Carrier Ethernet and NFV

July 2016

Table of Contents

List of Figures

List of Tables

1. Introduction and Overview

1.1 Abstract

The MEF's Third Network[1] vision leverages the performance and security assurances of Carrier Ethernet 2.0 (CE 2.0) to enable delivery of enhanced services which are more agile, assured and orchestrated. The MEF will achieve this vision by augmenting its foundational CE 2.0 services with Lifecycle Service Orchestration (LSO) capabilities. LSO will encompass existing WAN infrastructure elements as well as software defined networking (SDN), and network functions virtualization (NFV) elements.

The MEF's Carrier Ethernet and SDN papers[2] explain how Carrier Ethernet fits with Software-Defined Networking (SDN). This paper specifically examines how Carrier Ethernet relates to Network Functions Virtualization (NFV). Together, these papers describe the relationship between CE 2.0, SDN and NFV building blocks within the Third Network and their roles in implementing agile, assured and orchestrated services. LSO is only casually discussed in this paper. A more detailed discussion on the role of LSO with CE and NFV may be the subject of a future paper.

1.2 Target audience

Communication Service Providers (CSPs) including telecom service providers, Internet service provider (ISP), cable operators/MSOs, cloud service providers and wireless network operators.

1.3 Document Purpose and Scope

This paper explores the role of NFV in conjunction with delivering CE 2.0 services. The paper discusses options for introducing and implementing NFV to add new virtual network functions and services onto foundational Carrier Ethernet (CE) connectivity services including use cases for different delivery models for virtual network services at the customer premises or remotely from the service provider's network. The paper also discusses virtualization approaches for service demarcation equipment, e.g., Network Interface Devices (NIDs), at the customer premise for different network functions and services.

This paper focuses on the service offerings and deployment aspects of NFV. There are additional building blocks related to NFV deployment including NFV Infrastructure (NFVI) software and VNF service chaining and management and orchestration (MANO). These are important topics but are not discussed in this paper. The paper explores how network operators, who currently offer CE 2.0 services, can benefit from the adoption of network function virtualization to offer additional virtualized network services, to their subscribers resulting in new, differentiated service offerings and revenue opportunities.

1.4 Executive Summary

The market for Carrier Ethernet services is projected to exceed $60 billion in 2018[3]. CE 2.0 infrastructure and services will continue to be the foundation of business, residential, mobile services as they evolve to cloud based delivery models.

End users are embracing the cloud experience and requesting on demand and flexible services from their service providers. This is driving agile service deployment and rapid service innovation within

[1] MEF whitepaper "MEF Third Network Vision based on Network as a Service Principles"

[2] MEF white papers CE and SDN paper- Part 1 CE and SDN paper – Part 2

[3] IHS Infonetics Research: Carrier Ethernet equipment and Ethernet and IP MPLS VPN services forecast (2013-2018)

service provider networks. NFV technologies have attracted much recent attention. NFV transforms specific network functions that run on purpose-built platforms into software functions implemented on general-purpose computing platforms. This paper reviews the benefits of and considerations for combining CE 2.0 and NFV. Adding the virtualization layer to current MEF CE 2.0 services and infrastructure helps evolve and enhance CSP service offerings through new service deployment models.

2. Network Functions Virtualization (NFV)

2.1 What is NFV?

The following definition is from the original ETSI NFV white paper:

"Network Functions Virtualization aims to transform the way that network operators architect networks by evolving standard IT virtualization technology to consolidate many network equipment types onto industry standard high volume servers, switches and storage, which could be located in Data Centers, Network Nodes and in the end user premises."

2.2 What are the benefits of NFV?

NFV is expected to provide many benefits:

- **Add flexibility and velocity while reducing costs:** Deploying software-based functions and services on-demand will improve time-to-market and increase network operators' flexibility to address changing requirements quickly. The NFV approach also reduces operating expenses by eliminating truck rolls for new service introduction and upgrades. Capital expense may also be reduced by deploying fewer generalized compute platforms instead of a larger quantity of purpose-built platforms
- **Boost average revenue per customer (ARPU):** Service providers will be able to promote new and faster service adoption with low-risk "Try-before-you-buy" offerings as well as flexible "Pay-as-you-go" service equipment rentals so customer need not purchase and maintain their own equipment.
- **Improve customer satisfaction while reducing expensive churn:** Service providers will be able to provide more agile services that more immediately address customers' changing service requirements and utilize improved network diagnostic tools that help ensure quality of experience (QoE) by promptly identifying and resolving issues.

2.3 Carrier Ethernet, SDN and NFV

The MEF has defined services that are abstracted from the networking technologies used to deliver them. As part of its Third Network vision, the MEF is working towards defining a common service model to manage services across multiple technologies including new SDN and NFV in addition to existing technology infrastructure elements. The MEF LSO framework describes how these services are orchestrated for the entire service lifecycle.

The introduction of SDN and NFV technologies will lead to significant transformation within existing operator networks. Early adoption of SDN started within the data center (DC), to provide network virtualization within the DC network. SDN is expanding from the DC into the WAN (often referred to as Carrier SDN), providing service automation and network optimization within the wide area network. This will help enhance existing CE 2.0 services, making them more on demand, dynamic and assured.

Customer demarcation devices will evolve to support software-based implementations to complement existing CE 2.0 services. Additionally NFV and CE 2.0 can together enable several NFV based applications and services, by leveraging underlying CE 2.0 attributes. Equipment within the Carrier Ethernet network (CEN) may evolve to implement NFV with Carrier SDN. Network operators will use SDN to simplify their networks and streamline operations by centralizing control and providing an end-to-end perspective on services.

Carrier Ethernet services include retail and wholesale services for the business, mobile and residential market segments. SDN and NFV are part of a set of tools, enabling deployment of CE 2.0 and will leverage the strong foundation of Carrier Ethernet services to enable rapid service innovation and velocity. NFV, when used with a Carrier Ethernet infrastructure, can deliver agile services with added SLA performance assurances for critical business applications.

3. CE and NFV – Building blocks and deployment considerations

Before reviewing the options for implementing network functions virtualization within existing CE-based network infrastructures, let's first review the present mode of operation (PMO) related to implementation of CE services.

3.1 CE 2.0 Services Use Cases – Present Mode of Operation (PMO)

CE 2.0 services are used in a wide range of retail and wholesale applications including L2 VPNs, Mobile Backhaul (MBH), Off-Net E-Access services, Data Center Access (DCA), and Data Center Interconnect (DCI). An Ethernet NID is commonly deployed as the PMO to provide service demarcation for these service scenarios. The NID provides service demarcation between the service provider and subscriber or between network operators, e.g., Service Provider and Access Provider. The NID may support Carrier Ethernet functionality such as bandwidth profiles and Service Operations Administration and Maintenance (SOAM) for fault management and performance monitoring. This PMO can benefit from NFV by virtualizing the Carrier Ethernet functions plus additional services or service functions, e.g., router and firewall, to deliver new, differentiated service offerings.

3.2 Virtual Network Function (VNF) deployment models

VNFs are placed in the network based on feasibility, performance, economics, regulations and policy requirements. For example, VNFs for encryption, WAN optimization, and SLA monitoring may need to be located at the customer premises, whereas functions such as firewall or routing could be at the customer premises or elsewhere in the service provider's network.

There are three deployment models for NFV, all of which can leverage CE, as shown in Figure 1.

Centralized – In the centralized model, all virtualized functionality is located at a service provider's centralized point of presence (POP) such as a Central Office (CO), or data center. This deployment model enables VNFs to be deployed using existing networks without replacing any customer premises equipment. In this case, Carrier Ethernet is ideal for providing access to centralized VNFs from the customer premises.

Decentralized – In this model, all virtualized functionality is located at the customer premises. This deployment model requires replacing or augmenting equipment at the customer premises. This model is similar to current deployment scenarios using purpose built equipment and thus fits well into existing network operations processes and systems.

Distributed – In this model, network functionality is distributed between the service provider's POP, e.g., CO or data center, and the customer premises. The VNFs can be deployed where they provide the optimal feasibility, performance, regulatory, reliability, scalability, and cost considerations.

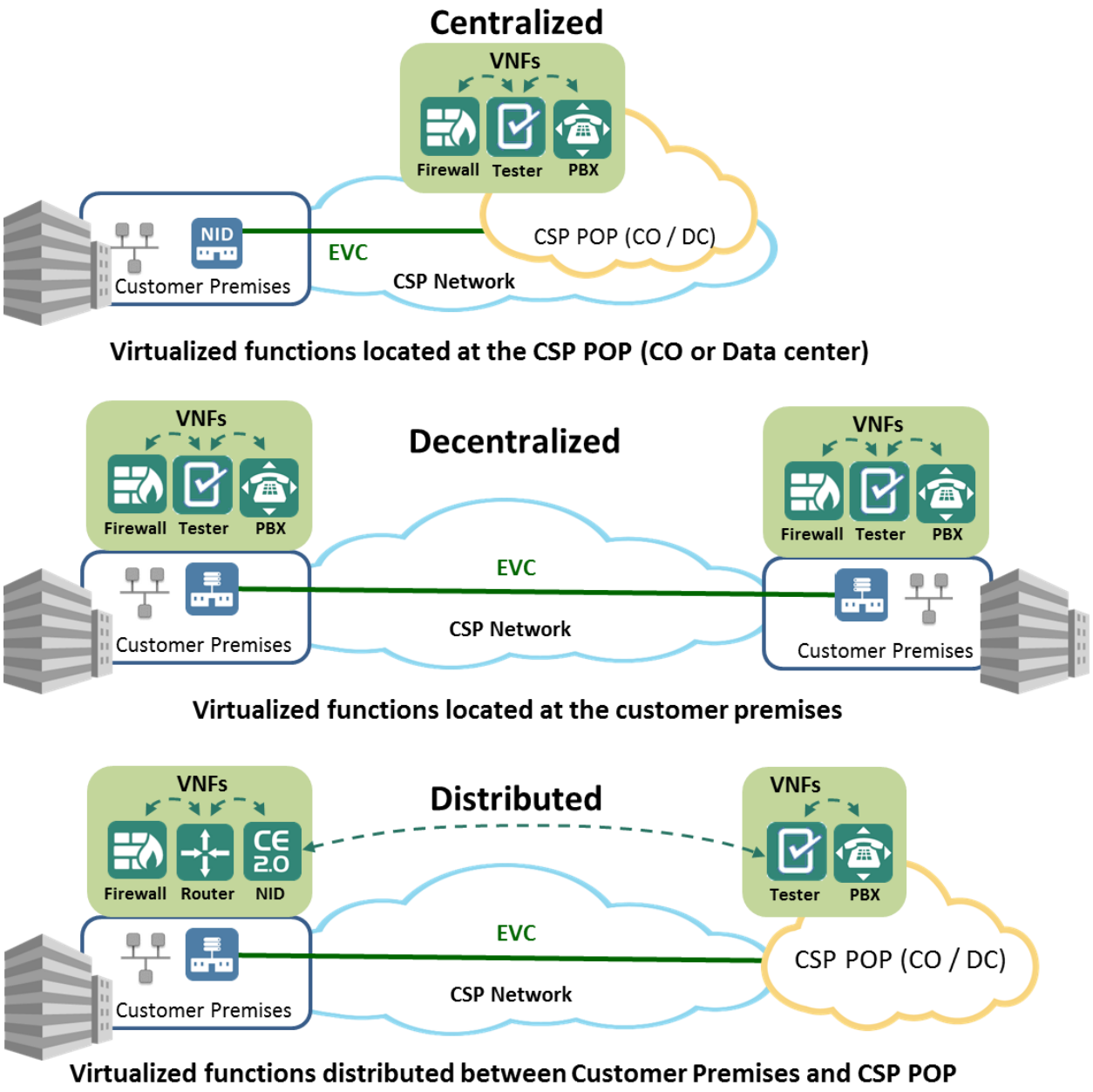

Figure 1: Virtual Network Function (VNF) deployment models

3.3 Customer Premises Deployment Options

Many service providers are looking to virtualize customer premises equipment (CPE) functions as a means to offer on-demand, virtual network services in existing and new markets. Depending on the VNF model implemented, there are choices for the type of CPE deployed at the customer premises. This section describes the choices and location of VNF placement.

3.3.1 Physical NID

In this deployment option illustrated in Figure 2, CE functions are supported at the customer premises with a physical NID. Additional services functions such as a router, firewall, etc., are implemented as VNFs deployed using the Centralized Deployment Model (described in section 3.2) at service providers POP, e.g., CO or Data Center. All CE functions are performed in the NID at the customer premises with additional service functions implemented as VNFs hosted in the CO or data center.

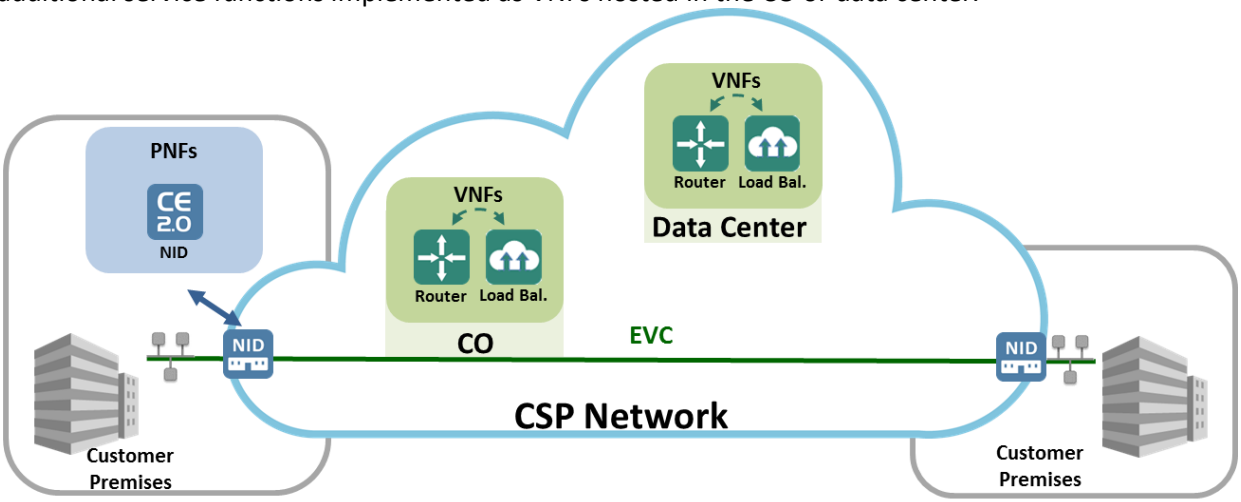

Figure 2: VNFs running in CO or Data Center with Physical NID at customer premises

3.3.2 Virtual CPE (vCPE)

A vCPE[4] is designed to replace and move some or all customer premises equipment functions to a commercial off-the-shelf (COTS) compute platform at the customer premises. This deployment option replaces multiple appliances at the customer premises with a single platform to deliver virtual network services.

In this deployment option, illustrated in Figure 3, Carrier Ethernet functionality (including service demarcation) and additional functions and services, e.g., router, firewall, etc., are implemented as VNFs running on a COTS compute platform deployed at the customer premises using the Decentralized Deployment Model (described in section 3.2). If additional VNFs cannot be added to the vCPE, they can be added to servers running in the service provider POPs, e.g., CO or data center, and service chained to those running on the vCPE using the Distributed Deployment Model.

[4] SDxCentral Definition – on-premise-vcpe

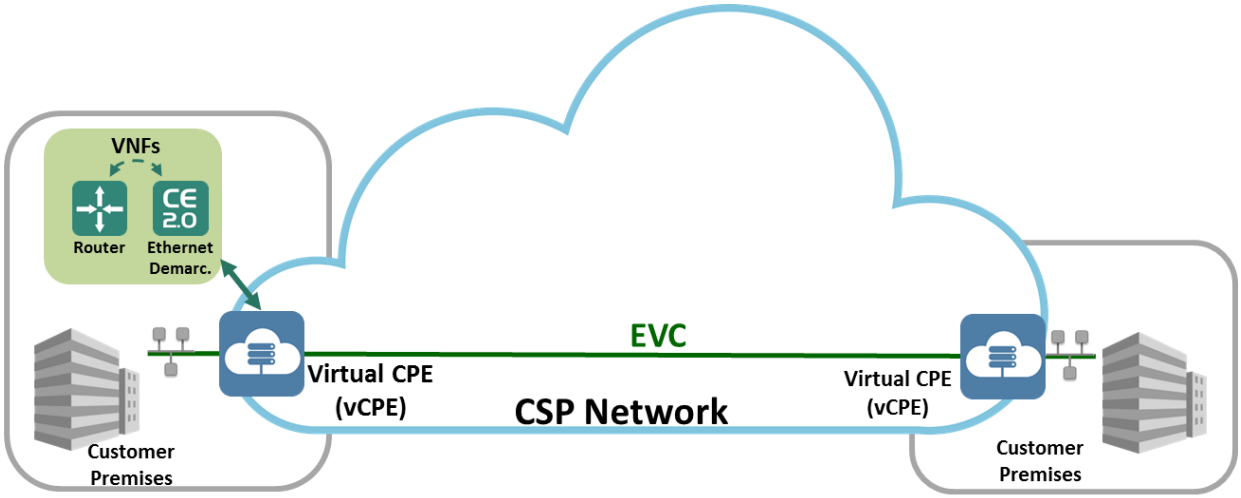

Figure 3: VNFs running on vCPE at customer premises

3.3.3 Hybrid implementation

In this deployment option, illustrated in Figure 4, some or all CE functionality (including service demarcation) are implemented as physical network functions (PNFs). Additional functions and services, e.g., router, firewall, etc., are implemented as VNFs running on an integrated or separate COTS compute platform deployed at the customer premises using the Decentralized Deployment Model (described in section 3.2). Additional VNFs can be added to servers running in the service provider POPs, e.g., CO or data center, and service chained to those running at the customer premises using the Distributed Deployment Model (described in section 3.2).

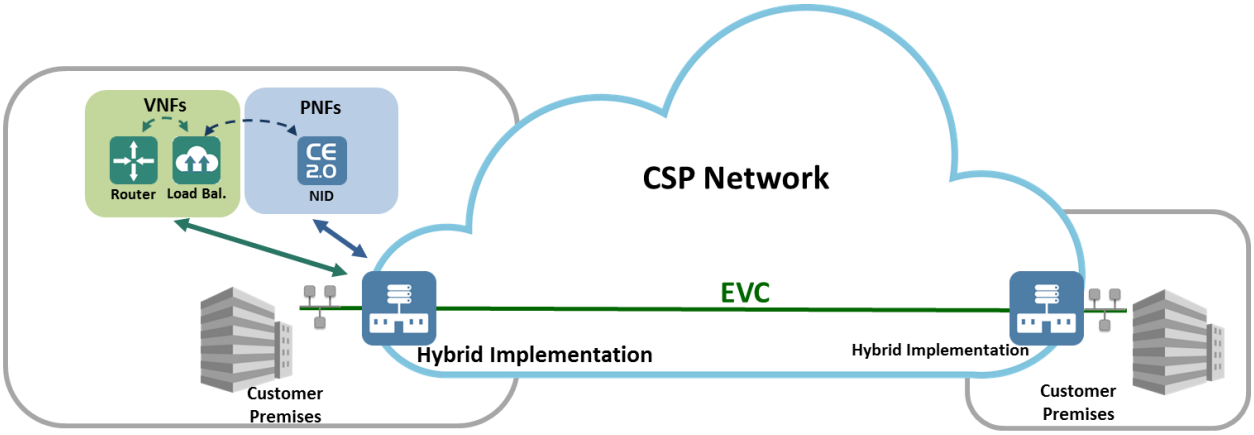

Figure 4: PNFs and VNFs running on Hybrid implementation at customer premises

3.4 Business/Operational Considerations when comparing Virtualization choices

As discussed previously, CSPs have a number of deployment and implementation options that need to be carefully considered from a business and operational perspective.

3.4.1 Business Considerations

When comparing virtualization options the following business considerations are applicable:

OPEX	Skill sets to support newer VNF-based functionality (IT skills) are needed in addition to traditional Physical Network Function (PNF) based functionality (networking skills).
CAPEX	Devices that offload processor intensive functions to optimized hardware require fewer CPU cores and less memory resources. The cost of optimized hardware should be compared with equivalently scaled COTS compute platforms with virtualized functions.
Available resources	Allocating CPU cores, memory and storage resources for virtualized CE functions reduces available resources for other VNF functions and services, e.g., router, firewall, IPsec, WAN acceleration. Some of these functions and services would then have to be run in other service provider POP locations. Note that some of these functions must remain on the customer premises, e.g., WAN acceleration.
Availability	Centralizing VNFs in larger service provider POPs may offer additional VNFs availability options to address resiliency, load balancing, location diversity, etc. Network resiliency is achieved by implementing failover mechanisms at the customer premises, such as G.8032v2 rings, LAG, dual homing, Hybrid VPN, etc.
Service Activation Testing functionality	Need to consider the capabilities for service activation testing (SAT). SAT functionality can be performed in a proprietary or standardized implementation as defined in MEF 49.
SLA assurances	Must compare the performance of OAM tools to the requirements of the service to enable verification of SLA performance metrics
Performance	Performance metrics, e.g., throughput and delay, may be impacted when forwarding packets in software and sharing compute and memory resources among VNFs. Proper analysis of VNF compute and memory requirements and performance testing is required to determine if service performance requirements are met for a given use case.
Security	Different security considerations are required when sharing compute resources among subscribers on a centralized server. vCPE deployments for subscribers at customer premises provides physical isolation. Security functions implemented at the customer premises may be enhanced by functions that can block, filter and rate limit traffic prior to being transmitted across the WAN.
Feasibility	Some functions, e.g., encryption, WAN optimization, and testing/monitoring, must run at the service end point at the customer premises

Table 1: Business Considerations for CE and NFV deployment

3.4.2 Operational Considerations

The following are important operational considerations when comparing virtualization options.

Established procedures	Disruption to established network operational procedures developed over years. Does operations have people trained to address NFV "IT issues" efficiently?
MTTR	Are there network and compute fault isolation tools to access the CO/DC and remote customer premise device, e.g., vCPE, or must service technicians be dispatched to the customer premises in the event of service outage?
Troubleshooting skills	Are technicians with their current diagnostic tools capable of troubleshooting customer problems? Do they have sufficient IT troubleshooting skills required for NFV?
Scalability	Must consider the compute, memory, and storage resources and the VNF performance requirements to determine how many VNFs can be instantiated on a given vCPE or server platform.
Service verification tests	Are service activation and verification tests disruptive to currently running VNFs?
Performance monitoring	Can performance of CE, VNFs and NFV compute, memory, and storage infrastructure (NFVI) be monitored?
Forwarding and throughput	Is there an impact to forwarding, switching, and routing performance depending on which VNFs are running?
Delay	Is the cumulative delay introduced by service chained functions satisfactory under load conditions?

Table 2: Operational Considerations for CE and NFV deployment

4. CE and NFV-based Services

The following sections provide examples of virtual network services which leverage the combined benefits of Carrier Ethernet and NFV.

4.1 Enhancing Existing CE services with NFV

Network operators who offer CE 2.0 services today or partner with third party CE 2.0 access providers can benefit from implementing NFV to complement their CE 2.0 services. CE 2.0 provides the baseline connectivity service with virtual network services using NFV technologies layered upon it. NFV, combined with CE and LSO, provides service agility and rapid service innovation which help create differentiation and revenue generating opportunities. As shown in Figure 5, the VNFs may be located at the customer premises using the Decentralized Deployment Model or within the service provider POP using Centralized or Distributed Deployment Models.

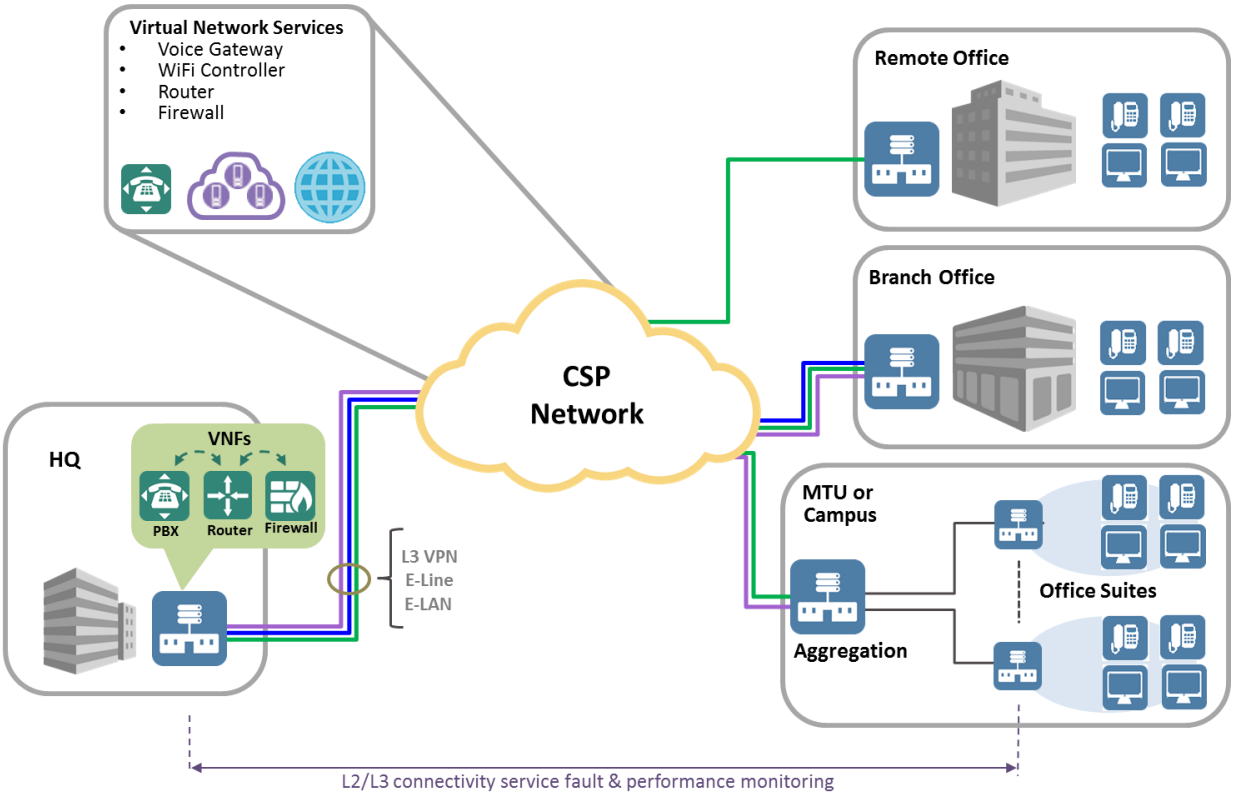

Figure 5: Layering additional virtual network services onto existing CE service using NFV

4.2 Assured CE Connectivity with Centralized VNFs

Enterprises and small medium business (SMBs) are increasingly adopting cloud services. Connectivity to public cloud providers is mostly achieved using Internet connections which may not provide sufficient service performance and reliability. This provides an opportunity for service providers to complement existing connectivity services and expand their service offerings to their enterprise and SMB subscribers. As illustrated in Figure 6, a CSP can leverage NFV by implementing VNFs within their POP (CO or data center). These VNFs may include Firewall and other L4-L7 functions which can be combined with the CE connectivity service to deliver the assured performance enterprises and SMBs requiring with their connectivity to cloud services. Load balancer VNFs can be used to increase availability.

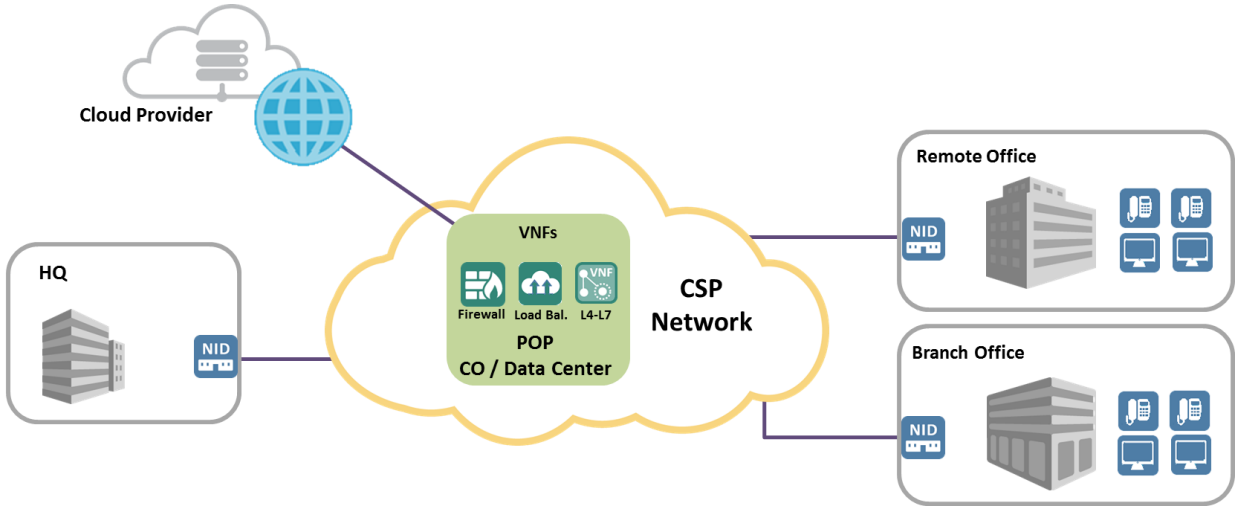

Figure 6: Assured CE connectivity with centralized VNFs

4.3 Virtualization Use Case for Off-Net E-Access Services

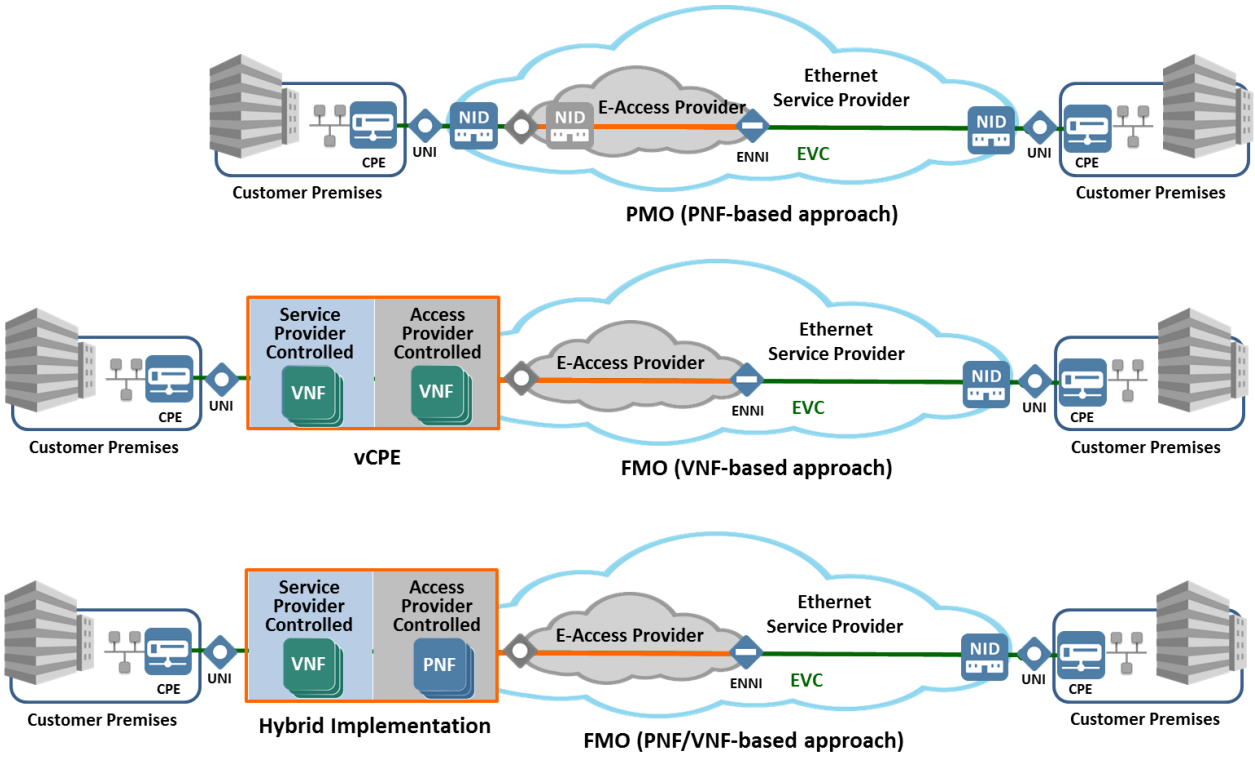

Figure 7: Virtualization Scenarios for Off-Net E-Access Services

To effectively and efficiently deliver service demarcation to provide service OAM fault management and performance measurements for SLAs, two service demarcations are required; one for the E-Access Provider and one for the Ethernet Service Provider. The challenge with this approach is that the Ethernet Service Provider may not have installation personnel available in the region to deploy and install Physical NIDs at the customer premises. If they cannot do this, they have to rely on the E-Access provider to perform this functionality as a proxy. Two different Future Mode of Operations (FMO)

virtualization paths using NFV technologies illustrated in Figure 7 can address this where all or some of the NID functions may be virtualized.

These FMO approaches benefit both network operators. The E-Access Provider can sell service demarcation functionality to the Ethernet service provider and the Ethernet Service Provider can create new revenue opportunities and service differentiation. The Ethernet Service Provider can then deliver better service OAM to off-net locations that are part of a multi-site VPN resulting in better SLAs and service differentiation. Additionally, with the VNF-based approach, both providers have the opportunity to add new functions and services beyond the foundational CE service demarcation functionality.

Because this use case has a single CPE (vCPE or Hybrid Implementation) that is shared between two service providers, special considerations must be made for security of management and control functions. The E-Access Provider owns the CPE (vCPE or Hybrid Implementation) and is responsible for managing the PNFs or VNFs specific to their service demarcation at the customer premises. In this use case, the Ethernet Service Provider manages the VNFs for their EVC end point service demarcation at the UNI. Therefore, there must be secure management access and control separation between the two providers.

5. Summary

NFV, defined by the European Telecommunications Standards Institute (ETSI) aims to transform the way that network operators design networks by virtualizing network equipment functions onto industry-standard compute platforms. CE provides the foundational connectivity providing performance and security assurances while NFV provides the agility to layer additional services onto the CE 2.0 network. This will help service providers offer, enhance, and expand their offerings with new and innovative services. As described in this paper, there are multiple deployment options that address different requirements, and no single option may satisfy all requirements. Therefore a mix of deployment options may be used depending upon the type of subscriber, operational considerations, SLA, and type of service being offered.

6. About the MEF

The MEF is the driving force enabling agile, assured and orchestrated Third Network services for the digital economy and the hyper-connected world, with user-directed control over network resources and cloud connectivity. Optimized for real-time, QoS-enabled, secured traffic and integration of value-added network functions-as-a-service, Third Network services are delivered over automated, virtualized, and interconnected networks globally powered by LSO, SDN, and NFV.

The MEF leverages its global 200+ network operators and technology vendor community, builds upon the robust $80 billion Carrier Ethernet market, and provides a practical evolution to the Third Network with LSO, SDN, and NFV implementations that build upon a CE 2.0 foundation. The MEF has established a technical and implementation framework that includes architecture, information models, service definitions, operational processes, open source community, and certification programs. MEF work is conducted internally and – under the guidance of the MEF UNITE program – in collaboration with global standards organizations and open source projects. See MEF.net for more information.

7. Glossary and Terms

A glossary of terms used in this document can be found online at MEF.net.

8. References

Source	Link
MEF	MEF Third Network Vision based on Network as a Service Principles
MEF	CE and SDN paper- Part 1, CE and SDN paper – Part 2
SDxCentral	Most popular virtual customer edge use cases
ETSI	Network Functions Virtualization (NFV); Management and Orchestration
MEF	MEF 49 - Service Activation Testing Control Protocol and PDU Formats

9. Acknowledgements

Editor: Anthony Peres, Nokia

Principal Authors:

- Anthony Peres, Nokia
- Eitan Schwartz, RAD
- Prayson Pate, ADVA
- Ralph Santitoro, Fujitsu Network Communications

Contributors:

- Greg Spear, Accedian
- Ghassan Semaan, Verizon
- Rami Yaron, Telco Systems
- Marlon Roa, Transmode
- Scott Mansfield, Ericsson
- Anthony Magee, ADVA
- Mehmet Toy, Comcast
- Michael Bugenhagen, CenturyLink