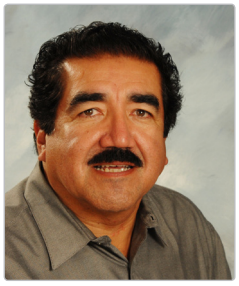

# Decision Factors in Service Providers' vCPE Migration

## Evaluating the trade-offs in applying NFV to enterprise services delivery

# Contents



# About the author



**Mike Sapien**

Mike Sapien is responsible for Ovum's US Enterprise Practice. Based in southern California, Mike is focused on North American and global enterprise telecom markets. This includes WAN, managed, and advanced voice and data services to address Global MNC, large enterprise, and SMB customers. His focus areas also include data center services, emerging cloud and hosted services, enterprise mobility services and related product development, market launch, and channel programs of enterprise services. Mike has also been ranked 2nd out of the top 100 analysts, this is constituted by their level among all ARchitect users.

Mike leads the design, development, and implementation of Ovum's research and advisory services on enterprise network services and managed solutions in North America with a major emphasis on the tier 1 carriers, infrastructure vendors and providers. Mike works directly with clients to help them understand and implement recommended strategies from Ovum research, consulting experience and his extensive telecom services expertise. He is a regular contributor to Ovum's enterprise research, and provides analysis of industry, vendor, and product trends included emerging managed services such as SIP trunking, unified communications, VoIP, and complex managed services.

# Summary

## In brief

Enterprise services are typically delivered with a handful of single-function, proprietary hardware appliances located at the customer premises and connected to a network. Virtualized CPE (vCPE) is a new networking framework based on the ETSI NFV architectural framework that leverages cloud and virtualization technologies to deliver network services from a virtualized platform located at the customer premises, the provider cloud node, or both.

Installing, managing, and maintaining equipment at the customer premises is complex, labor-intensive, and costly. Service providers are excited about the potential for vCPE to reduce their costs and improve margins by replacing vendor-specific hardware appliances with virtualized network functions (VNFs) running on commercial off-the-shelf (COTS) hardware. They also recognize that service innovation enabled by vCPE network agility will bring additional customer value, especially in delivering managed IP access and VPN services to small and medium businesses (SMBs).

Although there is industry activity aimed at virtualizing some residential services, such as set-top boxes and home gateways, vCPE for delivering business services is emerging as a leading use case for NFV deployment in 2016. This report discusses many of the decision factors and implementation options service providers should consider in evaluating vCPE deployment.

## Ovum view

- **Many vendors are now ready with vCPE products.** In addition to the large ecosystem of VNF specialist suppliers, vCPE hardware and software platforms are available from vendors such as Accedian, Anuta Networks, Cisco, Huawei, Juniper, NEC, and RAD.
- **vCPE does not completely eliminate the need for some service functionality at the customer premises.** Whether provided by a physical device or even virtualized within a customer device, there remains a need for some basic service demarcation capabilities at the customer site.
- **VNF placement is the first question service providers typically raise with suppliers.** Does a VNF belong at the customer premises or should it be moved into the service provider's network? Early deployments are relying on manual provisioning of VNFs, although control systems often allow some level of drag-and-drop configuration, self-provisioning, and automation.
- **A reliable connection to the customer is critical.** vCPE uses network functions virtualization infrastructure (NFVI) and cloud technology to deliver on-demand virtualized network and value-added services (e.g. security services) from the service provider cloud to the customer edge. The connection to the customer must be highly reliable and offer consistent quality of service for this model to succeed, which again may require demarcation at the customer site.
- **vCPE adoption involves three main elements.** vCPE implementation consists of a management and orchestration (MANO) software stack, a new customer premises platform, and a set of VNFs.
- **vCPE can support integration of service automation with telco back-end systems.** Customers can initiate service requests from a self-service portal, and services can be turned up automatically in minutes—a convenience that service providers' customers expect and may be willing to pay for.
- **Operational over-complexity is a potential hazard.** Hardware abstraction with vCPE can support a multi-vendor environment and an easy path to platform upgrades. However, service providers need to be careful not to inject new operational complexity with too many vCPE hardware and software options.

### Recommendations for service providers

- Service providers need to have a long-term view of vCPE deployment, seeing it not as an approach to delivering an individual service or set of services but as a platform for providing existing and future services.
- Service providers need to identify which network functions can be effectively virtualized, which may be best left at the customer premises, and any performance impacts that result from VNF placement decisions.
- Service providers should consider the benefits of incorporating some form of intelligent network interface device (NID) for service demarcation and QoS and QoE monitoring at the customer site to provide consistent, reliable visibility into the customer experience and network performance.
- Customer feedback on the provider's service delivery, portal, and service choices needs to be understood and integrated into the service provider's business model with continuous improvement in mind. Service portals should report actual performance and usage for each service, in addition to allowing customers to provide feedback (closed-loop, real-time).
- vCPE can improve a service provider's market position. The ability to offer network flexibility and innovative customer-focused services can help a provider differentiate itself with customers and solidify its position as a technology leader.
- Service providers need to be very careful not to confuse customers with too many choices as they deploy vCPE.

## Why transform CPE?

Service providers offer a wide variety of enterprise services, often with numerous customer-selectable options. In order to deliver traditional enterprise services with the legacy network appliance model, service providers needed to make a large investment in sourcing, installing, configuring, updating, and maintaining a wide array of customer premises equipment. Depending on the services provided to each individual customer, they had to select and deliver, install, cable, configure, and test a variety of discrete platforms from multiple vendors for firewall, intrusion prevention and detection (IPS/IDS), routers, network address translation (NAT), WAN optimization, and many other functions. Obviously installing, managing, and maintaining equipment at the customer premises is complex, labor-intensive, and costly to the service provider and the customer.

Although most enterprise customers want a better solution for CPE, small to medium businesses are a prime target market for vCPE. Service providers that have presented vCPE capabilities to their SMB customers have found they are willing to pay for features the technology enables. These customers welcome the rapid service turn-up and service reconfiguration, flexible managed services options, and pay-for-use service models that can be offered with a vCPE implementation.

Virtualized CPE is an early use case for SDN and NFV, and its deployment will have a big impact on service provider infrastructure and operations. Many service providers, including mobile operators, cable MSOs, and wireline operators, have made progress in evaluating the business case for enterprise vCPE and are moving along the path to deployment. Trials and proof-of-concept (PoC) demonstrations of vCPE have been run by many providers including Telefonica, China Telecom, and Telekom Austria. In 2012 Colt Technology Services developed a commercial managed router capability for Colt's IP access and IP VPN services that relocated the functions of a customer premises router into a Colt network node. Orange Business Services introduced its Easy Go Network as a live trial In March 2015. The Easy Go architecture virtualizes the dedicated appliances that typically would be installed at the customer location, remotely hosting customer-selected services as VNFs within an Orange cloud data center. AT&T has performed trials and expects to begin vCPE deployment in mid-year 2016.

The virtualization of CPE will also support service providers' long-term transformation from being connectivity providers to delivering value-added services that effectively monetize their networks. Moving to

vCPE can help service providers avoid vendor lock-in, improve margins, and move to a lower cost structure with a virtualized infrastructure and the benefits of COTS hardware elements and open source software.

**Table 1: Benefits of vCPE for service providers and customers**

| Service provider benefits | Customer benefits |
|---|---|
| Reduced capex | Faster, simpler installation |
| Reduced opex | Access to rapid service innovation |
| Faster time to market | New lower-cost pricing models |
| More rapid service innovation | Lower opex |
| Reduced management complexity | More control and configuration options |
| Fewer site visits | Greater reliability |

Source: Ovum

## Service provider benefits with vCPE adoption

While cost reduction is an important consideration driving vCPE deployments, rapid time to market, service flexibility, and an ability to easily introduce innovative customer services will be the long-term benefits of these deployments. The most important benefits of implementing a vCPE architecture for the service provider are presented below.

**Reduced capex** – vCPE relies on a hardware device or NID at the customer premises that combines switching and computing elements to implement an NFV infrastructure. These hardware devices are much less expensive than a collection of service provider–owned physical devices. Further capex savings accrue when additional customer services are delivered from the existing virtualized platform without having to install and configure new hardware elements at the customer premises. With fewer and more standardized platforms at the customer location, the cost of managing spares inventory is also reduced.

**Reduced opex** – With fewer devices at the customer premises, the costs involved in sourcing, installing, configuring, and maintaining customer premises equipment are lower with vCPE deployments than with the legacy hardware appliance model. Fewer devices means a lower risk of equipment failure, and therefore less need for expensive truck rolls to configure, repair, and replace CPE. Automated vCPE configuration can simplify service provisioning, reduce manual errors, and even support customer control of service turn-up and changes. Simpler customer premises hardware means easier troubleshooting and a reduction in the time to locate and repair faults that do occur.

**Faster time to market** – vCPE delivers virtualized network services with a fully automated platform. This means customers can initiate service requests from a network-supported self-service portal—rather than requiring a time-consuming manual configuration process, network services can be turned up automatically in minutes.

**More rapid service innovation** – A vCPE architecture allows the service provider to operationalize a new approach (really a new platform) for enterprise services. Dynamic service chaining employed with vCPE can deliver service flexibility and a cost-effective, highly customized user experience. The ability to rapidly reconfigure the network to launch new services, or make changes to existing services, without having to deliver, install, configure, and test new physical devices at customer locations opens the door to rapid service innovation, something customers may be willing to pay for as a premium service. The service provider can now deliver services in an integrated and on-demand manner that can provide connectivity with new cloud-based applications and services. Automation and network agility may lead to more marketing involvement in developing new services, and this may even lead to short-term promotional or freemium offers.

**Reduced management complexity** – Centralized management and orchestration of software, accompanied by a simplified customer premise, reduces the complexity of many of the management tasks associated with a CPE deployment. Software updates can be automatically implemented network-wide rather than requiring updates that have to be manually delivered to each customer premises device. This ease in delivering software upgrades means customers are always using the latest version, which can lower opex (for the service provider and customers) and simplify troubleshooting. Centralized management and orchestration of software can also automate the software licensing management task, an important consideration with software-based technology.

**Fewer site visits** – In this model, site visits are dramatically reduced, if not eliminated. Field technicians' work is simplified: they no longer need to be experts in the detailed configurations and interdependencies of multiple, physical appliances, which means reduced on-site visit time for initial installation as well as any upgrades of remaining on-site CPE.

## Customer benefits with vCPE adoption

Many of the benefits of implementing a vCPE architecture accrue to the service provider. Typically, customers care more about service availability and cost than about the technology used to deliver their services. However, enterprise customers served with a vCPE architecture can expect to receive additional value from deployment of this technology, and service providers can effectively market these benefits to differentiate their services.

**Faster, simpler installation** – Services will be installed faster, and in some cases a customer self-install service model will become the norm, even with a complex set of services.

**Access to rapid service innovation** – vCPE enables network services to incorporate dynamic capabilities that allow rapid turn-up (and turn-down) of new value-added services and changes to existing services. It will also support the rapid introduction of new innovative services—for example, services customized to a particular market vertical—that may not have been technically or economically feasible with the hardware appliance–based implementation model.

**New lower-cost pricing models** – With a more efficient cost structure, service providers will be able to offer enterprise customers more attractive pricing options. While some pay-as-you-grow pricing is available today based on access bandwidth, value-added services or combinations of services will allow more creative, cost-effective packaging.

**Lower opex** – Requirements now placed on the customer for managing the CPE needed for network termination and service delivery will be eliminated, along with the related support tasks including managing software upgrades and version control. Troubleshooting should take less effort and will in some cases be automated. Requirements for power, floor space in terminal rooms, and staffing for personnel with the skills to support on-site hardware will be greatly reduced.

**More control and configuration options** – vCPE implementation will come with automation and self-service options to provide customers with more control over their services, including a customer portal to configure services in real time. With network-supported on-demand instantiation and configuration of vCPE, customers can self-provision or change their service in a few minutes.

**Greater reliability** – Effective vCPE strategies result in highly simplified customer premises. With fewer physical appliances, reliability will be enhanced if a high-availability deployment model is employed.

# Developing a vCPE strategy

## Planning for vCPE

Service providers typically deploy managed services with a collection of single-function, proprietary hardware appliances installed at each customer service location. These appliances are usually sourced from a variety of manufacturers, with different vendors supplying discrete functions such as switching, routing, NAT, load balancing, firewall, IPS/IDS, and web filtering. The service provider takes responsibility for designing, deploying, and configuring all of the individual functions that make up a customer's service. The service provider, or the customer, has to manage the on-site CPE.

Because of the many manual tasks and technical skills involved, service turn-up can take weeks or months, and any customer requests for service changes can mean truck rolls to multiple customer locations for equipment upgrades or installation of additional equipment. Even remote software upgrades can require days of work and service disruption. As a result, the customer premises location is usually operationally costly for service providers even with some local customer support.

Service providers need to carefully design the end-to-end future mode of operation (FMO) from this present mode of operation (PMO) to provide these same services via vCPE. This planning has to include all the elements of the service and a complete lifecycle view of the platform, not just consideration of one service or one customer.

## vCPE will drive changes in the service provider business model

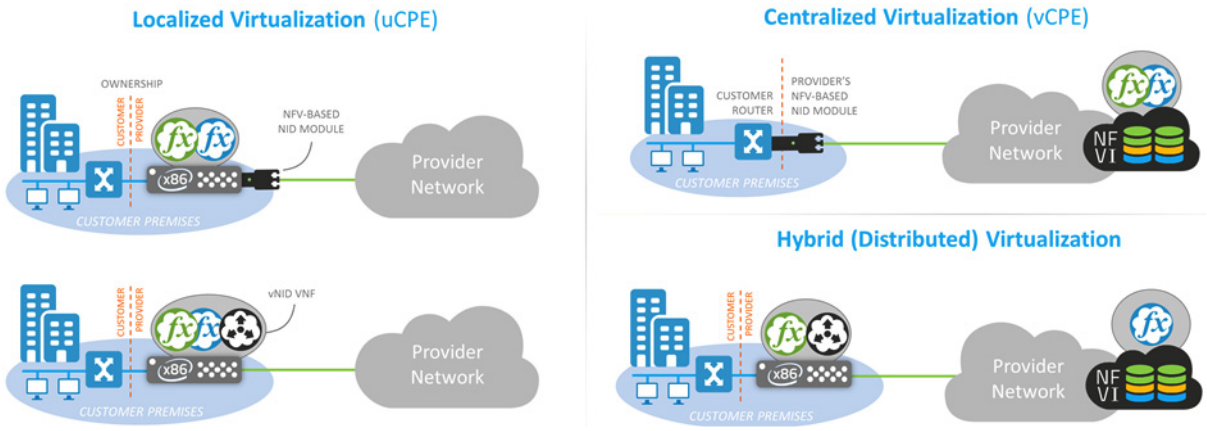
The implementation of vCPE will enable a new service provider model for managed services delivered to the enterprise market. Service providers will need to manage the existing customer base while transitioning to this new platform that will enable more flexible pricing options, flexible service configuration, enhancements to existing services, and previously unfeasible services. Pricing of the service elements within vCPE platforms will require new supplier pricing models and some flexibility as service providers test new services and gather customer adoption information. Co-development and joint innovation will be part of the common lexicon of any SDN/NFV and vCPE service provider–vendor discussion.

# Selecting an architectural approach

## Localized virtualization architecture

Ovum sees three common deployment models for vCPE.

Figure 1: vCPE deployment options




Source: Accedian Networks

The first is a localized virtualization architecture, shown on the left of Figure 1, where physical appliances at the customer premises are virtualized, and the NFVI and VNFs that implement network services remain

located within the customer premises on what is typically a simple Linux-based platform. AT&T uses the term universal CPE (uCPE) to describe the customer premises equipment in this deployment model. VNFs are run and service-chained within compute platforms that act as the NFV infrastructure. As shown in Figure 1, the NID function can be implemented via a smart module installed in the compute platform or integrated as a VNF within the platform.

With virtualization placed at the customer edge, the localized virtualization architecture does not require a major upfront investment by the service provider in data center deployments or upgrades or network redesign. This model can provide an effective vCPE solution with costs proportional to the number of served locations. It also offers the benefits of simplified orchestration, as each site's NFVI is self-contained and can be deployed to minimize dependencies on other remotely located functions or elements in the service chain.

This approach is especially attractive to service providers for early NFV-based vCPE deployments. The idea of universal CPE is attractive in its simplicity, as it replaces the operationally and logistically complex situation presented by the legacy use of a wide variety of single-function appliances to a single NFVI instance (COTS appliance with appropriate virtual infrastructure manager, hypervisor, etc.).

However, service providers are already discussing multi-vendor vCPE hardware environments, higher- and lower-performance vCPE platforms to match expected user requirements, and varying business cases that risk returning complexity to customer premises hardware. When compared to using centralized data centers to host functions, this solution is inelastic: the captive compute capacity of uCPE hardware needs to be overprovisioned to be future-proofed, and VNFs will continue to multiply and require increasing amounts of compute resources as they become more sophisticated.

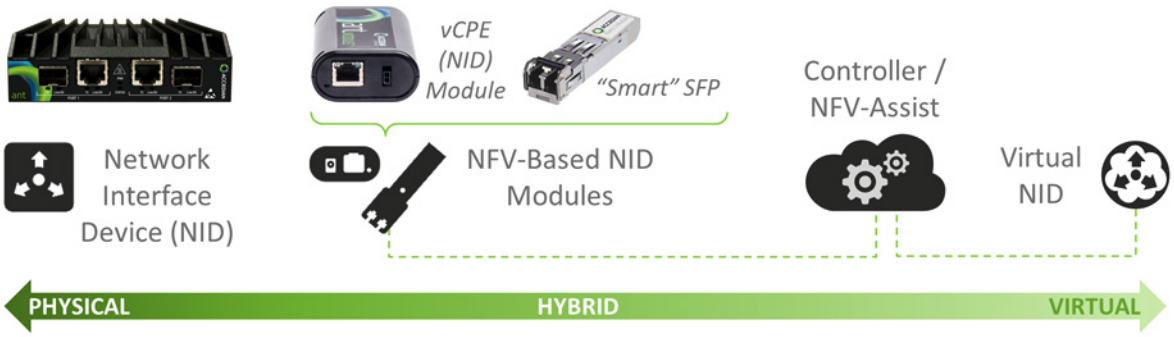
### Centralized virtualization architecture

With a centralized virtualization vCPE architecture (shown on the top right of Figure 1) the functions previously physically located in CPE are pulled back into the network as VNFs that are run on an NFVI in a service provider data center, or an edge PoP that looks like a data center (NFVI-enabled PoP). This allows the service provider to effectively share pooled network resources as needed among different customers. The hardware that remains at the customer premises is a simple and inexpensive NID installed at the customer premises that serves as the service demarcation point between customer-owned wiring and the provider's local loop.

As shown in Figure 2, the NID function can take several forms. It can be a standalone physical device, a "smart" SFP transceiver that plugs directly into customer equipment, or a virtualized function running in a customer device. Replacing a handful of on-premises equipment with a NID results in a very simple architecture at the customer premises.

The trade-off in this thin-client delivery model is that the service provider needs to make an upfront investment in a full NFV infrastructure (suitably performing data centers and interconnections) in convenient locations in its network, including a pool of COTS hardware resources, an NFVI framework, and the VNFs that provide customer services. The advantage is that as VNFs scale in number and sophistication, it is simple to add compute capacity to the pool on an as-needed basis.

Figure 2: Customer site network demarcation options




Source: Accedian Networks

## Distributed virtualization architecture

The distributed virtualization deployment model is a hybrid of the localized and centralized models and is the most flexible and the most complex implementation of vCPE. With a distributed virtualization architecture a service provider can place VNFs on an NFVI located either on the customer premises or within the service provider cloud, as shown on the bottom right of Figure 1.

Network services can be instantiated by service-chaining VNFs placed in either location, determined by the performance requirements of each delivered service. Of course this requires policy and orchestration sophistication to determine the best placement of VNFs for each workflow. While this deployment model has the drawback of an upfront investment in an NFVI in the service prover cloud, in addition to implementing an NFVI in every served customer premises location, it gives service providers great flexibility in VNF placement. The use of an overlay network between end locations and the service provider's cloud to link the elements of a distributed vCPE architecture can be an attractive option allowing service providers to extend their managed services outside their geographic footprint.

Providers who opt to start with a localized uCPE approach can scale up to this distributed model without losing their investment in on-premises COTS. It also extends the life of on-premises NFVI by permitting the transfer of all but location-critical VNFs to shared, centralized NFVI when local compute capacity approaches high levels of utilization.

## Where should VNFs be located?

Service providers Ovum has talked with readily see value in vCPE, although they typically have questions about where VNFs should be placed: at the customer premises, centralized in the data center, distributed in network nodes, or in a combination (hybrid) of locations. The decision on VNF placement should be based on an evaluation of the requirements of the use cases employed. In some cases, customer input may be part of this placement decision. Some important characteristics for consideration are presented here.

- Performance – Use case requirements for response time, QoS, or survivability may make some applications more effective when placed at the customer premises. What is the impact of any additional bandwidth overhead that results from moving network functions deeper into the network? Does available bandwidth capacity support this? What is the impact on delay-sensitive applications? Some functions such as end-to-end encryption and WAN optimization may need to be placed at the customer premises to be effective.

- Security and policy – Regulatory requirements placed on data storage locations, as well as customer policies on access control, can factor into VNF placement decisions. Does relocation of network functions expose customer data?
- Cost – Understanding start-up costs, operational costs, the operator's "virtualization skill set," and total cost of ownership can impact VNF placement.
- Operations – Effective tools are needed to identify and locate traffic impairments no matter where a VNF is located. Configuration tools may need to understand situations where service-chained VNFs need to be co-located to avoid speed or performance impairments.

Although most VNFs can be deployed in on-premises NFVI or centralized locations, the need for scalability, resilience, agility, and cost efficiencies point to data center locations as a preferred long-term location of choice for most functions, pending the availability of mature, efficient, standards-based NFV orchestration (NFVO).

As a hybrid or migratory approach will likely be employed by most operators unwilling to wait for this ideal to emerge, it is critical that NIDs—or virtualized demarcation and monitoring functions—are in place to cover the full transition to vCPE. With the ability to benchmark and trend quality of service, the user experience, and the performance of individual network functions, providers can assure their adoption of the vCPE model, optimize the deployment, and prove its effectiveness over time—to themselves and their customers.

## ABOUT OVUM

Ovum is a leading global technology research and advisory firm. Through its 180 analysts worldwide it offers expert analysis and strategic insight across the IT, telecoms, and media industries. Founded in 1985, Ovum has one of the most experienced analyst teams in the industry and is a respected source of guidance for technology business leaders, CIOs, vendors, service providers, and regulators looking for comprehensive, accurate and insightful market data, research and consulting. With 23 offices across six continents, Ovum offers a truly global perspective on technology and media markets and provides thousands of clients with insight including workflow tools, forecasts, surveys, market assessments, technology audits and opinion. In 2012, Ovum was jointly named Global Analyst Firm of the Year by the IIAR.

For more details on Ovum and how we can help your company identify future trends and opportunities, please contact us at enquiries@ovum.com or visit www.ovum.com. To hear more from our analyst team join our Analyst Community group on LinkedIn www.ovum.com/linkedin and follow us on Twitter www.twitter.com/OvumTelecoms.

## ABOUT ACCEDIAN

Accedian delivers exceptional end-to-end network performance visibility, for control over the best possible user experience. Accedian generates actionable insights for peak reliability and quality of service (QoS), and enables providers to overcome escalating network complexity, increase agility, and reduce cost. In addition, Accedian proactively ensures maximum uptime for peak quality of experience (QoE). Since 2005, Accedian has turned performance into a key competitive differentiator for hundreds of thousands of networks globally.

Accedian vCPE solutions are used by over 85% of Tier-1 business services providers, globally, assuring on and off-net services, and providing the most flexible mix of physical and virtualized service delivery options available. Accedian solutions were awarded the MEF's vCPE Award in 2015.

For more information, visit Accedian.com. Twitter: @Accedian