level virtualization where the operating system kernel allows the existence of multiple, isolated user-space instances.

Fixed Mobile Convergence (FMC)

In a given network configuration, the capabilities that provide service and application to the end-user irrespective of the fixed or mobile access technologies and independent of user's location, based on [1].

Forwarding Information Base (FIB)

The table containing the information necessary to forward IP packets, based on [2].

Internet Key Exchange (IKE)

a component of IP Security used for performing mutual authentication and establishing and maintaining security associations, based on [4].

Logical Subscriber Link (LSL)

A logical point to point L2 connection between the physical Business Gateway (pBG) and the virtual Business Gateway (vBG).

Management Control Orchestration (MCO) Engine

Component of the CloudCO Domain Orchestrator that expresses a continuum of Management, Control and Orchestration (MCO) tasks as well as CloudCO state transitions and supervision tasks.

Multicast Forwarding Information Base (MFIB)

a Forwarding Information Base built from the multicast distribution trees state available at a router in order to perform forwarding, based on [3].

NFV Orchestrator (NFVO)

Component of the CloudCO Domain Orchestrator. It has two main responsibilities: (1) the orchestration of NFVI resources across multiple Virtualized Infrastructure Manager (VIMs) and (2) the lifecycle management of network services. For a complete list of NFVO capabilities refer to section 5.4 of [31].

Physical Business Gateway

The equipment located at the business customer premises that contains all hardware-dependent Business Gateway functions that must be performed at the customer premises. It may have a built-in NFVI.

PNF and VNF SDN Managers&Controllers

Responsible for Fault, Configuration, Accounting, Performance, Security (FCAPS) and Flow Control management functionalities respectively for PNFs and VNFs.

Retailer (or Virtual) ISP

An Internet Service Provider (ISP) who purchases resources from a wholesaler in order to offer ISP services to a customer. The retailer ISP does not own the infrastructure directly, but differentiates themselves on the service itself.

Service Instance

One instantiation of a Service on a CloudCO Domain.

User Plane

Defines the part of the router architecture that decides what to do with packets arriving on an inbound interface. In routing, the user plane, is sometimes called the data plane.

Virtual Business Gateway

A virtual entity located at the network and/or at the customer site, serving one or more pBG entities, supporting some network and service functions such as IP routing.

VBG system

A system that includes the pBG component at the customer site and the vBG component at the CloudCO and/or at the customer site. It also includes their connection over the LSL as well as their interfaces and management system.

Virtualized infrastructure manager (VIM)

Responsible for controlling and managing the NFVI compute, storage and network resources, usually within one Operator's Infrastructure Domain. For a complete list of VIM capabilities refer to section 5.4 of [31].

Virtual Machine (VM)

Emulation of a computer system, providing the full functionality of a physical computer to the applications running on it.

VNF Manager (VNFM): Responsible for the lifecycle management of VNF instances. For a complete list of VNFM capabilities refer to section 5.4 of [31].

Wholesaler ISP A third-party provider handles all of the needs of the end user but is invisible to the end user who only sees the retailer (virtual) ISP.

Workload An instance of a process or processes running on a VM or container.

2.4 Abbreviations

This Technical Report uses the following abbreviations:

3GPP	Third Generation Partnership Project
AAA	Authentication, Authorization, Accounting
AC	Access Controller
ACS	Auto-Configuration Server
ADF	Analysis and Diagnosis Function
AN	Access Node
AN-id	AN-identifier
AP	Access Point
API	Application Programming Interface
BGP	Border Gateway Protocol
BNG	Broadband Network Gateway
BPCF	Broadband Policy Control Framework
BRG	Bridged RG
CloudCO	Cloud Central Office
CPE	Customer Premises Equipment
CO	Central Office
COF	Configuration and Optimized Function
C-Tag	Customer -Tag
C-VLAN	Customer VLAN
DC	Data Center
DCF	Data Collection Function
DHCP	Dynamic Host Configuration Protocol
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
EAP	Extensible Authentication Protocol
eBNG	Evolved BNG
EMS	Element Management System
eNodeB	Evolved Node B

ePDG	Evolved Packet Data Gateway
ETSI	European Telecommunications Standards Institute
FANS	Fixed Access Network Sharing
FCAPS	Fault, Configuration, Accounting, Performance, Security
FMC	Fixed Mobile Convergence
GTP	General packet radio service Tunnelling Protocol
IGMP	Internet Group Management Protocol
InP	Infrastructure network Provider
IPoE	Internet Protocol over Ethernet
IPTV	Internet Protocol Television
ISP	Internet Service Provider
L2	Layer 2
L2VPN	Layer 2 VPN
L3	Layer 3
L3VPN	Layer 3 VPN
L4	Layer 4
LDP	Label Distribution Protocol
LLID	Logical Link identifier
LSL	Logical Subscriber Link
LTE	Long Term Evolution
LAN	Local Access Network
MAC	Media Access Control
MANO	Management and Orchestration
MCO	Management Control Orchestration
MEF	Metro Ethernet Forum
MFIB	Multicast Forwarding Information Base
MLD	Multicast Listener Discovery
MSBN	Multi Service Broadband Network
NAT	Network Address Translation
NAPT	Network Address Port Translation
NB	Northbound
NB API	Northbound Application Programming Interface
NBI	Northbound Interface
NERG	Networked Enhanced Residential Gateway
NF	Network Function
NFV	Network Function Virtualization
NFVI	NFV Infrastructure
NFVO	NFV Orchestrator

OLT	Optical Line Termination
ONU	Optical Network Unit
OPEX	Operational Expenses
OSS	Operations Support System
pBG	Physical Business Gateway
PCRF	Policy and Charging Rule Function
PDP	Packet Data Protocol
PNF	Physical Network Function
PGW	Packet Data Network Gateway
PMIPv6	Proxy Mobile IPv6
PON	Passive Optical Network
PPP	Point to Point Protocol
PPPoE	Point to Point Protocol over Ethernet
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RG	Residential Gateway
SGW	Serving Gateway
SBI	Southbound Interface
SDN	Software Defined Networking
SO	Service Orchestrator
SP	Service Provider
S-Tag	Service –Tag
S-VLAN	Service-provider Virtual LAN
ToR	Top of Rack
VAS	Value Added Service
vBG	virtual Business Gateway
vBNG	Virtual BNG
VIM	Virtualized Infrastructure Manager
vEPC	virtual Evolved Packet Core
vG	Virtual Gateway
VLAN	Virtual LAN
VLAN-id	VLAN-identifier
VM	Virtual Machine
VNF	Virtual Network Function
VNFM	VNF Manager
VPN	Virtual Private Network
VTEP	VXLAN Tunnel End Point
VXLAN	Virtual Extensible LAN

WAN	Wide Area Network
ZTP	Zero Touch Provisioning

3 Technical Report Impact

3.1 Energy Efficiency

Implementation of the service scenarios and Use Cases described in this document 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 specification does not quantify these opposite effects on energy efficiency.

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

3.2 IPv6

WT-416 has no impact on IPv6.

3.3 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 API's. In addition, it is expected that management and control plane interfaces are protected from security risks with consideration that the CloudCO framework 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 MSBN apply. However, some new or amplified concerns also appear and without appropriate precautions, the above conditions could impact a network's security.

The BBF will work in collaboration with other industry organizations to apply and/or adapt protocols for security where appropriate.

3.4 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.

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:

- CloudCO should prevent data, from being copied to a non-intended destination.
- Users may encrypt data so that it cannot be understood even if it is intercepted. CloudCO may also encrypt at points of contact.

This document does not define any specific mechanisms.

4 Introduction

This Technical Report elaborates on what exactly encompasses the CloudCO specified in TR-384 [5]. In particular, it is considered that a CloudCO domain should not behave differently to a service user from a black-box perspective and should as a minimum support the same services that can be supported with a legacy broadband architecture.

Section 5 of this Technical Report describes the Existing Broadband Scenarios as a way of testing this black-box behavior. Furthermore, these scenarios were used in TR-384 [5] to specify how legacy network nodes like a BNG, Access Node (AN) or CPE can be potentially disaggregated into various network functions.

Section 6 describes how to use the CloudCO architectural framework specified in TR-384 [5], to establish Use Cases. The Use Case list is not meant to be exhaustive or meant to be complete. The Use Cases described in this section would need to enable the Legacy Scenarios described in section 5. The Use Cases would need to enable the Legacy Scenarios described in section, but new, CloudCO-only Use Cases are also described.

Section 7 describes the Next Steps.

5 Existing Broadband Scenarios

5.1 Introduction & Scenario Template

The aim of this chapter is to identify typical flows between a broadband service user and the broadband system, and the resulting processing flows between various nodes inside the broadband system. This needs to be at a necessary level of granularity, to clearly identify what functions are triggered inside the various nodes inside the broadband system as a result.

The following template will be used to fill in the Scenarios:

Title	*Short title, reminiscent of key aspects*
Story Highlights	*A few key points to further characterize the Scenario/application*
Involved actors	*Indicate who are the involved actors and how they interact with the broadband environment*
High-level architectural context	*Start by a simple and easy to understand drawing (please try to stay consistent with drawings from existing scenarios), WITHOUT implying any detailed architectural choice.* *Identify the legacy broadband nodes that are involved when the Scenario/application is implemented via legacy architecture. Describe the processing flows that arise between those legacy nodes as a result of an actor interacting with the broadband system.*

5.2 Scenario 1: Residential Broadband Access Using PPPoE

Story Highlights
The residential subscriber is authorized for broadband access using Point to Point Protocol over Ethernet (PPPoE), see Figure 1, [10] and [13].

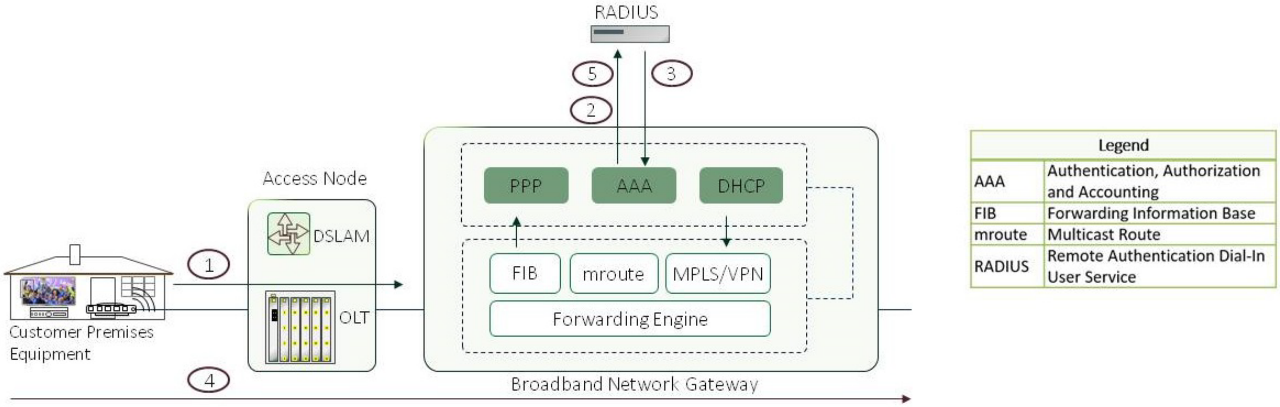
Involved actors
The involved actors are Subscribers. The subscriber gets access to the Internet via the broadband network.

The interaction flows are given as follows:

1. The PPPoE packets are exchanged between the CPE and the BNG for setting up a PPPoE session.
2. The subscriber’s credentials are handed off to the external Remote Authentication Dial-In User Service (RADIUS) server for Authentication.
3. If the credentials match and authentication process succeeds, the subscriber will be authorized to access its permitted network resources and subscribed services. The information is returned to the BNG to enforce the capabilities and restrictions.
4. The subscriber starts accessing services through the BNG.
5. The BNG keeps monitoring the subscriber’s activity and reports usage statistics to the RADIUS server for the accounting process.

High-level architectural context

The involved legacy broadband nodes are CPE, BNG and RADIUS.



Legend	
AAA	Authentication, Authorization and Accounting
FIB	Forwarding Information Base
mroute	Multicast Route
RADIUS	Remote Authentication Dial-In User Service

Figure 1: Involved functions inside the BNG node and the interaction between RADIUS and BNG

5.3 Scenario 2: Residential Broadband Access using IPoE/EAP

Story Highlights

The residential subscriber enjoys services such as Internet Protocol TeleVision (IPTV) via the broadband network, see Figure 2.

Involved actors

The involved actors are Subscribers.

The interaction flows are described as follows:

1. After being powered on, the CPE interacts with the AN, using Extensible Authentication Protocol (EAP) and preparing for the IEEE 802.1x authentication.
2. The subscriber's credentials (i.e., user name and password) get forwarded to the RADIUS server for authentication. If the credentials match and the authentication passes, the subscriber is authenticated into the network.
3. The CPE initiates a Dynamic Host Configuration Protocol (DHCP) request to the BNG.
4. The BNG forwards the DHCP request to the DHCP server.
5. The DHCP server assigns an IP address which is forwarded to the CPE by the BNG.

High-level architectural context

The involved legacy nodes in the broadband system are CPE, BNG, RADIUS, and DHCP.

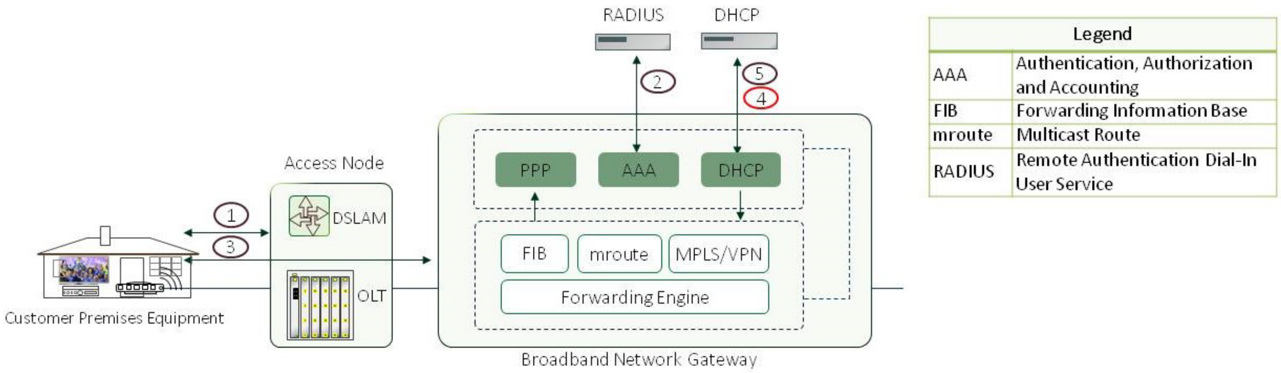

RADIUS
DHCP
2
5
4
Access Node
DSLAM
OLT
1
3
Customer Premises Equipment
PPP
AAA
DHCP
FIB
mroute
MPLS/VPN
Forwarding Engine
Broadband Network Gateway
Legend
AAA
Authentication, Authorization and Accounting
FIB
Forwarding Information Base
mroute
Multicast Route
RADIUS
Remote Authentication Dial-In User Service

Figure 2: Involved functions inside the BNG node and the interaction between RADIUS, DHCP and BNG

5.4 Scenario 3: Fixed Mobile Convergence - Interworking

Story Highlights

The vision of full Fixed Mobile Convergence (FMC) is to provide customers seamless service experience anywhere, anytime, regardless of the access technologies (i.e., fixed, mobile, and wireless), see Figure 3, [16], [17], [28], and [29]. The typical offloading procedure from Long Term Evolution (LTE) to un-trusted non-3GPP access network is used as an example.

Involved actors

The involved actors are:

- Subscribers.
- Network Service Providers.

In the legacy broadband system:

1. The User Equipment (UE) is initially attached to the 3GPP access network, and connected to the Evolved Packet Core (EPC) through bearers (radio and S1/S4) and Proxy Mobile IPv6 (PMIPv6) / General packet radio service Tunneling Protocol (GTP) tunnel to the Serving Gateway (SGW) and Packet Data Network Gateway (PGW).
2. When the UE moves to an un-trusted non-3GPP access network:
   2.1 UE sends DHCP discover message including its Media Access Control (MAC) address to the evolved BNG (eBNG).
   2.2 The eBNG in turn exchanges RADIUS Access messages (Request/Accept) with the Fixed Access Authentication, Authorization and Accounting (AAA) Server to obtain a local IP address for the attached UE.
   2.3 The eBNG then exchanges IP Session Establishment messages (Request/Response) with the Broadband Policy Control Framework (BPCF). If needed, the BPCF exchanges, via the S9a interface, IP connectivity access network Session Establishment messages (Request/Answer) with the Policy and Charging Rules Function (PCRF) to enable policy control (the obtained policy control and charging rules will be mapped to Quality of Service (QoS) rules by BPCF and forwarded to eBNG).
   2.4 The eBNG exchanges DHCP messages (Offer/Request/Ack) with the UE for the IP Session establishment between the UE and the eBNG.

3. UE starts the Internet Key Exchange v2 (IKEv2) tunnel establishment procedure to the evolved Packet Data Gateway (ePDG) which is discovered via a DNS query sent by UE.
4. 3GPP procedures take place between the ePDG, the PGW and the PCRF to establish the 3GPP IP connectivity access network session and the PMIPv6/GTP tunnel between ePDG and PGW, and then the ePDG sends an IKEv2 response to the UE. Finally, the IP connectivity between the UE and the PGW is set up.
5. The ePDG will tunnel any received packets from the non-3GPP access network to the 3GPP domain for accessing 3GPP Providers' services, Cloud services, or Internet.

High-level architectural context

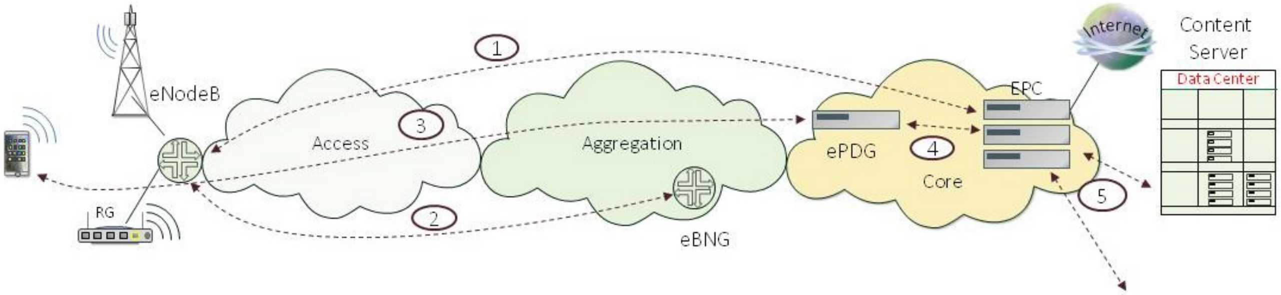


Figure 3: Interactions of involved actors with the broadband system

5.5 Scenario 4: IPv4 Address optimization with CGNAT

Story Highlights
In order to deal with public IPv4 address depletion, some subscribers are handed out private IPv4 addresses. The BNG provides Network Address and Port Translation (NAPT) function, so that the same public IPv4 address is shared across multiple subscribers, using separate layer 4 ports. Public IPv4 addresses are available as an option, so not all subscribers are subject to NAPT in the BNG, see Figure 4.

Involved actors

- Subscriber.
- Network Service Provider.

High-level architectural context
The involved nodes in the broadband system are: RG, BNG, AAA server and Syslog server, which keeps track of the mapping between [public IPv4 address; ports] and subscribers.

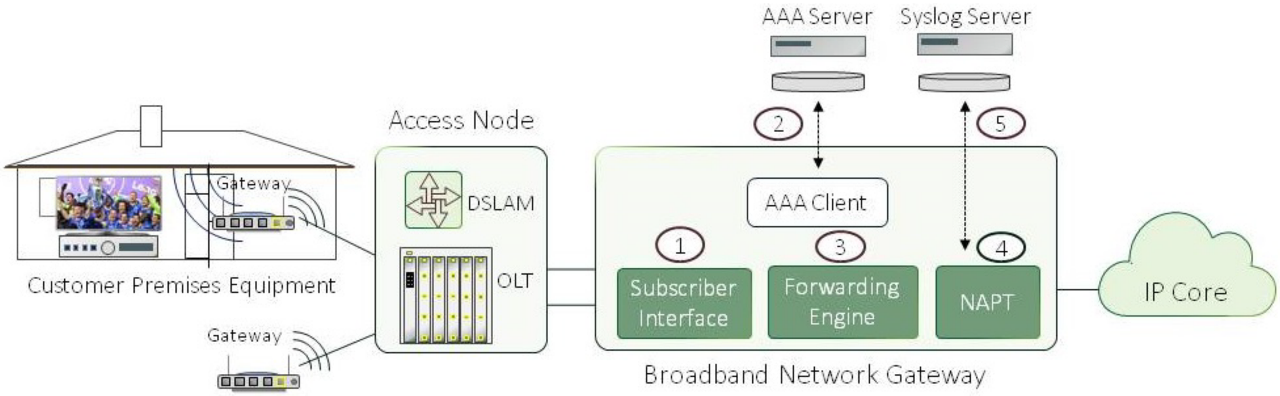


Figure 4: Involved functions and interactions for Carrier Grade Network Address Translation (CGNAT)

The interaction flows are described as follows:

1. RG establishes a Point to Point Protocol (PPP) connection terminated on an access interface of the BNG.
2. BNG AAA client sends an Access-Request with the subscriber credentials; AAA server returns an Access-Accept that contains.
   a) a private IPv4 address (or the name of a pool with private addresses);
   b) a policy to send this subscriber's traffic to the NAPT module in the BNG.
3. BNG forwarding rule is added to override routing and force subscriber's traffic to the NAPT module.
4. As subscriber generates IP packets, the NAPT module adds entries in the flow table and translates addresses and ports in the IP packet header.
5. BNG NAPT module sends logs to a syslog server, containing the binding information between a subscriber and a public IPv4 address + ports. This information is stored in a database, to satisfy lawful requirements in some countries.

5.6 Scenario 5: Parental Control

Story Highlights

A subscriber can register for a parental control service, where web traffic is submitted to URL filtering. The parental control function is external to the BNG. See Figure 5.

Involved actors

- Subscriber.
- Network Service Provider.

High-level architectural context

The involved nodes in the broadband system are: RG, BNG, Parental Control appliance and AAA server.

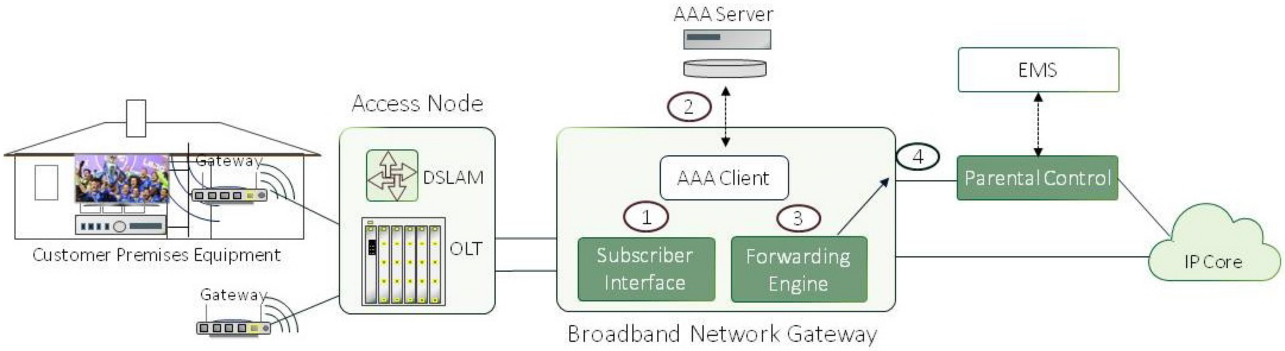


Figure 5: Involved functions and interactions for Parental Control

The interaction flows are described as follows:

1. RG establishes a PPP connection terminated on an access interface of the BNG.
2. BNG AAA client sends an Access-Request with the subscriber credentials; AAA server returns an Access-Accept that contains a policy to send this subscriber's traffic to a Parental Control appliance.
3. BNG forwarding rule is added to override routing and force subscriber's traffic to the Parental Control appliance (subscribers without a Parental Control service are routed directly to the IP core).
4. Subscriber's traffic is processed by the Parental Control appliance. URLs are inspected and inappropriate requests are filtered / redirected to a portal with some warning message. Filtering policies can be customized by the subscriber (parents) on a portal and configured in the Parental Control appliance through an Element Management System (EMS).

5.7 Scenario 6: Lawful Intercept

Story Highlights

A lawful authority delegates some of its privileges to the network service provider, who must be able to deliver a copy of the traffic, for subscribers who are subject to a legal warrant.

The lawful intercept must be imperceptible to the intercepted subscriber, but also to the network service provider's operational team (even staff with management access to the BNG cannot see or reverse engineer if a subscriber is intercepted or not). Traffic sent to the lawful authority is encrypted before exiting the BNG. See Figure 6.

Involved actors

- Subscriber.
- Network Service Provider.
- Lawful authority.

High-level architectural context

The involved nodes in the broadband system are: RG, BNG, AAA server, Mediation Device (a system owned by a lawful authority).

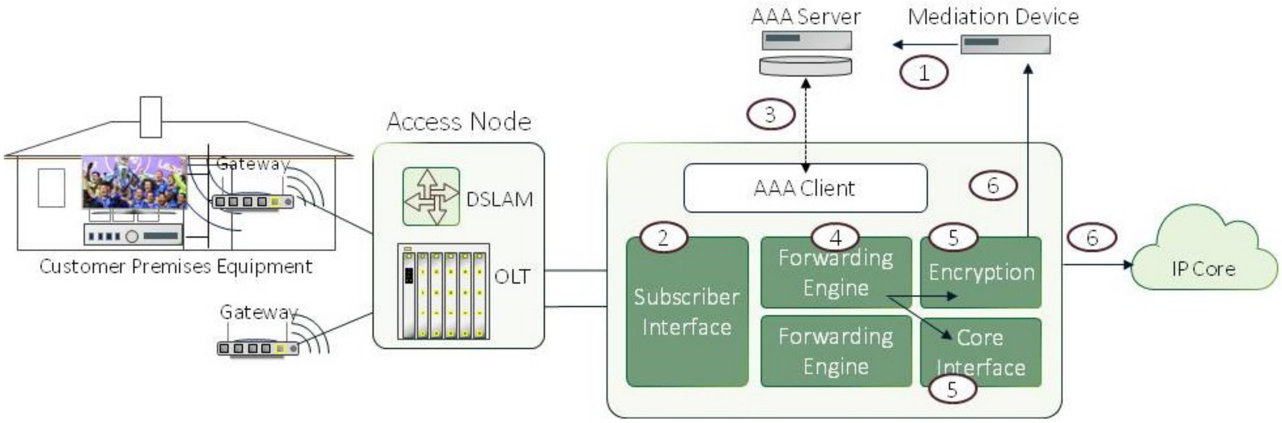


Figure 6: Involved functions and interactions for Lawful Intercept

The interaction flows are described as follows:

1. Through the Mediation Device, the lawful authority instructs the network service provider to intercept a subscriber, based on specific subscriber information. Subscriber's network identity is retrieved and the AAA database is updated.
2. RG of intercepted subscriber establishes a PPP connection terminated on an access interface of the BNG.
3. BNG AAA client sends an Access-Request with the subscriber credentials; AAA server returns an Access-Accept that contains opaque attributes related to lawful interception.
4. BNG installs a policy to intercept packets for this subscriber. All IP packets for this subscriber are mirrored:
   - The original copy is forwarded to the core interface, as any subscriber's traffic.
   - The mirrored copy is added a lawful intercept header, which contains information relevant to the Mediation Device (e.g., Subscriber information). The destination of this encapsulated packet is the Mediation Device. Fields are based on attributes received in step #3.
5. Mirrored copy is encrypted (e.g., IPSec) in BNG.
6. IPSec packet containing the intercepted traffic is sent to the Mediation Device. Original copy is sent to its initial destination, over the IP core.

Note that return traffic is also subject to interception/ mirroring. Also, step 1 may happen while the subscriber is already logged in. In that case, a Change of Authorization can be used, during step 3.

5.8 Scenario 7: Network Enhanced Residential Gateway (NERG)

Story Highlights

The Network Enhanced Residential Gateway (NERG) disaggregates the Residential Gateway (RG) into two components, see Figure 7.

- A Bridged Residential Gateway (BRG), that acts at layer 2.
- A vG, that includes at least a DHCP function to give private IP addresses to hosts in the home and a NAT function, to provide a public IP address for the home. The vG is the default IP gateway for the hosts in the home.

Business drivers for a NERG as well as architecture aspects are defined in TR-317 [19]. The information in this scenario is based on the flat Ethernet connectivity described in TR-317 [19].

© The Broadband Forum. All rights reserved

Involved actors

- Subscriber.
- Network Service Provider.

High-level architectural context

The involved nodes in the broadband system are: RG, BNG, AAA server, vG (part of a vG hosting infrastructure; this is a logical component).

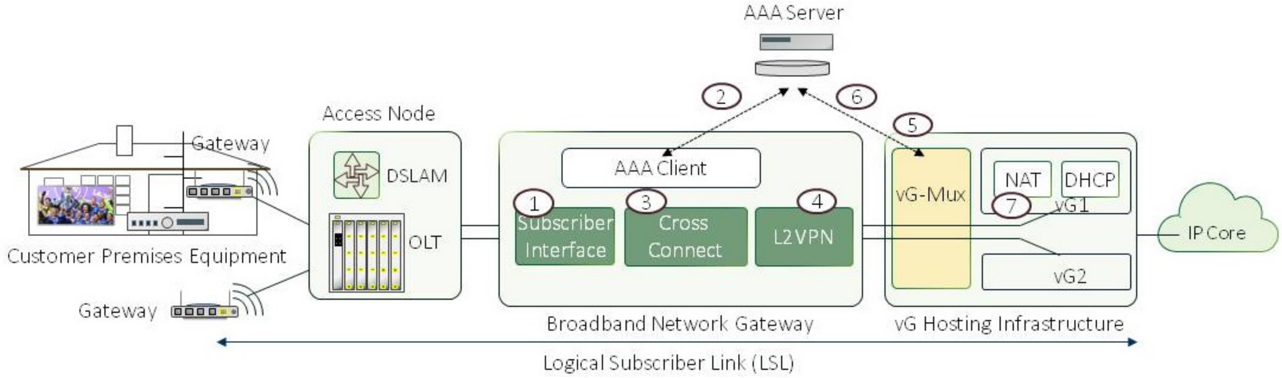


Figure 7: Involved functions and interactions for NERG

The interaction flows are described as follows:

1. The BNG receives a first sign of life on a Customer-VLAN Customer-Virtual Local Access Network) (typically, a DHCP request from a host device in the home). This event activates AAA.
2. The BNG sends an Access-Request to the AAA server, containing option 82. AAA server identifies it is a NERG subscriber and returns the applicable policy to extend the Ethernet layer to a remote system, part of the vG Hosting infrastructure.
3. BNG establishes a cross connect to extend the LAN.
4. The Ethernet frame is transported toward a remote entity called vG-MUX. For example, Ethernet VPN (EVPN)/ Virtual Extensible LAN (VXLAN) is used for transport (other methods such as plain VLAN, Multi-Protocol Label Switching (MPLS), Layer 2 Tunneling Protocol Version 3 (L2TPv3), etc can be used too, but this is not relevant for the context of this document).
5. vG-MUX receives the encapsulated frame and queries the AAA server to retrieve the subscriber information. The frame is mapped to a vG dedicated to the subscriber (depending on how the vG is implemented, it may have been created on demand in parallel with this flow). At this point, the Logical Subscriber Link (LSL) is established. The DHCP server in the vG can answer the DHCP request from the host in the home.

5.9 Scenario 8: Hybrid Access

Story Highlights

Combining LTE and fixed line access allows for an improved customer experience with regards to available aggregate data capacity as well as redundancy in case of failures of one of the access technologies, see Figure 8.

Involved actors

- Residential subscriber.
- Enterprise subscriber.

The subscriber gets access to the internet via the broadband network and the LTE access network. A load sharing mechanism ensures use of both links in parallel according to the service provider's policies.

High-level architectural context

The involved legacy broadband nodes are CPE, AN, BNG, Hybrid Access Gateway (HAG), RADIUS server and BPCF. Furthermore, the 3GPP access network and Evolved Packet System (EPS) is involved.

On a functional level, the architecture looks like Figure 8, which is based on the BBF work in progress (*Nodal Requirements for Hybrid Access Broadband Networks).*

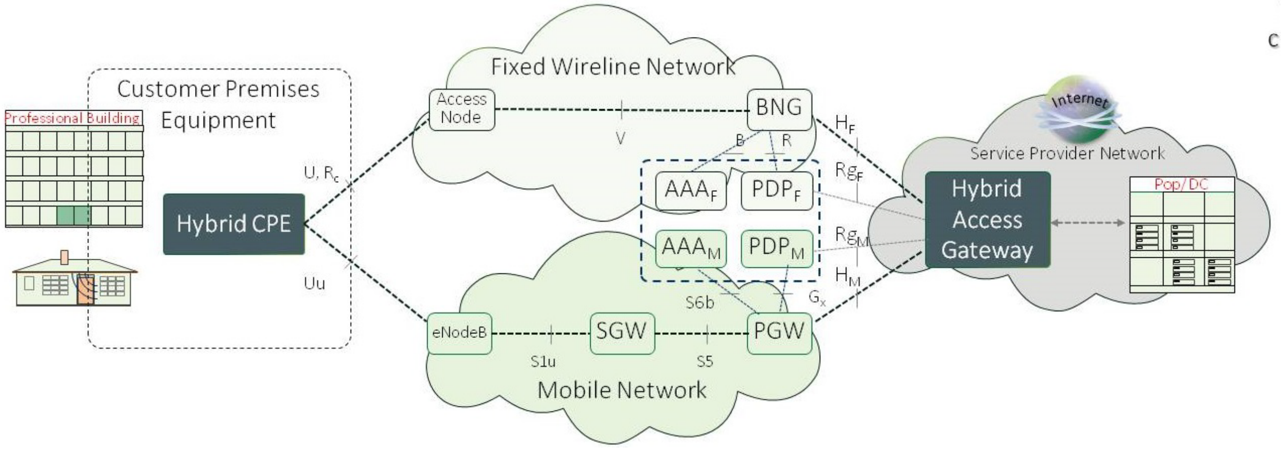


Figure 8: Example Hybrid Access network architecture and reference points

The reference points/interfaces are defined in Table 1.

Reference Point	Description	Source
U	Digital Subscriber Line (DSL) Access	BBF TR-101 [6]
V	Access/Aggregation	BBF TR-101 [6]
B	MS-BNG to fixed broadband AAA	BBF TR-134 [9]
R	MS-BNG to fixed broadband Packet Data Protocol (PDP)	BBF TR-134 [9]
R_{gf}	HAG to fixed broadband PDP	BBF WT-348 [22]
H_f	MS-BNG to HAG	BBF WT-348 [22]
Uu	Mobile Access	3GPP TS23.002 [27]
S1u	eNodeB to SGW	3GPP TS23.002 [27]
S5	SGW to PGW (non-roaming)	3GPP TS23.002 [27]
S6b	PGW to 3GPP AAA	3GPP TS23.002 [27]

Gx	PGW to 3GPP PDP	3GPP TS23.002 [27]
R_{gm}	HAG to 3GPP PDP	BBF WT-348 [22]
H_m	PGW to HAG	BBF WT-348 [22]

Table 1: Hybrid Access network architecture reference points summary

The respective message flows are left open for individual implementations and thus not described here in detail. Basically, the hybrid CPE attaches to both, the fixed and the mobile network and the mechanisms described in TR-348 [22] allow for a load sharing mechanism on top of these access sessions.

Expected CloudCO impact/benefits

In addition to general benefits described in section 5.3 of TR-384 [5], deploying hybrid access on a CloudCO based infrastructure is expected to lead to additional benefits specific to this scenario.

Figure 9 marks entities that are prime candidates for being deployed in a CloudCO in green.

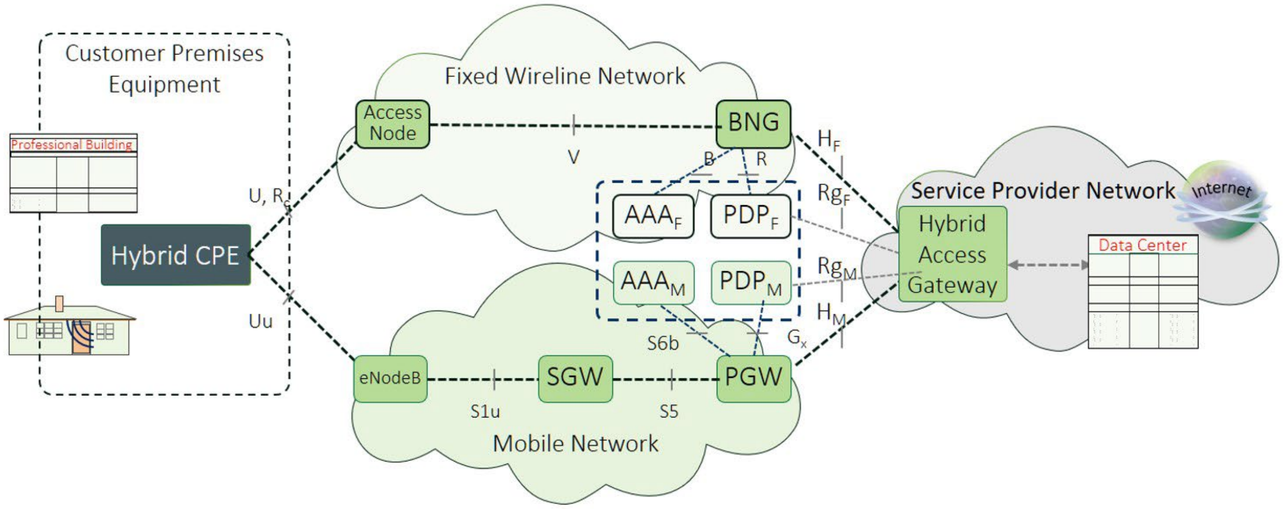


Figure 9: Example Hybrid Access network architecture; green marked entities are prime candidates for being deployed in CloudCO

While the AN and the BNG are fundamental elements of the CloudCO concept, their counterparts in the mobile networks are also expected to become deployed in CloudCOs. The SGW/PGW as the counterpart of the BNG is a natural choice, providing IP connectivity in geographically dispersed locations. In the case of the eNodeB, it has to be taken into account that it is expected to be deployed in locations even further out towards the customer, making it not a natural choice. In a split eNodeB scenario, e.g., in Cloud Radio Access Network (CloudRAN) cases, some selected functionality such as the baseband processing may well be hosted in the CloudCO.

AAA and Policy Control functions such as BPCF and PCRF are expected to reside in more central locations e.g., the Mobility Management Entity (MME).

Some reference points which are defined as external may become internal in a CloudCO model, implying that they might be not be exposed to functions outside the CloudCO Domain.

While deploying the aforementioned functions inside a CloudCO is expected to lead to benefits described in section 5.3 of TR-384 [5], such as scale out and encapsulation into a self-contained instance, the hybrid access scenario may also have the following benefits:

- Traffic and control plane signaling optimization due to local traffic offloading / hybrid session binding inside the CloudCO Domain.
- LTE tunnel routing and termination in the same CloudCO Domain as a fixed access session by coupling the signaling.
- Integration of HAG function into the CloudCO.
- Convergence of IP edge functionality (PGW, BNG, HAG).

5.10 Scenario 9: Virtual Business Gateway

Story Highlights

TR-328 [25] specifies the vBG architecture. By virtualizing some of the functionalities of a Business Gateway to a vBG component, the vBG architecture provides more flexibility to business user services. The architecture allows distributing the vBG component to either a customer premises or an Operator's network or a combination of the both. The vBG component could be deployed in CloudCO taking advantage of NFV and SDN techniques to coordinate with physical Business Gateway (pBG) and vBG located in the customer premises. See Figure 10.

TR-328 [25] uses a similar architecture as in TR-317 [19], which disaggregates the Business Gateway into two components:

- A pBG, that acts at L2 or L3.
- A vBG, that includes IP address management, Network Address Translation (NAT) and VPN services.

The major differences include**:**

- vBG cloud be placed in customer premises other than Central Office, Point of Presence (POP) or Cloud Data Center.
- vBG component has different functionalities including routing, routing protocol and VPN services.
- A single vBG needs to support multiple pBGs.
- The vBG-MUX, which is involved in providing LSL overlay connections between the pBG and the vBG, needs to support more tunnel encapsulation, including L2TPv3 over UDP, Layer 2 over Generic Routing Encapsulation (L2oGRE) and VXLAN.

There are two LSL connectivity models between the pBG and the vBG. The overlay model is described in this scenario.

Involved actors

- Enterprise subscribers.
- Network Service Providers.

High-level architectural context

The involved nodes in the broadband system are: pBG, BNG, AAA server, vBG (this is a logical component).

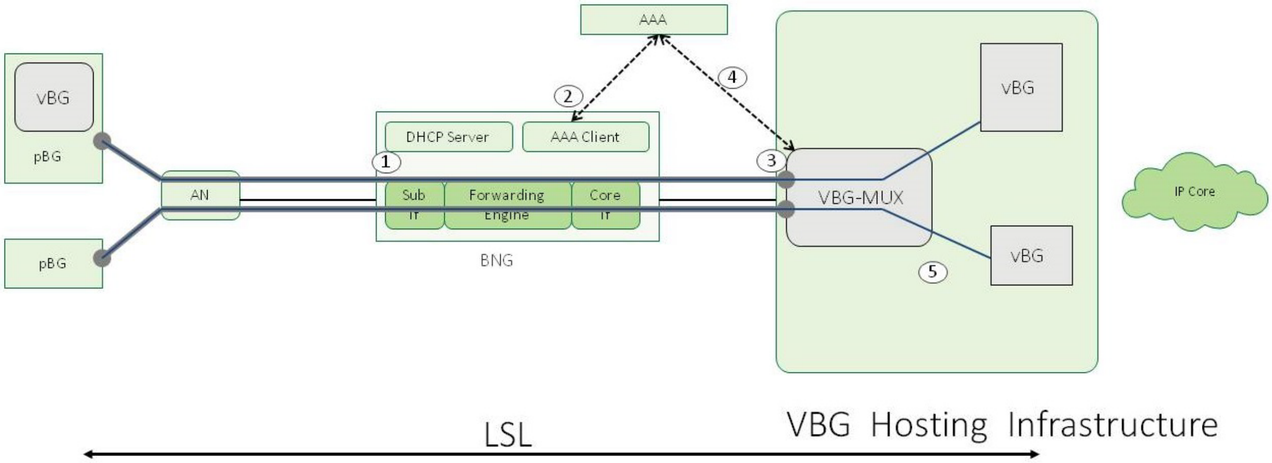


Figure 10: Involved functions and interactions for vBG, modified from WT-328 [25]

In Figure 10, the vBG could be placed at hosting infrastructure or at CPE. This choice might impact how to implement this virtual network in CloudCO.

The interaction flows are described as follows:

1. The pBG requests an IP address for its Wide Area Network (WAN) interface with a DHCP request message.
2. The BNG intercepts the DHCP request and generates a RADIUS Access-Request to authenticate the pBG, containing option 82. AAA server identifies it is a vBG subscriber and returns the tunneling information required for LSL setup. The DHCP server assigns an IP address to the pBG and also provides the tunneling information.
3. The pBG initiates a Layer-2 over IP tunnel, using the information for tunnel setup (source address, endpoint and protocol) provided by various DHCP options obtained.
4. vG-MUX receives the first packet encapsulated in this tunnel and queries AAA server to retrieve the vBG information.
5. The vG-MUX decapsulates the tunneled traffic and forwards it to the identified vBG.

5.11 Scenario 10: Residential Broadband Access, User watches IPTV broadcast

Story Highlights

A Set-Top-Box, or Internet enabled TV is connected inside the home LAN. Channel changing is achieved via sending Internet Group Management Protocol (IGMP) Joins and Leaves messages. As a result of the IGMP Joins and Leaves messages, different multicast groups are delivered to the subscriber's home. The TR-178 [13]-based legacy broadband infrastructure needs to replicate multicast in the most optimal way, by leveraging IGMP snooping at the AN, and IP Multicast routing at the BNG. It is assumed that Multicast is delivered across a Multicast VLAN from BNG to AN, and that the AN replicates multicast untagged to the access line, while unicast packets (including IGMP joins) are received in the context of the Service-provider (S)/ Customer (C) VLAN pair associated to the access line, see Figure 11.

Involved actors

- Service user watching IPTV.
- Service Provider providing Life Broadcast TV services using IP multicast.

Architectural Context

The involved broadband nodes are RG, AN, BNG and the multicast server, connected somewhere across the Service Provider's core network.

The necessary information flows, as illustrated in Figure 11 are as follows:

1. The Set-Top-Box (STB) or the television set sends out an IGMP Join when changing a TV channel.
2. The RG receives the IGMP join and sends it upstream untagged towards the AN.
3. The AN receives and snoops the IGMP Join and sets up the correct replication forwarding state.
4. The AN forwards the IGMP Join inside the context of the S/C VLAN pair configured for that subscriber access line across the uplink towards the BNG.
5. The BNG receives the IGMP Join and adds the subscriber sub-interface to the Multicast Forwarding Information Base (MFIB) for the right multicast stream.
6. The BNG starts streaming multicast towards the AN.
7. The AN replicates the multicast stream to the appropriate access line, depending on the replication forwarding state established in step 3.
8. The RG forwards the multicast stream inside the Home LAN, and STB receives it.

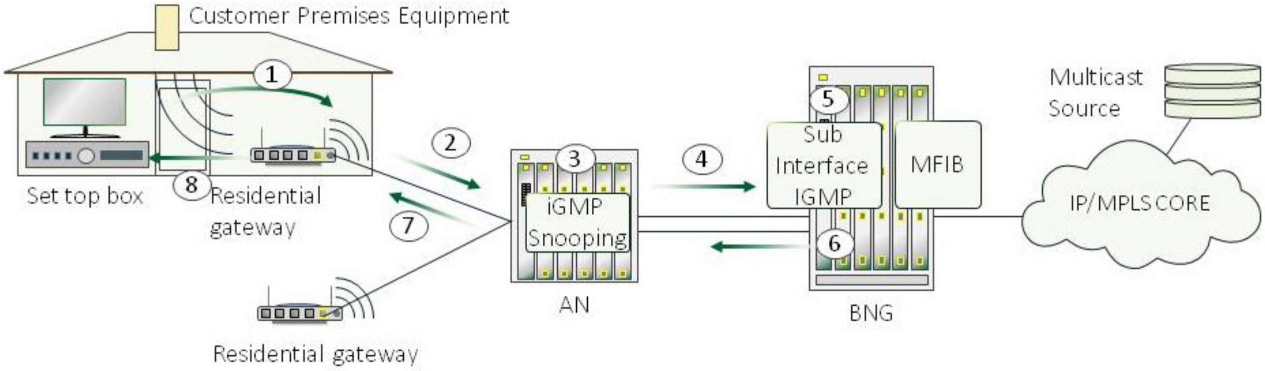


Figure 11: Residential Broadband Access, user watches IPTV broadcast

5.12 Scenario 11: Business Broadband Access, L2VPN activation

Story Highlights

Multiple sites are equipped with a L2 CPE that attaches the site to the local AN. Every access-line is given a Service-provider Virtual LAN (S-VLAN), and the AN double tags all Customer VLANs (C-VLANs) unconditionally with the S-VLAN. This configuration is done at AN deployment time. The BNG can then use the S and C-tags to allocate the traffic to an L2VPN instance. This configuration is done at service provisioning time. The L2VPN instance is configured via an EMS, and is typically signaled using Border Gateway Protocol (BGP) or Label Distribution Protocol (LDP), typically at service provisioning time, see Figure 12.

Involved actors

- Service user.
- Service Provider providing the L2VPN service.

Architectural Context

The involved Broadband nodes are L2 CPE, AN's aggregating the CPEs, and BNG aggregating AN's. Here are the information flows, according to the figure below:

1. The AN EMS configures every Access Line with a dedicated, service unspecific S-VLAN.
2. At L2VPN Service configuration time, all participating BNGs join an L2VPN instance, typically leveraging BGP or LDP signaling.
3. At L2VPN Service configuration time, the appropriate S/C VLAN combinations are added to the appropriate L2VPN Service instance by the L2VPN EMS.

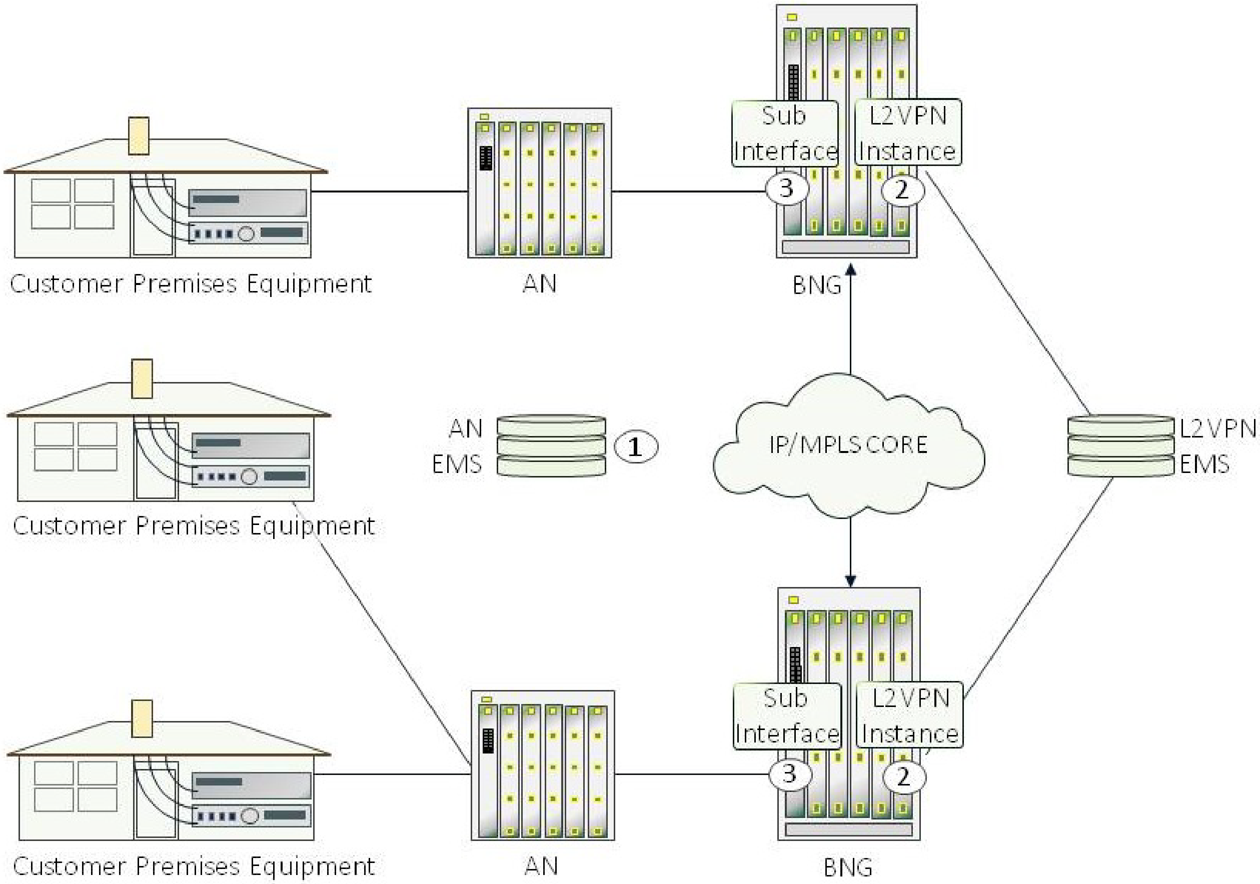


Figure 12: Business Broadband Access, L2VPN activation

5.13 Scenario 12: Fixed Access Network Sharing (FANS)

Story Highlights

In current fixed access networks, network elements are usually "closed" systems, often with limited and vendor-specific control interfaces. Therefore, once in production and deployed, it is quite difficult for current network infrastructure to evolve.

The challenge for Operators is to provide services to their customers in a more elastic, flexible and scalable way. This could be done by sharing the network resources between different telecom Operators. TR-101 [6] /TR-178 [13] describe the L2 Ethernet-based aggregation for a broadband multi-service network, defining a Wholesale model.

TR-370 [26] enhances the shared network model, introducing the Fixed Access Network Sharing (FANS) architecture that allows compliance with the above standards.

Involved actors

- Infrastructure Provider (InP).
- Virtual Network Operator (VNO).
- Residential/Business Customers.

High-level architectural context

Compared to the current traditional access network architecture which requires at least one physical AN per Operator, the FANS system allows hosting multiple VNOs (at least one virtual AN per VNO) on a single physical AN (host) or on top of a High-Volume Server in one or more Central Offices, as described in Figure 13.

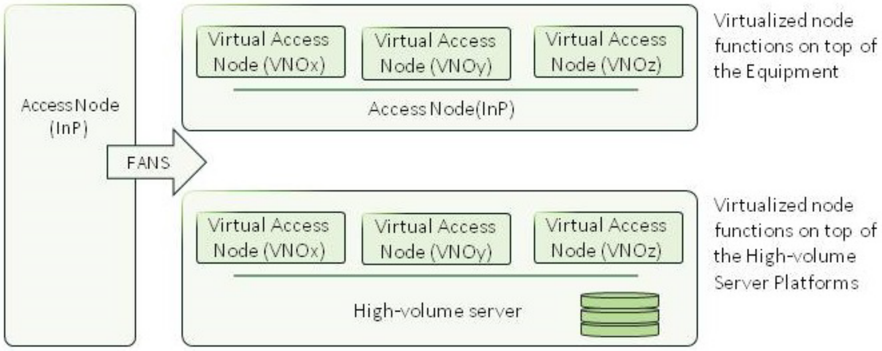

Access Node (InP)
FANS
Virtual Access Node (VNOx)
Virtual Access Node (VNOy)
Virtual Access Node (VNOz)
Access Node(InP)
Virtualized node functions on top of the Equipment
Virtual Access Node (VNOx)
Virtual Access Node (VNOy)
Virtual Access Node (VNOz)
High-volume server
Virtualized node functions on top of the High-volume Server Platforms

Figure 13: Deployment scenarios for FANS

5.14 Scenario 13: Public Wi-Fi Access

Story Highlights

BBF TR-321 [20] specifies architectures and solutions to incorporate Wi-Fi access technology into existing broadband networks. Many service providers offer public Wi-Fi as part of their basic broadband services. Public Wi-Fi is here different from legacy Wi-Fi hotspot because they cover a relative large geographic area and may offer QoS capabilities.

Involved actors

- Wi-Fi Access Points.
- Access Controller (AC).
- Broadband Network Gateways (BNG).

High-level architectural context

Section 6 of TR-321 [20] describes three architectures for the public Wi-Fi network, which are aligned with TR-101, TR-145 and TR-178 architectural principles:

- Stand-alone AC.
- BNG integrated AC.
- Distributed AC.

In case of a Stand-alone AC architecture, all of the access points traffic (user and management) is first aggregated at the AC and then forwarded to the BNG.
Two architectural options are possible for the AC in the case of a stand-alone AC architecture:

- AC deployed closer to the access points than the BNG if there is a high density of access points, see Figure 14.
- AC co-located with the BNG, see Figure 15.

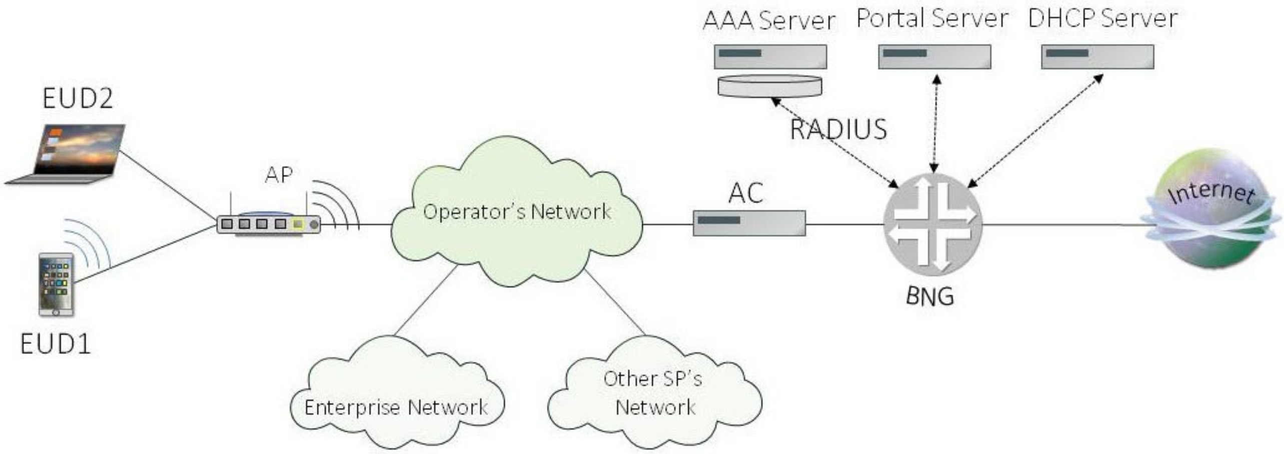


Figure 14: AC deployed in close proximity to the access points

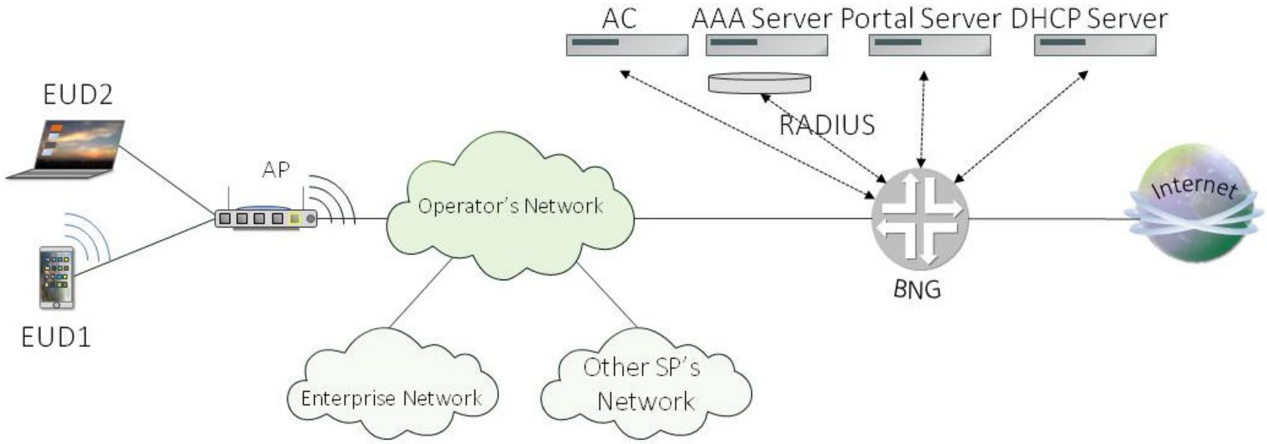


Figure 15: AC co-located with BNG

In this architecture (Figure 14 and Figure 15), the AC is responsible for control and management of the access points, while the BNG manages traffic on a per subscriber basis.

In the other case, i.e., BNG integrated AC architecture, see Figure 16, the AC functionality is incorporated within the BNG. All of the Access Points traffic (user and management) is aggregated at the integrated AC&BNG node.

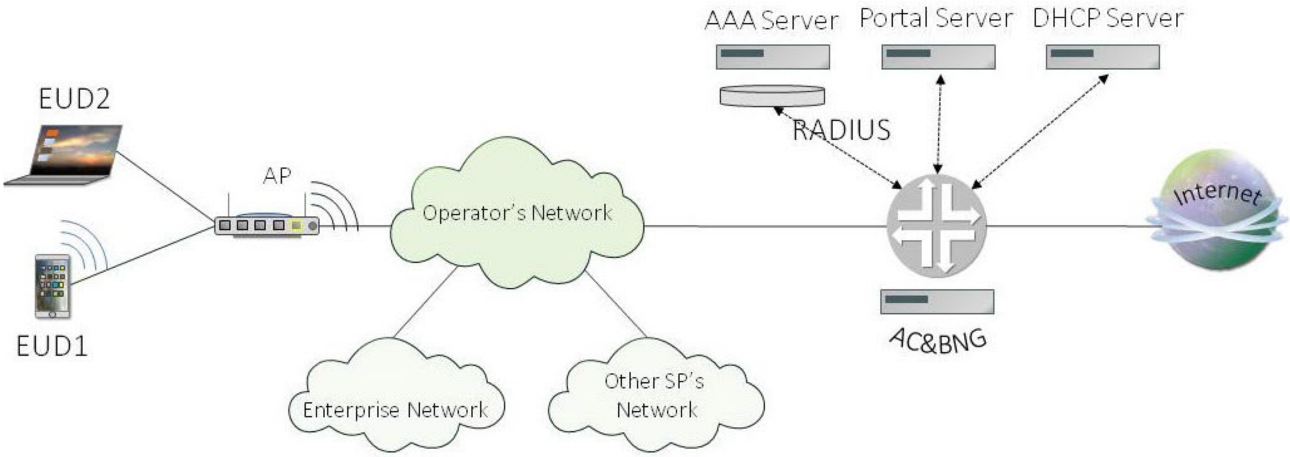


Figure 16: BNG integrated AC architecture

AC is responsible for control and management of the access points, while the AC&BNG manages traffic on a per subscriber basis.

In case of a Distributed AC architecture, see Figure 17, only access points' control and management traffic is forwarded to the AC, while the Wi-Fi user traffic is directly forwarded to the BNG. Thus, AC is no longer in the user path, but it just handles the control and management traffic.

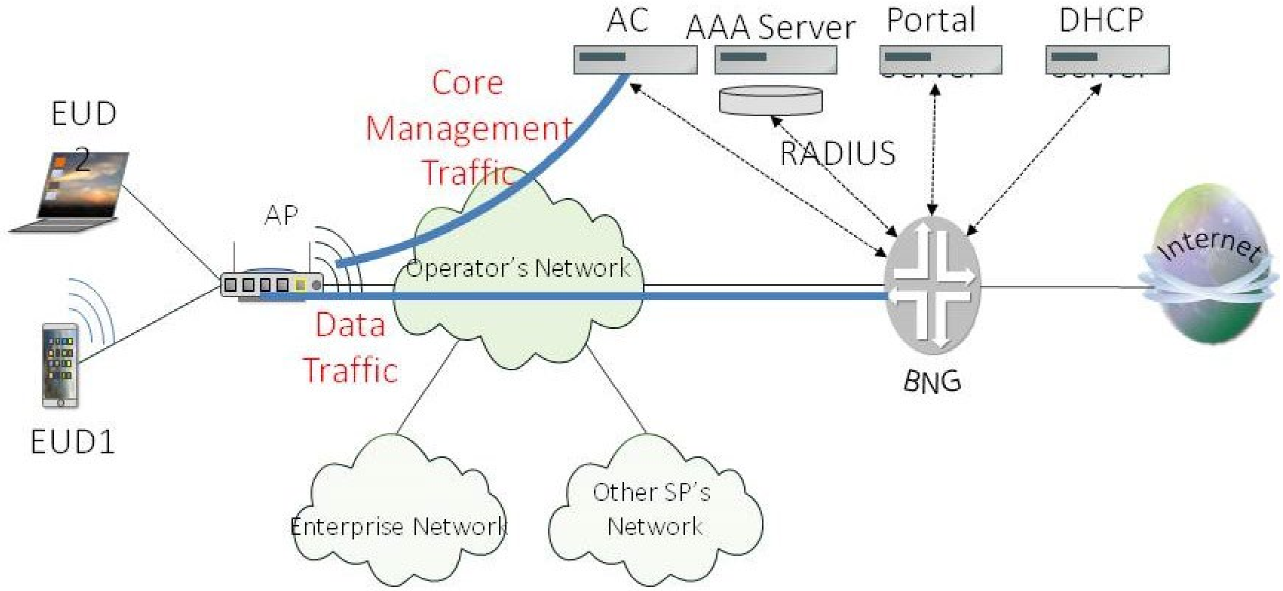


Figure 17: Distributed AC architecture

5.15 Scenario 14: Home network virtualization scenario

Story highlight

Rapid and iterative upgrades of intelligent operating systems, such as the Android4.0 to 7.0, increase significantly the (1) prices of Random Access Memory (RAM)/Flash, applications and (2) the STB Capital Expenses (CAPEX) that can became a heavy burden for operators;
In virtualized STBs, most applications can be installed and be run on the network side that (1) greatly reduces the Central Processing Unit (CPU) usage, (2) lowers the Flash/RAM requirements and (3) drops the upgrade frequency of the operating system. With all these advantages, vSTB has the potential to be applied in future video delivery deployments.
Based on the high utilization of Android App store and on the millions of APPs running in intelligent Android STBs, it may be more attractive and reasonable to stimulate the STB virtualization instead of the CPE virtualization (vCPE). Therefore, it is expected that a vCPE will not be applied on a large scale in Value Added Services.
In the context of this scenario, it is recommended that vSTB should be considered as an Optional virtualized network terminal example, which can be deployed into a CloudCO Domain as a VNF.

Involved actors

- Residential users who order IPTV services.
- Network Service Provider.

High-level architectural context

The involved nodes in the broadband system are: pSTB, vSTB, AN, CPE, hosting environment for vSTB, see Figure 18.

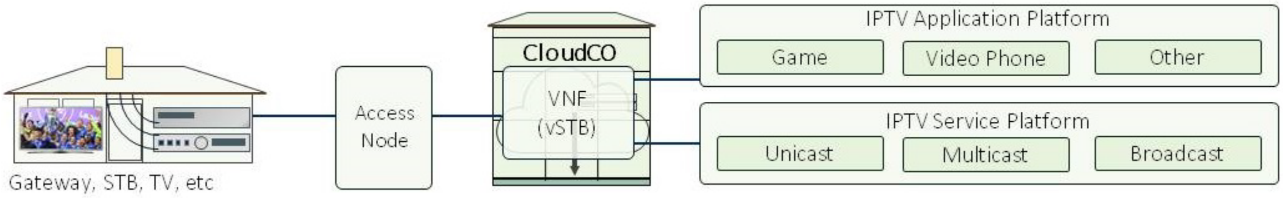


Figure 18: Logical Architecture for a vSTB

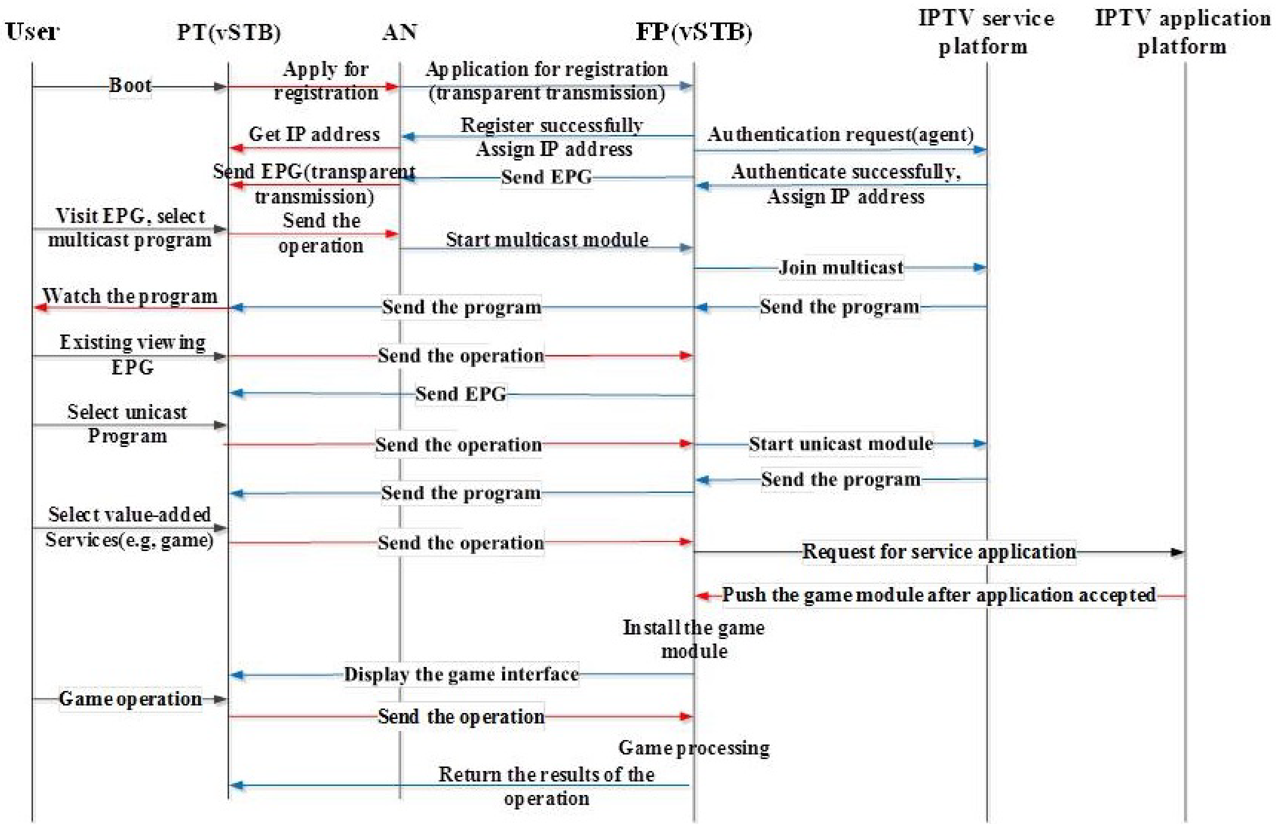

User
PT(vSTB)
AN
FP(vSTB)
IPTV service platform
IPTV application platform
Boot
Apply for registration
Application for registration (transparent transmission)
Get IP address
Register successfully Assign IP address
Authentication request(agent)
Send EPG(transparent transmission)
Send EPG
Authenticate successfully, Assign IP address
Visit EPG, select multicast program
Send the operation
Start multicast module
Join multicast
Watch the program
Send the program
Send the program
Existing viewing EPG
Send the operation
Send EPG
Select unicast Program
Send the operation
Start unicast module
Send the program
Send the program
Select value-added Services(e.g. game)
Send the operation
Request for service application
Push the game module after application accepted
Install the game module
Display the game interface
Game operation
Send the operation
Game processing
Return the results of the operation

Figure 19: vSTB involved interactions

The message sequence chart for the vSTB involved interactions is shown in Figure 19 and is realized as follows.

1. PT(vSTB) request registration. In this context, PT represents the Physical Terminal that is deployed at CPE. This request is forwarded through AN transparently. FP(vSTB) detects the request and assigns an IP address for the PT(vSTB). In this context, FP represents the Function Platform that is deployed in the CloudCO Domain.
2. FP(vSTB) requests authentication from the IPTV service platform. When the IPTV service platform accomplishes the authentication, an IP address is assigned to FP(vSTB). Afterwards the FP sends Electronic Program Guide (EPG) to PT(vSTB).
3. Once a multicast program is chosen by users, the request is sent to AN by PT(vSTB). After receiving the request, AN starts the multicast module and the FP(vSTB) joins a multicast group with the IPTV service platform. Then the program is sent directly from the IPTV service platform to the PT(vSTB).
4. Once a unicast program is chosen by users, the request is sent directly to the FP(vSTB). The unicast module requests the unicast program from the IPTV service platform. Afterwards the program is sent directly to the PT(vSTB).
5. Once a value-added service (e.g., online game) is chosen by users, the request is sent to FP from PT. The request for service application is initialized by FP and is forwarded to the IPTV application platform. Then a request to install the game module is sent to the FP. Afterwards the installation of the module is accomplished by FP. The game interface is displayed by the FP and the corresponding stream is sent to PT side. The online gaming operation requests coming from users are sent by the PT and processed by the FP side.

6 CloudCO Use Cases

This section describes how the CloudCO architectural framework can be applied to establish/develop use cases. Some of the use cases are enabling legacy scenarios. However, also new CloudCO-only use cases are also described.

The use cases in section 6.1 describe examples of how the scenarios in section 5 can be instantiated across a CloudCO architecture. These examples are not meant to be exhaustive, and they are not the only way to instantiate the given scenario across a CloudCO architecture. As this Working Text describes an architectural framework, it will not elaborate on certain deployment choices, or mandate them. Rather, the use case will be used to test the validity of the architecture, and will allow consideration of the information that needs to be exchanged across the interfaces between the functional blocks of the architecture.
For services that can be delivered over legacy (non-CloudCO) networks, there should be no observable difference to a user between a service delivered via a legacy broadband architecture or via a CloudCO Domain.

6.1 Use Cases as a result of Scenarios

6.1.1 NERG with Flat Logical Subscriber Link (LSL); Static Model Use Case based on Scenario 7

Section 5.8 describes Scenario 7, where a TR-317 [19] /TR-178 [13] -based broadband system uses or establishes the NERG functionality. TR-317 [19] disaggregates the RG into two components:

- A BRG at the service user's home, that acts at layer 2, and connects into the access link.
- A vG, that includes at least a DHCP function to give private IP addresses to hosts in the home and a NAPT function, to provide a public IP address for the home. The vG is the default IP gateway for the hosts in the home.

Furthermore, it establishes the concept of a LSL, a logical L2 link that interconnects the BRG and vG. It also defines a vG-MUX component, which is essentially an aggregation function for multiple LSLs able to terminate them into the appropriate vG. This vG-MUX is defined as a network function that maps L2 traffic between a subscriber's BRG and its unique vG, and ensures traffic isolation between NERG customers. Mapping may be statically provisioned or obtained dynamically via AAA.

This use case proposes to use Virtual Machines or Containers to instantiate vG instances, and to use bridging between VLANs and virtual networks [30] created using network virtualization to interconnect the BRG and the vG instance. In particular, this use case aims to address only the connectivity requirements as specified in section 7.1.1 (NERG Flat LSL Connectivity) [19]. Further, it will only address the static model of establishing the connectivity as described in TR-317. Other items are left for further study or will be addressed in other use cases.

It can be mentioned that TR-317's vG-MUX [19] is disaggregated across the CloudCO Domain. Every compute host can offer the vG instance access to a virtual network. As the virtual network

© The Broadband Forum. All rights reserved

runs across the entire compute infrastructure, the vG-MUX is effectively running distributed across the CloudCO Domain.

Note that this use case does not elaborate on eventual service chaining of additional network functions like firewalling/NAT/parental control into the Service Graph. In this way, this use case is not meant to be a complete description of all aspects described in TR-317 [19]. It is also not meant to be the only possible implementation of the NERG scenario on the CloudCO Architecture. Moreover, the choice of using one vG instance per subscriber is not meant to describe the only way of achieving NERG like functionality. Furthermore, the use case also does not describe how the CloudCO supporting infrastructure, e.g., Management and Orchestration (MANO) stack, SDN Controllers, are set up.

Involved actors:

- CloudCO Operator, acting as a wholesale Service Provider.
- Retail Internet Service Provider (ISP), offering the Internet Access Service on the CloudCO Domain.
- Service user (i.e., subscriber of the Retail ISP).

Note that this use case does not cater for the possibility that a subscriber could do business with more than one provider, but could easily be extended to allow such behavior.

Pre-requisites:

- A fully initialized CloudCO domain.
- BRG is deployed at the service user home premise and connected to the access line.
- L2 Ethernet packets can flow between the BRG and the CloudCO AN U-Interface. This means also that the BRG node has been installed and provisioned accordingly. How this is done is for further study or described in another use case.
- An Internet Access Service Instance is pre-created inside the CloudCO Domain by the CloudCO service provider, acting as a wholesale provider. This essentially creates a routed and public-address space across the CloudCO Domain and associates it with a retail ISP. The retail ISP can use the CloudCO NB API to associate all of its service users with the instance. An instance of NERG VNF Manager (VNFM) is created for this retail provider's Internet Access Service Instance, allowing lifecycle management of all vGs attached to this Internet Access Service. The CloudCO NB API allows access to the functions relevant for the retail ISP. The necessary steps to be performed inside the CloudCO are:
    a) A distributed router is created across the NFV Infrastructure (NFVI) through the VIM, associated with a pool of public IP addresses. The distributed router uplink is attached to a pre-created virtual network (created through the VIM), and the virtual network is bridged to a pre-created VLAN configured on one of the network facing interfaces of the CloudCO Domain. The VLAN will need to be created on both the CloudCO physical infrastructure and the network-facing interface equipment e.g., by leveraging the SDN Controllers.
    Note that the Distributed Router can be seen as the disaggregated L3 forwarding component of the legacy BNG component.
    b) An instance of NERG VNFM is instantiated through the NFV Orchestrator (NFVO), and its functions are made accessible through the CloudCO NB API, to

allow consumption by the retail ISP. Each retail ISP may have its own flavor of VNFM in terms of lifecycle management of the vGs instances attached to its Internet Access Service, such as:

  a. Instantiation/Termination.
  b. Scaling up/down.
  c. Updating/Upgrading.
  d. State communication from/to other functional blocks in the CloudCO architecture.

  Each retail ISP will have its own Narrowband Interface (NBI), protected by its own security and policy safeguards.

- A per instance subscriber database is created by the CloudCO service provider, and is pre-populated and fully managed by the CloudCO Operator. Primarily the CloudCO Operator will need to associate a given service user (e.g., identified as user@instance) with an access line (e.g., using circuit-id, such as, access-node-id/C-VLAN). Note that although logically there is a separate database per instance, it is not specified how this is implemented.

Onboarding a new NERG instance onto the CloudCO Domain will happen as follows, as shown in Figure 20.

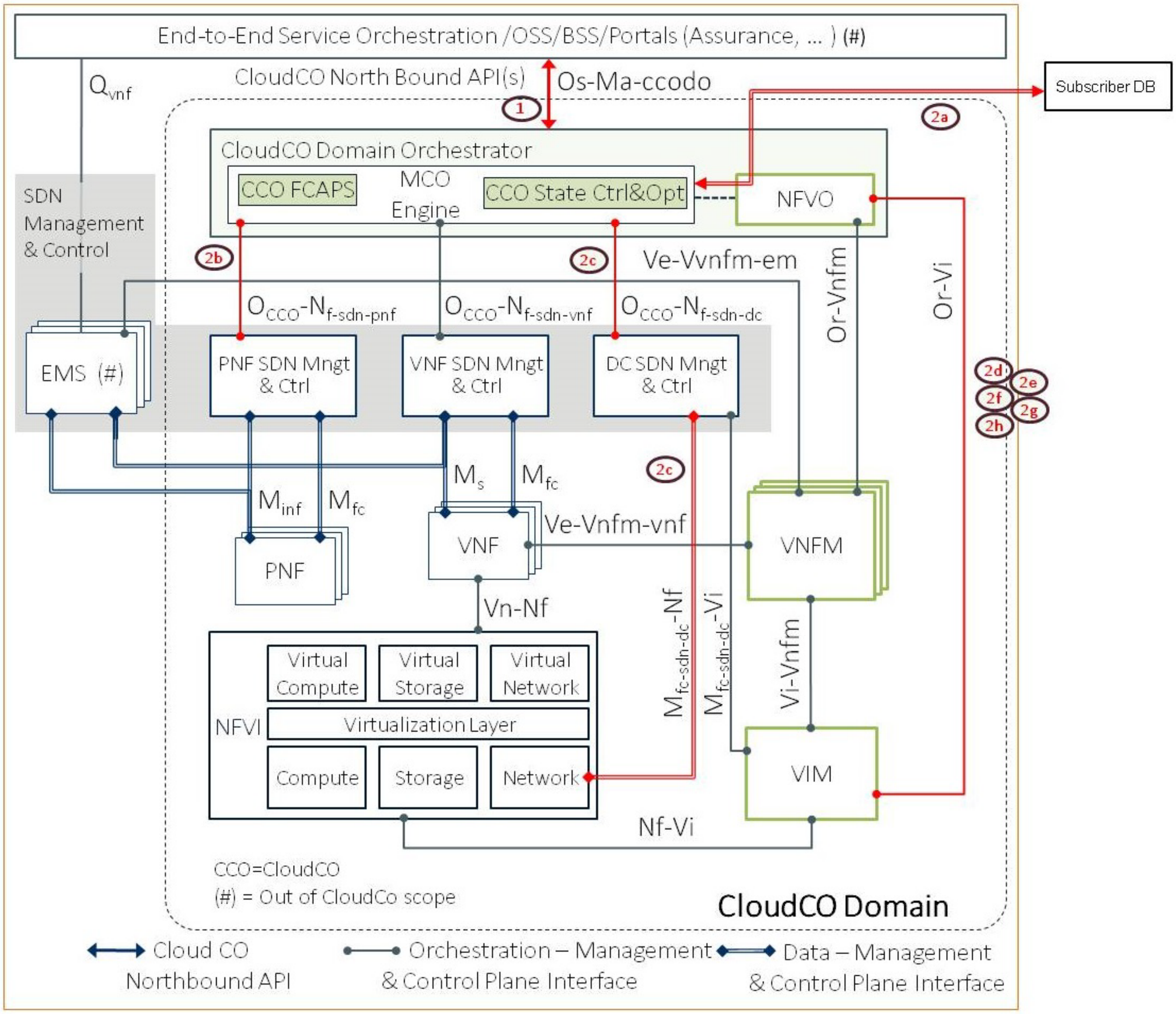


Figure 20: Onboarding a new NERG instance onto CloudCO Domain (when Static Model is applied)

1. The retail ISP uses the CloudCO NB API to associate the service user with the Internet Access Service Instance. The CloudCO Operator has to make sure that the retail ISP only has access to its Service Instances and its service users. The CloudCO Operator creates a list of Service Instances and a list of service users, and these lists are read-only when consumed by the retail ISP. The retail ISP therefore, cannot create new service users in this use case. Note that this issue can be addressed via a contract and policy solution.
   Among other things, this list will need to map subscriber name/street address to identifier (because that’s how subscribers will identify themselves to the retail ISP), and may well require information about which retail ISP currently owns the subscription. It is certainly needed to prevent retail ISP1 from slamming subscribers away from retail ISP2 or from the incumbent. This can be solved by careful configuration on the side of the CloudCO Operator, but errors can be made obviously.

2. Step 1 triggers the CloudCO Orchestrator to:
    a. Query the Subscriber database to figure out on which access-line the service user is attached to.
    b. Request the Physical Network Function (PNF) SDN Controller to allocate an unused VLAN-identifier (VLAN-id) on the AN uplink for that connection and report back with the VLAN-id. It is also possible to pre-provision the VLANs on the ANs uplink and furthermore pre-populate the subscriber database with information about AN-identifier (AN-id) and VLAN-id, making the use of the PNF SDN Controller optional for this use case.
    c. Request the Data Center (DC) SDN Controller to configure the Top of Rack (ToR) switch connected to the access node with the same VLAN-id. Note that this VLAN-id is only significant for that specific ToR. Again this VLAN could be pre-provisioned, making the use of the DC SDN Controller optional.
    d. Request the NFVO to, in turn request NFVI VIM to set up a new virtual network inside the NFVI (Note these virtual networks span the complete CloudCO Domain)
    e. Request the NFVO to, in turn, request NFVI VIM to set up a L2 bridge between the aforementioned VLAN-id and the virtual network on one of the compute hosts attached to the ToR that attaches to the AN.
    Note that this bridging can happen:
        - Either at the Compute Hosts,
        - or alternatively on the ToR‘s ability to become a Virtual Tunnel End Point (VTEP) of a given Virtual Network (Hardware VTEP).
    f. Request the NFVO to, in turn request the VNFM to instantiate a new vG instance, and connect the LAN facing interface to the aforementioned virtual network. The vG can be instantiated anywhere as the virtual network is spanning the complete CloudCO Domain. The NERG VNFM can perform lifecycle management for the vG instance, while the CloudCO Orchestrator handles abstract access for the retail ISP to the NERG VNFM through the CloudCO NB API. This allows the retail ISP to create e.g., LAN private address pools, set up the home DHCP Server, set up NAT rules, all through the CloudCO NB API. Note that it is assumed for this use case that the vG has all these functions implemented as part of the instance. This does not need to be the case for all deployments.
    g. Request the NFVO to, in turn request NFVI VIM to set up another new virtual network inside the NFVI and connect this virtual network to the WAN facing interface of the vG. Note that these virtual networks span the complete CloudCO Domain.
    h. Request the NFVI VIM to connect this *virtual network* also to the Distributed Router. The vG will need to autonomously request an IP address on its WAN interface and the Distributed Router helps this by relaying the request. This action will then create end-to-end connectivity between terminals in the home premises and upstream networks (e.g., Internet).

The Service Graph applied for this use case is depicted in Figure 21.

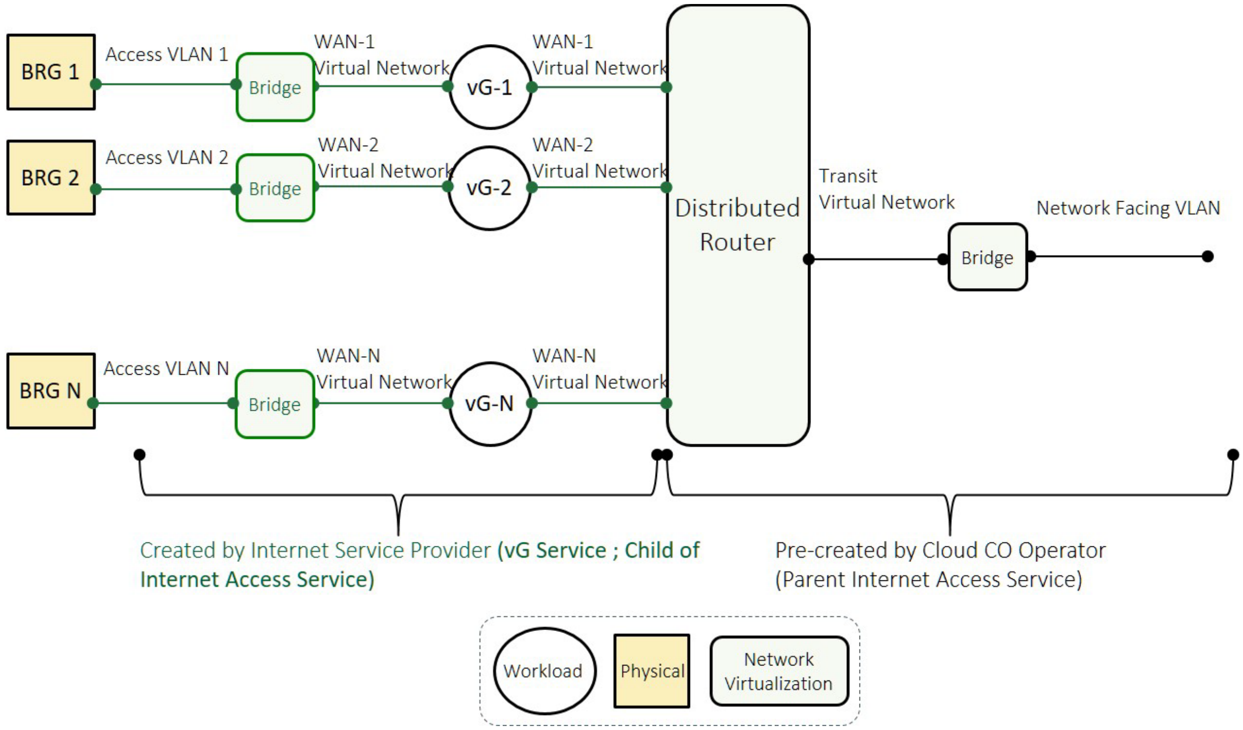


Figure 21: Service Graph applied for this Use Case (when Static Model is applied)

Figure 21 depicts whether the pre-created functions are achieved through (1) network virtualization, (2) a VM or Container, or (3) the function is physical. It can be observed that the Internet Access Service is a parent service for various vG Services.

6.1.2 NERG with Flat Logical Subscriber Link (LSL); Dynamic Model Use Case based on Scenario 7

It can be observed that a CloudCO can establish the dynamic set-up of the Flat LSL Use Case quite easily by extending the NERG use case described in section 6.1.1.

This set of functionality is capturing First-Sign-Of-Life (FSOL) user plane on all interfaces of the AN, while initially dropping everything else for that subscriber. These FSOL packets need to be redirected to a pre-instantiated SDN access control application for a variety of sub use cases such as:

- Authorization and authentication, either of the subscriber-line and the BRG attached to the subscriber line, or both. This means the BRG can now be managed by the retail ISP as the authentication process can link the BRG to the correct Internet Access Service Instance.
- Dynamically setting up the LSL connectivity across the CloudCO Domain, without any need for the retail ISP to use the CloudCO NB API to achieve this. Please refer to figure 11 of TR-317 [19] for the TR-317 call flow across a TR-101 [6] architecture.

Note that this use case does not elaborate on eventual service chaining of additional network functions like firewalling/NAT/parental control into the Service Graph. In this way it is not meant to be a complete description of all aspects described in TR-317 [19]. It is also not meant to be the

© The Broadband Forum. All rights reserved

only possible implementation of the NERG scenario on the CloudCO Architecture. Moreover, the choice of using one vG instance per subscriber is not meant to describe the only way of achieving NERG like functionality. The use case also does not describe how the CloudCO supporting infrastructure, e.g., MANO stack, SDN Controllers, are set up.

Involved actors

- CloudCO Operator, acting as a wholesale Service Provider.
- Retail ISP, offering the Internet Access Service on the CloudCO Domain
- Service user, i.e., subscriber of the Retail ISP.
  Note that this use case does not cater for the possibility that a subscriber could do business with more than one provider, but could easily be extended to allow such behavior.

Pre-requisites

- A fully initialized CloudCO domain.
- BRG is deployed at the service user home premise and connected to the access line.
- L2 Ethernet packets can flow between the BRG and the CloudCO AN U-Interface. This means also that the BRG node has been installed and provisioned accordingly. How this is done is for further study or described in another use case, but this could entail having the BRG equipped with the appropriate certificates to allow itself to authenticate.
  However, all user plane connectivity across the access node (from access to Network uplink) is initially blocked/filtered.
- An Internet Access Service Instance is pre-created inside the CloudCO Domain by the CloudCO Service Provider, acting as a wholesale provider. This essentially creates a routed and public address space across the CloudCO Domain and associates it with a retail ISP. The retail ISP can use the CloudCO Northbound API to access the instance to e.g., create and associate new service users with the instance. An instance of NERG VNFM is created for this Internet Access Service Instance, allowing lifecycle management of all vGs attached to this Internet Access Service.
- The PNF SDN Controller runs an instance of an authentication SDN Application, and are configured to interface with a subscriber database instance, which has a logical 1:1 mapping with a given Internet Access Service. The CloudCO NB API allows access to the database entries relevant for the retail ISP, without exposing e.g., the control plane interactions needed between the SDN authentication application and the subscriber database instance.
- The necessary steps to be performed inside the CloudCO are:
  a) A Distributed Router is created across the NFVI through the VIM, associated with a pool of public IP addresses. The Distributed Router uplink is attached to a pre-created virtual network (created through the VIM), and the virtual network is bridged to a pre-created VLAN configured (by using the PNF SDN Controller) on one of the network facing interfaces of the CloudCO Domain.
  Note that the Distributed Router can be seen as the disaggregated L3 forwarding component of the legacy BNG component
  b) An instance of NERG VNFM is instantiated through the VIM, and its functions are made accessible through the CloudCO Northbound API, to allow consumption by the retail ISP. Each retail ISP may have its own flavor of VNFM. Each retail ISP will have its own NBI, protected by its own security and policy safeguards.

c) An instance of an authentication application is instantiated logically on the PNF SDN Controller. This leads to the SDN Controller to program the ANs to punt relevant packets (e.g., DHCP and/or IEEE 802.1x) to the authentication application. The CloudCO NB API allows the retail ISP to set the authentication level (allow/deny; default deny) for its users, which is stored into its own instance of subscriber database.

Onboarding a new NERG instance onto the CloudCO Domain will happen as follows, as shown in Figure 22.

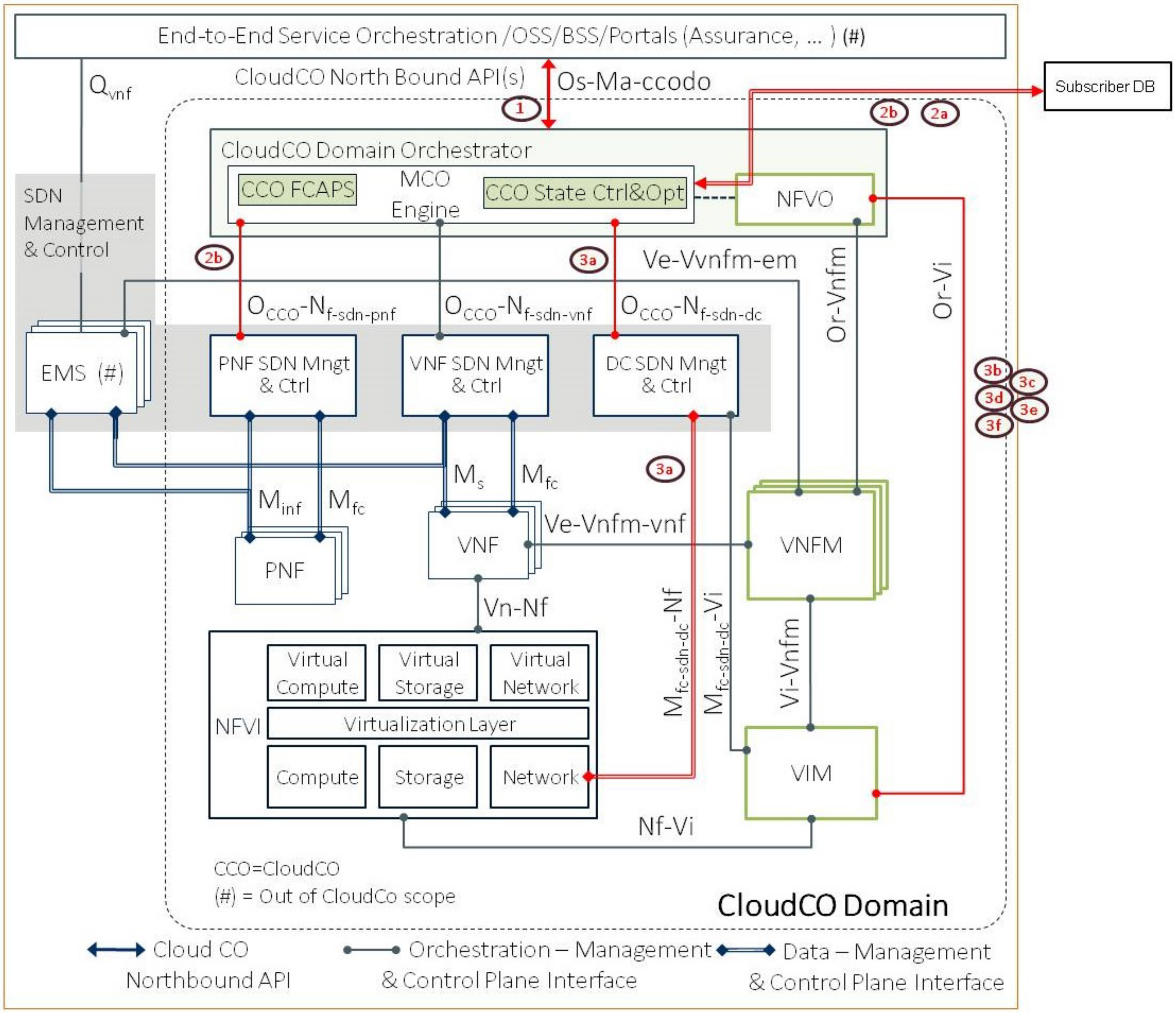


Figure 22: Onboarding a new NERG instance onto the CloudCO Domain (when Dynamic Model is applied)

1. The ISP uses the CloudCO Northbound API to associate the service user with the Internet Access Service Instance, and with the correct authentication level (deny/allow). The default authentication level can be pre-set to deny/allow. Start here

2.
   a) The CloudCO Orchestrator configures the Subscriber database instance with the right authentication level of the service user.
   b) The PNF SDN Controller starts to receive forwarded IEEE 802.1x packets from the ANs. These packets contain the VLAN-id allocated to the access port, as well as the IEEE 802.1x credentials. The access node could choose any unused VLAN-id for any new IEEE 802.1x receive event on an access port. Alternatively the SDN Controller can set the associated VLAN-ids. When IEEE 802.1x packets are received, the credentials are authenticated with the correct subscribe database instance and the port is blocked/unblocked, causing user plane packets to flow/not flow across the access node. As soon as an access port is successfully authenticated and opened, DHCP packets sent by the BRG will be forwarded to the same authentication SDN application. The DHCP Packets will be used to trigger the CloudCO Orchestrator to setup the LSL between the BRG and the vG. It can be noted that the DHCP exchange can also be used to create an IP/MAC binding table inside the SDN application. This IP/MAC binding table can be leveraged to e.g., prevent IP/MAC spoofing.
   Note that an alternative approach is to only use forwarding of DHCP packets originated from the BRG, although this approach has the disadvantage that the CloudCO Operator has to know which access ports are assigned to which retail ISP.

3. The CloudCO Orchestrator executes the following workflow that accomplishes:
   a. Requests the DC SDN Controller to configure the ToR switch connected to the access node with the same VLAN-id. Note that this VLAN-id is only significant for that specific ToR. Note that this bridging can happen at the Compute Hosts, or alternatively on the ToR. Note that in the latter case, the VIM controls the ToR – or the DC SDN Controller, which in turn controls the ToR - which is an option currently not shown in the reference architecture.
   b. Requests the NFVO to, in turn request NFVI VIM to set up a new virtual network inside the NFVI (Note these virtual networks span the complete CloudCO domain Note that this bridging can happen either at (1) the Compute Hosts or (2) alternatively on the ToR. Note that in the latter case, the VIM controls the ToR's ability to become a Virtual Tunnel End Point (VTEP) of a given Virtual Network (Hardware VTEP).
   c. Requests the NFVO to, in turn request NFVI VIM to set up a L2 bridge between the aforementioned VLAN-id and the virtual network on one of the compute hosts attached to the ToR that attaches to the AN.
   d. Requests the NFVO to, in turn request the VNFM to instantiate a new vG instance, and connect the LAN facing interface to the aforementioned virtual network. The vG can be instantiated anywhere as the virtual network is spanning the complete CloudCO Domain. The NERG VNFM can perform lifecycle management for the vG instance, while the CloudCO Orchestrator handles abstract access for the retail ISP to the NERG VNFM through the CloudCO NB API. This allows the retail ISP to create LAN private address pools, set up the home DHCP Server, set up NAT rules, etc, all through the CloudCO NB API. Note that it is assumed for this use case that the vG has all these functions implemented as part of the instance. This does not need to be the case for all deployments.

e. Requests the NFVO, to in turn request NFVI VIM to set up another new virtual network inside the NFVI (Note these virtual networks span the complete CloudCO Domain) and connect this virtual network to the WAN facing interface of the vG.
f. Requests the NFVO, to in turn request NFVI VIM to connect this virtual network also to the Distributed Router. The vG will need to autonomously request an IP address on its WAN interface and the Distributed Router helps this by relaying the request. This then creates end-to-end connectivity between terminals in the home premise and upstream networks (e.g., Internet).

The Service Graph applied for this use case can be seen in Figure 23.

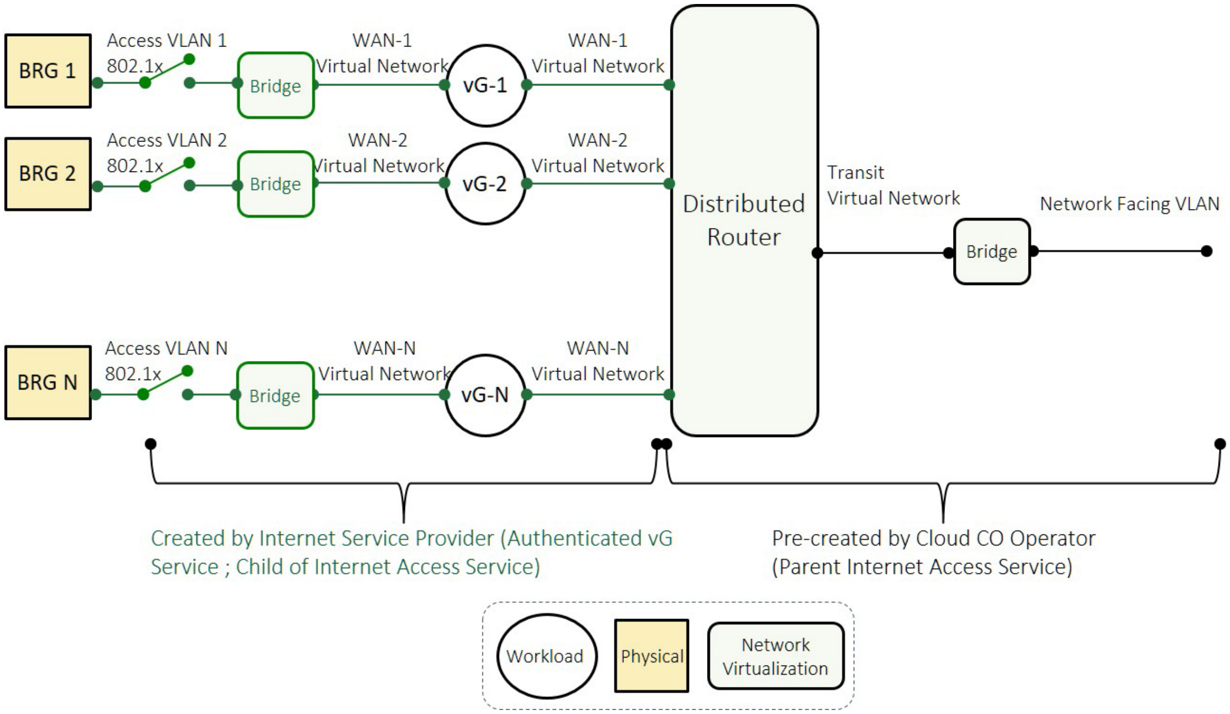


Figure 23: Service Graph applied for this Use Case (when Dynamic Model is applied)

6.1.3 Residential Broadband Access using PPPoE

Section 5.2 describes the Scenario 1 where a subscriber is getting internet access through PPPoE encapsulation terminating at a BNG. In particular, this use case describes a way to support these kind of existing Central Office services that are hard to disaggregate and partially virtualize because e.g., control plane and user plane are combined.

The use case described in this section proposes to fully virtualize a BNG i.e., a BNG running inside a VM or Container that has both control plane and user plane virtualized. Although this approach has scaling limitations, it is useful to allow this deployment next to NERG-like deployments because of its ease of use and its support for services which may be hard to virtualize. The use case further proposes connecting a subset of subscribers to a vBNG leveraging network overlays and bridging between access VLANs and these network overlays.

Involved actors

- CloudCO Operator, acting as an ISP.
- Service user (i.e., subscriber of the Retail ISP).
  Note that this use case does not cater for wholesale scenarios.

Pre-requisites

- A fully initialized CloudCO domain.
- A legacy RG is deployed at the service user home premise and connected to the access line
- L2 Ethernet packets can flow between the RG and the CloudCO AN U-Interface. This means also that the RG node has been installed and provisioned accordingly. How this is done is for further study or described in another use case.

The workflow, as depicted in Figure **24** is described below:

1. A PPPoE_Internet Access Service Instance is instantiated inside the CloudCO Domain by the CloudCO Operator through the CloudCO NB API. This instantiates a vBNG which is managed through the standard R and M interfaces of a legacy BNG. Note that this use case does not need a VNFM as the existing Central Office management interfaces are used. Therefore automated scaling of vBNG related resources are not dealt with in this use case.
2. The CloudCO Operator knows where subscribers are attached and instantiates[1] in this example a 1:1 S-VLAN and C-VLAN pair per subscriber on the AN via the PNF SDN Controller, or alternatively a N:1 S-VLAN for all subscribers needing this service on the access node. Note that no user plane SDN signaling is required for this use case to work.
3. The CloudCO Operator instantiates a network overlay via the VIM.
4. One of the following is done:
    a. The CloudCO Operator instantiates an S-VLAN on the appropriate TOR switch via the DC SDN Controller, instantiates a bridge function via the VIM and instantiates bridging between the S-VLAN to the network overlay, or
    b. The CloudCO Operator instantiates an S-VLAN on the appropriate TOR switch and extends the overlay to the ToR switch S-VLAN.

[1] The term instantiates refers to the principle of using an API on an upstream controller/VIM to establish the desired state, rather than using manual configuration. This instantiation can be performed by leveraging API calls, or by scripts or workflows that leverage these API calls that reside at the CloudCO Orchestrator.

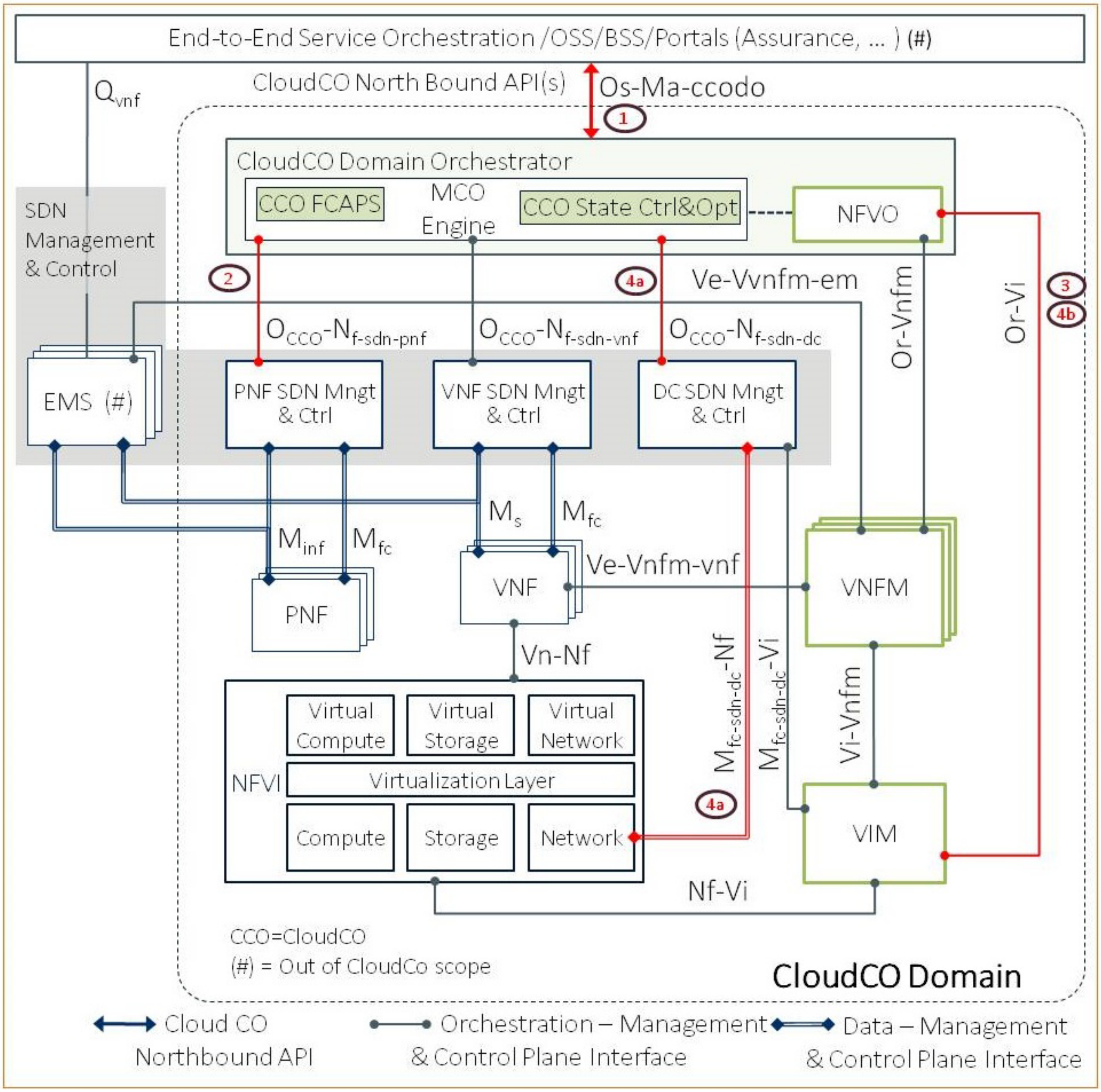


Figure 24: Residential Broadband Access using PPPoE Use Case

This result in the following (static) service graph, see Figure 25.

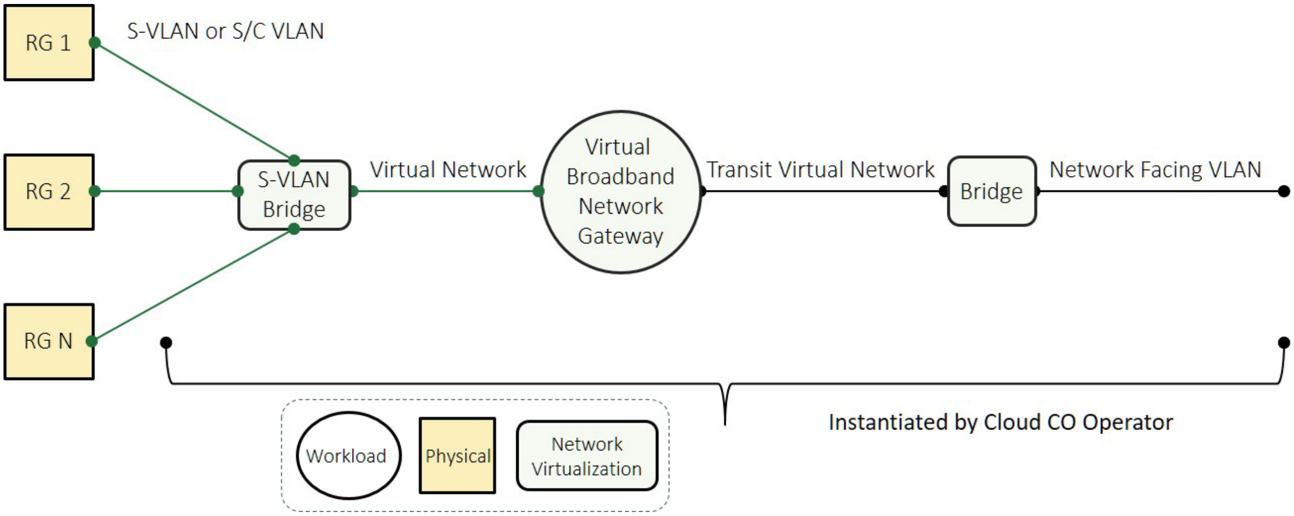


Figure 25: Service Graph applied for this Use Case, when applying S/C VLAN combination

From this point on subscribers can initiate PPPoE sessions towards the vBNG.

6.1.4 Residential Broadband Access Monitoring, Diagnostics, and Optimization

Story highlights

Fault and performance management are fundamental network management areas. Wireline residential broadband access over e.g., DSL, G.fast, Passive Optical Network (PON), Data Over Cable Service Interface Specification (DOCSIS), has many possible points of failure which should be monitored proactively. Diagnostic data are also important for reactive troubleshooting. Optimization of line configuration parameters is particularly important for DSL and G.fast [14]. CloudCO can improve monitoring, diagnostics and optimization by providing more compute and storage than network elements alone, with more rapid reaction than existing Central Office management architectures. This use case also shows that a unified CloudCO platform is amenable to supporting multiple inputs and interactions between multiple functions.

Involved actors

- CloudCO Operator, acting as a wholesale Service Provider.
- Infrastructure Provider (aka Network Operator). May be the same entity as the CloudCO Operator.
- VNO (aka Retail ISP), offering the Internet Access Service using the CloudCO Domain.
- Service user (i.e., subscriber of the Retail ISP).

High-level architecture and interfaces

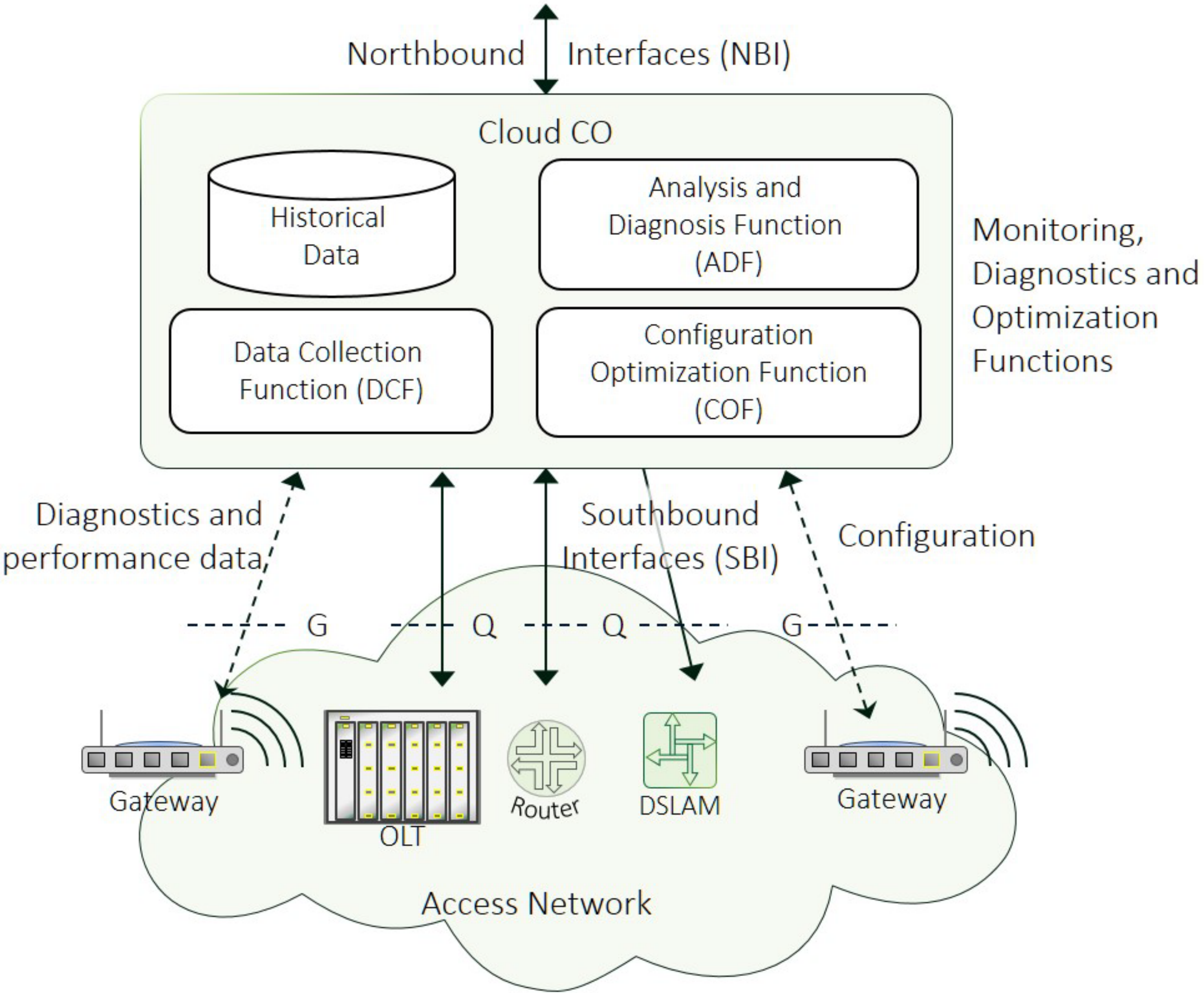

Northbound
Interfaces (NBI)
Cloud CO
Historical Data
Analysis and Diagnosis Function (ADF)
Monitoring, Diagnostics and Optimization Functions
Data Collection Function (DCF)
Configuration Optimization Function (COF)
Diagnostics and performance data
Southbound Interfaces (SBI)
Configuration
G
Q
Q
G
Gateway
OLT
Router
DSLAM
Gateway
Access Network

Figure 26: Broadband monitoring, diagnostics and optimization systems

Figure 26 is a generalization of the DSL Quality Management systems functional architecture [15]; Figure 26 adds a Southbound G-interface and puts profiling in the Configuration Optimized Function (COF). The G-interface generally uses the CPE WAN Management Protocol or User-Services Platform (USP) to connect to RGs. The Southbound Q-interface connects to access nodes using legacy protocols or NETCONF/YANG [23]. In current practice, Operators use the Q-interface to manage access nodes and broadband lines, while separately using the G-interface to manage CPE monitoring. This use case considers combining inputs of both the Q-interface and the G-interface. Broadband monitoring, diagnostics and optimization can also extend into the home LAN, e.g., for in-home Wi-Fi; then the G-interface is vital.

Agents in the CPE can communicate to controllers in the CloudCO communicating with the USP across the G-interface. For example, Wi-Fi diagnostics and optimization can be disaggregated. With real-time data collection and optimization performed by an agent in the CPE, and long-term data storage and deeper analyses performed by the controller in the CloudCO.

Monitoring, status, performance, test, and diagnostics data are gathered by the Data Collection Function (DCF) primarily from access nodes across the Q-interface, and possibly also from aggregation nodes and from residential gateways across the G-interface. Control and configuration change requests are passed to access nodes across the Q-interface, and possibly also to residential gateways across the G-interface. A DCF may be called a virtual probe (vProbe), e.g., a probe instantiated in the CloudCO software.

The Analysis and Diagnosis Function (ADF) distills and interprets monitoring and performance data to identify faults, performance problems, and root causes. The ADF can send monitoring alarms up the NBI.

The COF determines good configurations and re-configures nodes and lines to improve access network performance; this is often called "re-profiling" [14].

The historical database stores monitoring and performance data, network information, profiles, ticketing data, etc.

The NBI enables diagnostics and performance data to be sent to external orchestration/Operations Support System (OSS)/Business Support System (BSS). The NBI may input configuration optimization criteria to be used by algorithms in the COF, such as: data rate, delay, stability, error rates, or power usage.

Pre-requisites

1. A fully initialized CloudCO domain.
2. There are users with broadband connections.
3. There is a CloudCO Domain, with MANO (VIM/VNFM/CloudCO Orchestrator) systems instantiated and running.
4. There is a CloudCO NB API.
5. VNFs for the DCF, ADF, and the COF are on-board (templates are in the catalog).
6. Addressing and credentials are available for connecting Southbound across the Q-interface, and optionally also across the G-interface.

In this use case, service graphs do not forward user data packets, but they instead forward network state and configuration data. There are three uses here: Monitoring, Diagnostics, and Optimization.

6.1.4.1 Monitoring

Network monitoring involves passive data collection from equipment, and alarming to notify other systems and personnel of faults when appropriate, see Figure 27 and Figure 28.

© The Broadband Forum. All rights reserved

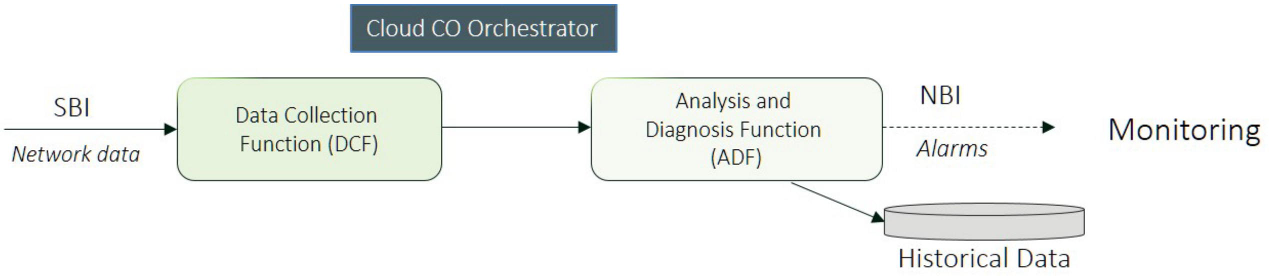


Figure 27: Monitoring network service built from DCF and ADF VNFs

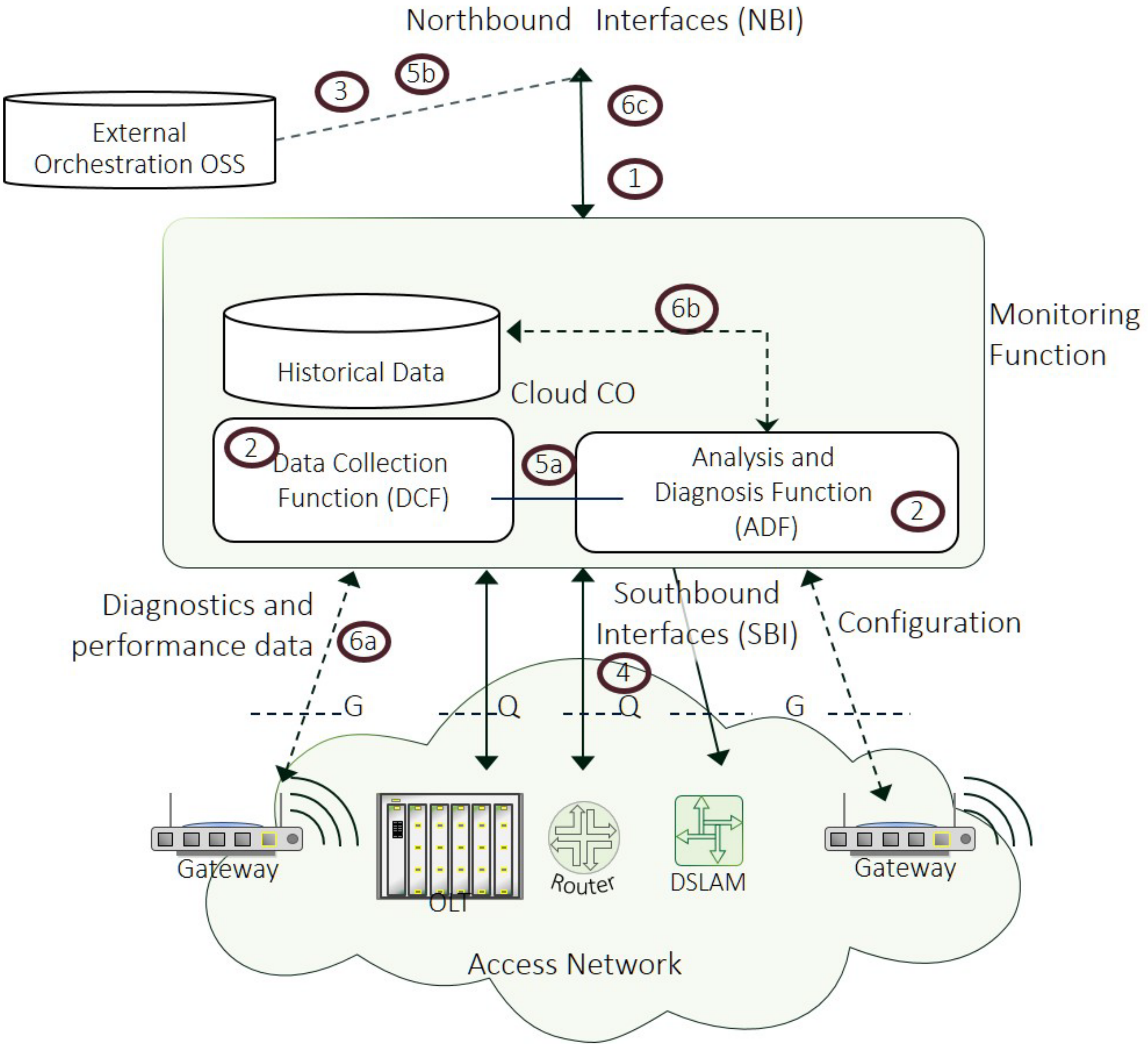

Northbound Interfaces (NBI)
3
5b
6c
1
External Orchestration OSS
6b
Historical Data
Cloud CO
Monitoring Function
2
Data Collection Function (DCF)
5a
Analysis and Diagnosis Function (ADF)
2
Diagnostics and performance data
6a
Southbound Interfaces (SBI)
4
Configuration
G
Q
Q
G
Gateway
OLT
Router
DSLAM
Gateway
Access Network

Figure 28: Broadband Monitoring system

1. A request for monitoring broadband node(s)/line(s) comes into the CloudCO across the NBI.
2. CloudCO Orchestrator and VNFM instantiate DCF VNF and ADF VNF.
    a. VIM assigns NFVI resources.
    b. Each VNF may monitor multiple nodes.
3. DCF queries external orchestration/ OSS database for equipment addresses.

© The Broadband Forum. All rights reserved

4. DCF establishes Southbound interface(s) (SBI) between the CloudCO and the equipment, including legacy and or CloudCO NETCONF/YANG interfaces. SBIs may include Q-interfaces to access node(s), G-interface to RG(s), and management interfaces to aggregation nodes. An SBI may connect through an intermediate system (e.g., an EMS or Persistent Management Agent (PMA)).
5. CloudCO Orchestrator instantiates the Monitoring network service instance by chaining DCF and ADF:
    a. VIM creates a virtual link from DCF to ADF.
    b. Alarm thresholds, data storage types and frequencies, etc., are determined according to defaults in the ADF and instructions from external orchestration/OSS passed through the NBI and CloudCO Orchestrator.
6. CloudCO Orchestrator oversees the running Monitoring service:
    a. DCF collects equipment status and performance data, passes this data to the ADF across the virtual link.
    b. The ADF populates the historical database with distilled monitoring data.
    c. The ADF issues alarms toward the NBI when appropriate.
7. Monitoring service is terminated at the end of broadband service or upon a request to stop monitoring.

Figure 29 depicts the logical flow of the Monitoring function.

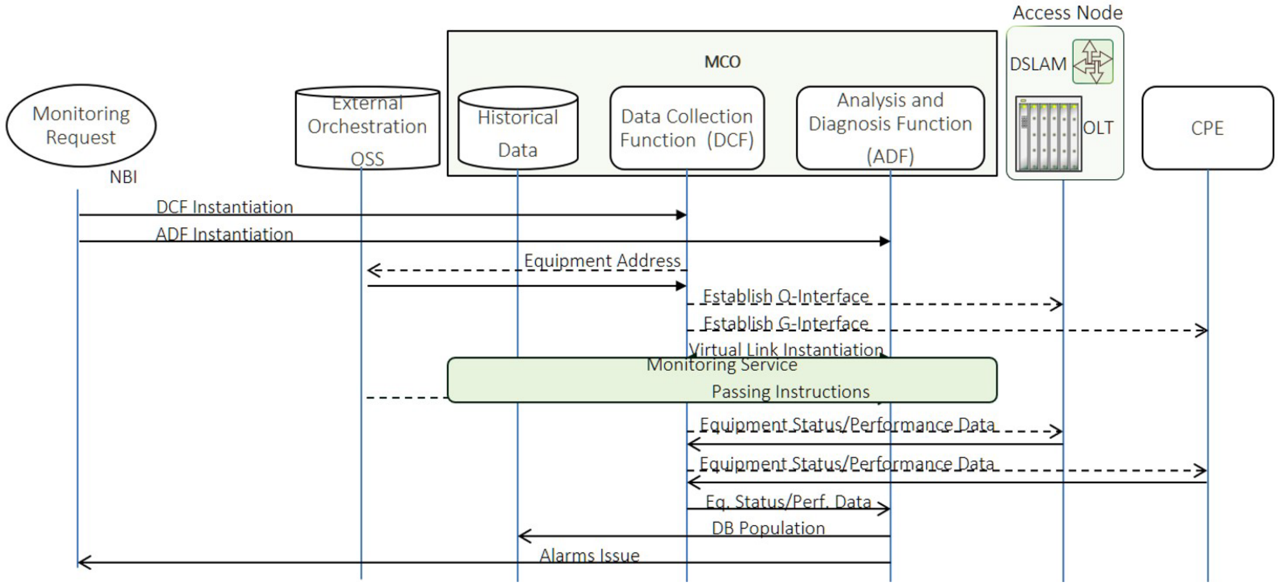


Figure 29: Monitoring Logical Process Flow

6.1.4.2 Diagnostics

Using the monitoring process described in section 6.1.4.1, diagnostics, or tests, are invoked in response to requests (“trouble tickets”) to identify the root cause of faults, see Figure 30 and Figure 31.

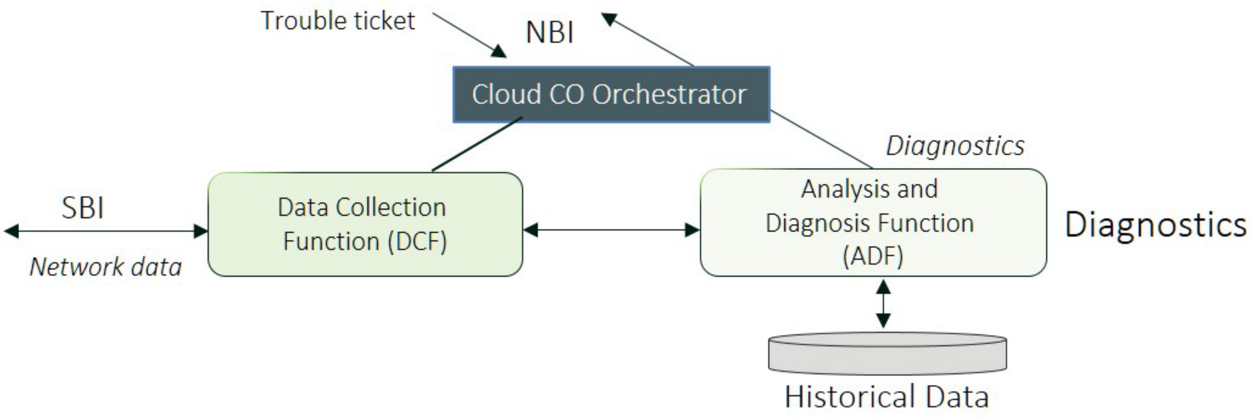


Figure 30: Diagnostics network service built from DCF and ADF VNFs.

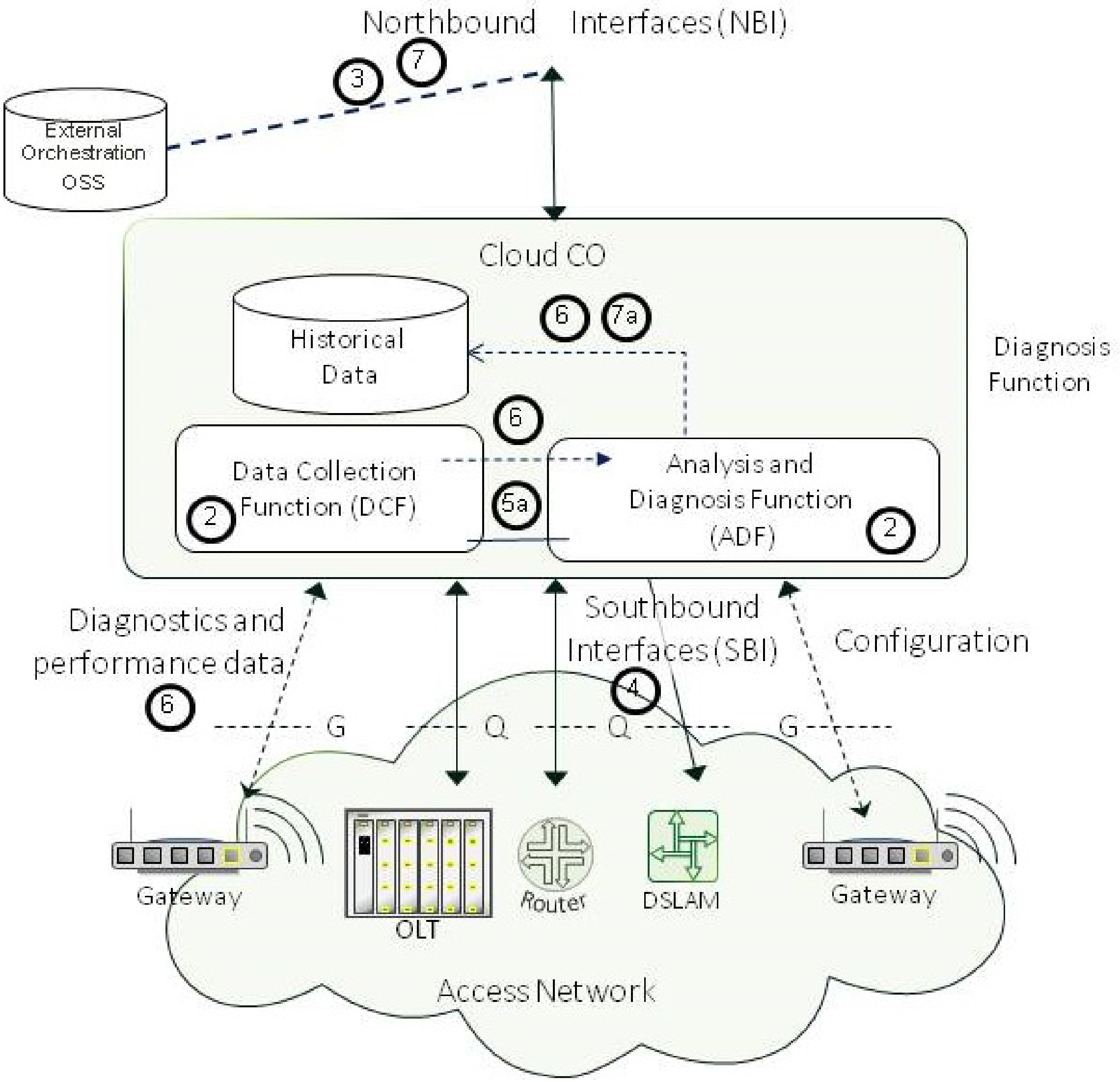

Northbound Interfaces (NBI)
3
7
External Orchestration OSS
Cloud CO
Historical Data
6
7a
Diagnosis Function
6
Data Collection Function (DCF)
2
5a
Analysis and Diagnosis Function (ADF)
2
Diagnostics and performance data
6
Southbound Interfaces (SBI)
4
Configuration
G
Q
Q
G
Gateway
OLT
Router
DSLAM
Gateway
Access Network

Figure 31: Broadband Diagnostic system

1. A request for diagnosing a broadband line or node(s) (aka a "trouble ticket") comes into the CloudCO across the NBI.

2-4 Steps 2-4 as in section 6.1.4.1 on Monitoring.

5. CloudCO Orchestrator instantiates the Diagnostics network service instance by chaining DCF and ADF:
   a. VIM creates a virtual link from DCF to ADF.
6. The ADF queries equipment through virtual link to the DCF then across the SBI, the ADF queries the database, and runs tests depending on the trouble ticket and node types.
7. Diagnostics results are sent upstream from the ADF across the NBI to external orchestration/OSS:
   a. Results are also stored in the historical database.
8. The Diagnostics service is terminated.

Figure 32 depicts the logical flow of the Diagnostic function.

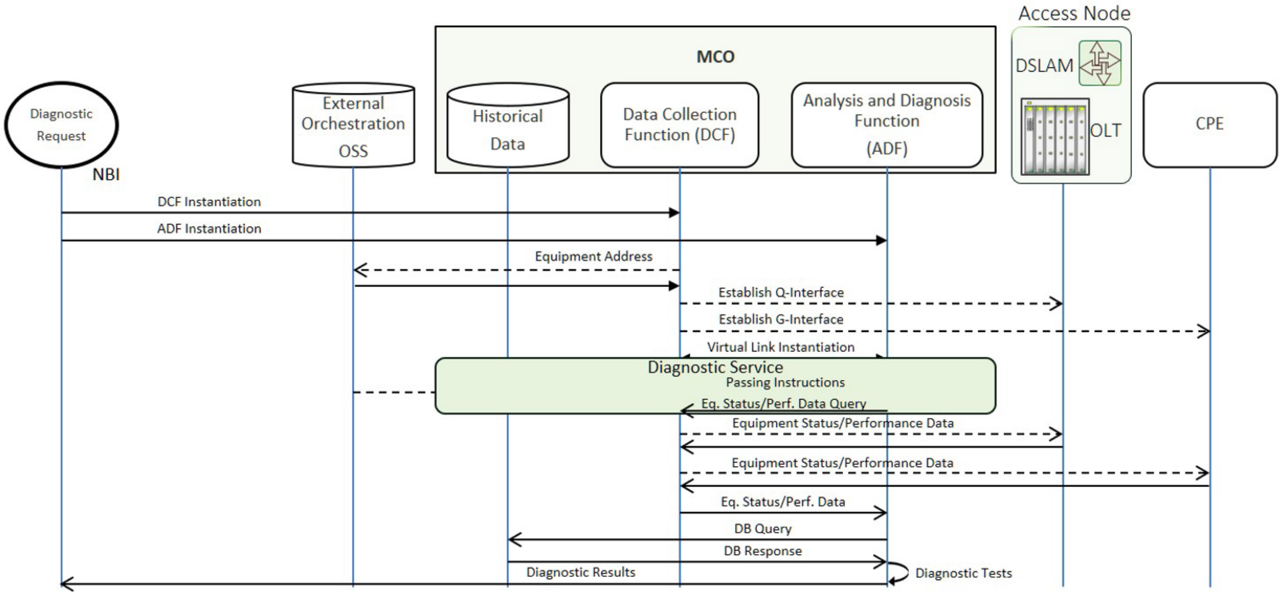


Figure 32: Diagnostic Logical Process Flow

6.1.4.3 Optimization

Network optimization can either run continuously in the background, or be a one-time operation invoked by request, see Figure 33 and Figure 34.

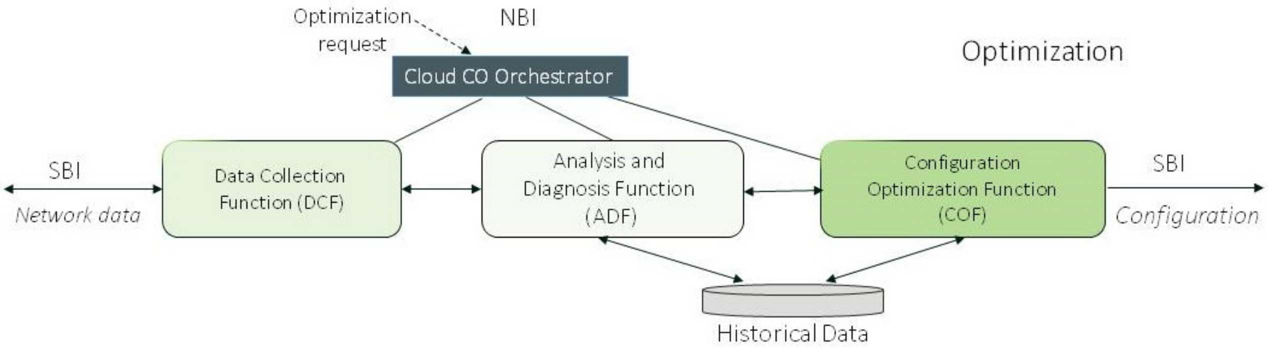

Optimization request
NBI
Cloud CO Orchestrator
Optimization
SBI
Network data
Data Collection Function (DCF)
Analysis and Diagnosis Function (ADF)
Configuration Optimization Function (COF)
SBI
Configuration
Historical Data

Figure 33: Optimization network service built from DCF, ADF, and COF VNFs.

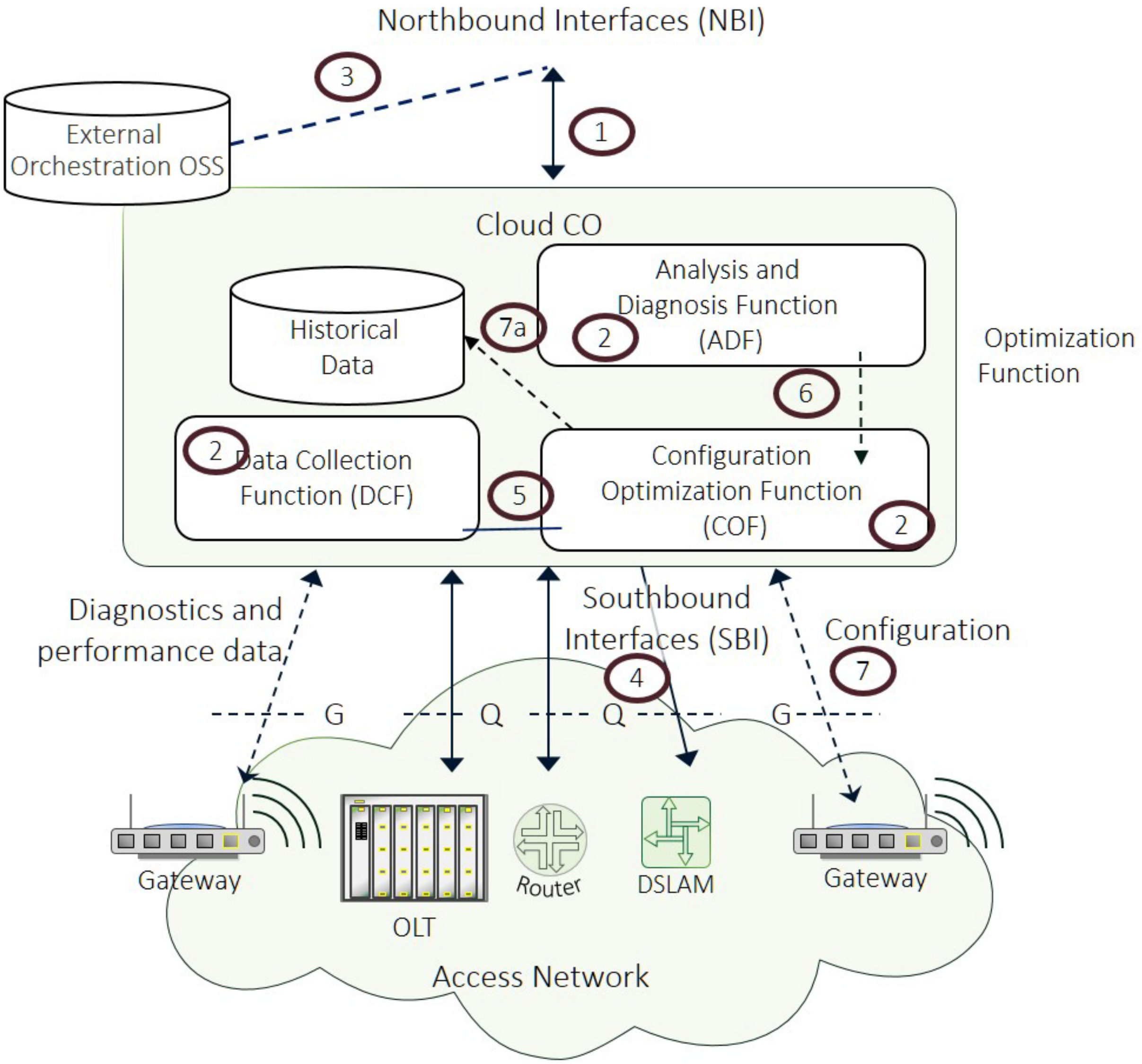

Northbound Interfaces (NBI)
3
1
External Orchestration OSS
Cloud CO
Historical Data
7a
Analysis and Diagnosis Function (ADF)
2
Optimization Function
6
2
Data Collection Function (DCF)
5
Configuration Optimization Function (COF)
2
Diagnostics and performance data
Southbound Interfaces (SBI)
Configuration
4
7
G
Q
Q
G
Gateway
OLT
Router
DSLAM
Gateway
Access Network

Figure 34: Broadband Optimization system

The following steps are used by the Optimization procedure:

1. A request for optimizing broadband node(s)/line(s) comes into the CloudCO across the NBI:
    a. Can either be a one-time request for a particular line or node, or a request for longer-term optimization of multiple node(s)/line(s).
2. CloudCO Orchestrator and VNFM instantiate DCF VNF, ADF VNF and COF VNFs:
    a. VIM assigns NFVI resources.
    b. Each VNF may monitor multiple nodes.

3-4 Steps 3-4 as in section 6.1.4.1 on Monitoring.

5. CloudCO Orchestrator instantiates the Optimization network service instance by chaining DCF, ADF, and COF:
    a. VIM creates virtual links from DCF to ADF and from ADF to COF.
6. COF imports network data from the ADF across the virtual link.
7. COF determines optimization configuration, writes new configuration to nodes across the SBI.
    a. The optimization configuration is stored in the historical database.
8. If this is a one-time request the Optimization service is terminated.
9. Otherwise, the CloudCO Orchestrator oversees the running Optimization service until the end of broadband service or when a request to stop monitoring is received over the NBI, upon which the Optimization service is terminated.

Figure 35 depicts the logical flow of the Optimization function.

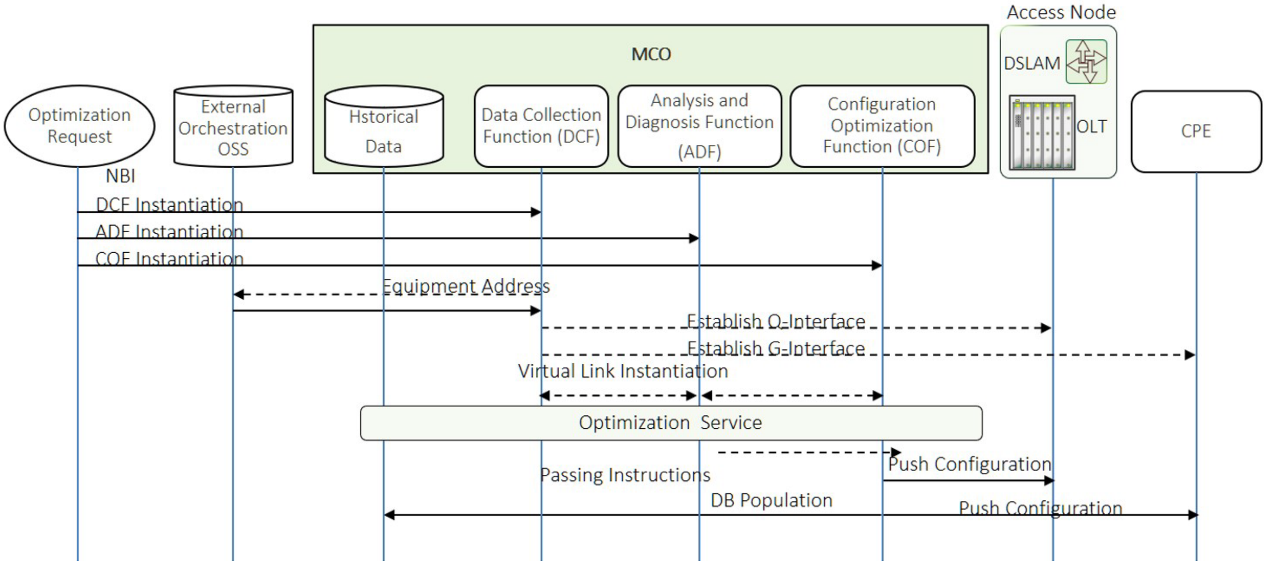


Figure 35: Optimization Logical Process Flow

CloudCO benefits

Incorporating broadband access monitoring, diagnostics, and optimization into CloudCO is expected to lead to benefits such as rapid reaction, agility, component re-use and flexible allocation of compute, memory and interfaces. Monitoring, diagnostics and optimization often benefit from rapid reaction which can be faster using a CloudCO instead of using traditional centralized management systems. "Virtual probe" software can be readily updated with resources scaled on demand.

Monitoring, diagnostics and performance data are useful inputs to many other potential CloudCO functions such as new services creation, resource allocation, network load-balancing, etc. The DCF is thus a useful function that can be re-used across the CloudCO. The historical database is likewise re-usable as a repository for network monitoring, diagnostics and configuration data.

6.1.5 Fixed Access Network Sharing (FANS)

Section 5.13 describes Scenario 12 that suggests the use of FANS architecture [26], in order to overcome the constraints of typical TR-101/TR-178-based broadband network when multiple Operators are involved in a shared environment.
Being based on ETSI NFV MANO, the CloudCO Domain can host the FANS architecture and reuse existing ETSI interfaces, as shown in Figure 36 and enumerated in TR-384 [5].

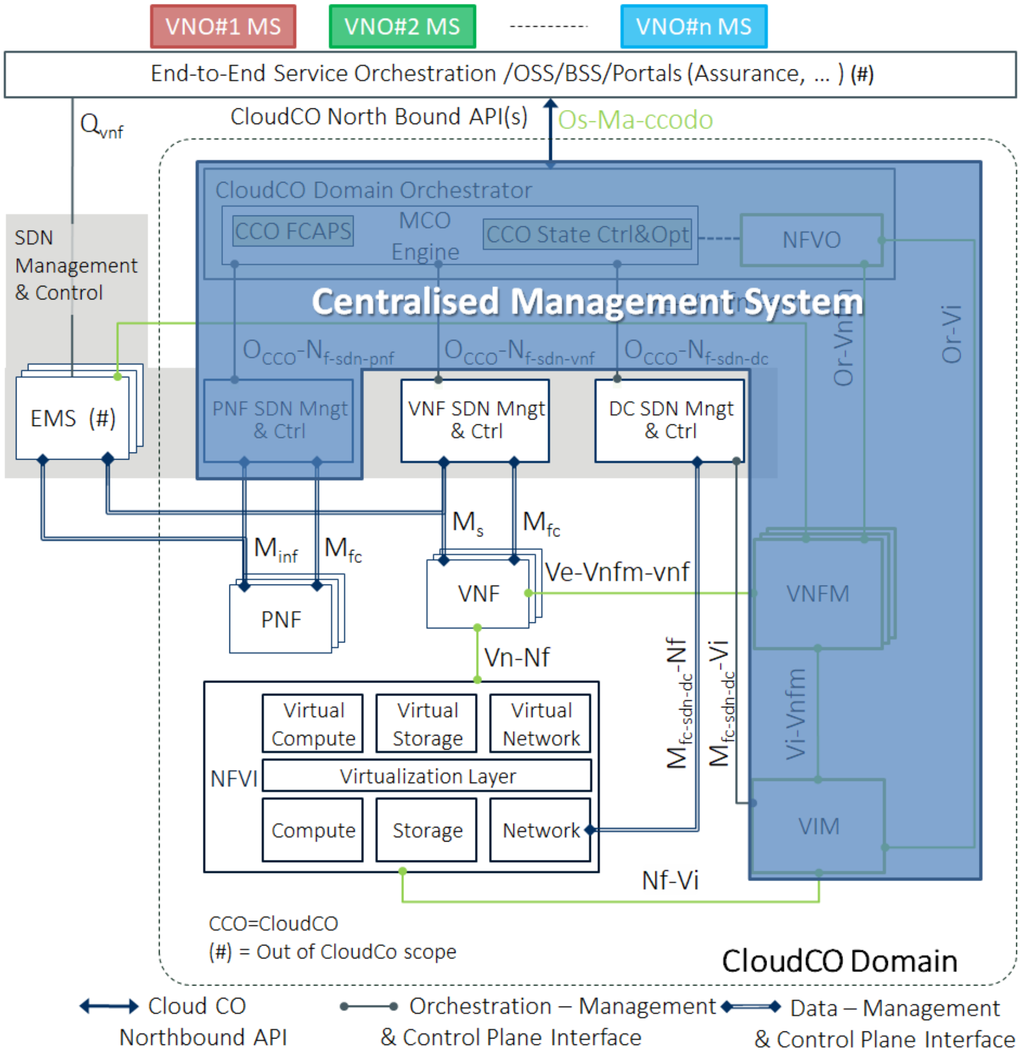


Figure 36 FANS in CloudCO Architectural Framework

As shown in Figure 36, the FANS Centralised Management System can be seen in the CloudCO Domain as a combination of multiple functions hosted in the CloudCO architecture, namely the CloudCO Domain Orchestrator, the VNFM, the VIM and the PNF Manager & Controller. Green reference points are also defined in FANS document, see [26], and are related to NVF reference points already defined in the ETSI standards and used in FANS architecture, while the blue reference points are the new ones defined by BBF for the CloudCO reference architecture to accommodate adding SDN capabilities. The “Os-Ma-ccodo” reference point may expose functions and attributes of the “Os-Ma-nfvo” reference point used in FANS directly to the E2E Service Orchestrator.

Some pre-requisites are needed to implement FANS in a CloudCO architecture:

- The CloudCO Provider (InP – Infrastructure network Provider in FANS) is responsible for creating network functions for retail ISPs (VNOs in FANS) in its network using Nf-Vi and/or Ve-Vnfm-vnf interfaces.
- VNFM functionalities and attributes are exposed by the Centralised Management System through the CloudCO Northbound API to allow consumption by the VNOs. Each VNO may have its own flavor of Management System (VNO#n MS) in terms of Fault, Configuration, Accounting, Performance and Security (FCAPS) management and flow control of its own virtual network.

Figure 37 indicatively depicts the deployment scenario for FANS in CloudCO, while further details about the functionalities hosted in certain blocks and information flows that describe the relevant interfaces would be reported in an Application Note.

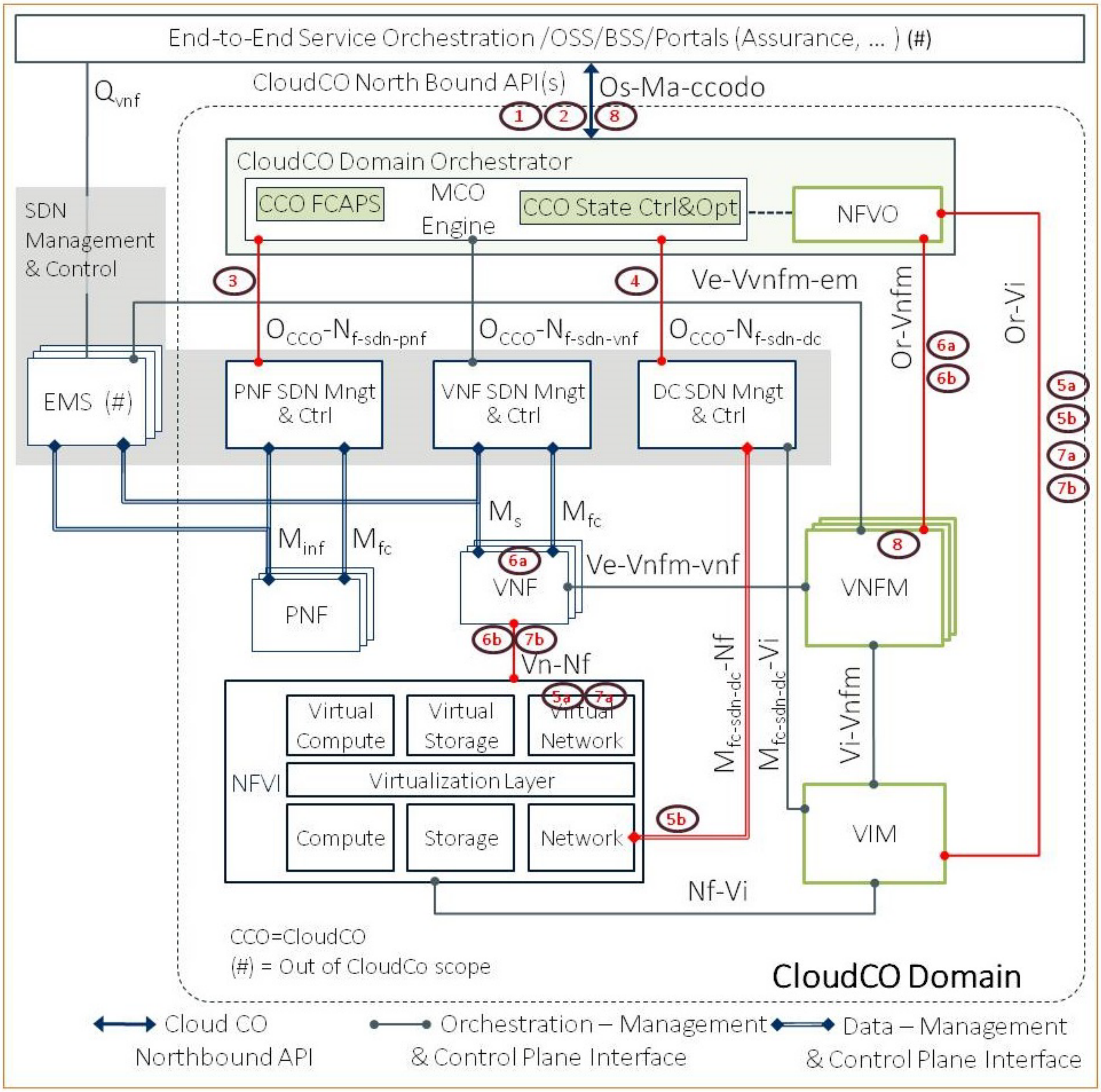


Figure 37: Deployment scenario for FANS

The deployment of FANS in CloudCO involves a logical sequence of steps:

1. The CloudCO NB API allows the retail ISP (VNO in FANS) accessing its relevant functions in CloudCO Domain.
2. The CloudCO Provider (InP in FANS) make sure that a VNO can have access only to its service instances and its service users. Within the CloudCO Domain Orchestrator (as part of the Centralised Management System in FANS) could be placed a central supervisor component (Data Repository) to enforce policies and avoid potential conflicts or discrepancy in resource sharing or line settings among VNOs. Alternatively, this kind of enforcement could be exercised by the PNF Manager & Controller.

© The Broadband Forum. All rights reserved

3. The CloudCO Domain Orchestrator requests the PNF SDN Controller to allocate an unused VLAN on the Access Node uplink and report back with the VLAN-id. It is also possible to pre-provision the VLANs on the Access Node uplinks, making the use of the PNF SDN Controller optional for this use case.
4. The CloudCO Domain Orchestrator requests the DC SDN Controller to configure the ToR switch connected to the Access Node with the same VLAN-id. It is also possible to pre-configure the ToR switch, making the use of the DC SDN Controller optional for this use case.
5. To allow the creation of management paths terminated in the different VNOs' Management Systems, the CloudCO Domain Orchestrator requests the NFVO to, in turn request NFVI VIM to:
    a. Set up a new virtual network inside the NFVI for the access-side connections. Note that this virtual network, span the complete CloudCO Domain.
    b. Set up a L2 bridge between the above-mentioned uplink VLAN and the virtual network on the compute hosts attached to the ToR switches that attaches to the Access Node.
6. The CloudCO Domain Orchestrator requests the NFVO to, in turn request VNFM to:
    a. Instantiates new VNF instances, including shaping as described in section 6.4 of TR-384 [5], as required for the VNO's services. Note that these instances can be instantiated anywhere inside the CloudCO NFVI as the virtual network is spanning the complete CloudCO Domain.
    b. Connects the LAN facing interface of the instance to the aforementioned virtual network.
7. The CloudCO Domain Orchestrator requests the NFVO to, in turn request NFVI VIM to:
    a. Set up another new virtual network inside the NFVI for the WAN-side connections. Note that this virtual network, span the complete CloudCO Domain.
    b. Connect this virtual network to the WAN facing interface of the instance.
8. VNFM performs lifecycle management for the virtualized instances and CloudCO Domain Orchestrator handles abstract access for the VNO through the CloudCO NB API.

Note that steps 3 to 8 are performed by the Centralised Management System and its internal modules in a FANS architecture.

Definitely, the CloudCO framework enables FANS as an SDN application. In future implementations, it needs a tighter integration between SDN Controllers and the Centralised Management System as some notes throughout this section refer to.

6.1.6 Public Wi-Fi Access

The main scope of TR-321 is to simplify access point requirements by placing more functions into the AC and/or BNG. The AC functionality of public Wi-Fi access presents a good application of the CloudCO.
The AC element provides centralized control, management, and troubleshooting of access points. The following is a basic function list that AC performs on the access points:

- Performance monitoring.
- Fault reporting.

- Automatic radio channel selection and adjustment.
- Automatic transmit power level adjustment.
- Load balancing based on subscriber numbers or traffic load.

The CloudCO can thus support at least a subset of the scenarios that are part of Scenario 13, described in section 5.14 depending on the AC architectural options.
For instance, the “Stand-alone AC co-located with the BNG” and “BNG integrated AC” architectures can be thought of as additional scenarios for the CloudCO, even using a vBNG (as per section 5.14). Also the “Distributed AC” architecture can be a good candidate for a CloudCO use case. In fact, the AC can be deployed in a more centralized location to manage a higher number of spread access points and thus it can be virtualized into a CloudCO Domain.

Figure 38 depicts the onboarding of a new vAC instance into the CloudCO architectural framework.

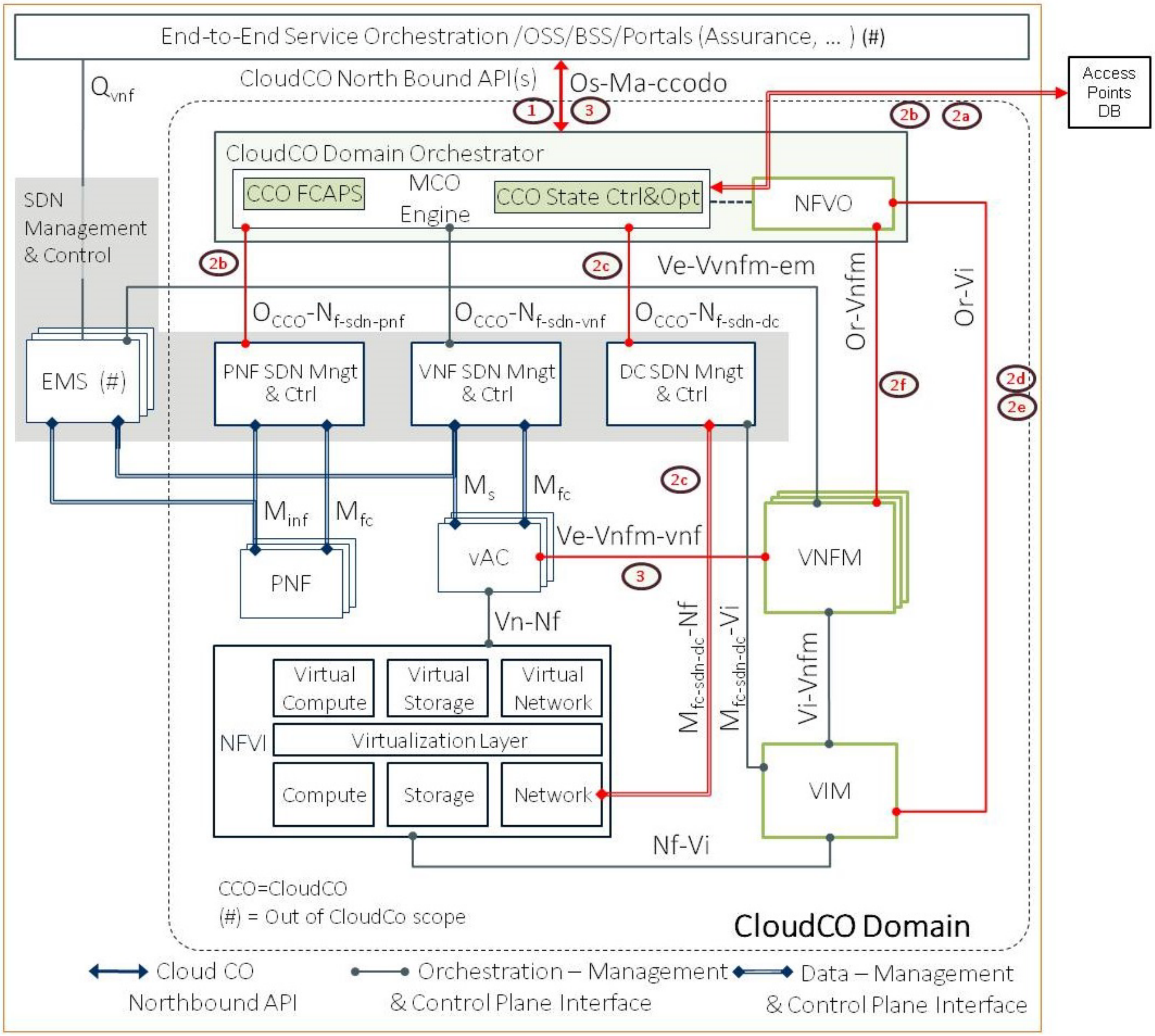


Figure 38: vAC in CloudCO Architectural Framework

1. The Service Provider uses the CloudCO Northbound API to associate a vAC Instance with a physical Access Point.
2. This triggers the CloudCO Domain Orchestrator to:
   a. Query the APs database to figure out on which Access Point the vAC should be attached to.
   b. Request the PNF SDN Controller to allocate an unused VLAN-id on the Access Node Uplink where the Access Point (AP) is connected and report back with the VLAN-id. It is also possible to pre-provision the VLANs on the ANs Uplink and furthermore pre-populate the APs database with information about Access Node-identifier (AN-id) and VLAN-id, making the use of the PNF SDN Controller optional for this use case
   c. Request the DC SDN Controller to configure the access-facing ToR switch. connected to the AP-relative Access Node with the same VLAN-id. Note that this VLAN-id is only significant for the specific ToR switch. Again this VLAN could be pre-provisioned, making the use of the DC SDN Controller optional.
   d. Request the NFVO to, in turn request NFVI VIM, to set up a new Virtual Network inside the NFVI. Note that these virtual networks span the complete CloudCO Domain.
   e. Request the NFVO to, in turn request NFVI VIM, to set up a L2 bridge between the aforementioned VLAN-id and the Virtual Network on one of the compute hosts where the ToR relies on.
   f. Request the NFVO to, in turn request the VNFM, to instantiate a new vAC instance, and connect the LAN facing interface to the aforementioned virtual network.
3. The VNFM perform lifecycle management for the vAC instance, while the CloudCO Orchestrator handles abstract access to VNFM through the CloudCO NB API.

This results in the following Service Graph for this Use Case, see Figure 39.

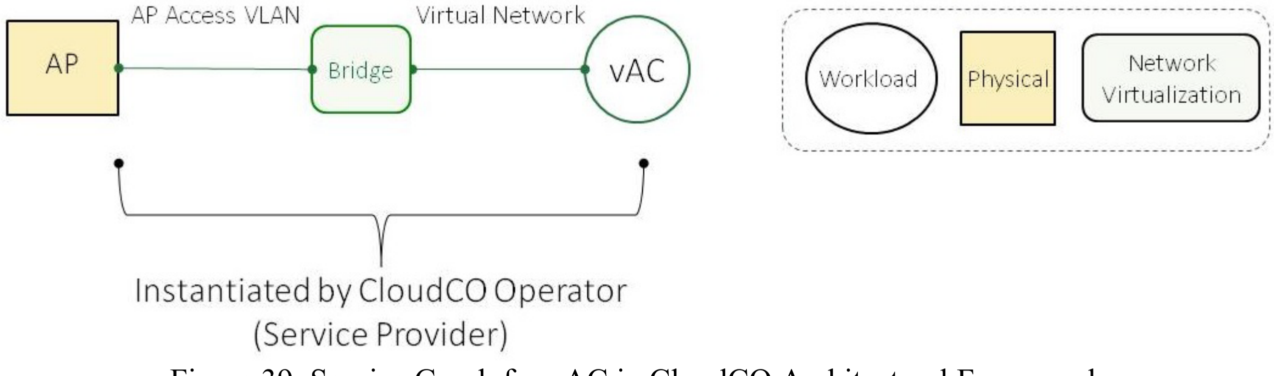


Figure 39: Service Graph for vAC in CloudCO Architectural Framework

It should be noted that the above Service Graph is only limited to management and control connectivity between AP and vAC, and as such it not representing any end to end service.

6.1.10 Value Added Services on NERG

Building on the Use Case description in section 6.1.2, which describes how NERG can be deployed on a CloudCO Architecture, while allowing a dynamic setup of the flat LSL model. It is easy to understand how this Use Case be easily extended to enable service chaining to additional services in a variety of ways. Figure 40, shows a number of ways in which this can be achieved.

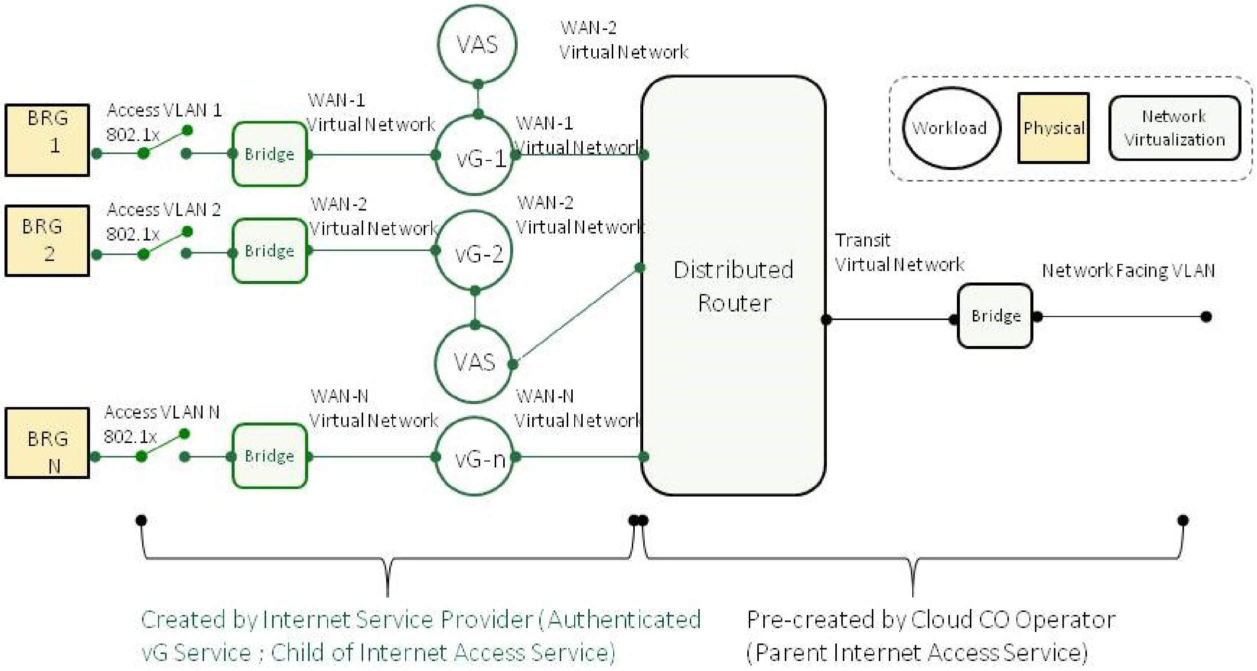


Figure 40: Ways on enabling service chaining to additional services

For subscriber One (represented by BRG 1), turning on the VAS attribute for the service will allow the vG to access the VAS. Note that the VAS can be multitenant and offer services to multiple vG's or can be single-tenant.

For subscriber Two (BRG 2), turning on the VAS attribute for the service will dynamically re-chain the service chain to integrate the VAS as a 'bump-in-the-wire'. This re-chaining can be done during the lifecycle of the service.

6.2 New Use Cases Enabled by CloudCO

6.2.1 IPTV Support for NERG

This Use Case builds on the Use Case described in section 6.1.2, and the interactions described in Figure 22. In order to support multicast a couple of extra steps need to be performed:

There are two approaches/options that are documented here:

1. Option 1: An additional network overlay is created and extended up to the AN. Multicast is sent on this overlay and is redirected into subscriber port after IGMP snooping on the AN/SDN Controller combination.

2. Option 2: (1) Multicast support is enabled on the Distributed Router and (2) IGMP snooping is enabled on ToR and AN aiding VLAN-based replication.

The following extra steps are needed for option 1:

Prerequisites

- Multicast based IPTV is being sent and delivered to the CloudCO across the Network I/O. The CloudCO Operator makes sure this multicast is sent across a pre-instantiated Multicast network overlay.
- An IGMP Snooping application is instantiated on the PNF SDN Controller.

Workflow (in addition to the steps in Use Case described in section 6.1.2):

4. The Retail ISP uses the CloudCO NB API to enable support for IPTV for a certain subscriber.
5. This in turn instructs the CloudCO Orchestrator to:
    a. Extend the Multicast Overlay to the appropriate AN (if not already done, based on subscriber location).
    b. Enable IGMP user plane packets to be redirect from the appropriate AN towards the IGMP Snooping application.
    c. Upon receipt of IGMP packets, instruct the AN user plane to replicate the multicast from the multicast overlay to the subscriber VLAN.

The following extra steps are needed for option 2.

Prerequisites

- Multicast-based IPTV is being sent and delivered to the CloudCO across the Network I/O. The CloudCO Operator makes sure this multicast is sent across the pre-established Distributed Router.
- An IGMP Snooping application is instantiated on the PNF and DC SDN Controllers.

Workflow (in addition to the steps in Use Case described in section 6.1.2):

4. The Retail ISP uses the CloudCO NB API to enable support for IPTV for a certain subscriber.
5. This in turn instructs the CloudCO Orchestrator to:
    a. Turn on Multicast routing on the appropriate interfaces of the Distributed Router
    b. enable IGMP user plane packets to be redirected from the appropriate AN towards the IGMP Snooping application.
    c. Upon receipt of IGMP packets, instruct the AN and DC user plane to replicate multicast packets to the right receiver ports.

6.2.2 Residential Broadband Access using DHCP

In the CloudCO architecture, the control plane of the legacy entities, e.g., Access Node, would be split from the user plane, the control functions are clear candidates for virtualization. In this Use Case, the DHCP relay agent and MAC/IP anti-spoofing control functions in the control plane are disaggregated from the AN and virtualized as VNFs.

In the MSBN architecture, the AN is considered as a single device whether it is a Digital Subscriber Line Access Multiplexer (DSLAM) or a combination of an Optical Line Termination (OLT) and an Optical Network Unit (ONU). Therefore, when virtualizing the control functions, it shall support both DSLAMs and OLTs combined with ONUs. The applicable access nodes include ANs that comply with the reference TRs (TR-101 [8], TR-178 [13], TR-301 [18], TR-156 [11] and TR-167 [12]).

In this Use Case, the BNG can be a legacy physical entity or a disaggregated BNG as described in section 5.2.5.1 of TR-384 [5]. In the following step, a fully virtualized BNG, i.e., a BNG running inside a workload that has both control plane and user plane virtualized is taken as an example.

Involved actors

- CloudCO Operator.
- Service user.

Pre-requisites

- A fully initialized CloudCO domain.
- A CloudCO Physical Instance of one or more racks, each equipped with a ToR switch and Compute Hosts, and the associated NFVI/MANO/SDN workloads running on the Compute Infrastructure. CloudCO ANs connect to one rack's ToR, while CloudCO Network Facing interfaces connect to the same or a different ToR.
- The virtualized control functions of DHCP Relay and MAC/IP anti-spoofing are instantiated on the PNF SDN Controller.
- The PNF SDN Controller controls the ANs and the DC SDN Controller controls the TORs.
- The CloudCO communicates with the AAA Server and the DHCP Server through a NB API. It is important to note that the AAA Server and DHCP Server may also be virtualized as software running on the servers.
- There are service users who request broadband access using DHCP.
- The interactive messages between the AN and the SDN Controller can be sent through a tunnel.

Figure 41 shows the procedure description of DHCP and Anti-spoofing and Figure 42 shows the corresponding workflow in the CloudCO architecture.

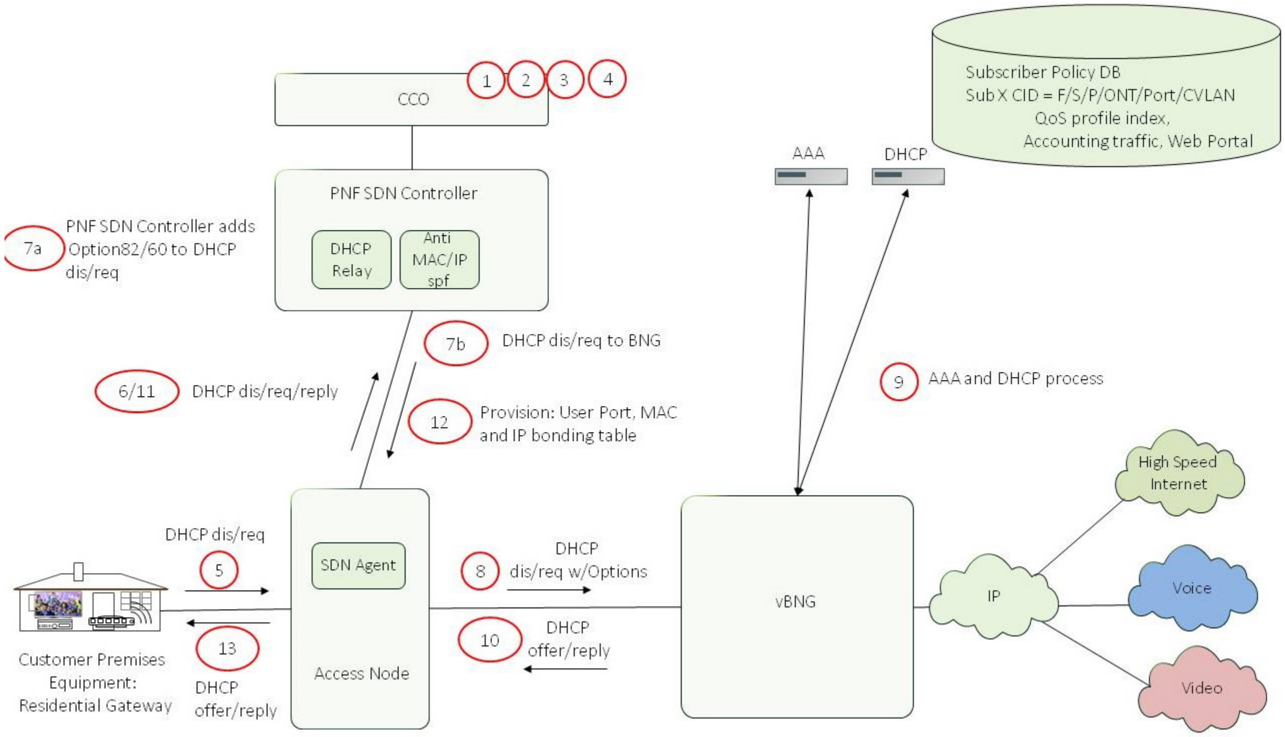


Figure 41: DHCP and Anti-spoofing

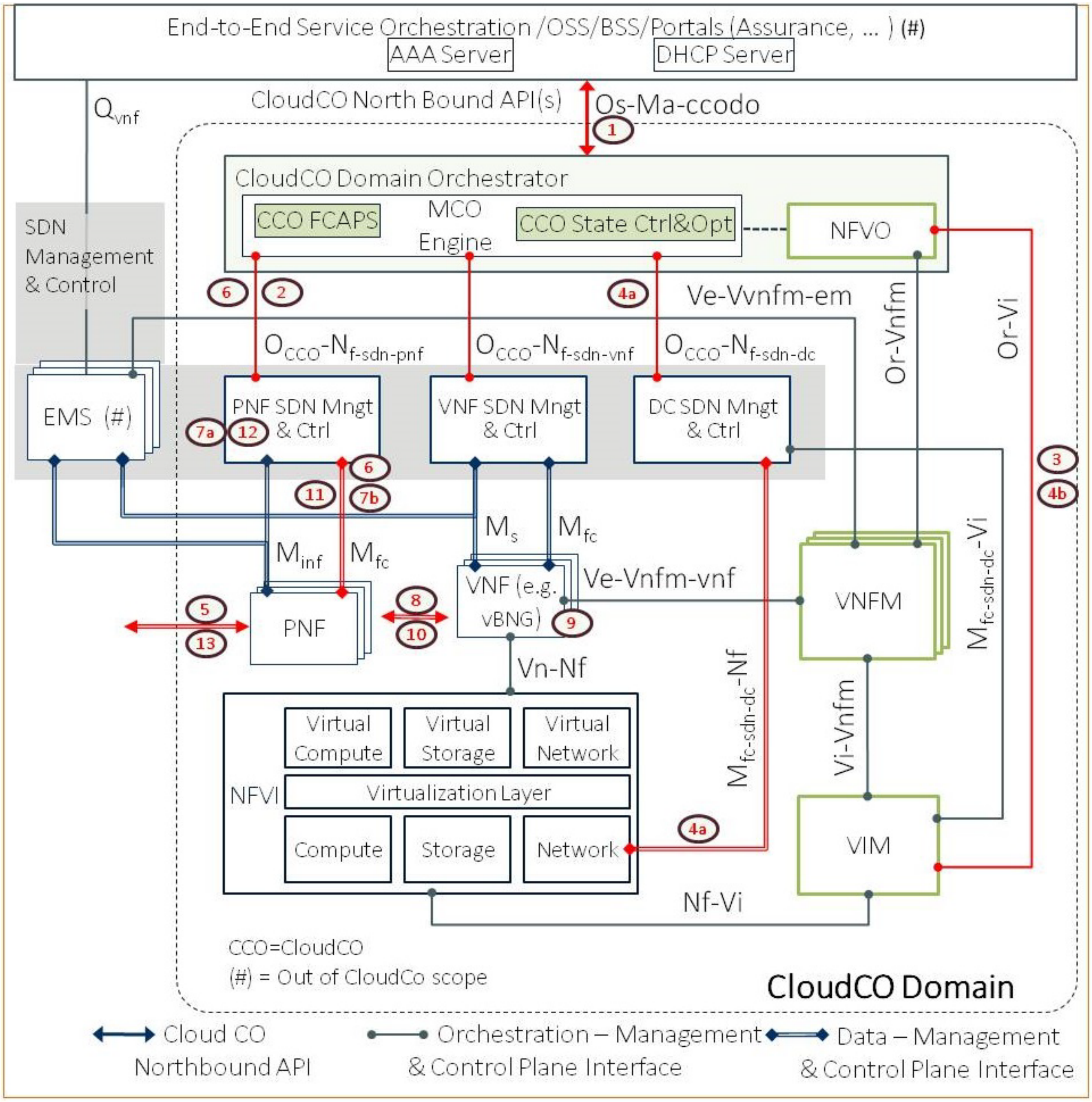


Figure 42: DHCP and Anti-spoofing Workflow in CloudCO Domain

1. An *IPoE_Internet Access Service Instance* is instantiated inside the CloudCO Domain by the CloudCO Operator through the CloudCO NB API. This instantiates a vBNG which is managed through the standard R and M interfaces of a legacy BNG. Note that this Use Case does not need a VNFM as the existing Central Office management interfaces are used. Therefore, automated scaling of vBNG related resources are not dealt with in this Use Case.
2. The CloudCO Operator knows where the subscriber are attached and instantiates an 1:1 S- and C-VLAN pair per subscriber on the Access Node via the PNF SDN Controller, or alternatively a N:1 S-VLAN for all subscribers needing this service on the Access Node.
3. The CloudCO operator instantiates a Network Overlay via the VIM.
4. One of the following is done:

   a. The CloudCO operator instantiates an S-VLAN on the appropriate TOR switch via the DC SDN Controller, instantiates a Bridge function via the VIM and instantiates bridging between the S-VLAN to the Network Overlay, or
   b. The CloudCO operator instantiates an S-VLAN on the appropriate TOR switch and extends the overlay to the ToR switch S-VLAN.
5. The equipment (e.g., CPE) at the service user's home sends the DHCP messages to request an IP address.
6. The AN (shown as the PNFs in Figure 41) forwards the DHCP messages to a DHCP relay agent that is conceptually a component of the SDN controller. The complete Ethernet frame of a DHCP packet with the user MAC address will be forwarded to the PNF SDN controller. Typically, the access loop identification is used for authentication, authorization and IP address allocation. In TR-101 [8], it is inserted by the AN and carried in a DHCP Option 82. In the CloudCO architecture, the access loop identification, that is compiled with the definition from TR-101 [8] (section 3.9.3), is sent to the PNF SDN Controller by the AN together with the DHCP message, and the DHCP Option 82 is inserted by the PNF SDN Controller. A request for DHCP processing is sent to the Management Control Orchestration (MCO) Engine.
7. By receiving the above messages sent from the AN, and the reply for DHCP processing from the MCO Engine, the PNF SDN Controller:
   a) Adds the Option 82 to the DHCP messages with the received access loop identification.
   b) Sends the DHCP messages with option 82 back to the AN.
8. The AN forwards the DHCP messages with option 82 to the vBNG.
9. The vBNG communicates with the AAA server and DHCP server for AAA and DHCP process.
10. The vBNG forwards the DHCP reply message back to the AN.
11. With a successful subscriber authentication and IP address allocation, the DHCP reply message will be sent to the PNF SDN controller by the AN for IP/MAC spoofing prevention process.
12. By inspecting upstream and downstream DHCP packets, the PNF SDN controller discovers the mapping of IP address to MAC address and user ports and configures it on the AN for this CPE.
13. The CPE gets the IP address from the DHCP reply messages.

The service graph that applies to this Use Case is depicted in Figure 43.

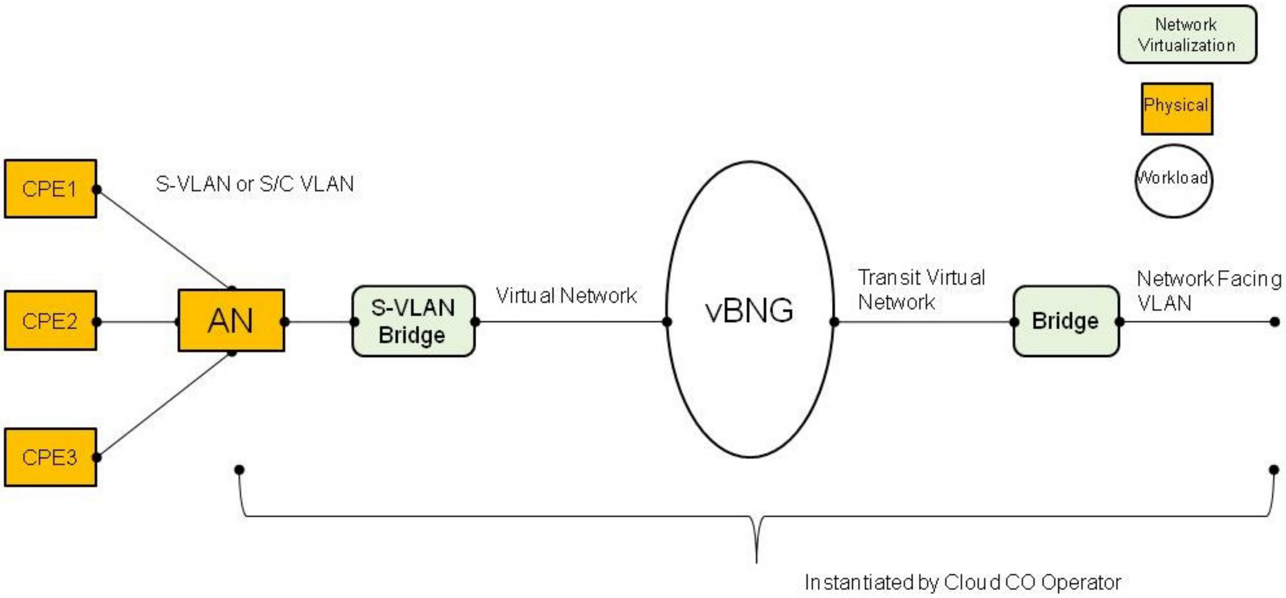


Figure 43: Service Graph applied for the Residential Broadband Access using DHCP Use Case

6.2.3 Multicast Control in CloudCO

The multicast control functions of CloudCO entities (e.g., AN) related to IGMP/ Multicast Listener Discovery (MLD) processing can be virtualized as VNFs which are instantiated in the SDN controller. The AN forwards all the IGMP/MLD packets to the SDN controller for processing. The multicast forwarding tables (group tables) on the AN and other network elements (e.g., ToR and Network Facing Node) on the multicast path can be configured by the SDN controller. The SDN controller makes a decision on IGMP/MLD packet forwarding, dropping or configures the corresponding multicast forwarding tables for the user plane.

In this Use Case, the BNG can be a legacy physical entity or a disaggregated BNG as described in section 5.2.5.1 of TR-384 [5]. In the following step, a fully virtualized BNG, i.e., a BNG running inside a workload that has both control plane and user plane virtualized is taken as an example.

Involved actors

- CloudCO Operator.
- Service user.

Pre-requisites

- A fully initialized CloudCO domain.
- A CloudCO Physical Instance of one or more racks, each equipped with a ToR switch and Compute Hosts, and the associated NFVI/MANO/SDN workloads running on the Compute Infrastructure. CloudCO ANs connect to one rack’s ToR, while CloudCO Network Facing interfaces connect to the same or a different ToR.
- The virtualized IGMP/MLD control functions are instantiated on the PNF SDN Controller and DC SDN Controller.
- The PNF SDN Controller controls the ANs and the DC SDN Controller controls the TORs.

- There are service users who request multicast service. The CloudCO Operator uses the CloudCO NB API to enable support for Multicast service for a certain subscriber.
- Multicast service is being sent and delivered to the CloudCO across the Network I/O.
- The SDN Mngt&Ctrl has the information of: 1) the access network topology; 2) the mapping between the access loop identification and the port information of each network element on the multicast path; 3) the mapping between the multicast IP group address and the multicast MAC group address. These topology and mapping information can be pre-configured on the SDN controller, or they can be obtained from the AAA server.
- The interactive messages between the Access Node and the SDN Controller are sent through a tunnel.

Figure 44 shows the procedure description of IGMP/MLD Join process and Figure 45 shows the corresponding workflow in the CloudCO architecture.

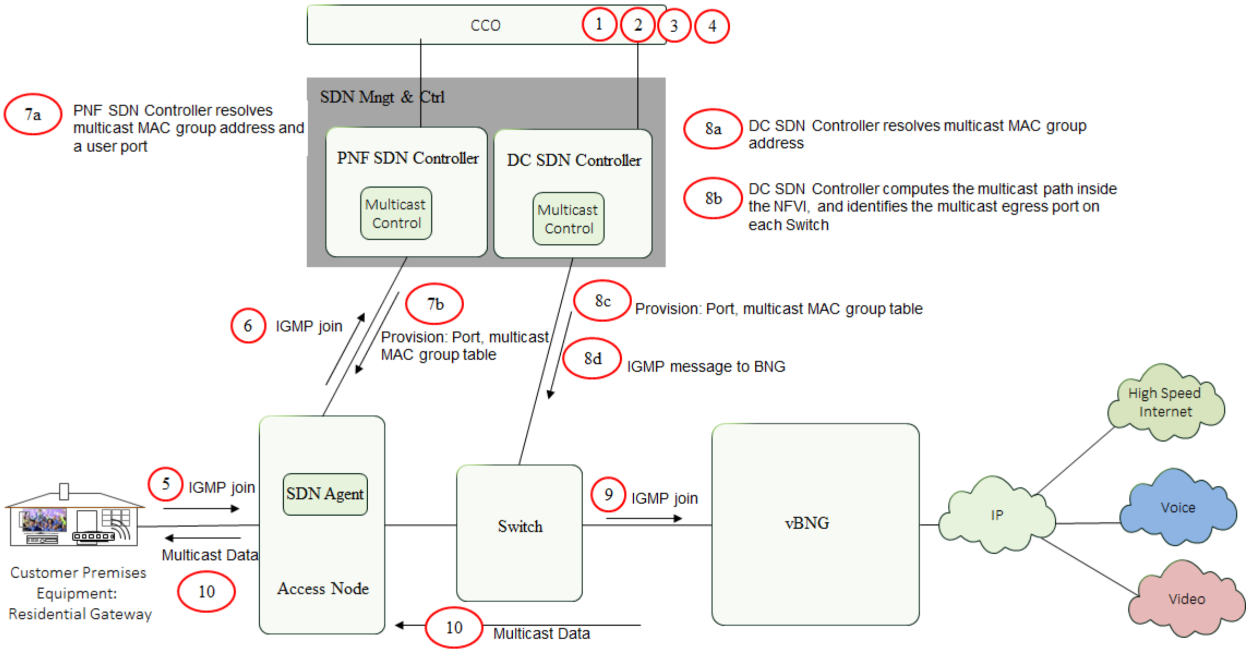

CCO
1
2
3
4
SDN Mngt & Ctrl
PNF SDN Controller
Multicast Control
DC SDN Controller
Multicast Control
7a
PNF SDN Controller resolves multicast MAC group address and a user port
8a
DC SDN Controller resolves multicast MAC group address
8b
DC SDN Controller computes the multicast path inside the NFVI, and identifies the multicast egress port on each Switch
6
IGMP join
7b
Provision: Port, multicast MAC group table
8c
Provision: Port, multicast MAC group table
8d
IGMP message to BNG
High Speed Internet
5
IGMP join
SDN Agent
Multicast Data
Access Node
Customer Premises Equipment: Residential Gateway
10
Switch
9
IGMP join
vBNG
IP
Voice
Video
10
Multicast Data

Figure 44: An Example of IGMP/MLD Join Process

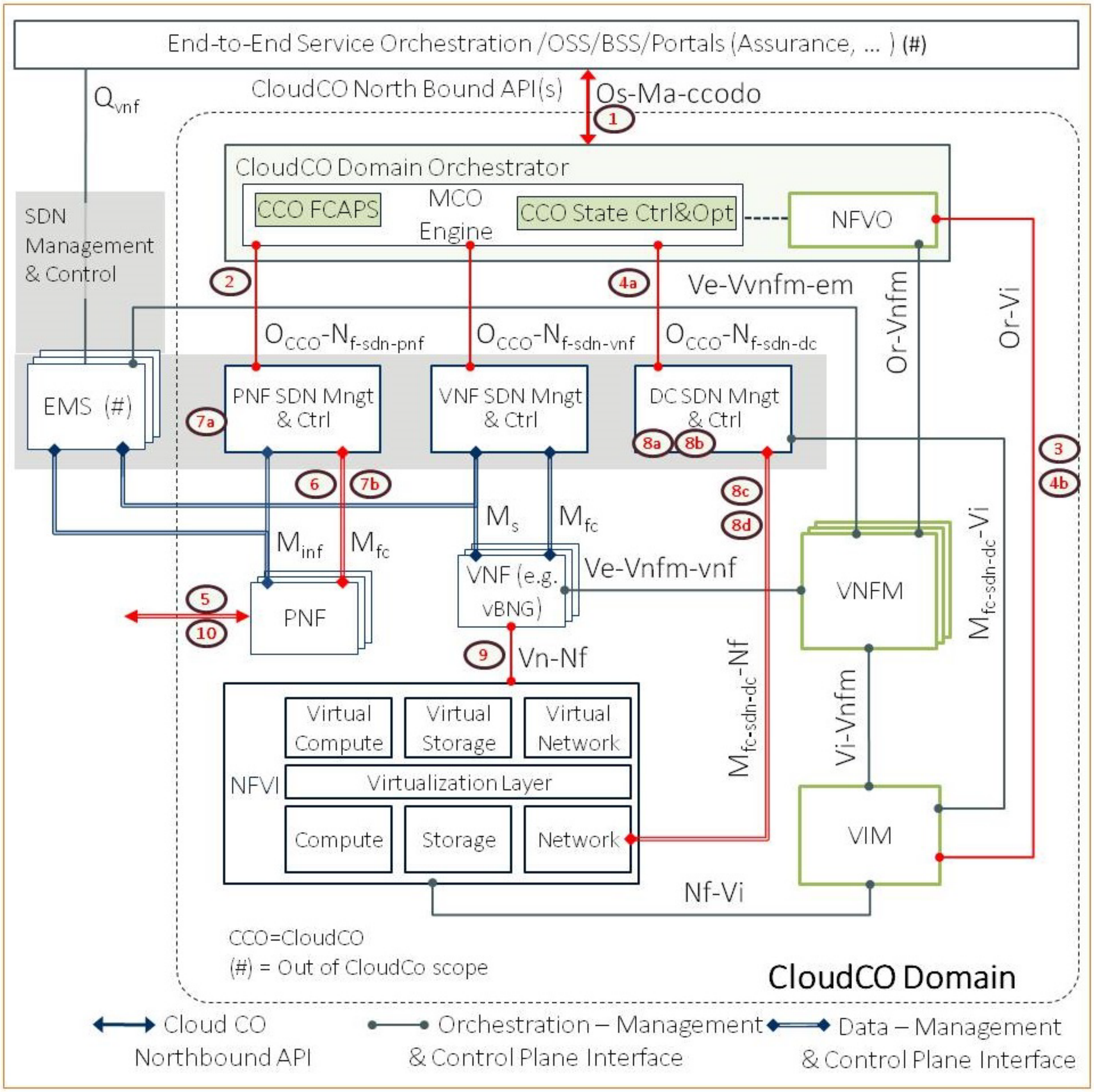


Figure 45: An Example of IGMP/MLD Join Process Workflow in CloudCO Domain

1. A *Multicast Service Instance* is instantiated inside the CloudCO Domain by the CloudCO Operator through the CloudCO NB API.
2. The CloudCO Operator instantiates a N:1 Multicast VLAN on the AN for the user port via the PNF SDN Controller.
3. The CloudCO operator instantiates a Network Overlay via the VIM.
4. One of the following is done:
   a. The CloudCO operator instantiates a Multicast VLAN on the appropriate TOR switch via the DC SDN Controller, instantiates a Bridge function via the VIM and instantiates bridging between the Multicast VLAN to the Network Overlay, or

    b. The CloudCO operator instantiates a Multicast VLAN on the appropriate TOR switch and extends the overlay to the ToR switch Multicast VLAN.
5. The equipment (e.g., CPE) at the service user's home sends an IGMP/MLD Join message.
6. The Access Node (shown as the PNFs in Figure 44) forwards the IGMP/MLD join message to the PNF SDN Controller. The access loop identification, as defined in TR-101 [8] (section 3.9.3), is sent to the PNF SDN Controller by the AN together with the IGMP/MLD join message, so that it can be used by the PNF SDN controller to identify the access port associated with the IGMP/MLD message. A request for Multicast processing is sent to the MCO Engine.

By receiving the above message sent from AN, and the reply for Multicast processing from the MCO Engine, the IGMP/MLD join message and the access loop identification will be processed by the PNF SDN Controller and DC SDN controller as follows:

7. The PNF SDN Controller:
    a. Resolves a corresponding multicast MAC group address from the IP group address in the IGMP/MLD join message according to the pre-stored mapping between them, and resolves a user port from the received access loop identification.
    b. Generates and configures the multicast forwarding tables on the AN, with an indication to replicate the multicast packets to the user port.
8. The DC SDN controller:
    a. Resolves multicast MAC group address in the same way as the PNF SDN controller.
    b. Computes the multicast path inside the NFVI, and determines the port identifications of the Switches on the multicast path according to the received access loop identification and the information kept on the SDN Mngt&Ctrl consisting of the access network topology and the mapping relationship. The ports of the network elements mentioned here are the multicast egress ports.
    c. Generates and configures the multicast forwarding tables which includes the above mentioned egress port and multicast MAC group address on the NFVI Switches.
    d. Sends the IGMP Join message to the Switch.
9. The Switch forwards the IGMP Join messages to the vBNG for further process.
10. After a successful join, the multicast traffic will be distributed to the CPE.

This result in the following service graph, see Figure 46.

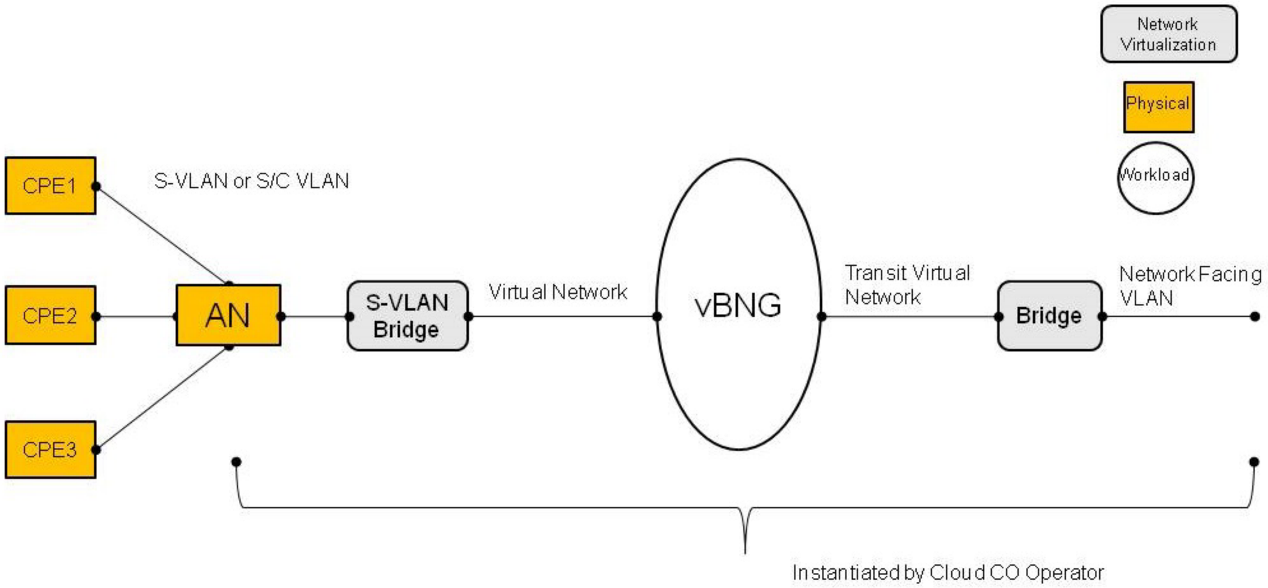


Figure 46: Service Graph applied for the Multicast Control in CloudCO Use Case

6.2.4 vBG deployed in the DC and customer site using Overlay LSL Connectivity

TR-328 [25] defines the overlay LSL that supports the vBG to pBG connectivity. In addition, it defines architectures of deploying the vBG in (1) the network, (2) in the pBG or (3) in both in the network and pBG.

To setup the Overlay LSL, the pBG must be provided with the necessary tunneling information. This means that the pBG must own one IP address on its WAN interface (i.e., the pBG WAN interface IP address) prior to tunnel establishment. Note that the subscriber's pBG can have multiple IP addresses on its WAN interfaces, for example, the management client function on the pBG can access the vBG management system through one pBG' WAN IP address, which can be stored as default setting and be activated at its boot time or be provided by a DHCP server. WAN IP address can be obtained via DHCP or PPPoE or statically configured however in this Use Case we will use DHCP option.

When the pBG has one IP address on its WAN interface, the subscriber's pBG will contact the vBG management system for further getting the tunneling information between itself and the vBG_MUX. TR-328 [25] suggests the following methods for getting the LSL parameters and tunnels:

- Provisioned by the EMS/ Network Management System (NMS), using NETCONF/YANG or Simple Network Management Protocol (SNMP).
- Provisioned by the ACS, using TR-069 [7].
- Obtained from the network via DHCP.

In this Use Case, the applied DHCP method is based on the one described in section 6.1.4 of TR-328 [25].

The vBG management system includes the subscriber information repositories, authentication function (like AAA), configuration function (like ACS) and other functions as described in section 5.1 of TR-328 [25].

Note that the CloudCO AN in this Use Case is an SDN-enabled component which is controlled by the PNF SDN Controller, so that the registration packets from the subscriber will be forwarded to the PNF SDN Controller by the CloudCO AN. The CloudCO AN could also be a legacy network equipment, as defined in the BBF CloudCO Migration Project and will not be discussed herein.

As soon as the registration to the vBG Management System is successful, the tunnel can be established. Meanwhile, the vBG service for the subscriber is also configured inside the vBG Management System via the CloudCO NB API.

Note that this Use Case does not elaborate on eventual service chaining of additional network functions like firewalling/NAT/parental control into the service graph. In this way, it is not meant to be a complete description of all aspects described in TR-328 [25]. It is also not meant to be the only possible implementation of the vBG scenario on the CloudCO Domain. The choice of using one vBG instance per subscriber is not meant to describe the only way of achieving vBG like functionality. Moreover, the Use Case also does not describe how the CloudCO supporting infrastructure, e.g., MANO stack, SDN Controllers, are set up.

Involved actors

- CloudCO Operator, offering the CloudCO Domain.
- vBG Service Provider, offering the vBG Service on the CloudCO Domain.
- Service user (i.e., subscriber of the vBG Service Provider).

Pre-requisites

- A fully initialized CloudCO domain.
- A CloudCO Domain and the associated NFVI/MANO/SDN VMs or Containers running on the Compute Infrastructure.
- The PNF SDN Controller controls CloudCO ANs and DC SDN Controller controls the entities in the DC.
- The vBG-MUX functionality is preconfigured in a dedicated VNF.
- pBG is deployed at the service user business premise and connected to the access line.
- The pBG node has been installed and provisioned accordingly.

At the boot time of pBG, steps shown in Figure 47 are being realized.

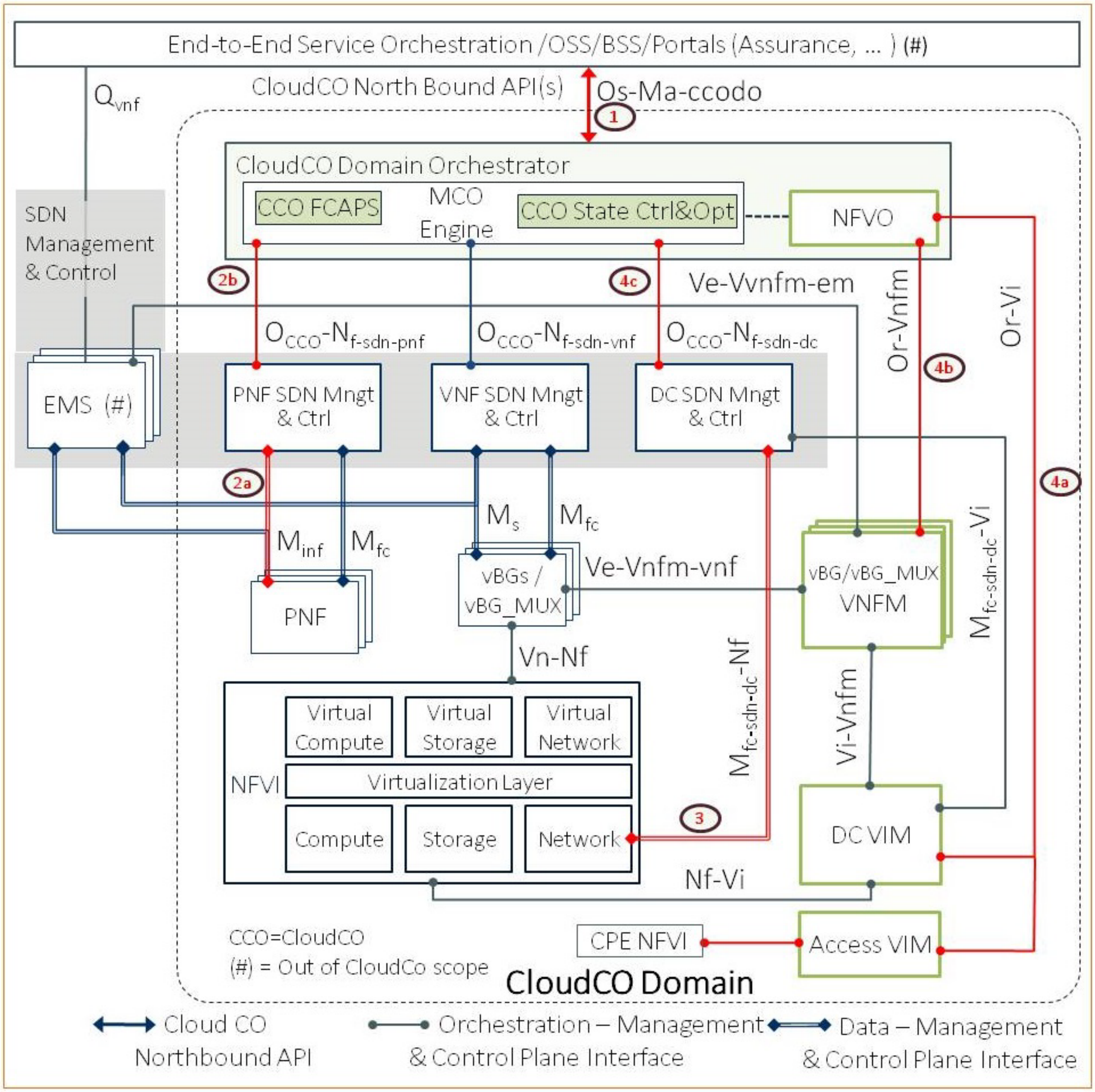


Figure 47: Onboarding a new vBG system instance onto the CloudCO Domain when using the Overlay LSL model

1. The subscriber's pBG gets one WAN IP address from the DHCP server. In addition, it gets all tunneling information between the pBG and the vBG-MUX via the DHCP as well. After that, the subscriber contacts and registers itself to the vBG management system.
2. The PNF SDN Controller receives the registration packets forwarded from the AN, and delivers it to the vBG management system that resides as a VNFM.
3. As soon as the subscriber is successfully registered on the vBG management system, the tunnel information (tunnel endpoint, tunnel protocol) can also be provided to the vBG-MUX
4. Based on the above vBG service configuration, the CloudCO Orchestrator executes the following workflow:

   a. Requests the vBG VNFM to configure the vBG-MUX connected to the AN with the same tunnel information (tunnel endpoint, tunnel protocol). Requesting the NFVO to request NFVI DC-VIM to setup a new overlay network inside the NFVI, and connects the overlay network to the aforementioned vBG-MUX. Note that these virtual networks span the complete CloudCO Domain. The tunnel between the pBG and the vBG will be automatically established as the pBG has the necessary information via DHCP, and the vBG-MUX has been authorized to receive packets from that tunnel.
   b. Requests the NFVO to request the VNFM to instantiate a new vBG instance as follows:
      - For the vBG-in- CloudCO option: use the DC-VIM to instantiate the vBG and to connect one of the DC vBG interfaces to the aforementioned overlay network. The vBG can be instantiated anywhere in the CO as the overlay network is spanning the complete CloudCO Domain.
      - For the vBG-in-CPE part: use the Access-VIM to instantiate the CPE vBG part (vBG') and connect its interfaces in the pBG using the Access-VIM as well.
      - The VNFM can perform lifecycle management for the vBG instance. The CloudCO Orchestrator handles abstract access for the vBG Service Provider through the CloudCO NB API.
5. Inform the vBG service provider that the appropriate vBG instance is active and a vBG service for the subscriber is successfully provided. The AN receives the packets from the pBG-LSL interface and then forwards these packets to the vBG-MUX based on the destination IP address of these packets Original L2 frame components must be obtained.
6. When the vBG-MUX receives the first packet encapsulated in the L2-tunnel, it learns which vBG it has to forward the packet based on the subscriber tunnel attributes like source IP + VNI in the case of VXLAN, or Source IP in the case of Generic Routing Encapsulation (GRE).
7. The pBG and vBG use the monitoring mechanisms, such as Address Resolution Protocol (ARP) requests and Internet Control Message Protocol (ICMP) ping, to detect the availability of connectivity between them.

The service graph associated with this Use Case is depicted in Figure 48.

© The Broadband Forum. All rights reserved

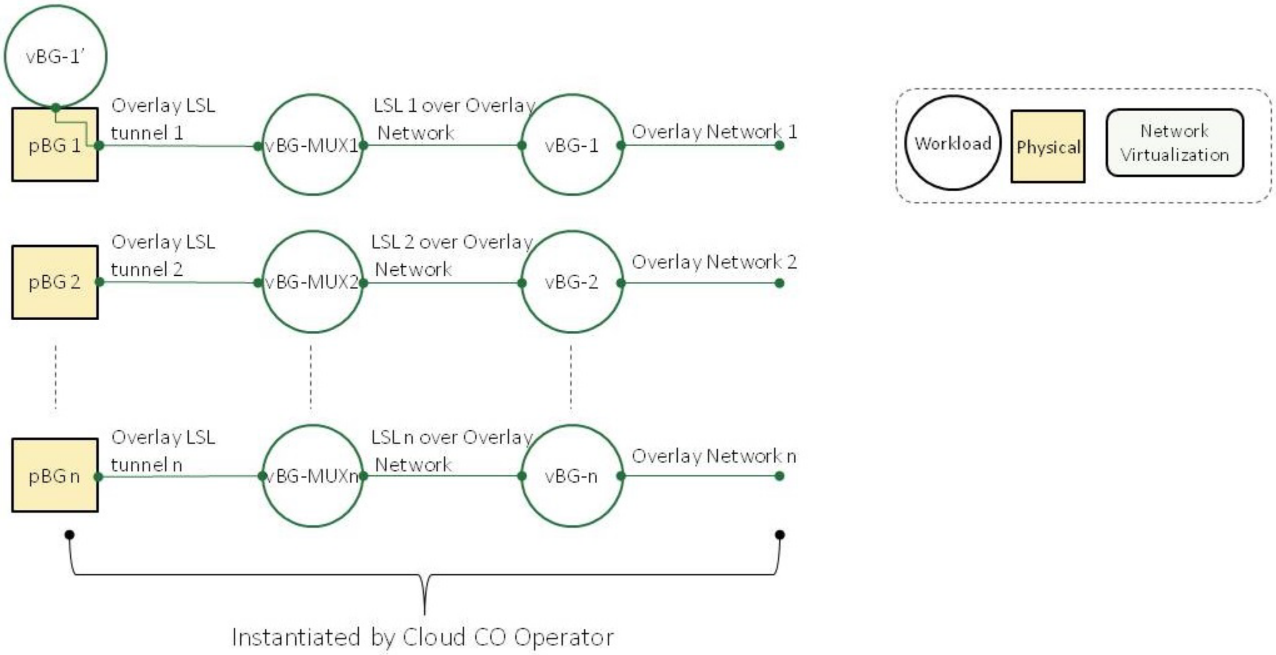


Figure 48: Service graph for vBG when using Overlay LSL Connectivity

6.2.5 Deploying an off-network vBG with SD-WAN functionality

In some cases the pBG and vBG owned by a service provider X will be connected via another internet service provider's Y network. In such cases the pBG and vBG can be still managed by the same service provider X. The customer's branches can be connected with a VPN running over the internet or other transport lines. In this Use Case the SD-WAN function will be used for this connectivity. The SD-WAN part controlled by the VPN controller will be implemented in the vBG. In the in-network location the vBG will reside in the DC and the pBG will reside at the customer site. In the Off-network case the vBG resides on the pBG at the customer's site.
The deployment process will consist of the following stages:

1. Secured Zero Touch Provisioning (ZTP) process, in order to connect the pBG to the management functions in the CloudCO.
2. Deployment of the vBG on top of the pBG, as described in Use Case section 6.2.4
3. Configuring the SD-WAN function.

The following terms are applied in this Use Case:

- ***Off-Network Location***: Enterprise Branch Office, in which the WAN Interfaces cannot be attached directly to the Access Network of the CloudCO Provider. In this case, Third Party Internet Service Providers will be used as a "Pipe" for OTT (Over The Top) traffic.
- ***Off-Network Link:*** Overlay Internet Tunnels between Off-Network and In-Network vBGs.
- ***In-Network Location***: Enterprise Branch Office, in which the WAN Interfaces are attached directly to the Access Network of the CloudCO Provider.
- ***In-Network Links***: Links between vBG, residing in the CloudCO.
- ***VPN Controller***: is a CloudCO entity for configuration of VPN Components on vBG, creating peer-to-peer links cross over Internet (*Off-Network Link*).

- ***ZTP Server / ZTP Flow***: standard framework for initial bootstrap configuration of CPE Device. The ZTP Flow is performed only once, starting from purchasing, till "Ready to be managed" message.

Involved actors

- CloudCO Operator, offering the CloudCO Domain.
- VBG Service Provider, offering the vBG Service on the CloudCO Domain.
- Service user (i.e., subscriber of the vBG Service Provider).
- VPN Controller.
- ZTP Bootstrap Server / ZTP Manufacturer Server.

Pre-requisites

This Use Case can be treated as an extension of the Use Case described in section 6.2.4 and its pre-requisites can be inherited with some additions:

- VPN Controller deployed on one or several CloudCO instances.
- ZTP Bootstrap Server deployed on one or several CloudCO instances.
- pBG complete purchasing part of ZTP flow, mounted, and here we will start from the stage, when CPE "power button is ON".
- Internet is available for pBG.

The Off-Network Use Case is depicted in Figure 49.

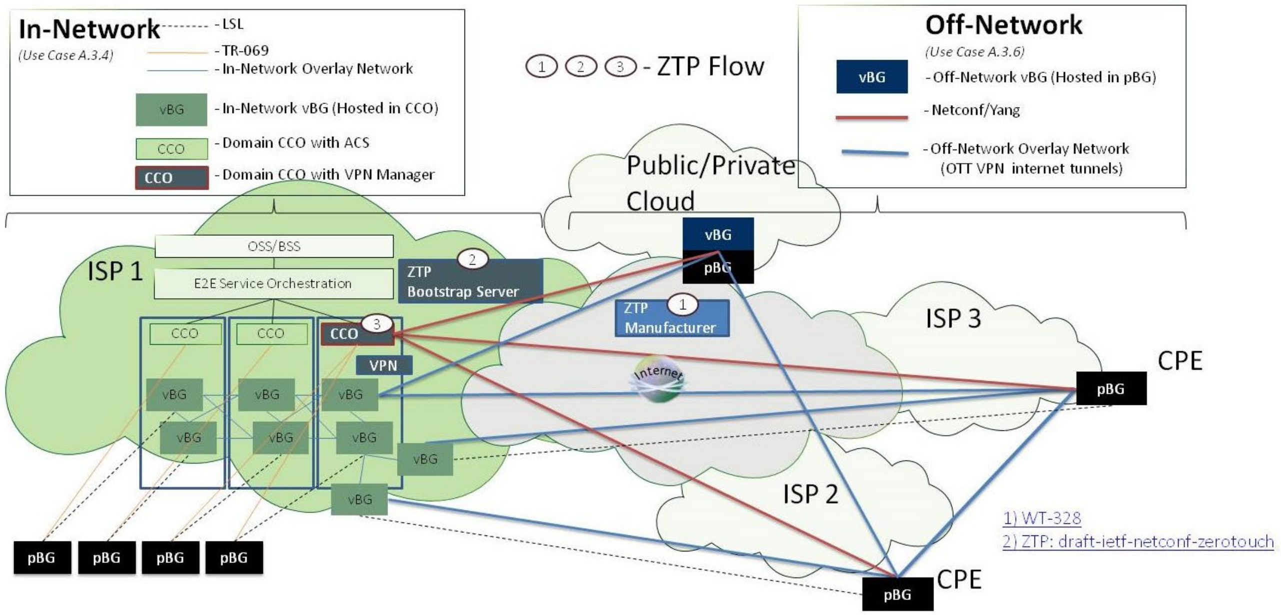

In-Network
(Use Case A.3.4)
- LSL
- TR-069
- In-Network Overlay Network
vBG - In-Network vBG (Hosted in CCO)
CCO - Domain CCO with ACS
CCO - Domain CCO with VPN Manager
① ② ③ - ZTP Flow
Off-Network
(Use Case A.3.6)
vBG - Off-Network vBG (Hosted in pBG)
- Netconf/Yang
- Off-Network Overlay Network (OTT VPN internet tunnels)
Public/Private Cloud
vBG
pBG
ISP 1
OSS/BSS
E2E Service Orchestration
ZTP Bootstrap Server
2
ZTP Manufacturer
1
CCO
CCO
CCO
3
VPN
vBG
vBG
vBG
vBG
vBG
vBG
vBG
vBG
Internet
ISP 3
ISP 2
CPE
pBG
CPE
pBG
pBG
pBG
pBG
pBG
1) WT-328
2) ZTP: draft-ietf-netconf-zerotouch

Figure 49: Off-Network Use Case

In contrast to the Use Case described in section 6.2.4, where the LSL link between pBG and vBG is applied, in this Use Case the LSL link is not needed, because the Off-Network CPE appear as being the pBG that is hosting the vBG.

ZTP Flow started and finished in 3 steps:

1. CPE (pBG) is powered on and gets internet connectivity. CPE reaches the ZTP Manufacturer Server, and redirects information according to the behavior described in draft-ietf-netconf-zerotouch.
2. CPE (pBG) reaches the ZTP Bootstrap Server of the Network Provider and downloads and implements the new initial boot file.
3. CPE (pBG) sends the "Ready to be Managed" Message to the VPN Manager.

The WAN interfaces of the CPE Device are configured following the pBG configuration process performed by VPN Manager, which realizes the vBG instantiation on the pBG. The WAN Interfaces are establishing the Off-Network links.

The control and management information interfaces (e.g., NFVI control, SD-WAN control, device management) will run securely between the CloudCO, the pBG, and the vBG.

The onboarding flow diagram associated with this Use Case is shown in Figure 50

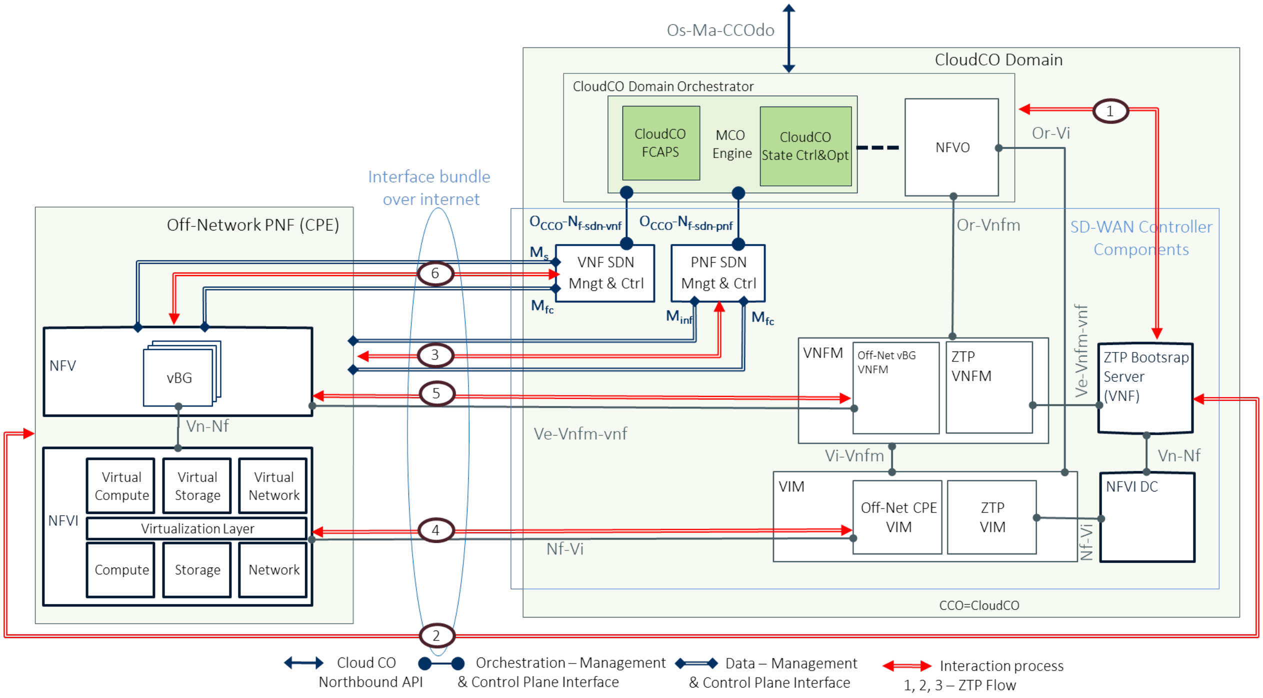


Figure 50: Onboarding a new VBG system instance onto the CloudCO Domain when using the Off-Network vBG model

1. The ZTP Bootstrap Server, deployed as a VNF, is configured by CloudCO-Domain (by means of ZTP VNFM) to generate new boot files for new CPE.
2. The ZTP Bootstrap Server sends the boot file to the Off-Network PNF (CPE). NETCONF/YANG is preferable, as described in draft-ietf-netconf-zerotouch. This is out of scope BBF specification.
3. The CPE implements the boot file and sends the "Ready to be managed" message to the PNF SDN Mngt & Ctrl.

4. The Nf-Vi interface is up and running and the CPE NFVI is ready for vBG instantiation.
5. Ve-Vnm-vnf interface is up and running and the vBG is instantiated by the VNFM.
6. The VNF SDN Mngt & Ctrl performs the configuration of the WAN Interfaces on CPE to create VPN tunnels to other vBGs, which are controlled by the vBG Provider.

The service graph associated with this Use Case is depicted in Figure 51.

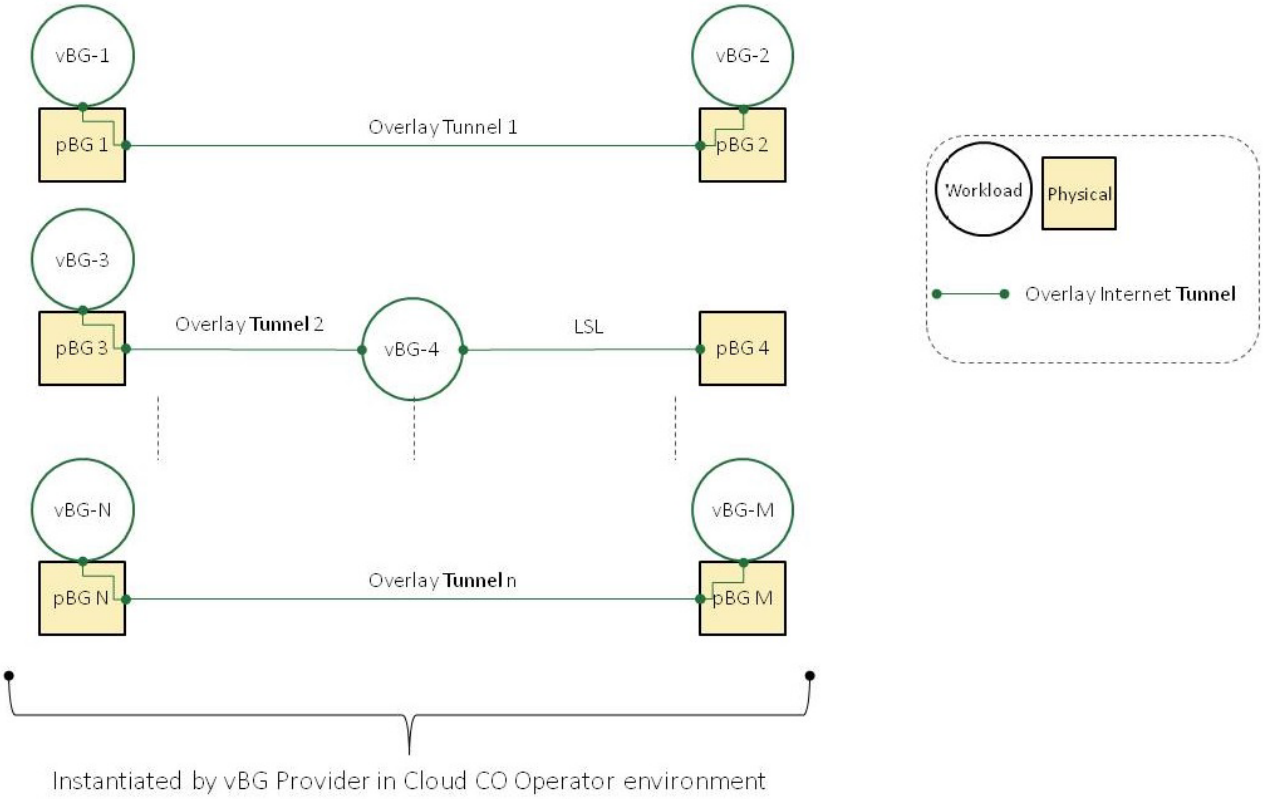


Figure 51: Service graph applied for above Use Case in Off-Network model

This Use Case provides the basic VPN tunneling functionality, which is also known as “SD-WAN Solution”. An advanced Use Cases can become available on top of it, which is also known as “SD-WAN Service”, but which is out of the scope of this document. Such “SD-WAN Service” examples are:

- Service Function Chaining.
- Multiple tunnels between two vBG.
- Full Mesh topology between vBG on Service Graph.

7 Next Steps

The content of this Technical Report can be used:

- To provide guidance on how the CloudCO architectural framework can be applied in Use Cases.
- To derive the Application Notes, mentioned in TR-384 that will lead to a detailed description of how interfaces between CloudCO functional elements need to function, and what attributes need to be exchanged to make the Application Note work.
- Together with the Application Notes and Interface descriptions to derive the CloudCO Test Cases.

End of Broadband Forum Technical Report TR-416

© The Broadband Forum. All rights reserved