INTEL® NETWORK BUILDERS
SOLUTION BRIEF

USING SERVICE CLASSIFICATION TO BUILD AN APPLICATION-AWARE NFV INFRASTRUCTURE FOR VIRTUAL CPE SERVICES

Reduced costs, simpler subscriber equipment, stronger services, and increased service agility

intel XEON® inside™

QOSMOS

In order to increase profitability and compete effectively, especially against cloud service providers and over-the-top (OTT) services companies, communications service providers are looking to reduce costs, simplify customer infrastructure, and increase service agility.

One way to achieve this is through support of virtual customer premise equipment (vCPE) as a new service delivery architecture. With vCPE, the carrier installs basic customer premise equipment (CPE) at the subscriber site, and delivers more advanced CPE service functions from a data center in a central office, point of presence (PoP) or other central location.

This Intel® Network Builders solution brief covers how technology from Qosmos and Intel can help network equipment, platform, middleware, and software suppliers build the application-aware network needed to deliver high performance vCPE applications.

vCPE IS TAKING OFF

vCPE is one of the 10 original NFV use cases in a list[1] developed by the European Telecommunications Standards Institute (ETSI), the standards body in charge of NFV. With vCPE, communications service providers can reduce costs, simplify CPE and increase service agility by hosting all virtualized CPE functionality in the network, at a PoP or in another type of data center.

Virtual CPE is an alternative way of delivering broadband services to subscribers, where most of the CPE functions are delivered by the communication service provider's network and located near the service edge. In this new network architecture, the on-premise CPE acts as a simple layer 2 forwarding device that helps a business or residential subscriber to physically connect their network to the communication service provider network. Services such as DHCP, firewall, NAT, routing, VPN, etc. are delivered by virtual network functions (VNFs) running at the communication service provider data center as virtual machine (VM) instances configured for each broadband subscriber.

Telefónica is a communication service provider that has actively publicized[2] its success with its vCPE architecture, claiming that it is able to deliver network functions such as IP routing, IP address management (DHCP), network address translation (NAT), firewall, and set-top box functionalities (live TV, VoD, etc.) to homes from a central location. The company states that it has been able to deliver new services in 50% less time with the vCPE architecture, and it has reduced the cost to deliver the services because they are maintained and upgraded from a central location.

NFV IS THE FOUNDATION OF vCPE ARCHITECTURE

The networking and telecommunications industries have begun to incorporate virtualization technology in ways similar to data centers. Adopting principles outlined by

1 Network Functions Virtualisation (NFV); Use Cases (PDF download: http://www.etsi.org/deliver/etsi_gs/NFV/001_099/001/01.01.01_60/gs_nfv001v010101p.pdf)
2 Telefónica's Virtualized CPE (https://communities.intel.com/community/itpeernetwork/datastack/blog/2014/03/04/telef%C3%B3nica-s-virtualized-cpe)

network functions virtualization (NFV), network functions are being consolidated onto standard, high-volume servers, switches, and storage in order to increase flexibility, equipment utilization, and operating efficiencies. This has set the stage for extending this virtualization to the customer premise through vCPE applications. But some challenges remain, including:

1. Optimizing the number and sequence (chain) of service functions needed to process traffic
2. Securing network traffic in a virtualized multi-vendor and multi-application infrastructure
3. Ensuring traffic visibility per subscriber

APPLICATION-AWARE NETWORKS – A STARTING POINT FOR vCPE

To resolve the three challenges that stand in the way of a successful vCPE solution, communications service providers need application-aware networks; that is, there must be embedded network intelligence to understand what data is being transmitted on the network in order to apply the right service chain or policy.

Solving Technical Challenge 1: Optimizing Service Chaining

The Qosmos Classifier* is an IETF-compliant layer 7 classifier, in the form of a VNF, providing full network application visibility. It is used to optimize services delivered to premises, based on real-time application and subscriber information. The classifier can be configured using reference controller implementations such as OpenDaylight SFC* for service function chaining. It is a standards-based, pure software product that colors IP traffic with application awareness, using the upcoming IETF network service header (NSH) service chain header tagging standard, or existing type of service (ToS) differentiated services code point marking, vLAN tagging, or others.

The Qosmos Classifier makes use of Intel technology to help deliver the performance needed for vCPE applications. This starts by optimizing the Qosmos Classifier VNF to run on Intel® Xeon® processor-based servers. To avoid latency from the Linux kernel, Qosmos implemented Qosmos Classifier using the Data Plane Development Kit (DPDK), a set of software libraries and drivers developed by Intel, but now available as open source software. DPDK provides enhanced packet processing and forwarding capabilities, letting Xeon-based servers deliver very high packet throughput rates.

Suppliers of equipment, platforms, middleware, and software can leverage this Qosmos and Intel technology to rapidly build application-aware solutions for service providers, data centers, and enterprises. The Qosmos Classifier is especially well suited to enable intelligent, dynamic service chaining for cloud-based vCPE environments.

Solving Technical Challenge 2: Securing Network Traffic in a Virtualized Environment

Third-party VNF applications inside the vCPE data center provide a range of value-added services, such as NAT, VPN, and security. Micro-segmentation is a new approach to strengthen cyber security by controlling inter-VM communication and applying security policies to

individual or groups of interfaces. For example, this can be implemented using OpenStack security groups based on Linux Iptables firewalling. By embedding DPI and network intelligence directly into the NFV infrastructure, micro-segmentation and firewalling becomes application aware, which leads to even more efficient and accurate security.

Solving Technical Challenge 3: Ensuring Traffic Visibility per Subscriber in a Virtualized Infrastructure

A DPI-based virtual probe (vProbe) plays a key role in the infrastructure by duplicating and forwarding traffic to a VNF reporting function and sending statistics to the NFV orchestrator.

CONCLUSION

With an application-aware NFV infrastructure based on Qosmos Classifier and Intel technology, service providers are able to build out a cost-effective vCPE architecture including service chaining that has the potential to deliver services faster, at a lower cost, and with advanced firewall and micro-segmentation security. vCPE is an architecture of the future for carriers that can improve competitiveness and fully leverage NFV technology for rapid service delivery.

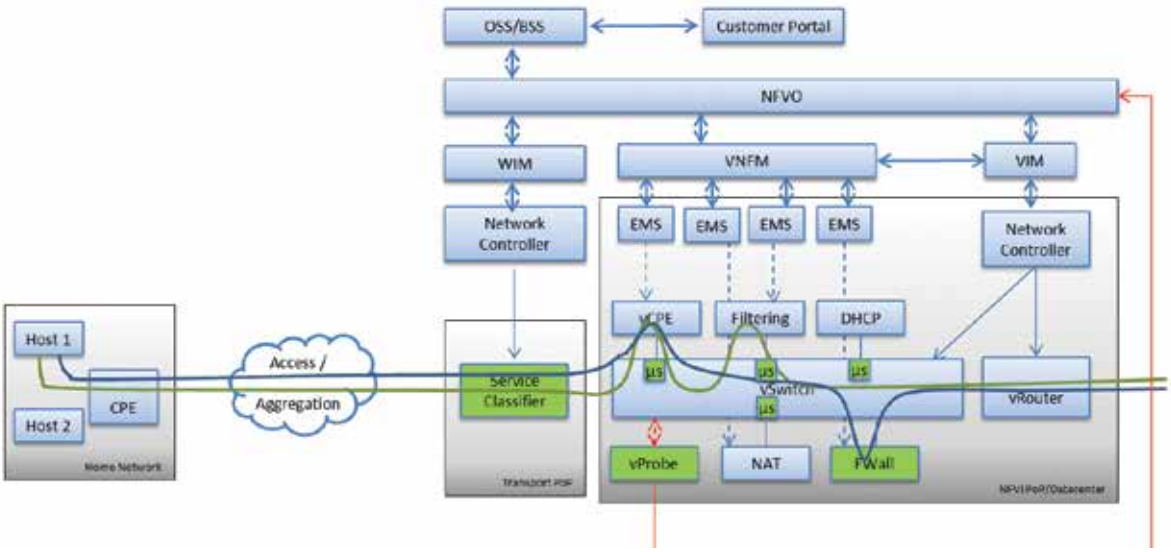


Figure 1: Overview of vCPE architecture leveraging application-aware functions embedded into the NFV infrastructure (green boxes)

BENEFITS SUMMARY FOR OPERATORS: vCPE based on Application-Aware NFV Infrastructure

- A new way for communications service providers to compete effectively against OTT players and increase profitability
- Possibility of reducing cost for procurement and maintenance of CPEs, since simple layer 2 CPEs do not require frequent replacement or upgrades
- Communications service providers can provide traditional private line service and value-added NFV services using the same transport network platform
- A practical way to launch value-added services, such as network control, VPN, security, etc. in the traditional transport network without complicating the existing CPE devices
- A way to let users define their own services, service order, and sequence

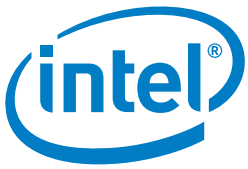
About Intel

Intel (NASDAQ: INTC) is a world leader in computing innovation. The company designs and builds the essential technologies that serve as the foundation for the world's computing devices. As a leader in corporate responsibility and sustainability, Intel also manufactures the world's first commercially available "conflict-free" microprocessors. Additional information about Intel is available at newsroom.intel.com and blogs.intel.com and about Intel's conflict-free efforts at conflictfree.intel.com.

About Qosmos

Qosmos leads the market for Deep Packet Inspection (DPI) and network intelligence technology used in physical, SDN and NFV architectures. The company supplies software to vendors who embed real-time application awareness in their products for traffic optimization, service chaining, quality of service, analytics, cyber security and more. Qosmos brings fast time to market for network intelligence and continuous protocol signature updates inside physical, SDN and NFV networking products. As the leading supplier of network intelligence software, Qosmos contributes actively to open source projects and international standards, and serves 75% of the market.

For more information, please visit www.qosmos.com



Disclaimers

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at intel.com.