SOLUTION BRIEF

vE-CPE for Communications Service Providers

Executive Overview

Intel is accelerating network function virtualizations with unique capabilities that enable optimal use of data center technologies. These technologies will enable communications service providers (CSPs) to deliver competitive customer premises equipment (CPE) services. Virtual customer premises equipment provides the CSP the ability to quickly deliver managed services using different virtualized network functions in addition to decreasing time to market for new and enhanced services. More than ever, traditional operators must keep pace in a world where application developers bring to market new services and capabilities through the network that take the CSPs years to produce within the network. To remain relevant, retain users, and grow revenues, CSPs need the ability to launch new capabilities more rapidly, and many are looking to virtualized networks to enable this speed and agility.

Many system integrators, software vendors, and platform providers rely on Intel® technologies to deliver the performance and scalability required for virtualized enterprise CPE or (vE-CPE) solutions. Using vE-CPE solutions based on Intel technologies, CSPs can offer a full range of services without having to use multiple purpose-built systems.

This document details the vE-CPE functions, the required technologies, and Intel's role in the ecosystem to migrate toward realizing these technologies in CSP production deployments.

Introduction

Increasing market pressures, such as the demand for new and enhanced services, and the search for more cost-effective solutions are driving communications service providers (CSPs) to adopt network functions virtualization (NFV). Virtualizing services onto standard, off-the-shelf hardware and taking advantage of software-defined networking (SDN) can increase network flexibility and slash costs, as well as enable operators to quickly launch new revenue-generating services more efficiently.

CSPs are seeking new ways to increase agility, improve the manageability of their services and equipment, and reduce costs. To achieve their goals, some CSPs are rethinking the architecture of customer premises equipment (CPE) that resides on their customers' premises and provides the platform for delivering connectivity services, security capabilities, and more. Virtual enterprise CPE (vE-CPE) solutions—also known as virtual business CPE (vB-CPE) solutions—can help CSPs accelerate provisioning of new services, streamline management, and cut operating expenses.

For CSPs, the key benefits of virtualized network functions like vE-CPE are the reduction of capital expenditure (CapEx) and the elimination of end-of-life issues with on-premise appliances. These benefits also allow CSPs to deliver a more unique service mix, based on software and an open ecosystem, supported by developers and partners. The use of these technologies is transforming network service delivery, easing service orders and upgrades, and improving manageability by enabling on-demand software service delivery through customer portals. As a result, CSP revenues grow by accelerating service deployment and service upgrade times.

For CSPs, the implementation of a vE-CPE strategy for delivering broadband and enterprise services represents one of the largest business opportunities for positively impacting top-line revenue, reducing expense, and retaining and even growing customers.

Table of Contents

IDC forecasts[1] that the global managed network services (MNS) segment will grow from USD 72 billion in 2013 to USD 102 billion by 2017, a CAGR (compound annual growth rate) of 10 percent. IDC predicts that implementing vE-CPE solutions will enable CSPs to transform and improve the cost structure, speed of delivery, and flexibility to offer and support new and existing enterprise services compared with the current business CPE delivery models.

Two of the largest vE-CPE applications today are managed Multiprotocol Label Switching (MPLS/IP) VPN enterprise services and firewall services, which together account for over USD 45 billion of global MNS revenue.

Many system integrators, software vendors, and platform providers rely on Intel® technologies to deliver the performance and scalability required for vE-CPE solutions. Using vE-CPE solutions based on Intel technologies, CSPs can offer a full range of services without having to use multiple purpose-built systems.

This paper describes the technologies required to enable and mature vE-CPE technologies that in turn will enable CSP production deployments.

Market Opportunity

NFV provides the potential to deliver virtualized service network functions (firewalls, VPN, load balancers, call managers, and so on) to managed network service customers much faster than was previously possible with physical service functions, where a truck roll was required to deploy a new service.

A 2015 Infonetics CSP survey[2] found that vE-CPE was the most promising NFV use case for revenue generation, operational efficiency, and CapEx reduction. In these areas, CSP networks have not kept pace with the software-oriented "over-the-top" (OTT) infrastructure found in the data center. The carrier's current solutions are hardware-based, manual, and rigid, have costly installs and maintenance, and are slow to deploy new services. This legacy, proprietary model stifles innovation and makes it difficult for the CSP to compete effectively (see Figure 1).

Despite these challenges, the CSP is ideally positioned to deliver the greatest return on CPE virtualization. In a recent ACG Research[3] study of managed network CSPs, CSPs had a stronger total cost of ownership (TCO) payoff across a wide range of decision criteria in comparison to other providers (see Figure 2).

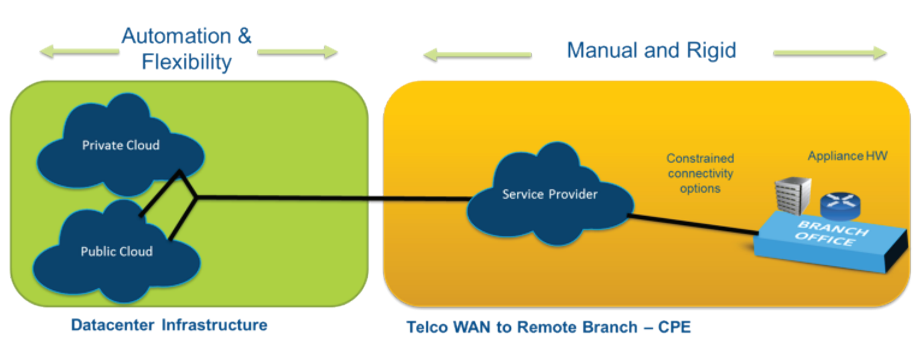

Figure 1. Challenges for communications service provider.

DECISION/CRITERIA PROVIDER	CARRIER	EQUIPMENT VENDOR	IT INTEGRATOR OR VAR	CLOUD PROVIDER
End-to-End Management	Strong	Weak	Average	Weak
Reliable	Strong	Weak	Average	Weak
Secure	Strong	Weak	Average	Average
Customize/Consulting	Average	Average	Strong	Weak
Dedicated Support	Strong	Average	Average	Average
Best-of-Breed Technology	Strong	Strong	Strong	Average

Strong Average Weak

Figure 2. TCO payoff for managed network services.

There are many reasons for this. CSPs have an end-to-end service chain view, with a deep understanding of the network from radio access to the data center. They are clearly the experts at providing 24-hour, mission-critical support to enterprises. CSPs also have an influential role with vendors in technology development given their size, investment profile, legacy relationships, and strong views on the technology evolution.

While meeting the competitive threat and reducing service delivery costs and TCO are compelling, CSPs benefit greatly from other aspects of vE-CPE deployment:

- **Time to money** Deployment of vE-CPE helps reduce service up-time in remote geographies from weeks to hours. It aids the removal of slow and costly multi-vendor installs and enables an easy service upsell capability.
- **Service innovation**. Virtualizing the CPE environment helps break the hardware development cycle and allows for the quick introduction of software-empowered value-added services. It simplifies the service delivery and focuses the opportunity on value-as-a-service (VaaS) upselling.
- **Brand and customer relationship**. vE-CPE deployment gives the CSP powerful branding and service creation opportunities. It also enhances the relationship with the end user by removing the ponderous and costly supply chain from CPE delivery and provisioning.

vE-CPE can help CSPs and their customers increase agility. With a virtualized solution, CSPs can introduce new services, and maintain and modify existing services without having to deploy new physical hardware. For example, a CSP could offer a new encryption capability, add firewall services, close a security gap, or incorporate bandwidth compression by making changes to the software rather than installing new systems. vE-CPE can be scaled—increasing bandwidth or supporting more users, at any time, while minimizing the need to add more hardware.

Enterprises and end users also benefit from vE-CPE deployment. Virtualized CPE solutions reduce capital outlay and network operating expenses. Logistics become simpler with the ability to turn sites up or down at scale. Service fulfillment velocity increases and fault fixes and patches become easier to do via software (in comparison to hardware).

Total Cost of Ownership Benefits

On behalf of Intel Corporation, PA Consulting studied the impact of deploying vCPEs to small, medium, and large enterprise sites, where the virtualized network function (VNFs) are hosted in the network cloud or on an onsite vE-CPE server. This was done for four developed markets: Asia Pacific, Europe, Latin America, and the United States. Although there is a general consensus in the industry that the main driver for vE-CPE implementation is cost reduction, there is little information on the quantification of the associated costs and benefits. The benefits are likely to include reduced time to roll out new services to customers and easier management of a less varied fleet of installed purpose-built CPEs.

The study produced the following findings:

Cost reduction of between 32 percent and 39 percent by implementing vE-CPE in the cloud

The enterprise vCPE solution represents an attractive opportunity for CSPs in the geographies analyzed. The impact of vE-CPE implementation in the cloud represents greater savings for large enterprises than small and medium enterprises (SMEs) and is similar in the four geographies: the cost reduction is 32 percent in the United States, 36 percent in Europe and Asia, and 39 percent in Latin America. The calculations in the analysis showed potential savings worth USD 259 million over a period of 5 years for operators with a 10 percent market share of large enterprises in the European market.

The cost savings are on average 17 percent lower for large enterprises and 71 percent lower for SMEs if CPE virtualization is at the customer premises rather than in the network cloud. This is mostly due to the increase in software costs and decrease in hardware savings as the efficiencies of scale are reduced. The efficiencies of scale for a NFV platform include the possibility of sharing that platform with other users (that is, multi-tenancy). Most of the software cost increase is due to on-demand CPE virtual network functions, such as WAN acceleration and optimization costs.

Up to 90 percent reduction in hardware costs for large enterprises

Traditionally, purchasing and managing hardware on the customers' premises represents around 42 percent of the total CPE costs for a large enterprise and can be as high as 59 percent for individual large offices and 62% in SMEs.

Hardware purchase, installation, and maintenance costs are a large part of any CSP's costs. So the potential for cost reduction here is driving CSPs to implement vE-CPE solutions. Calculations showed that moving the equipment, services, and human assets to the carrier's network may result in cost savings of 48 percent for SMEs and 60 percent of the overall costs for large enterprises.

Service costs can be reduced by up to 48% when serving SMEs

Reducing the hardware on customer premises lowers the likelihood of truck rolls to a site to deploy, upgrade, or swap CPE hardware. The associated service costs related to site visits for maintenance, commissioning of services, and decommissioning are much lower. Figures 3 and 4 below capture these results from an European deployment analysis.

NOTE: Graphs are read as a change % (+/-) from conventional

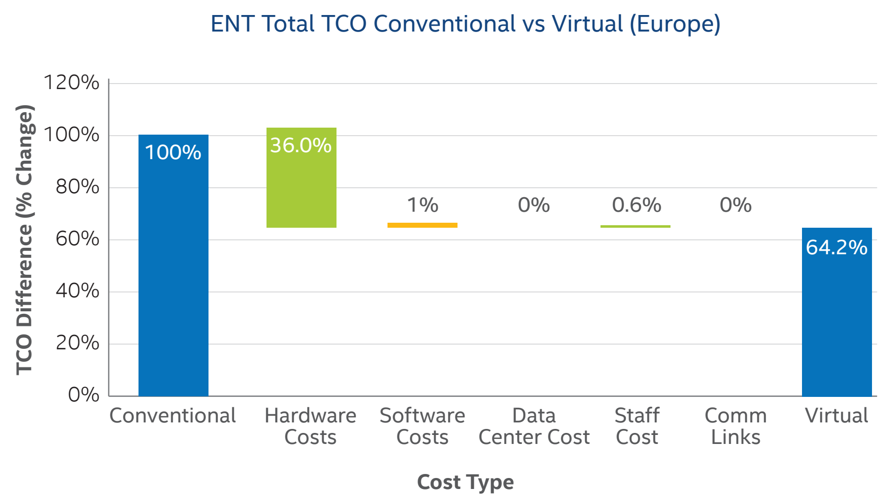

Figure 3. Comparison of conventional versus virtual enterprise TCO (Europe).

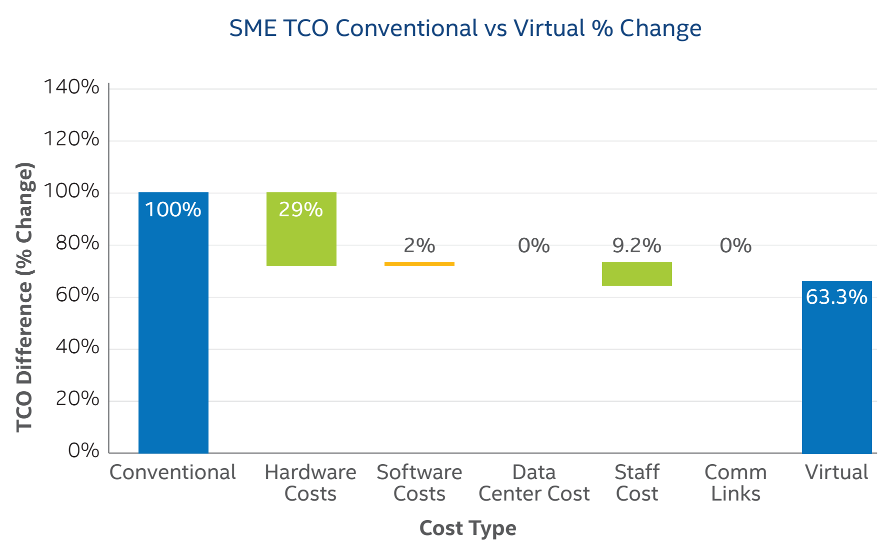

Figure 4. Comparison of conventional versus virtual SME TCO (Europe).

Industry Challenges

The CSP industry today is undergoing a transformation. Instead of focusing on a single type of service, such as telephony, twenty-first century CSPs deliver a broad array of services, from voice, video, and data to the security capabilities that power enterprise networks. Success for CSPs serving enterprise and small and medium businesses (SMBs) depends on the ability to rapidly accommodate evolving customer requirements, deliver responsive service management and support, and control the costs of all the services provided. Providing an agile and secure service delivery platform is critical for addressing customer needs.

CSPs must be able to quickly introduce new services to different parts of the network and make modifications in existing ones. A customer might need to increase bandwidth to support a new enterprise application, add a firewall to better protect the network, or upgrade the Wi-Fi* network to accommodate a growing number of mobile devices. If the CSP provides only purpose-built devices, making these changes might be difficult, if not impossible. The customer is forced to deploy additional equipment, which adds time and costs for the customer while potentially creating management and maintenance burdens for the CSP.

No matter how much equipment is deployed, CSPs also need to improve manageability and maintainability. When customers lease or rent equipment, they rely on CSPs to make changes and repairs rapidly, in order to minimize downtime.

CSPs are eager to develop new service offerings that take advantage of technology improvements and design innovations. They want to reduce the costs associated with provisioning, management, and support. Customers that manage their own equipment want to avoid the expenses of employing highly skilled staff to manage and maintain hardware appliances. At the same time, all customers want to reduce the costs of purchasing, renting, or leasing physical equipment. If each physical system has a redundant system, the cost savings from consolidating hardware can quickly add up.

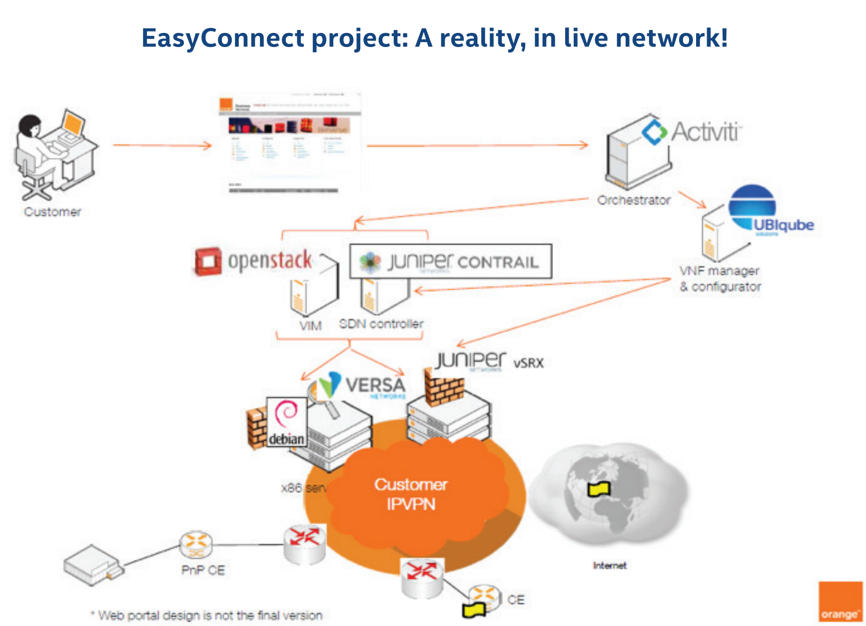

Figure 5. Orange EasyConnect* project.

State of the Industry

The case study for vCPE is well understood by the carriers: fewer truck roles means larger profits and adaptable platforms means less costly introduction of new services or features. In addition, for the enterprise customers the value of the model may depend on the local business model. In some regions the carrier is responsible for the TCO of the enterprise CPE, while in others it is the enterprise itself that bears the TCO. In the latter case, the enterprise is free to size the vE-CPE to the needs of their current business, and as the business case changes either through expansion or through the introduction of new services carried over the WAN, the enterprise is able to chain these functions into the vE-CPE without introducing new hardware into the flow.

Many in the industry are actively working to develop deployable use cases and complete trials. Colt and Orange have both been public about the capabilities of the technology, as showing in Figure 5 and Figure 6.

In addition, there are CSPs that have completed trials of vCPE deployment:

- Telekom Austria: http://telecoms.com/399981/telekom-austria-begins-home-gateway-virtualization/
- China Telecom and Huawei: http://pr.huawei.com/en/news/hw-371867-vcpe.htm#.Vp5u6vkrKUk
- Liberty Global and Benu Networks: http://venturebeat.com/2015/05/19/liberty-global-selects-benu-networks/

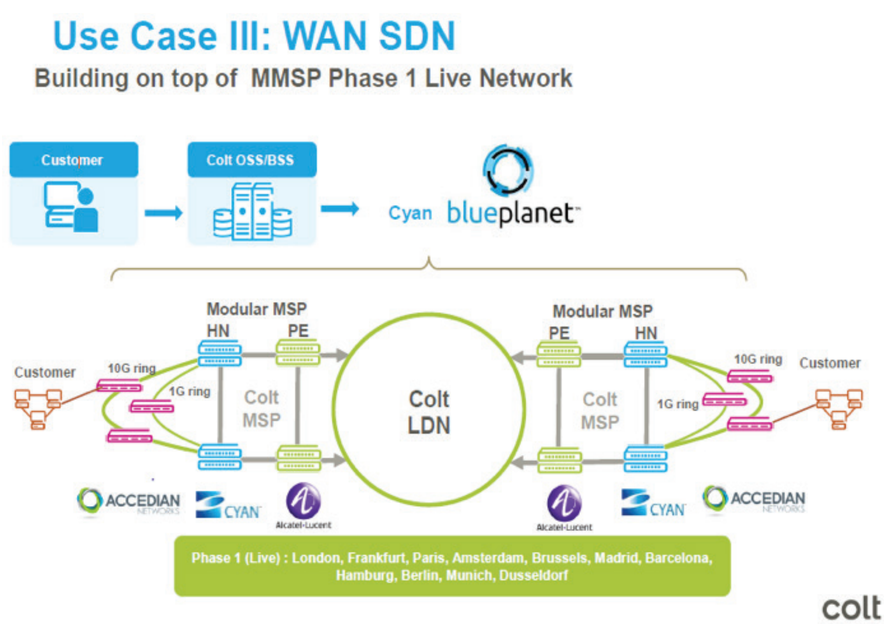

Figure 6. Colt WAN SDN use case.

Intel's Role in Addressing Market Pain Points

To accelerate adoption of VNFs, including vE-CPE, CSPs require that technology innovations solve a business problem or enable a new capability. Intel is driving the ecosystem forward by our participation in the Open Platform for NFV (OPNFV), European Telecommunications Standards Institute (ETSI), Open vSwitch* (OvS), OpenDaylight*, and other forums, contributing leadership and software to advance the state of the art in NFV. Several key areas Intel is working in this advancement include improved packet processing and inter-VNF communications. These two critical areas improve the performance of moving traffic from physical interfaces to the application layer and back out to the physical network. In addition, inter-VNF communications enable cooperative VNFs to communicate without requiring the data to flow to the physical interface. This technology enables the VNFs and routing applications to scale more efficiently to optimally deliver end-to-end services. Having an ecosystem where common software-defined programmability of virtualized functions and routing between these functions improves the ability to scale and steer traffic more efficiently.

Intel technology supports a number of potential vE-CPE deployment models (see Figure 7):

- Virtualized services on the router in the branch office
- Virtualized router and services running in the branch office
- Virtualized services in the data center, either centralized or distributed

Using a vE-CPE design that incorporates Intel® processors helps ensure the solution will have the performance and scalability to run multiple virtualized services on a single system. CSPs can draw from the Intel processor portfolio to offer a full range of vE-CPE solutions, sized for different numbers of virtual network functions and users. For example, CSPs can create small, medium, and large-scale solutions using the Intel® Atom™ processor C2000, Intel® Xeon® processor D product family, and Intel® Xeon® processor E5 family.

SDN/NFV For vE-CPE Network Functions

SDN and NFV promise to revolutionize the industry by driving reduced cost and increased service revenue. However, the transition to NFV will require a number of new, disparate technologies to work collaboratively. The maturity of these technologies is captured in Intel's Network Maturity Model for CSPs.[4]

Technology Overview

Virtualization of the CPE can be sized based on the capacity demand (for example, the number of expected users and data rate needs), and in addition it may be deployed on-premises or in the cloud. Earlier we segmented the size into three categories: small, medium, and large enterprises. This sizing spans from ~25 users to ~2000 users. While the location of the CPE may be critical to the TCO model the VNFs remain relatively independent of this decision. Furthermore the key is

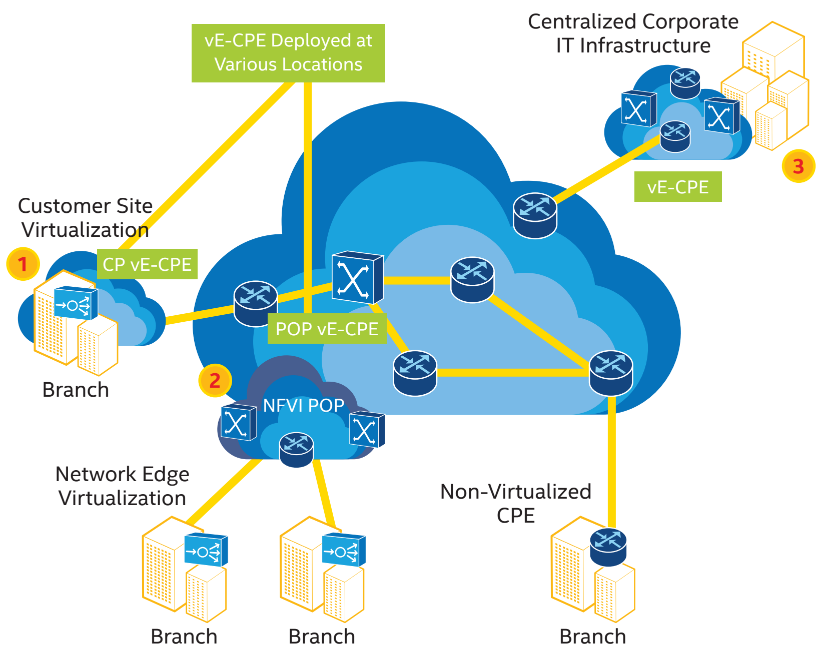

Figure 7. vE-CPE deployment models.

that the virtualized network functions are independent of the underlying hardware. As the enterprise scales, the customer or CSP can easily upgrade the hardware while maintaining the same upper-layer software and being assured of continued performance with increased capacity. This model drives savings for the CSP and enables faster service-creation capabilities.

Customer-Premise-Delivered Services

The delivery of CPE VNFs to the customer through software is targeted at the broad spectrum of enterprises, including those that typically outsource their network management functions. The functionality of WAN acceleration can only be delivered with an NFV at the premise (see Figure 8). In addition, some business models such as finance or health care may mandate premise firewalls. These are only two examples of the business drivers that may force placement of VNFs on Standard High Volume Servers that are resident at the customer site rather than in the network as we will see below.

In this solution, the NFV orchestrator remotely deploys the VNFs at the customer site onto a pre-delivered, secure Intel® architecture-based server. Security is tantamount, particularly at this stage of the operation, and Intel provides server identification (Intel® Trusted Platform Module technology), secure boot, and Intel® Trusted Execution Technology (Intel® TXT).[5] An SDN OpenDaylight controller configures, and centrally manages, the CPE policy. The controller also configures the Open vSwitch fabric to enable service chaining.

NOTE: There are issues with OpenStack* being used to deliver these remote site VNFs. Intel is working to solve these issues and, in the meantime, solution providers are developing their own simple agents that respond to the cloud controller (OpenStack)

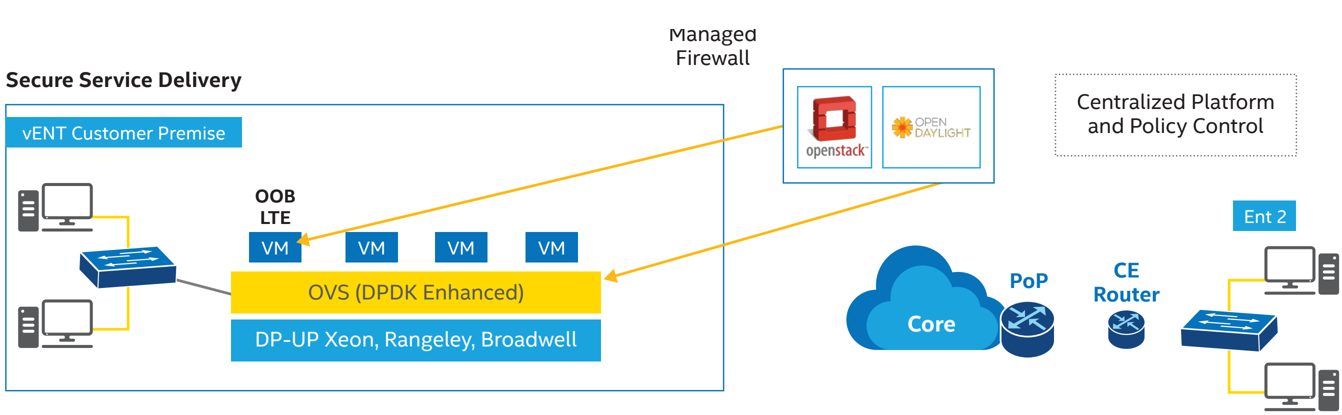

Figure 8. vE-CPE implementation at the customer premise.

Network- Or Cloud-Delivered Services

For this implementation, significant VNFs are deployed at the network or in the cloud, rather than at the customer premises (see Figure 9). Scale may be one driving force in CSPs desiring centralized placement in addition to greater levels of automated control of services delivered to the enterprise.

In this solution, enterprise access speeds range from 10–100 Mbps and up to 1 Gbps, which may be much faster than in the prior example. Provider Edge (PE) router VNFs are expected to support up to 1 Gbps, which will enable multi-tenant PE routing solutions. These routers are located in the CSP's central office or regional data center. The NFV orchestrator deploys the VNFs in the point of presence (PoP) or data center. The SDN OpenDaylight controller centrally configures the stored CPE policy and configures Open vSwitch. With this solution, solution providers should see an improvement in the timely delivery of value-added services.

While operators may choose to deploy either model, it is common to deploy both depending on business needs. For example, one site may require a simple L2 switch, which can be provided as a service in the PoP or network edge. This is a common scenario when there is no IT onsite and the capability is completely outsourced. Another example is deploying VNFs on the vE-CPE, managed by either the network operator or customer, depending on preference and/or business needs. Customer management of the VNFs is accomplished through a vendor-specific cloud portal.

Intel® Technologies and Ecosystem Enablers

For network CSPs who intend to deploy vE-CPE solutions, Intel architecture and ecosystem contributions are significant. Intel's product performance, unique platform awareness capabilities, software portability from network edge to core, and contributions to open source communities and standards bodies all support solution realization.

Intel's chipset and platform capabilities enable vE-CPE network functions to facilitate efficient resource utilization through optimal performance and programmability. Intel continues to work with the ecosystem to enable optimal use of these capabilities with seamless integration by the NFV/SDN architecture.

VNFs benefit from the ongoing efforts to enable and enhance the horizontal platform. Platform capabilities based on Intel's chipsets supporting open source ingredients (including the Data Plane Development Kit (DPDK)[6] and Open vSwitch[7]), are leveraged by VNF providers to achieve the benefits of NFV. The horizontal platform provides the foundation for a virtualized infrastructure. Capabilities such as CPU/memory virtualization, I/O virtualization, workload isolation, and acceleration are the foundation of NFV.[8]

Intel works closely with ecosystem participants to develop reference architectures that maximize the value of vE-CPE. These architectures capitalize on open, industry-standard technologies to help CSPs reduce vendor costs, more easily produce scalable solutions, and accelerate time to market for new solutions. Purpose-built devices require CSPs and their hardware partners to qualify each version of a device, whether it is produced to offer a distinct service or to accommodate a different number of users. With vE-CPE based on industry-standard technologies, CSPs can produce—and qualify—fewer variations for their solutions. The virtualized environment allows them to support different services and to scale more easily.

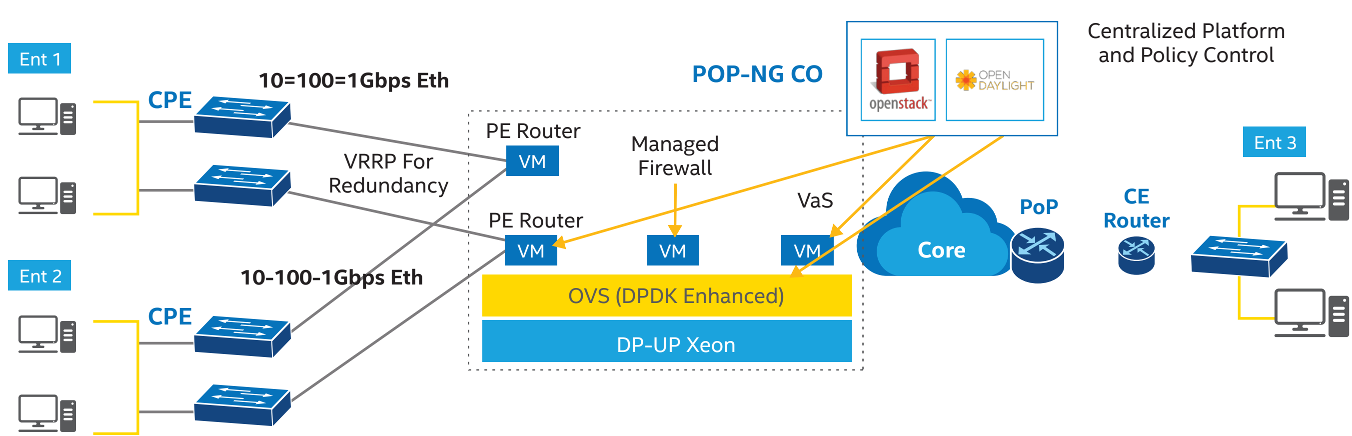

Figure 9. Network-edge enterprise implementation.

Technologies from ecosystem participants provide the range of network service functions available through a vE-CPE solution. CSPs and their customers can choose from multiple vendors that offer:

- Virtual machine manager (VMM) and virtual switch functions
- Low-end virtual customer-edge (CE)/PE routers
- Virtual firewalls
- WAN acceleration solutions
- Value-added services

CSPs can use fully commercialized solutions for vE-CPE or integrate open source components, either by using in-house engineers or by working with an integration vendor. No matter which approach they take, CSPs and their customers will benefit from the openness and flexibility that the virtualized solution provides. Customers can select the services they need from the virtualized capabilities offered by their preferred vendors without having to add more purpose-built hardware. Meanwhile, CSPs can meet each customer's unique requirements without having to offer numerous hardware versions of their solution.

Intel's Chipset and Architecture Capabilities

Specific Intel capabilities that drive optimal performance and security for vE-CPE type functions are identified below. Some of these capabilities include Enhanced Platform Awareness (EPA),[9] platform QoS, Intel® QuickAssist Technology,[10] Intel TXT, and Intel® Advanced Encryption Standard New Instructions, among others.

Table 1 provides links to more information on these specific capabilities.

Table 1. Links to Intel's Chipset and Architecture Capabilities.

PLATFORM QOS	http://www.intel.com/content/www/us/en/communications/cache-monitoring-cache-allocation-technologies.html https://01.org/packet-processing/cache-monitoring-technology-memory-bandwidth-monitoring-cache-allocation-technology-code-and-data
INTEL® QUICKASSIST TECHNOLOGY	http://www.intel.com/content/dam/www/public/us/en/documents/white-papers/communications-quick-assist-paper.pdf https://01.org/packet-processing/intel®-quickassist-technology-drivers-and-patches
INTEL® TRUSTED EXECUTION TECHNOLOGY	http://www.intel.com/content/www/us/en/architecture-and-technology/trusted-execution-technology/malware-reduction-general-technology.html http://www.intel.com/content/www/us/en/architecture-and-technology/trusted-execution-technology/trusted-execution-technology-security-paper.html http://www.intel.com/content/dam/www/public/us/en/documents/guides/intel-txt-software-development-guide.pdf
INTEL® ADVANCED INSTRUCTION STANDARD NEW INSTRUCTIONS	https://software.intel.com/en-us/articles/intel-advanced-encryption-standard-instructions-aes-ni http://www.intel.com/content/dam/www/public/us/en/documents/white-papers/aes-ipsec-performance-linux-paper.pdf
ENHANCED PLATFORM AWARENESS	https://software.intel.com/sites/default/files/managed/8e/63/OpenStack_Enhanced_Platform_Awareness.pdf https://networkbuilders.intel.com/docs/openStack_Kilo_wp_v2.pdf
OPEN VSWITCH*	https://networkbuilders.intel.com/docs/open-vswitch-enables-sdn-and-nfv-transformation-paper.pdf
DATA PLANE DEVELOPMENT KIT	http://www.intel.com/content/www/us/en/intelligent-systems/intel-technology/dpdk-packet-processing-ia-overview-presentation.html https://networkbuilders.intel.com/docs/aug_17/Future_Enhancements_to_DPDK_Framework.pdf
HW OFFLOAD	http://www.intel.com/content/www/us/en/ethernet-products/controllers/overview.html

Open Source And Standards:

Intel is driving software contributions and broad market capabilities through open source communities.

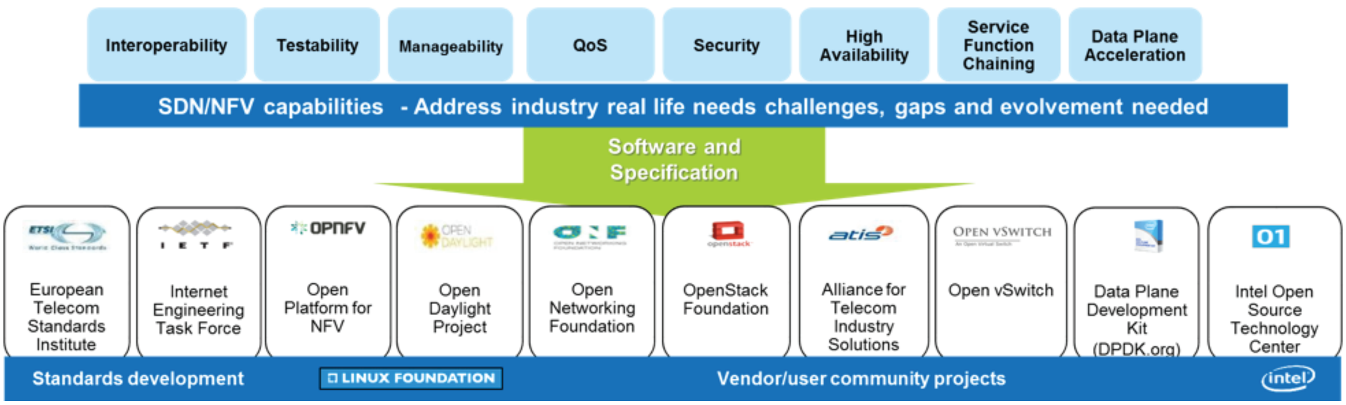

Figure 10. Network-edge enterprise implementation.

Intel invests in 10 open source and standards initiatives shown in Figure 10, from the ETSI-NFV group to Intel's own packet processing project on 01.org.

Contributions are driven both by the market and by specific customer requirements, including real-life deployment and business needs, target performance metrics, closing development gaps, and providing management tools needed to ensure service levels.

Intel's contribution spans the entire spectrum, including technical specifications, code development, testing and benchmark tools, and reference platforms.

Intel® Open Network Platform Reference Architecture

Intel® Open Network Platform (Intel® ONP) Server is an enablement program with a reference architecture integrating Intel® hardware and open source software ingredients for easier ecosystem adoption. One of the key objectives of Intel ONP Server is to align and optimize key open community software ingredients for architects and engineers targeting high-performing SDN and NFV solutions. The Intel ONP provides a convenient reference platform to evaluate the latest performance contributions for OpenStack,[11] DPDK,[12] and accelerated OvS.[13]

Intel® Network Builders

Intel recognizes that part of enabling network transformation requires a strong ecosystem of partners. The Intel® Network Builders community (www.networkbuilders.intel.com) has more than 180 partners developing SDN/NFV solutions on Intel architecture. Within this community, there are more than 30 software vendors for critical SDN/NFV use cases, including vE-CPE. The work of the community extends to proofs of concept, reference architectures, and trials. With the help of its ecosystem partners, Intel remains committed to the development of technology solutions and capabilities that will improve the performance of VNFs for CSPs.

Figure 11. The Intel® Network Builders community.

The following table provides a list of Intel's vE-CPE ecosystem partners.

Table 2. Intel's vE-CPE ecosystem partners.

vE-CPE Ecosystem Vendors	
VMM and Virtual Switch	
Canonical	www.canonical.com
HP	www.hpe.com
Red Hat	www.redhat.com
VMware	www.vmaware.com
Virtual CE/PE Router	
Brocade	www.brocade.com
Cisco	www.cisco.com
HP	www.hpe.com
Juniper Networks	www.juniper.net
Virtual Firewall	
McAfee	www.mcafee.com
WAN Acceleration	
Array Networks	www.arraynetworks.com
Blue Coat	www.bluecoat.com
Cisco	www.cisco.com
Riverbed	www.riverbed.com
vE-CPE Cloud and NG-CO Ecosystem Vendors	
PE Router	
Alcatel Lucent	www.alcatel-lucent.com
Brocade	www.brocade.com
Cisco	www.cisco.com
HP	www.hpe.com
Huawei	www.huawei.com
Juniper Networks	www.juniper.net

vE-CPE Ecosystem Vendors	
Enterprise VoIP	
Alcatel Lucent	www.alcatel-lucent.com
Genband	www.genband.com
Mavenir	www.mavenir.com
Metaswitch Networks	www.metaswitch.com
Oracle	www.oracle.com
Sonus Networks	www.sonus.net
Wi-Fi* Controllers	
Cisco	www.cisco.com
Juniper Networks	www.juniper.net
Virtual Firewall	
Cisco	www.cisco.com
McAfee	www.mcafee.com
WAN Acceleration	
Array Networks	www.arraynetworks.com
Blue Coat	www.bluecoat.com
Cisco	www.cisco.com
Riverbed	www.riverbed.com

Additional Information

- OpenDaylight Contribution and IETF efforts on NSH
  https://tools.ietf.org/pdf/draft-ietf-sfc-nsh-00.pdf
  https://wiki.opendaylight.org/view/Project_Proposals:Service_function_chaining
- OpenStack EPA contributions
  https://01.org/sites/default/files/page/openstack-epa_wp_fin.pdf
  https://networkbuilders.intel.com/docs/openStack_Kilo_wp_v2.pdf
  https://www.brighttalk.com/webcast/12229/181563
- Intel Open Network Platform
  https://01.org/packet-processing/intel%C2%AE-onp

Intel Network Builders:

- https://networkbuilders.intel.com/docs/Intel-Virtual-VOIP-Orch-RA.pdf
- https://networkbuilders.intel.com/solutionscatalog/session-border-controller-74

[1] https://www.idc.com/getdoc.jsp?containerId=IDC_P567
[2] http://www.infonetics.com/pr/2015/NFV-Strategies-Survey-Highlights.asp
[3] www.http://acgcc.com/?s=managed+network+service+providers
[4] http://www.intel.com/content/www/us/en/communications/service-provider-network-maturity-paper.html
[5] http://www.intel.com/content/www/us/en/architecture-and-technology/trusted-execution-technology/malware-reduction-general-technology.html
[6] http://www.dpdk.org
[7] http://openvswitch.org
[8] http://www.intel.com/content/www/us/en/virtualization/virtualization-technology/intel-virtualization-technology.html
[9] https://software.intel.com/en-us/articles/openstack-enhanced-platform-awareness
[10] https://01.org/packet-processing/intel%C2%AE-quickassist-technology-drivers-and-patches
[11] http://www.openstack.org
[12] http://www.dpdk.org
[13] http://openvswitch.org