
**ATIS-0200012**

ATIS Standard on -

# NFV FORUM USE CASES

As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global ICT companies to advance the industry's most pressing business priorities. ATIS' nearly 200 member companies are currently working to address the All-IP transition, network functions virtualization, big data analytics, cloud services, device solutions, emergency services, M2M, cyber security, network evolution, quality of service, billing support, operations, and much more. These priorities follow a fast-track development lifecycle — from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open source solutions, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). The organization is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of and major U.S. contributor to the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org.




ATIS-0200012, *NFV Forum Use Cases*

Is an ATIS Standard developed by the **ATIS Network Functions Virtualizations Forum (NFV)**.

*Published by*

**Alliance for Telecommunications Industry Solutions**
**1200 G Street, NW, Suite 500**
**Washington, DC 20005**

**ATIS-0200012**

ATIS Standard on

# NFV Forum

# Use Cases

**Alliance for Telecommunications Industry Solutions**

Approved May 2015

**Abstract**

Network Functions Virtualization (NFV) and Software Defined Networking (SDN) are part of a sweeping evolution that is moving the ICT industry from integrated, hardware-centric solutions to modular, hardware-agnostic frameworks by abstracting the hardware resources into a consistent operating environment for the software.

This Document defines priority use cases, such as virtual network operator, that emphasize the benefits of NFV in a multi-administrative domain environment and require improved service integration and portability between network operators, web scale companies, and enterprises.

## Foreword

The Alliance for Telecommunications Industry Solutions (ATIS) serves the public through improved understanding between carriers, customers, and manufacturers. The Network Functions Virtualization (NFV) Forum provides the inter-provider technical requirements and solutions to help ICT companies realize the benefits of rapidly advancing software-defined networking and NFV technologies.

The mandatory requirements are designated by the word *shall* and recommendations by the word *should*. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages. The word *may* denotes an optional capability that could augment the standard. The standard is fully functional without the incorporation of this optional capability.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, NFV-F, 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time of consensus on this document, NFV-F, which was responsible for its development, had the following leadership:

T. Anderson, NFV-F Co-Chair (Cisco)

B. Campbell, NFV-F Co-Chair (Oracle)

L. Laporte, Technical Editor (Sprint)

**Table of Contents**

## Table of Figures



## Table of Tables

ATIS Standard on –

# NFV Forum Use Cases

# 1 Executive Summary

## *1.1 Background*

Network Functions Virtualization (NFV) and Software Defined Networking (SDN) are part of a sweeping evolution that is moving the Information and Communications Technology (ICT) industry from integrated, hardware-centric solutions to modular, hardware-agnostic frameworks by abstracting the hardware resources into a consistent operating environment for the software.

It has been identified that among the emerging business opportunities enabled by these programmatic frameworks, one of the most consequential impacts of this implementation is the ability to integrate software across one or more administrative domains, in a uniform and automated way, and to scale application instances to meet changing demand.

## *1.2 Problem Statement*

Virtualization of network functions provides operators with opportunities to create and offer network services that can cross one or more administrative domains (e.g., spanning combination of communications service providers, enterprise, over-the-top providers, public safety entities). By placing some, or all, of the network functions needed for a given service in the tenant domain of another service provider, a provider may lower economic barriers to virtual network operations, roaming, and virtualized network function-as-a-service business opportunities, among others.

To ensure that standards for NFV meet the needs of a multi-administrative domain environment, reference use-cases are required to represent and develop specific technical and business opportunities.

## *1.3 Objective*

Creation of network services as discussed above will require identification of key parameters necessary for establishing a network service composed of virtualized network functions residing in multiple administrative domains. The objective of this document is to define priority use cases, such as virtual network operator, that emphasize the benefits of NFV in a multi-administrative domain environment and require improved service integration and portability between these administrative domains.

## *1.4 Scope*

The specification defines use cases that emphasize the benefits of NFV in a multi-administrative domain environment. These use cases include wireline, wireless, cable, and enterprise scenarios. The intent of this Document is to build on the ETSI ISG on NFV work and to be complementary with other work that is being developed in the industry.

The following use-cases are included:

- Virtual Network Operator – a network operator that virtualizes some or part of their network
- Cooperative, Cloud-Based CDN Arrangements
- Virtualized Content Delivery across Multiple Access Domains by using a Virtualized CDN
- Roaming – improving the efficiency of service provision to mobile roaming subscribers
- Efficient Home Routed VoLTE Roaming Arrangements
- Efficient Enterprise Voice/Collaboration Arrangements

- Enabling Service Function Chains with Third Party VNF Application Providers
- Enabling Third Party VNF Applications

## 1.5 Assessment & Conclusions

Use cases for multi-administrative domain NFV have been identified which are highly relevant to today's needs of wireline, wireless, cable, and enterprises. These use cases are not yet addressed in the available NFV standards and further activity to define requirements and technical solutions will enable new business opportunities based on open standards to the communications industry.

In assessing the set of use cases as a whole, we see that in all cases, a service/application is being delivered to an end-user as enabled by service/application functions physically located in multiple administrative domains. Each of these functions is under the control of the administrative domain which is offering the service/application. However, any of the functions may be physically located in a separate administrative domain. The controlling administrative domain is delivering the service with assistance from other (host) administrative domains by specifically:

- Choosing service or application elements from a catalog of available services in the host administrative domain(s) and/or
- Instantiating their own service/application function in the host administrative domain itself.

In effect, the service delivered to the end-user is comprised of an inter-administrative domain service chain.

The use cases further identify the specific business value of these arrangements (for all administrative domains involved) as well as the added value delivered to the end-user.

In order to support efficient deployment of these inter-administrative domain use cases, mechanisms should be put in place to create a set of service capabilities, including standard capabilities provided by multiple administrative domains, described in a standardized manner (e.g., a service catalog). This would better allow a controlling administrative domain the ability to see what is being offered by other administrative domains in a clear, unambiguous, structure to support inter-administrative domain service creation.

## 1.6 Recommendations

It is recommended that organizations working towards the support of NFV utilize these use cases to help create their requirements and technical solutions.

Specifically it is recommended that the ATIS NFV Forum continues this work by capturing technical requirements from these use cases. This analysis should consider:

- Existing industry state of the art and how the use cases may be met by evolving technologies;
- Different ways the use case could be implemented which will effectively identify various architecture options and their associated requirements;
- Issues that arise as edge cases when the use cases are considered as inter-provider implementations of different architectural options;
- Common requirements across use cases and architecture options as well as where differences exist; and
- Mechanisms such as shared service enabler catalogs to enable standardized service descriptions between administrative domains.

# 2 References

The following standards contain provisions which, through reference in this text, constitute provisions of this Document. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this Document are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

[3GPP 23.401], 3GPP 23.401 "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access"[1]

# 3 Definitions, Acronyms, & Abbreviations

## *3.1 Definitions*

For a list of common communications terms and definitions, please visit the ATIS Telecom Glossary, which is located at < http://www.atis.org/glossary>.

**3.1.1 devOps:** In the context of this document, devOps refers to the synthesis of operations methods, procedures, and staff with those of development and integration resulting in a new role whose staff rapidly brings new capabilities from ideation to instantiation.

**3.1.2 Service:** A set of functionality enabled by a provider for customers – e.g., providing IP with QoS connectivity, providing an IPTV service, providing instant messaging (IM) public connectivity.

**3.1.3 Service Function (SF):** Service Function is responsible for a specific function within a network infrastructure, which has well-defined external interfaces, which can be a virtual instance or be embedded in a physical network element.

**3.1.4 Service Function Chain (SFC):** A service function chain defines an ordered set of service functions that must be applied to packets selected as a result of classification. The implied order may not be a linear progression as nodes may copy to more than one branch.

**3.1.5 Administrative Domain (AD):** A collection of systems and networks operated by a single organization or administrative authority.

**3.1.6 Inter-administrative domain service function chaining:** The application of Service Function Chaining to scenarios that involve Service Functions in multiple Administrative Domains.

**3.1.7 Virtual Network Operator (VNO):** An entity that does not own a telecom network infrastructure but provides telecom services by purchasing capabilities from telecom carriers.

## *3.2 Acronyms*

AD – administrative domain

API – application programing interface

APN – access point name

B/OSS – business/operations service support

CDN – content distribution network

CPE – customer premises equipment

[1] This document is available from the Third Generation Partnership Project (3GPP) at < http://www.3gpp.org/specs/specs.htm >.

FMC – fixed mobile convergence

ICT – Information and Communication Technology

IMS – IP multimedia subsystem

LBO – local break-out

NS – network service

NSP – network service provider

PCRF – policy and charging control function

PGW – packet gateway

PNF – physical network function

PSAP – public safety answering point

PSTN – public switched telephone network

QCI – QoS class identifier

QOE – quality of experience

QOS – quality of service

RCS – rich communication suite

SIP – session initiation protocol

SP – service provider

UE – user equipment

USIM – universal subscriber identity module

VNF – virtual network function

VNO – virtual network operator

VoLTE – voice over LTE

VPN – virtual private network

# 4 Use Cases

The following use cases have been produced by the ATIS NFV Forum with contributions from the ATIS TOPS Council SDN/NFV Focus Group.

## *4.1 Virtual Network Operator*

### 4.1.1 Story Highlights

Entities wishing to offer specialized (or otherwise) telecommunication services may opt to virtualize some or part of their network in order to reduce their startup capital and/or operational needs. These entities may be considered Virtual Network Operators (VNO). For the purposes of this document, a VNO is considered as "*an entity that does not own a telecom network infrastructure but provides telecom services by purchasing capabilities from telecom carriers*" (modified version of http://www.gartner.com/it-glossary/virtual-network-operator).

A VNO can be facilitated through the use of tenant domains, which are administratively and operationally separate from the Host Service Provider's network. The functions/applications required to complete a given service are instantiated via cross-administrative domain service function chaining. These

functions/applications can be within the VNO, in the host SP network, in another SP network, or any combination of the three.

Virtualization of network infrastructure and/or applications additionally affords any service provider the alacrity to instantiate new (or expand existing) services rapidly via the devOps operational paradigm. Such service agility affords the opportunity to rapidly trial services, cull those that don't work, and exploit those that do. Long-tail business models can also be more readily supported as the marginal cost of maintaining such business may be substantially lower than by today's deployment and operational models.

Since a VNO may not have sufficient resources (e.g., staff and/or finances) with which to launch its business, an alternative approach to developing services may be warranted. Specifically, one or multiple functions/applications needed for a given service may be a virtual network function residing outside of the VNO's network. Some VNOs may utilize physical network functions for a vast majority of their service, but rely upon virtualized network functions to complete their service portfolio. As an extreme example, one can envision a VNO that owns no physical infrastructure of its own, relying entirely upon virtualized functions to provide both core services (i.e., those necessary to establish voice and/or data sessions) and value added services (e.g., html header enrichment, data accelerators, deep packet inspection, filtering proxies, location). With a rich ecosystem of network functions, a VNO (or any network operator) could be afforded the capability of selecting the best components (based on price, performance, etc.) with which to create a service.

### 4.1.2 Business Drivers

VNOs provide a lower barrier to market entry for entities that do not have sufficient capital and/or interest available with which to build and operate a network. Typically, these opportunities represent segments that are outside the "typical" network operator's scope and/or interest, such as long-tail business opportunities which are constrained by time, location, affinity group, etc. The business drivers for the virtual network operator in a virtualized tenant domain include:

- low- to no-capital expenditure;
    - linearized opex model (pay-as-you-grow).
- ease of expansion as the customer base grows;
- elimination of:
    - procurement;
    - hardware maintenance;
    - hardware inventory (deployed assets and spares);
- rapid time-to-market for new services;
- reduced need for specialized developers;
- ability to focus on core business functions; and
- opportunities for new business models and relationships (e.g., Infrastructure as a Service, VNF as a Service).

### 4.1.3 Deployment Models

Table 4.1 shows a summary of the many possible combinations for cross-administrative domain service function chaining between three different types of actors: a) the VNO; b) a Hosting Network Service Provider (providing physical access and potentially hosting network functions); and, c) Other Network Service Provider. Further complexity could be enumerated by considering the Network Function Service Provider (as shown below in Figure 4.9). However, the added complexity is not warranted as this case appears to be identical to the Other Network Service Provider in terms of the constraints that are imposed on the solution space.

**Table 4.1 – Possible Combinations for Cross-Administrative Domain Service Function Chains**

| | VNF Provided By: | | |
|---|---|---|---|
| **Deployment Model** | **Other Network Service Provider** | **VNO** | **Hosting Network Service Provider** |
| 1 | | | 100% |
| 2 | | 100% | |
| 3 | 100% | | |
| 4 | % | | % |
| 5 | % | % | |
| 6 | | % | % |
| 7 | % | % | % |

TABLE NOTE: % indicates that some of the virtual network functions needed for a network service are provided by the given entity. 100% indicates that all of the virtual network functions needed for a network service are provided by the given entity.

The first three deployment models do not require any service chaining between administrative domains and are thus excluded. We will thus only focus on the last four deployment models. Of these, deployment models four, five, and six are essentially equivalent in their descriptions and interworking of the various actors. Deployment model seven is clearly distinct from models four, five, and six as it comprises service function chaining across multiple administrative domain boundaries.

### 4.1.4 Actors

- Virtual Network Operator – entity that utilizes virtualized network components, residing in a tenant domain of a Hosting Network Service Provider data center, to offer commercial service to businesses and/or consumers.
- Network Service Provider – entity offering commercial telephony and/or network services (e.g., CableCo., Broadband, Wireless) to businesses and/or consumers. In addition, an NSP may function as an:
    - Hosting Network Service Provider – entity that operates a virtualization data center for use by VNOs and others.
    - Other Network Service Provider – a service provider other than the Hosting Service Provider.
- Network Function Service Provider – an entity that only provides Virtualized Network Functions and does not provide any Information and Communication Technology (ICT) services to either consumers or businesses.
- Transit Service Provider – an entity across which virtual links that interconnect all or part of a service function chain are hosted. This may be a distinct entity from those providing virtualized network functions, but will most likely be one or more of the entities involved in the service function chain.

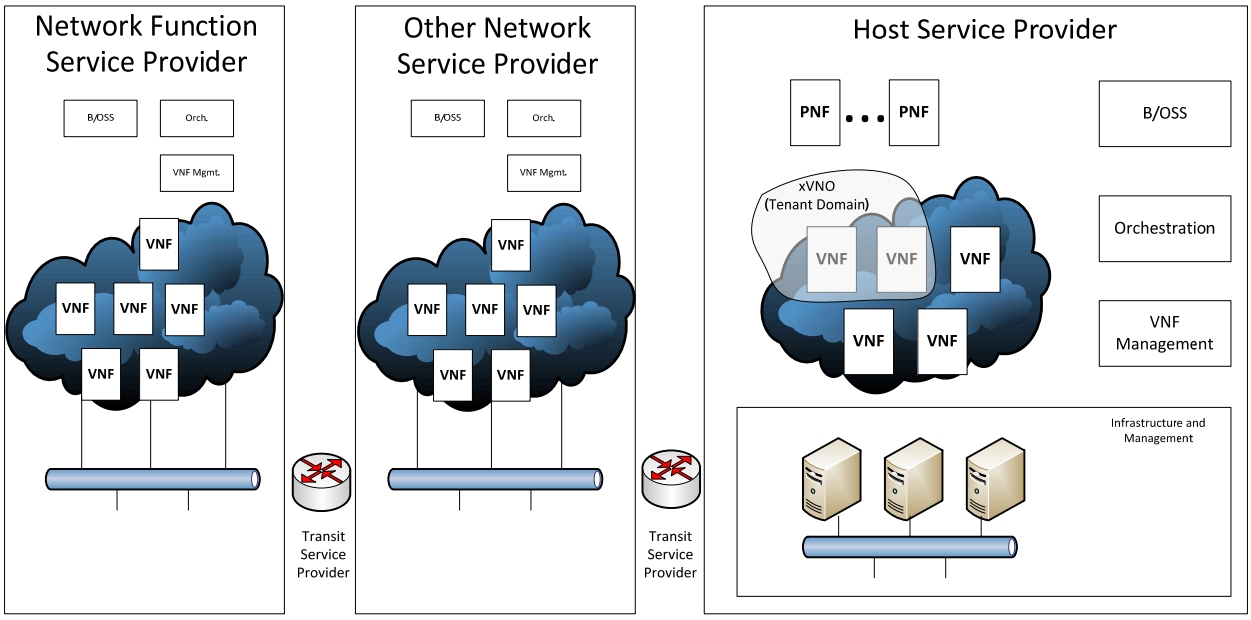


**Figure 4.1 - Actors that may participate in a service function chain**

### 4.1.5 High Level Architectural Attributes

#### 4.1.5.1 Deployment Models 4, 5, & 6

The architecture of the first scenario, representing deployment models 4, 5, and 6, is depicted in Figure 4.2, below. Rather than depict the entirety of the service function chain, we will simplify the depiction by only showing the necessary elements and some key interfaces that need to be considered.

The virtual network operator's DevOps console is represented by user "A" in the upper left-hand corner of the Figure 4.2. There are two basic options that warrant consideration:

1. The VNO configures their network services via an interface to the hosting network service provider's OSS. This would be in the form of a (semi)-customized GUI from which network services are defined, lifecycle is managed, performance and faults are observed, etc. In this case, network details are largely obscured from the VNO and the VNO's ability to create and manage their virtual network and services is constrained by what is exposed by the hosting network service provider. The hosting network service provider manages the virtual infrastructure, policies, lifecycle, VNF catalog, allowable virtual machine parameters (e.g., memory, IO, CPU, and storage), and decides what is exposed to the VNO.
2. The VNO has direct access to the orchestrator and, by inference, the VNF manager, and the VNF infrastructure manager as represented by the grey boxes on the left of each of these functional blocks. Network service orchestration, policy management, VNF lifecycle, service function chaining, etc., are now all under the direct control of the VNO. Such a scenario requires, at a minimum, role-based access control, security, and policy mechanisms to limit the VNO's span of control.
3. We do not consider the case where the VNO "owns and operates" its own virtualization environment (i.e., orchestrator, NFV manager, VNF infrastructure manager, virtual infrastructure). In this case, the VNO would be considered either a Network Function service provider or a Network service provider (albeit utilizing virtualized means).

In Figure 4.2, the red line represents a service function chain that is composed of two virtualized network functions VNF_1 and VNF_2. The number of VNFs is arbitrary and there could be any number in either of the two administrative domains shown. At a minimum, one in each administrative domain is necessary in this scenario.

Regardless of which of the above options are operative, the key question is the nature of the interaction with VNF_2, which resides in the hosting network service provider's administrative domain. Some issues that must be considered include:

- How is VNF_2 managed and included in a service function chain when it is under the control of the hosting network service provider?
- VNF_2 may appear as a node in a VLAN, thus participating in an IP administrative domain, but how is VNF_2 described in the service function chain?
- How is policy decided (i.e., is there an agreed-upon meta-model amongst the actors)?
- How are VNF flavors determined and scaling accomplished so as to assure consistent QoS/QoE for the entire network service?
- How are changes in the service function chain propagated to all involved components?
- How is VNF-2 monitored?
- How are faults in VNF-2 mitigated and managed?
- How is billing-related information captured?

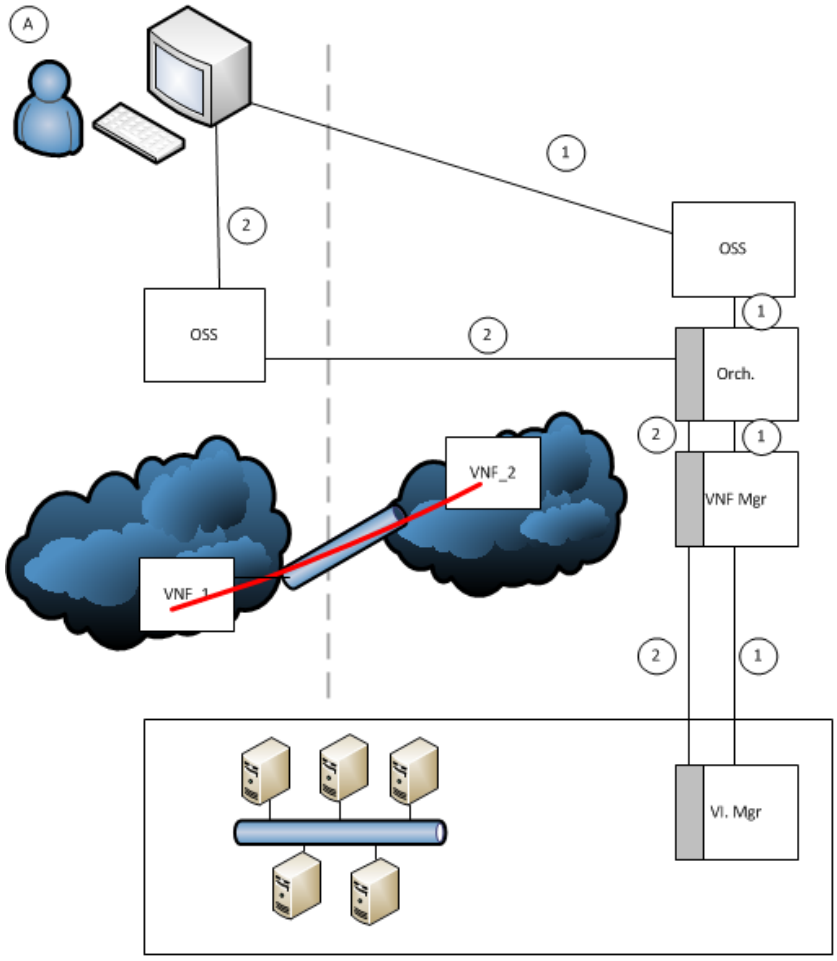


**Figure 4.2 – First scenario option for VNO**

### 4.1.5.2 Deployment model 7

Our second scenario is depicted in Figure 4.3 below where the red line represents a service function chain (SFC) spanning multiple administrative domains. Rather than depict the entirety of the SFC, we will

simplify the depiction by only showing the necessary elements and some key interfaces that need to be considered.

It should be noted that a possible permutation of this scenario includes the case where one of the entities is a network function service provider. Such a network function service provider could supply access to content that is needed on an ad-hoc basis or where it is otherwise uneconomical for a network operator to have a persistent license. This type of permutation would allow for capturing long-tail and/or dynamic business opportunities that are not currently feasible.

One aspect of this use case, which is potentially applicable to all involved entities, is service discovery. As a service provider (either network function or network) enables new network functions they could elect to make these functions discoverable to other entities. Doing so facilitates the creation of a new ecosystem where entities may shop a marketplace of virtualized network functions and utilize those that best suit their business needs. Such an ecosystem contributes to the creation of services on demand where it is not economically viable for an entity to have a perpetual license for a given subcomponent of a network service.

As in the previous scenario, the DevOps console of the VNO is shown as A, but this time in the top center of the figure (see Figure 4.3). As with the previous scenario, in order to create the complex service function chain, the VNO will need to access either the OSS or the Orchestrator that resides in other administrative domains.

In this scenario, the VNO will need to orchestrate the chaining of VNF's across three distinct administrative domains. Unlike the previous scenario, the present scenario has four basic options that warrant consideration:

1. The VNO configures their network services via an interface to the OSS of each of hosting network service providers. This would be in the form of a (semi)-customized GUI or abstracted API from which network services are defined, lifecycle is managed, performance and faults are observed, etc. In this case, network details are largely obscured from the VNO and the VNO's ability to create and manage their virtual network and services is constrained by what is exposed by the hosting network service provider. The hosting network service provider manages the virtual infrastructure, policies, lifecycle, VNF catalog, allowable virtual machine parameters (e.g., memory, IO, CPU, and storage), and decides what is exposed to the VNO.
2. The VNO has direct access to the orchestrator and, by inference, the VNF manager, and the VNF infrastructure manager of each hosting network service provider (as represented by the grey boxes in each of these functional blocks). Network service orchestration, policy management, VNF lifecycle, service function chaining, etc., are now all under the direct control of the VNO. Such a scenario requires, at a minimum, role-based access control, security, and policy mechanisms to limit the VNO's span of control.
3. Split model where option 1 is utilized for one of the hosting network service providers and option 2 is utilized for the second hosting network service provider.
4. We do not consider the case where the VNO "owns and operates" its own virtualization environment (i.e., orchestrator, NFV manager, VNF infrastructure manager, virtual infrastructure). In this case, the VNO would be considered either a Network Function service provider or a Network service provider (albeit utilizing virtualized means).

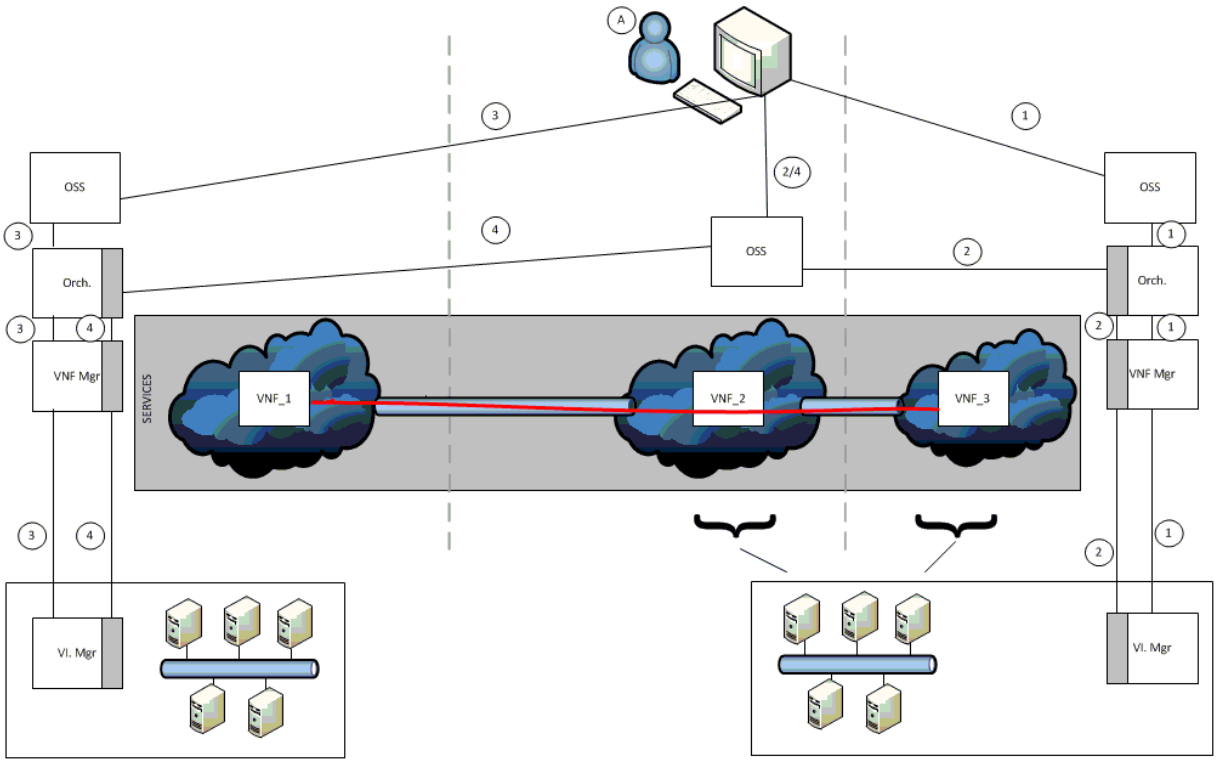


**Figure 4.3 - Second scenario option for VNO**

In order to instantiate a network service in this scenario, some of the following issues must be considered:

- Service discovery.
  - How are services discovered and utilized by various entities?
  - Are services openly advertised or limited?
- Policy.
  - Disjoint policy parameters/semantics between Ads.
  - How are policy updates perpetuated between ADs?
- VNF Flavors/Network Service flavors.
  - Standardized semantics to describe flavors.
  - How will E2E service scale?
- VNF issues.
  - Standardized semantics for VNF descriptors and packages.
- Cross carrier billing and accounting.
  - Resource (infra, transport, VNF) identification.
- Fault detection.
  - How will faults and performance be handled across ADs?
- How is real-time service instantiation addressed?
- Cross domain orchestration.
  - Inter-orchestration (likely) or inter-OSS? In either case, need to define how service function chains will be constructed and orchestration “orchestrated” between Ads.
- Security.
  - Application and Network.
  - Lawful Intercept.
  - 911 – (e.g., text to 911, application to 911, etc.). Who owns routing to the PSAP? (third NPRM FCC 14-118 – text to 911).

## *4.2 Cooperative, Cloud-Based CDN Arrangements*

### 4.2.1 Story Highlights

CDNs provide a common focal point for thousands of brands to access multiple services on multiple carriers – providing added functionality and application awareness. By instantiating CDN technology as a tenant in the service provider network, the CDN can effectively be deployed much closer to the network edge while enabling new services and capabilities by taking advantage of network information such location, subscriber attributes and application attributes available to the network.

The key aspect of this use case centers on a service provider's ability to open a tenant environment for a CDN provider to allow the CDN provider to instantiate and manage CDN specific services and functions in the service provider network. This allows the CDN and network infrastructure to more easily exchange information and control/policy directives to create/manage new service capabilities such as:

- Navigation applications in the cloud with a content provider/mobile operator agreement. For example, real-time user location data along high-traffic information can be used to inform applications of traffic jams.
- Cell site identification can be made to work in any app/browser using OS and a client.
- Subscriber identification and authorization via a webservice. Unique subscriber identity for payments/authentication.
- Respond to Network Conditions with Adaptive Image Compression.
- Application awareness using an operator asset (e.g., PCRF) to accelerate both fixed and mobile applications with critical performance needs.

To enable these capabilities, the service provider may choose to avail an interface (e.g., through an API within the virtual environment) to exchange network information (such as location and network congestion information) and policy directives with the CDN instance.

### 4.2.2 Business Drivers

CDNs already connect a multitude of content providers and network operators for better visibility and ecosystem collaboration. By enabling the CDN provider to instantiate its CDN solution in the network operator's edge infrastructure, we can more efficiently:

- Enable Application Aware servicers where both operators and the CDN provider can understand the network context on an app by app basis, exposing the right assets per application.
- Apply technology to accelerate content while better utilizing network resources and information.

Improve end user quality of experience with more expansive relationships providing value added services.

### 4.2.3 Deployment Model

It is envisioned that the proposed use case is implemented by enabling the network operator to offer a hosted tenant environment specific for the CDN provider with access to:

- The bearer/user plane traffic (e.g., on the SGi interface for mobility).
- Policy interfaces (e.g., PCRF Rx) to support policy based services.

Performance, location, application and subscriber information known by the network (e.g., mobile ECGI/Cell site, subscriber profile).

### 4.2.4 Actors

- Network Service Provider (both mobile and wireline).
- CDN Provider.

### 4.2.5 High Level Architectural Context

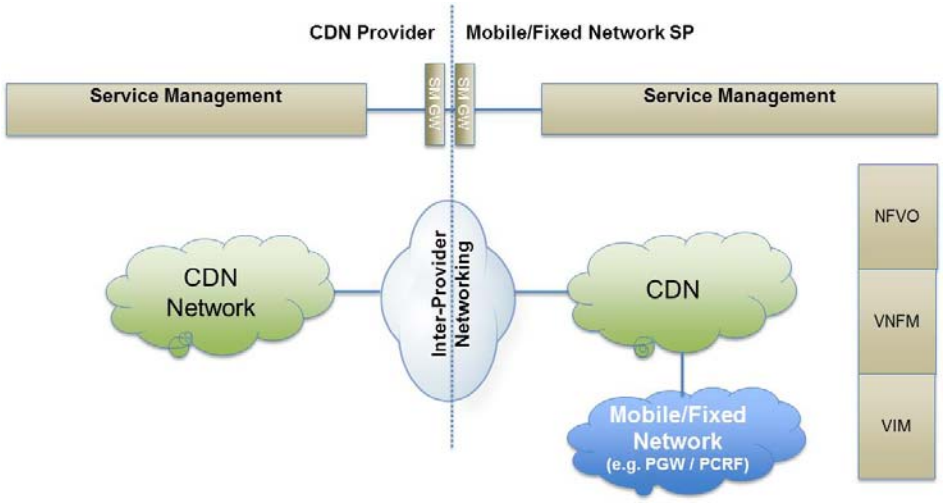


**Figure 4.4 - High-level Functional Distribution in a Cooperative, Cloud-based CDN**

Architectural attributes (functional view):

The CDN Provider would use NFV orchestration standards to manage the CDN as a tenant in the network service provider's network.

The interface/API between the Mobile/Fixed Network and the CDN cloud would include:

- User plane traffic interface (SGi interface for mobile networks).
- Rx policy interface to allow the CDN to manage QoS and policy for CDN flows.
- Other OAM related interfaces/APIs to avail network, subscriber, or application information available to the network. These APIs may or may not be standard and are outside the scope of this document.

The Service Management (SM) Gateway interface is intended to show the necessary interconnection to allow the CDN provider to life-cycle manage VNF software and images located in the mobile/fixed service provider network.

## *4.3 Virtualized Content Delivery across Multiple Access Domains*

### 4.3.1 Story Highlights

The virtualized CDN domain would be capable of distributing content across wireless, wireline, and cable access domains from locations designed to support these multiple access types. This system utilizes common hardware and virtualization layers to elastically scale CDN virtual functions assigned to each access type as users transition their content consumption from mobile, fixed, and WiFi.

The flexible allocation of virtualized CDN software to a common pool of hardware allows the applications to be scaled with user demand while improving utilization of the underlying hardware. Previous tight coupling of hardware and software increased the likelihood that the CDN system will have stranded capacity and/or will be unable to meet peak demand.

### 4.3.2 Business Drivers

Content-based applications and services driving large increases in traffic stress peering, core and access networks. At the same time, time-of-day, special events, and other factors vary demand patterns on wireless, wireline, and cable.

The content delivery is further complicated by variability in packaging with specific protocols, codecs, targeted screen size, and often DRM requirements depending on the device and method of delivery. The wide array of requirements and demand complicates deployment of purpose-built systems and makes a flexible system attractive.

Service providers that operate multiple access networks have the need to share contents among different access venues to save content ownership and delivery costs.

The resulting solution increases content distribution efficiency and flexibility through distributed and converged (wireline/wireless/cable) SDN/NFV-based CDN use cases.

### 4.3.3 Deployment Model

The proposed deployment model establishes a separate CDN administrative domain that is separate from the access domains and replaces purpose-built deployments with a flexible CDN system that can deliver content to wireless, wireline, and cable users depending on demand.

- Consolidated content catalog where all access domains view the same available content and end users have access to that content across domains.
- Segregated content catalog where each access domain has an independent content catalog and end users only have access to content within the domain.

### 4.3.4 Actors

- Content Administrative Domain – The Content Administrative Domain supports CDN resources that store and distribute content in a manner consistent with the format and mechanism required by the end user and while enforcing the distribution rules or the content (e.g., licensing agreement).
- Access Administrative Domain (e.g., Wireless, Wireline, Cable) – The access network provides last mile connectivity between the user and other network destinations.
- End User – The end user is the target of the distributed content.

### 4.3.5 High Level Architectural Context

The functional delivery of content from the CDN through the access network to the end user is unchanged, but virtualizing the CDN components into a separate content delivery domain provides flexibility in allocation of processing and storage capacity across the specific access domains. Each access administrative domain continues to support management of the end user device, but content requests are orchestrated across the domain boundary to a consolidated content delivery administrative domain. Each access domain calls these functions using a common service catalog that is specific to the virtualized environment. This construct also aggregates and simplifies content licensing into a single system.

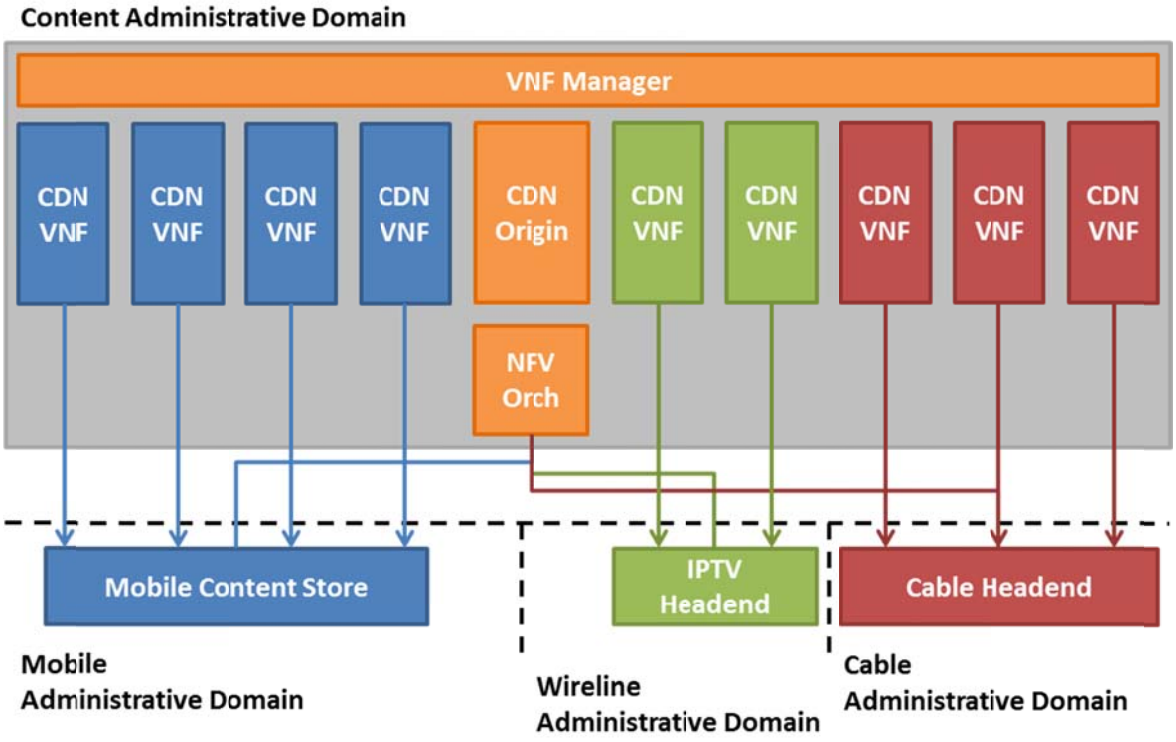


**Figure 4.5 - High-level Functional Distribution for Virtualized Content Delivery Across Multiple Domains**

## *4.4 Roaming*

### 4.4.1 Story Highlights

Roaming is a very common behavior for subscribers in mobile networks. In the current mode of operation (home routing) the roaming subscriber's services are anchored in the home network. The practical impact of home routing is a limitation on the portability of any given data service when crossing service provider network boundaries.

In this use case, a Home Network Service Provider (Home NSP) deploys instances of certain network functions in the tenant domain of a roaming partner to provide a network service (NS) utilizing local break out, thus eliminating expensive (from a cost and performance perspective) routing to the home network. These network function instances may be deployed on an ad-hoc basis or semi-permanent basis depending upon the Home NSP's needs. In doing so, roaming subscribers may experience continuity of data services as they move from network to network. Voice over LTE is a particular service that could benefit from such a scenario by locally breaking out to virtualized applications in the Visited Network Service Provider's tenant domain.

Regardless of the longevity of the virtualized NS, in order for the Home NSP to provide such a roaming service, the Home NSP will need to on-board, instantiate, maintain, monitor, recover, and remove virtualized network functions in the Visited NSP's data center. Additionally, a clear mechanism to allow for inter-operator billing as well as creation of call detail records for customer billing of the virtualized services will be paramount.

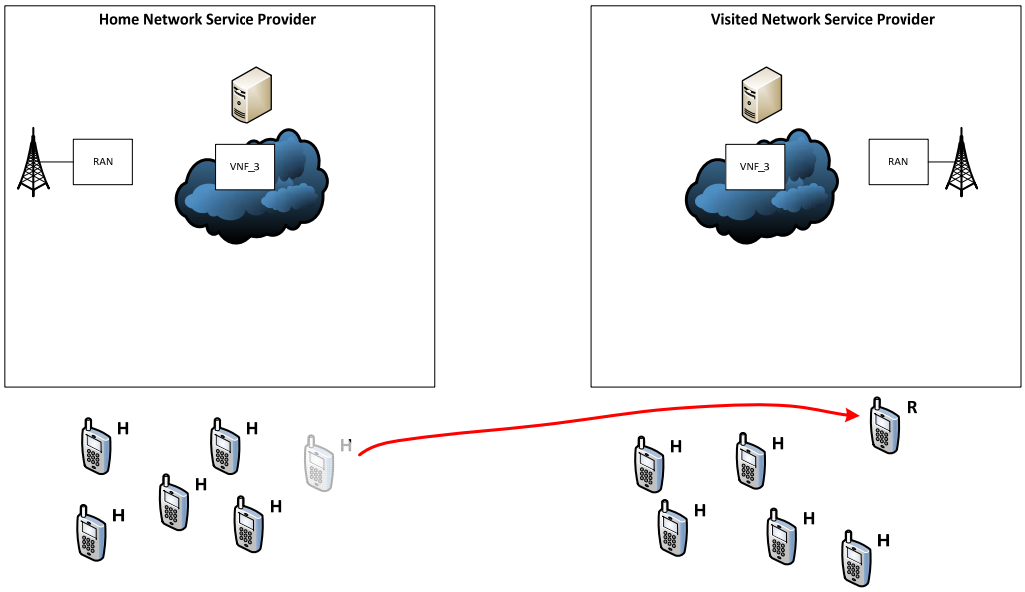


**Figure 4.6 - Actors that may participate in the roaming use case**

Figure NOTE: The user engaged in roaming is depicted by the shaded device in the Home Network Service Provider domain with the red arrow leading to the device marked with an "R" in the Visited Network Service Provider domain.

### 4.4.2 Business Drivers

Virtualization of network functions in a Visited Network Service Provider is undergirded by the following business drivers:

- Increased customer satisfaction due to service continuity.
- Decreased churn arising from increased customer satisfaction.
- Increased revenue opportunities for both Home and Visited NSP's as subscribers consume data services out of the home network.

### 4.4.3 Deployment Model

In this use case, there are three possible deployment models, but only two will be considered. The options are shown in Table 4.2, below. Scenario 0 will not be considered as it does not require any cross-administrative domain service function chaining nor is it a roaming scenario, but is presented for completeness of the discussion. The latter two scenarios vary in degree with respect to the magnitude of the need to host VNFs and/or PNFs in the Visited Network Service Provider's tenant domain. Factors that tip the scale between Scenario 1 and Scenario 2 include:

- Sensitivity of any database that is needed for a VNF;
- Latency and/or jitter concerns; and
- Interconnection agreement terms and conditions.

It is possible that some functions and related service function chains may employ Scenario 1 while others, within the same set of actors, may employ Scenario 2. The decision as to what scenario to utilize, when, and for how long, is an implementation decision that will not be addressed here. It should be noted here that the service function chain may also incorporate physical network functions (PNFs) in the Home NSP, Visited NSP, or both. In this use case, we will only consider the case where the VNFs are utilized and utilization of PNFs is out of scope. We will leave for future study how to incorporate PNFs from either or both NSPs into the roaming service function chain. Also, we will leave detailed discussion support systems as out of scope.

**Table 4.2 - Major Deployment Scenario Considered in the Roaming Use Case**

| Major scenario | Home Network Service Provide hosts VNF's | Visited network Service Provider hosts VNFs | Scenario type |
|---|---|---|---|
| 0 | All | None | Non-Roaming |
| 1 | Some<br>(x%) | Some<br>(100% - x%) | Roaming |
| 2 | None | All | Roaming |

Table NOTE: The two categories refer to the extent of virtualized network functions instantiated in the Home Network Service Provider and Visited Network Service Provider, respectively. For the purpose of the use case the degree of virtualization split between Home and Visited NSP in Major Scenario 1 is not relevant; only the fact that the Home NSP has virtualized network functions in both.

### 4.4.4 Actors

The following actors are key to the present use case:

- Roaming subscriber – a subscriber who utilizes service outside of their home network.
- Home NSP – entity offering commercial telephony and/or network services to businesses and/or consumers. Each subscriber is associated to one Home NSP.
- Visited NSP – entity offering commercial telephony and/or network services to businesses and/or consumers and who may provide such service to subscribers with whom they have no persistent association, subject to agreements in place between the Home NSP and the Visited NSP.
- IP exchange provider – entity providing IP interconnection points between the Home NSP and Visited NSP in this use case.

### 4.4.5 High Level Architectural Attributes

The high-level architecture for both scenario 1 and scenario 2 is shown in Figure 4.7, below. For clarity, only VNFs, peering network, and basic wireless access network are shown. Figure 4.7 highlights three sub-scenarios as shown in Table 4.3. These sub-scenarios are depicted as the red lines in Figure 4.7. Sub-scenario A demonstrates a service function chain that is entirely contained within the tenant domain in the Visited NSP. Sub-scenario B shows a service function chain whose VNF's are wholly within the tenant domain in the Visited NSP, but which serves traffic to and from the Internet. Finally, sub-scenario C shows a service function chain that is composed of VNFs that are in both the Visited NSPs tenant domain and in the Home NSPs domain. In this latter case, there may be a need to instantiate the one or multiple VNFs in a specific NSP domain due to security concerns.

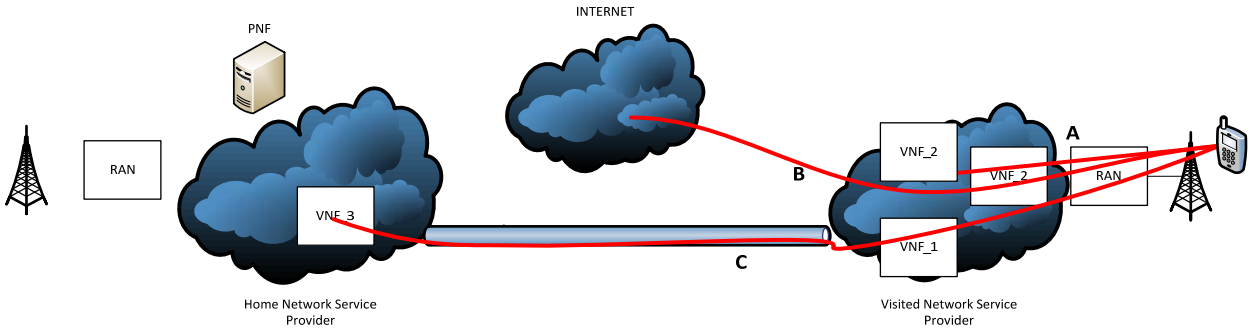


**Figure 4.7 - Three roaming sub-scenarios**

**Table 4.3 - Mapping of three roaming scenarios to the major deployment scenarios**

| Major scenario | Sub Scenario | Cross Administrative Domain SFC needed? | VNF Management and Orchestration Needed |
|---|---|---|---|
| 1 | C | Yes | Yes |
| 2 | A | No | Yes |
| 2 | B | No | Yes |

Sub scenario 1C, shown above in Figure 4.7 and Table 4.3, will be considered since it is the only one that will involve cross administrative domain service function chaining. The other two scenarios will require cross administrative domain VNF management and orchestration.

As briefly discussed in section 4.4.1, the Home NSP will require a consistent means of managing the VNF throughout its entire lifecycle. In order to manage the VNFs within the Visited NSP domain, the Home NSP will require a means of control of the virtualized network resources. Three main options present themselves, labeled 1, 2, and 3 in Figure 4.8. Option 1 will not be considered here as inter-OSS interactions and/or external OSS interfaces are typically highly customized and manifest to third-parties as pre-packaged user interfaces, with concomitant release-dependent features, functionalities, and process-encumbered development cycles. Options 2 and 3 represent essentially direct interactions between the Home NSP and the Visited NSP. Currently the existing NFV specifications do not address inter-Orchestrator federation (option 2), nor do the specifications currently address “layering” (as shown in the grey boxes in Figure 4.8) of the Orchestrator, VNF Manager, or Virtual Infrastructure Manager.

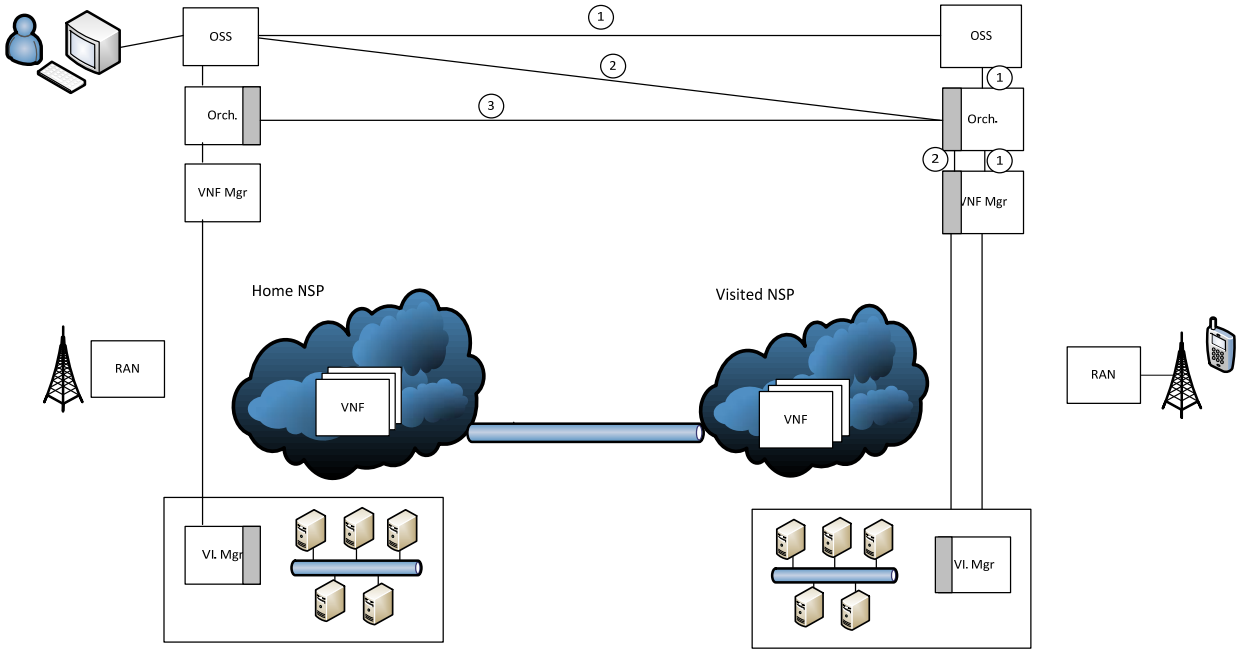


**Figure 4.8 - High-Level Architectural View for Roaming Use Case**

In order to facilitate the roaming use case, the following issues will need to be considered in detail:

- VNF package on-boarding.
- VNF lifecycle management.
- Affinity/anti-affinity implementation.
- End-to-end quality of service.

- Policy management.
- Fault management and mitigation.
- Performance monitoring.
- Subscription management.
- Fraud detection.
- VNF package validation.
- VNF authentication.
- Configuration, management, security, and maintenance of:
    - Data plane connection; and
    - Control plane connection.
- VNF descriptor nomenclature.

## *4.5 Efficient Home Routed VoLTE Roaming Arrangements*

### 4.5.1 Story Highlights

3GPP and GSMA have studied and implemented specifications for VoLTE roaming architecture models. Generally speaking, two broad options exist: one based on Local Breakout (LBO) and one based on the 3GPP 23.401 [3GPP 23.401] Home Routed architecture (Figure 4.2.2-1 in 23.401) commonly called S8 Home Routed (S8HR).

LBO options breakdown into 3 specific scenarios,

- Local Breakout with Home network Routed VoLTE (LBO HR).
- Local Breakout with Visited network Routed VoLTE (LBO VR).
- Local Breakout with Optimal Media Routing (OMR).

All of the LBO scenarios are characterized by the need for IMS (application specific) functions under visited network control (e.g., P-CSCF and session border control elements.) Alternatively, many operators favor the S8HR option which brings all roaming traffic back to the home network. In this case, all application functions are fully controlled and managed by the home network. The disadvantage of S8HR deployment scenarios is that all traffic is backhauled to the home network which could be geographically distanced from the visited network. This may result in non-optimal routing of traffic, particularly when the call is “local” to the visited network.

However, if the visited network opens a tenant environment to the home operator, the home operator can place the necessary application functions local to the visited network and still maintain full control of all application functions. Alternatively, the home operator could instantiate their application functions close to the visited point of presence using an independent data center hosting service.

### 4.5.2 Business Drivers

Common VoLTE roaming arrangements that use LBO mechanisms place both financial and operational constraints on the home service provider. For example:

- Since the visited network is providing application specific functions in LBO scenarios (e.g., P-CSCF and session border control functions for both signaling and data plane traffic), the cost of these functions must be passed on to the home provider.
- The visited application LBO functions are controlled, specified, and managed by the visited operator which limits the home operator’s ability to apply certain customer features to roaming calls. For example, Rich Communications Services (RCS) and more advanced IMS multi-media features may require additional features in the P-CSCF and border functions that may not be available from the visited network. Additionally, any custom home features that affect the P-CSCF or related bearer functions may not be possible in LBO options.
- These features may require special user plane charging/accounting and in that case, since the home operator may not have any visibility into that bearer traffic being processed and delivered by the visited network in LBO scenarios, charging mediation may be more difficult.

- Most data roaming is currently implemented using a home routed approach. As such, there is likely synergy and cost savings by utilizing the same mechanism for VoLTE traffic.

The financial and operational constraints placed upon the system due to an LBO arrangement can be addressed to a large extent through the use of an S8HR roaming arrangement. Financial impacts due to the backhaul of traffic to the home network can be largely addressed by enabling the home operator to instantiate their application functions in the visited network (or close to the visited point of presence using an independent data center hosting service).

### 4.5.3 Deployment Model

All deployment models for this use case utilize 3GPP 23.401 [3GPP 23.401] Home Routed architecture (Figure 4.2.2-1 in 23.401) commonly called S8HR. Within this model, two options would be considered:

- Instantiate home application functions (e.g., elements of VoLTE/IMS/RCS) within a tenant environment in the visited network. The visited network would expose home routed interfaces (e.g., S8, S6a).
- Instantiate home application functions (e.g., elements of VoLTE/IMS/RCS) within a tenant environment in a 3rd party data center host that is local to the visited network. Interconnection between this hosted home environment and the visited network could utilize standard IPX (GSMA IP Exchange) capabilities common to home routed data traffic delivery.

### 4.5.4 Actors

- Home Network Service Provider.
- Visited Network Service Provider.
- 3rd party NFV grade hosting service (local to the visited network geography).
- IPX operator.

### 4.5.5 High-level architectural context

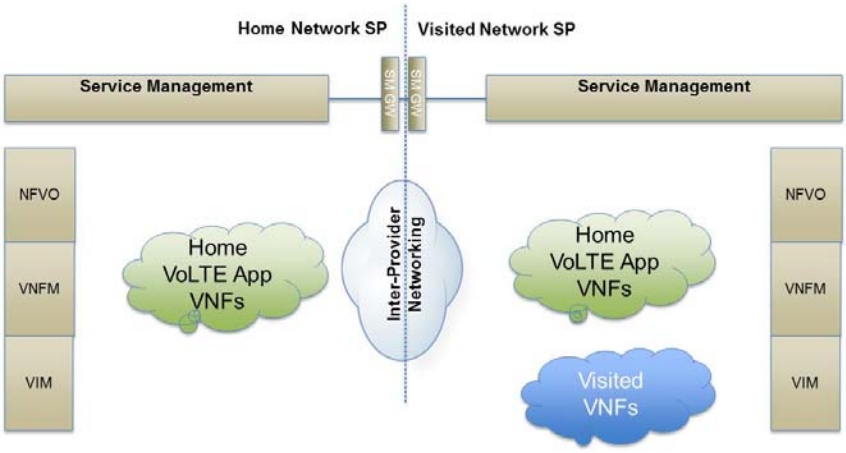


**Figure 4.9 - High-level Functional Distribution in an Efficient Home Routed VoLTE Roaming Arrangement**

Architectural attributes (functional view):

**Interfaces:**

- The interface(s) between the visited and home based "Home VoLTE App VNFs" are under the control and responsibility of the home network operator. For example, the home operator may establish a VPN to interconnect its home based elements with its application functions located physically in visited networks.
- The interface between the Home VoLTE App VNFs and the visited network would conform to standard home based routing procedures. For example IPX exchange services could be used to interconnect these two domains as is typical for home based routing of traffic.
- An interface will need to be made available to allow the home network operator to life-cycle manage VNF software and images located in the visited network (or in a local 3rd party hosting service provider).

**Visited Network Considerations:** The visited network would support standard home routed service with the additional support for all necessary VoLTE/RCS QCIs required by the home network. This would include policies to enable use of these QCIs and to create charging records as appropriate.

Support for regulatory services may require that encryption of the SIP signaling bearer (IMS Access Point Name – APN default bearer) to be disabled.

Emergency services could operate as before since typically, emergency services use a separate APN which could be routed to the visited network application functions.

### 4.5.6 Related & Derivative Use Cases

This use case is similar to the Roaming use except that the Roaming use case assumes the LBO option is being used. This use case assumes the S8HR option.

## *4.6 Efficient Enterprise Voice/Collaboration Arrangements*

### 4.6.1 Story Highlights

Many enterprises contract with one or more mobile service providers to create a managed VPN service where the mobile phones associated with the enterprise are configured to use a special APN for mobile data services. This APN is then connected directly to the enterprise's corporate data network. In effect, all mobile data traffic for these smartphones is routed directly to the enterprise with access to the enterprise corporate network. Further, the enterprise can then install applications on the mobile phone to support enterprise voice and collaboration services.

The mobile service provider can open a tenant environment for the enterprise to allow the enterprise to instantiate and manage their enterprise specific voice/collaboration functions in the mobile service provider network. This allows these application functions to better access QoS APIs for the enterprise APN in the mobile network and provide more efficient routing of traffic (e.g., enabling a breakout of traffic to the PSTN or Internet as appropriate). Additionally, the service provider may choose to avail an interface (e.g., through an API within the virtual environment) to pass network information (such as network congestion information) to the enterprise.

### 4.6.2 Business Drivers

Real-time services associated with voice and collaboration applications are very sensitive to QoS capabilities as well as backhaul and routing related latencies. These variables can be more efficiently managed for a good Quality of Experience (QoE) when voice/collaboration application functions can be placed at the edge of the network close to the subscriber.

This can be accomplished by creating a tenant environment in the mobile service provider's network to allow the enterprise to instantiate and manage their enterprise specific voice/collaboration functions. This allows these application functions to better access QoS APIs for the enterprise APN in the mobile network and provide more efficient routing of traffic (e.g., enabling a breakout of traffic to the PSTN or Internet as appropriate). Additionally, the service provider could provide network information (such as network congestion information) to the enterprise to enable the enterprise to make better application specific decisions relative to application specific bandwidth management. (e.g., control of a video codec) to better manage user QoE.

### 4.6.3 Deployment Model

This use case would be deployed on top of (in addition to) the typical enterprise VPN solution commonly offered by mobile service providers. The deployment model for enterprise VPN solutions typically include:

- Provisioning enterprise UEs with a USIM specifying a specific APN unique to the enterprise to be used for the data connection to the UE.
- The mobile service provider then provisions that APN to terminate to a PGW which then connects all APN traffic to the enterprise.

Given this base deployment, the proposed use case can be implemented in a number of ways including:

- The mobile service provider offers a tenant hosting environment local to the Enterprise APN PGW with access to the traffic on the SGi interface.

Alternatively, the enterprise VPN SGi traffic is forwarded by the mobile provider to a local third-party hosting service which has instantiated the enterprise voice/collaboration applications.

### 4.6.4 Actors

- Mobile Network Service Provider.
- Enterprise.
- 3rd party NFV grade hosting service (optionally).

### 4.6.5 High-level Architectural Context

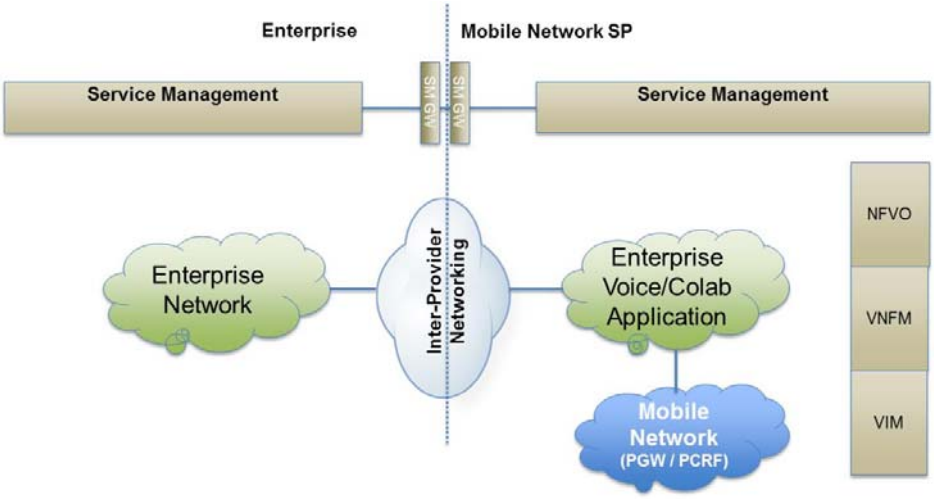


**Figure 4.10 - High-level Functional Distribution in Efficient Enterprise Voice/Collaboration Arrangements**

Architectural attributes (functional view):

The enterprise may or may not use NFV within their enterprise network (i.e., they may virtualize but may not adhere to NFV standards).

The interface between the Mobile Network and the Enterprise Voice/Colab Application clouds would include:

- SGi interface for the enterprise VPN traffic.
- Rx policy interface to allow the enterprise to create QoS enabled dedicated bearers for real-time media.

The interface from the Enterprise Voice/Colab Application cloud into the inter-provider networking cloud would include:

- Enterprise VPN.
- Access to the general Internet or PSTN networks for local breakout of Voice/Colab specific traffic.

An interface will need to be made available to allow the enterprise to life-cycle manage VNF software and images located in the mobile service provider network.

Optionally (not shown in the figure), the Enterprise Voice/Colab Application cloud could also be located in a third party hosting service that was local to the PGW breakout point.

## *4.7 Enabling Service Function Chains with Third Party VNF Application Providers*

### 4.7.1 Story Highlights

Consider the case of a sporting event and groups of fans related through affinity. Earlier in the day prior to a sporting event, avid sports fans arrive at the sporting venue to engage in pre-event festivities. These fans comprise an affinity group aligned around location (the sports stadium), time (the day of the game), and event (the game). This affinity group would be offered a network service that, for instance, offers exclusive content in concert with social media, location services, event-related contests, etc. The network service(s) would be offered for the duration of the sporting event and continue for a period of time after the event as the affinity group disperses through parking lots, mass transportation, etc. The network service is by nature temporary since the affinity group would diffuse shortly after the sporting event concludes. The network service could be instantiated by any number of actors, but would likely include Network Function Service Providers who own VNFs that would not otherwise be used on a continuous basis for a variety of factors (e.g., cost of ownership, unique needs, uniqueness of the VNF).

A second story involves VNO use case and is shown in Figure 4.1. The VNO may need to create a Network Service comprising of not only its own VNFs, but one or more VNFs provided by a Network Function Service Provider. In this manner, the VNO is able to provide a Network Service that they are otherwise unable to offer due to their lack of scale, limited knowledge, limited budget, or other factors.

In both of the stories discussed here, a new ecosystem may be enabled. The most obvious new ecosystem niche is the Network Function Service Provider. Network Function Service Providers may take many forms. For instance, a telecommunications service provider may act as a Network Function Service Provider by externally exposing a subset of VNF's for a fee. Alternatively, it is envisioned that brand new market entrants who only offer VNF's for use will emerge. These are only two illustrative examples. Many more are possible.

These stories entail two categories, both of which involve the use of one or multiple Virtual Network Functions (VNFs) provided by a Network Function Service Provider. The two story categories are a) semi-persistent network service; and b) dynamic network service.

*Semi-persistent network service:*

This is a subset of the VNO use case where the VNO needs one or multiple service functions in order to provide service, but lacks the means necessary to do so (i.e., cost to operate too high, licensing, lack of expertise). The VNO will create the network service (NS) in question by forming a service function chain with service functions from its own network as well as VNFs that reside in the Network Function Service Provider domain. In this paradigm, service providers of any ilk can take advantage of VNFs that may never reside in their own networks (contingent upon business, technical, and operational constraints), essentially utilizing a rent vs. buy model.

*Dynamic network service:*

In this use case, a network service is needed on an ad-hoc basis for a relatively short period of time. The business opportunities addressed by this type of network service may be thought of as "long-tail" opportunities. While no single network service will, on average, account for a large part of a service provider's revenue, the sum of these opportunities can amount to a significant revenue stream. Service agility as enabled by a nimble, dynamic DevOps development model in conjunction with network virtualization will equip service providers with the needed tools to capture revenue that is not currently realizable. This aspect is one of the pillars of the NFV value proposition, providing the service provider net-new capabilities that properly enabled will facilitate a drastic reduction in time-to-market. Such agility, while highlighted in the present use case, is equally useful in many other use cases.

### 4.7.2 Business Drivers

Opportunities as discussed in this use case are motivated by the following business drivers:

- Increased ability to address long-tail business opportunities via service agility, especially those that are ad-hoc in nature; and
- Expense deferral/reduction by utilizing "pay-as-you-go" or other subscription model for virtualized network functions either as a whole or part of a network service.

### 4.7.3 Deployment Model

While very complex deployment models are possible, we will limit our discussion to the most rudimentary model needed to elucidate the necessary features of this use case. At a minimum there will be one Network Service Provider in need of one or more VNFs and one Network Function Service Provider that provides the needed VNF(s), as shown in Figure 4.11. The Host Network Service Provider may be either a VNO or a Network Service Provider. The Network Function Service Provider may be a Network Service Provider; however, it is anticipated that the Network Function Service Provider will more likely be an entity that does not operate a traditional communication network. Whatever the case, the Network Function Service Provider will provide at least one VNF in the formation of a Network Service.

### 4.7.4 Actors

Network Function Service Provider – an entity offering access to its suite of VNFs. These VNFs may be of any sort, but for the purpose of this use case will be categorized as those that are too costly (i.e., in terms of licensing, maintaining, operating) for the implementer of a given Network Service (NS) to own in perpetuity.

Network Service Provider – entity offering commercial telephony and/or network services (e.g., Cable, Broadband, Wireless) to businesses and/or consumers.

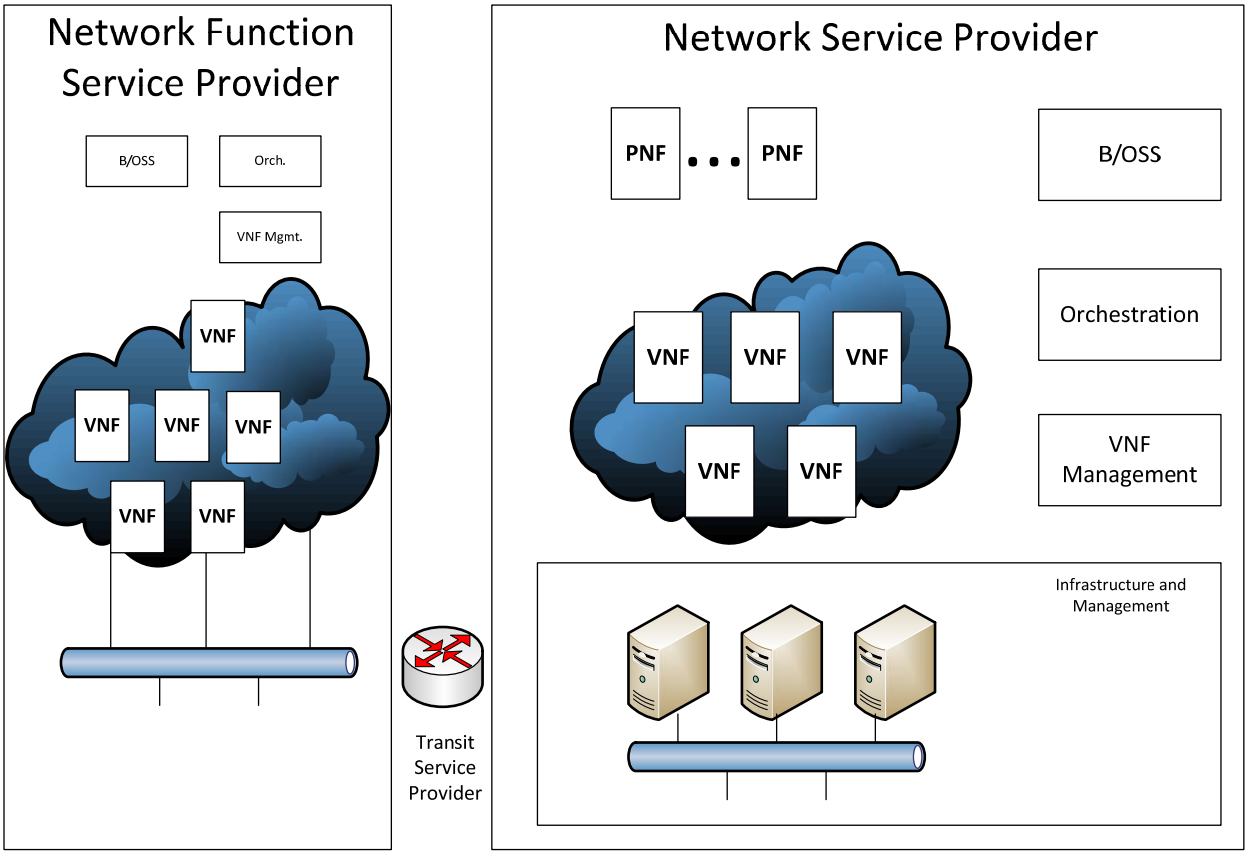


**Figure 4.11 - Actors Involved in a SFC That Utilizes Third Party VNF's**

### 4.7.5 High Level Architectural Context

The three likely architectural options (and some potential requirements) for deployment are shown in Figure 4.12.

- Option 1: the VNF management interface between the administrative domains is mediated between OSS systems. This option represents the highest level of abstraction between the Network Function Service Provider and the Network Service Provider. The former will expose the set of offered VNFs as well as a control panel from which to manage and monitor the selected VNFs.

- Option 2: the Network Service Provider's OSS interfaces to the Network Function Service Provider's orchestrator. The NFSP's orchestrator is controlled by the NSP either by a) the NFSP virtualizing an NFV infrastructure for each NSP; or b) by the NFSP allowing access to their orchestrator.

- Option 3: the Network Service Provider's orchestrator interfaces directly to the Network Function Service Provider's orchestrator (inter-orchestrator federation). As with option 2, the NFSP's orchestrator may be fully virtualized for each NSP thus creating separate operating environments or by direct access to the NFSP's orchestrator, albeit with access controls.

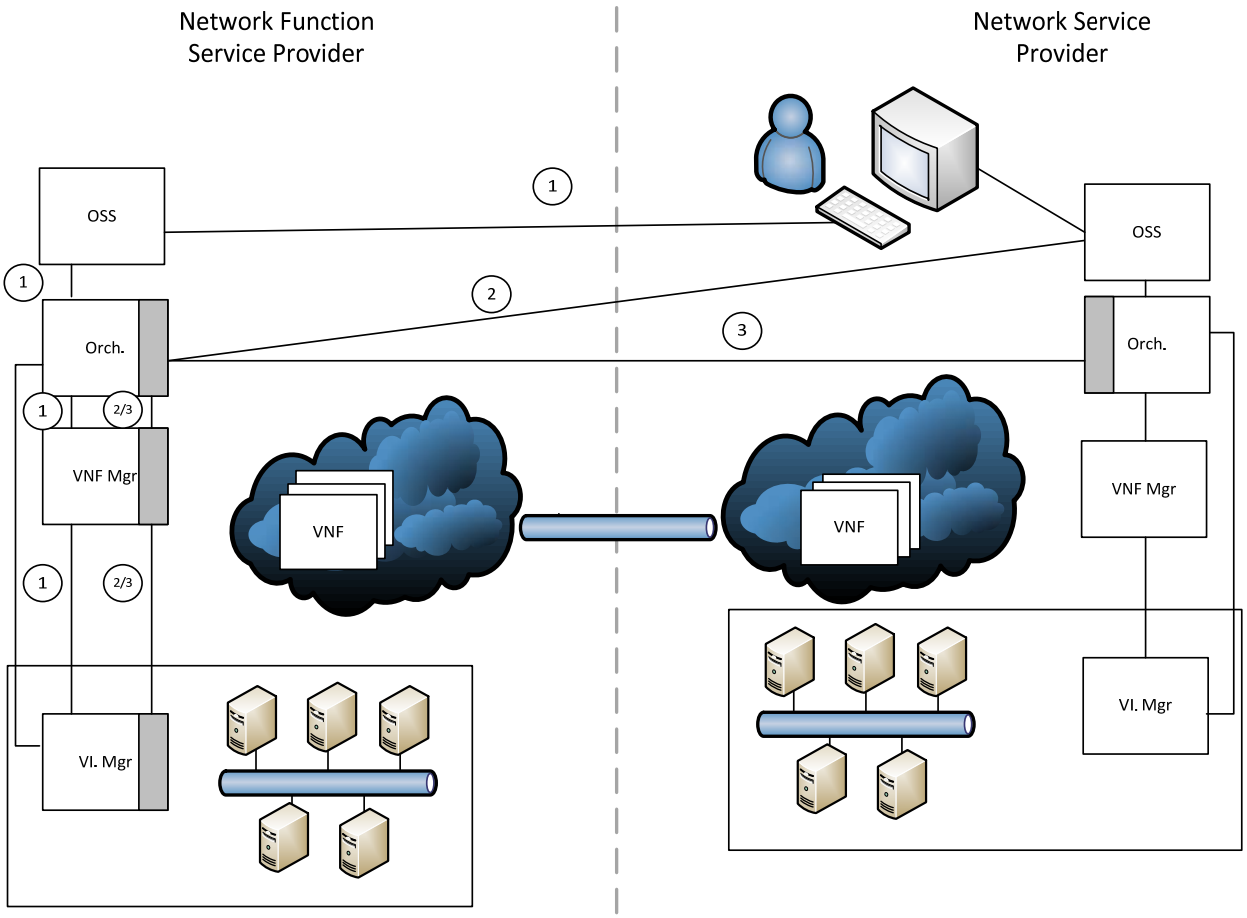


**Figure 4.12 - High-level Architectural Attributes for SFC's Utilizing Third party VFN Providers**

- Some of the potential requirements emerging from this use case include:
    - Modification of information and data models to allow for federation.
    - Communication of VNF capability (performance, reliability, elasticity, etc.).
    - Service function and capability discovery.
    - Description of federated operations and lifecycle.
    - Standardized service description language.
    - Access control.
    - Path cost sharing.
    - Topology hiding/sharing.
    - Standardized policy framework.
    - Security.
    - Service and performance metric reporting.

- Charging data reporting.
- Fault and alarm reporting.
- Capability to troubleshoot VNF and connection points in NFSP domain.
- Dedicated NFVI resource pools per NSP.

## *4.8 Enabling Third Party VNF Applications*

### 4.8.1 Story Highlights

This use case is for an inter-provider platform that fosters the development of innovative new apps, services, and VNFs from third-party sources that interwork with provider functions. Consumer-facing apps would be able to interface with provider VNFs, and perhaps with physical functions, through the use of published descriptors or catalogs. Apps/VNFs could be written by third parties similar to current smartphone apps.

No ecosystem currently exists for third-party VNFs, and so it is likely that third-party VNF developers will need to work in concert with an existing ecosystem for VNFs. This may be via a partnership program for an existing ecosystem, or perhaps via an "aggregator" (e.g., similar to an app store) that can groom the software to work within an NFV ecosystem.

### 4.8.2 Business Drivers

Third-party VNF apps can directly interact with consumers for high perceived value, for example through a Smartphone app interface. Specific applications could include:

- Augmented network services; e.g., a network-based firewall is enhanced by third-party virus protection. This may involve signaling through multiple infrastructures and between multiple locations. Information about a provider's virtual CPE environment would be needed by the third-party VNF in order to work within this virtual CPE environment.
- Real-time charging, e.g., utilize times of low-traffic in LTE networks for non-real-time downloads, upgrades. Here a consumer app may schedule, for example, software updates to occur when it receives notifications from a network provider VNF informing about times of low network utilization. The consumer app may further interact with a BSS to charge less for data usage during these "traffic valleys."
- FMC services. The app combines services across LTE and wireline broadband. An example is bonding LTE and wireline broadband to provide high peak bandwidth. The consumer app can interact with a VNF in the cloud to bond both ends of these routes.

Improved application-layer multicast. Application-layer multicast, using a variant of BitTorrent, is currently popular for receiving diverse video broadcasts, such as from other countries. However, the video quality is generally poor and is not at all coordinated with providers' OSS/BSS. Knowledge of network link performances, particularly layer-2 aggregation networks which are opaque to OTT systems, can be used to improve application-layer multicast.

The success of the Web and Smartphone apps is largely due to third-party innovation.

### 4.8.3 Deployment Model

**Administrative boundaries**: Each of the actors may have their own administrative domain, or these domains may partially interact. Divisions between administrative domains will need proper access control, resource management, integrity, and other security aspects.

### 4.8.4 Actors

- Infrastructure provider.
- Network Function Service Provider.
- Network Service Provider.
- Third-party app developer.

A platform supporting third-party apps may be implemented with different business relationships and infrastructure, possibly including having the third-party VNFs:

1. Developed by third parties but then provided to Service Providers via some business relationship. For example, with a supplier relationship, the VNFs then potentially become part of the Service Provider's catalog of functions available.
2. Instantiated in Service Provider infrastructure but maintained as a business asset of the third-party.
3. Instantiated in their own third-party infrastructure and accessed by Service Providers.
4. Instantiated on a separate infrastructure (e.g., a cloud service) and accessing the Service Providers VNFs/PNFs.

### 4.8.5 High-level Architectural Context

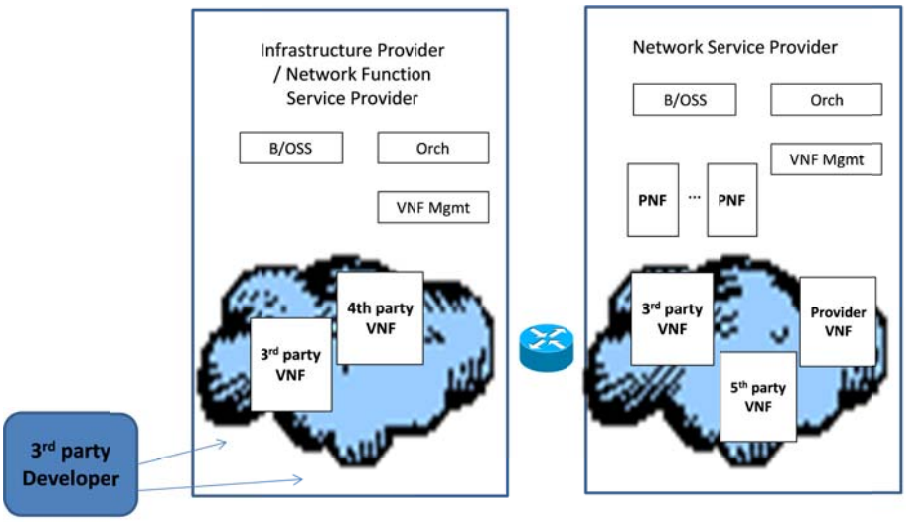


**Figure 4.13 - High-level framework for enabling third party VNF applications**

The figure shows that third-party apps/VNFs could be deployed in a variety of administrative domains and locations. The third-party app could also operate in a tenant domain.

Two salient aspects emerge from this use case:

1. There may be a need to specify how to route messages or chain VNFs that can be understood by

the various actors and VNFs involved here. The third-party app/VNF may be requested by a consumer, but then it can only work with provider apps if it has the knowledge needed to link to them.

2. The third-party developer may need to directly perform some lifecycle functions, in particular to perform software updates.

In order to facilitate this use case, the following issues will need to be considered in detail:

- **Service chain shape**: The third-party app could be chained to other VNFs, but specific service chains are not considered here.
- **Performance**: Physical or virtual networking between the VNFs, PNFs, and management and orchestration functions is a key component of this platform, so network performance is important. Some applications are likely to have high performance requirements, for the network and for the platforms.
- **Load balancing & Resiliency**: This use case involves multiple actors and functions, and resiliency and availability are important aspects of all systems involved. These may need explicit definitions and agreements between operators.
- **Lifecycle:** An interface may need to be made available to the third-party app provider to instantiate and update VNF software and images. The third-party app provider may “push” new images.
- **Traffic engineering**: The network may need to be engineered to connect the various functions with sufficient bandwidth.
- **Security:** Security may involve dividing administrative domains and enforcing these divisions. The third-party apps should only be able to access data and control as appropriate for their specific purpose.
- **Policy:** There are policy implications for the assignment of resources network bandwidth and Class of Service (CoS). The division of these between actors may need specification.

### 4.8.6 Related & Derivative Use Cases

**Existing use cases**: This can be expected to largely re-use the architecture and interfaces/APIs discussed in ATIS NFV use case for xVNO.