Service Assured vCPE

Helping CSPs deliver software-centric value added services (VAS)

RAD

Your Network's Edge®

Outline:

Network Disaggregation, Edge Virtualization and the Curious Case of vCPE

What Network Disaggregation Means for CSPs

No vendor lock-in

Open devices and protocols maximize flexibility

Run same software on different hardware, lower costs and MTTR

Faster development cycles and TTM for new service offerings

Requires in-house DevOps capabilities or outside support

Current market dynamics

The evolving industry trend of network disaggregation, specifically, the separation of software from the hardware appliance it runs on, is closely related to the recent developments in NFV and SDN technologies. This represents a dramatic market inflection point as it frees communications service providers (CSPs) to choose best-of-breed products and solutions to meet their operational and business needs.

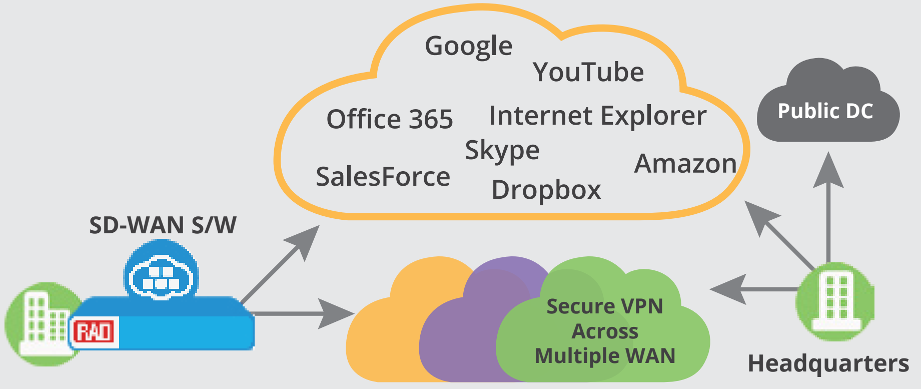
Network disaggregation, and NFV in particular, opens the door for CSPs to make their technology validation and procurement cycles more agile, and allows them to introduce new services faster, becoming less dependent on their traditional network equipment providers (NEPs) and avoiding vendor lock-in. In addition, NFV is changing not only pricing models, but the entire supply chain, with CSPs developing their own software. This redefines the role of NEPs and system integrators, who must adapt to a new set of game rules.

Market Dynamics

The most popular use case for NFV is the virtualized customer premises equipment – vCPE. Analyst firm Market Research Future predicts the vCPE market to reach a value of $3 Billion by 2022, showing an exceptional CAGR of 43% during the forecast period of 2016 to 2022[1].

$3 Billion
vCPE Market
by **2022**

43%
CAGR
2016-2022



SD-WAN in a Nutshell

SD-WAN is all about a unified, secure VPN across multiple public and private WANs to lower the cost of existing IP VPNs

vCPE enables CSPs to launch new value added services (VAS) bundled on a single universal CPE (uCPE) platform, including a combination of networking, security and IT services – point of sale (PoS) applications, CCTV DVR, etc., – which were not typically offered by CSPs before.

One of the key drivers for this accelerated adoption of vCPE is software-defined wide area network (SD-WAN). **SD-WAN** originated in the enterprise market as a lower-cost alternative to the pricey L3 VPN, one which can overlay secure VPNs on whichever infrastructure is available – including the internet or LTE.

Its ability to dramatically lower the costs of enterprise VPNs and multi-branch connectivity has a great appeal to CIOs and their CSPs. As a result, the ability to host SD-WAN as one of many edge services has greatly fueled the growing popularity of vCPE.

[1] Market Research Future, Virtual Customer Premises Equipment Market Research Report, 2019

Minding the gap(s)

When NFV and SDN were first introduced, they held the promise of a true revolution – nimble networks, automated service rollouts and general purpose, low-cost white boxes replacing dedicated appliances – straight out of IT operations. Most importantly, there'd be no more vendor lock-in, allowing service providers to choose whichever elements they desire, be it a server, VNF or an orchestrator. Six years on and vCPE-based business services remain at the top of carriers' agenda, but some aspects of the new technology have proven to be more difficult to realize than others.

Many CSPs, for example, are still struggling with the business case of vCPE, due to the high license costs of brand-name VNFs. Open source VNFs are increasingly being considered a viable alternative, but one which requires relevant support and maintenance to ensure a carrier-grade service.

In addition, CSPs have begun to offer their enterprise customers virtualized SD-WAN (vSD-WAN), in an attempt to prevent the loss of market share to SD-WAN vendors. It is positioned as a Best Effort connectivity option, offered as one of several services hosted on a powerful commercial off the shelf (COTS) server within the uCPE at the customer premises.

This represents a departure from the original monolithic offering of SD-WAN. This also forces service providers to remain competitive by supporting any number of vSD-WAN alternatives, to fit their enterprise customers' – especially the larger corporations – preferences.

Another gap is universal access, which in effect bars service providers that have any access infrastructure other than fiber Ethernet from using economical white boxes to deliver virtualized services, such as vSD-WAN, vRouter, or vEncryption to their customers. This affects the applicability of the vCPE use case in brownfields involving CSPs' TDM, GPON, DSL and other legacy installed base.

Other gaps include the lack of enhanced performance monitoring, OAM and diagnostics, and 1588 timing synchronization. These were not needed in the IT world, but are most definitely required by operators and cannot always be virtualized. There may be solutions to all these issues, but they require multiple, separate boxes (typically from the same vendor to ensure interoperability), each with its own management and orchestration.

Key CSP challenges in vCPE deployments

Carrier-grade assurance

service assurance becomes critical with virtualization, more demanding users and cloud service adoption. Redundancy and fault management – for the VNF service chains and entire service path – are not typically sufficient to meet SLA commitments.

Limited connectivity

available infrastructure does not always support vCPE, making it hard for CSPs to cover their entire service footprint.

Lack of expertise in automation

CSPs often don’t possess the resources and skillsets to handle the installation, orchestration and maintenance involved in programmable networks and services.

The cost of security

vCPE deployment obligates to CSPs to assume responsibility for maintaining security, which has become a fundamental element, and a cost factor, in any solution design.

Backward compatibility

CSPs need to keep legacy services that are still generating revenues and are required by their customers while introducing vCPE-based offerings.

The essential **vCPE Checklist**

CSPs are bound by scale, complexity, particularly in the access network, as well as service expectations of their enterprise end-customers. They therefore must ensure carrier-grade NFV/ vCPE implementation. This mandates a holistic view that takes into account every phase within the service lifecycle. Below is a list of best practices and agile tools to accelerate the adoption of NFV and vCPE:

✓ **Operating system**
Must provide true openness to prevent vendor lock-in and ensure high performance of all vCPE aspects, including third-party VNF hosting, yet remain slim and agile.

✓ **High availability**
Backup and redundancy of the network, connections, vCPE system uptime, NFV infrastructure (NFVI) stability and VNF performance, including service-chained VNFs.

✓ **Security**
A range of security measures, from TPM to secure tunneling/VPN and management channels over public networks to allow direct and secure connection to data centers.

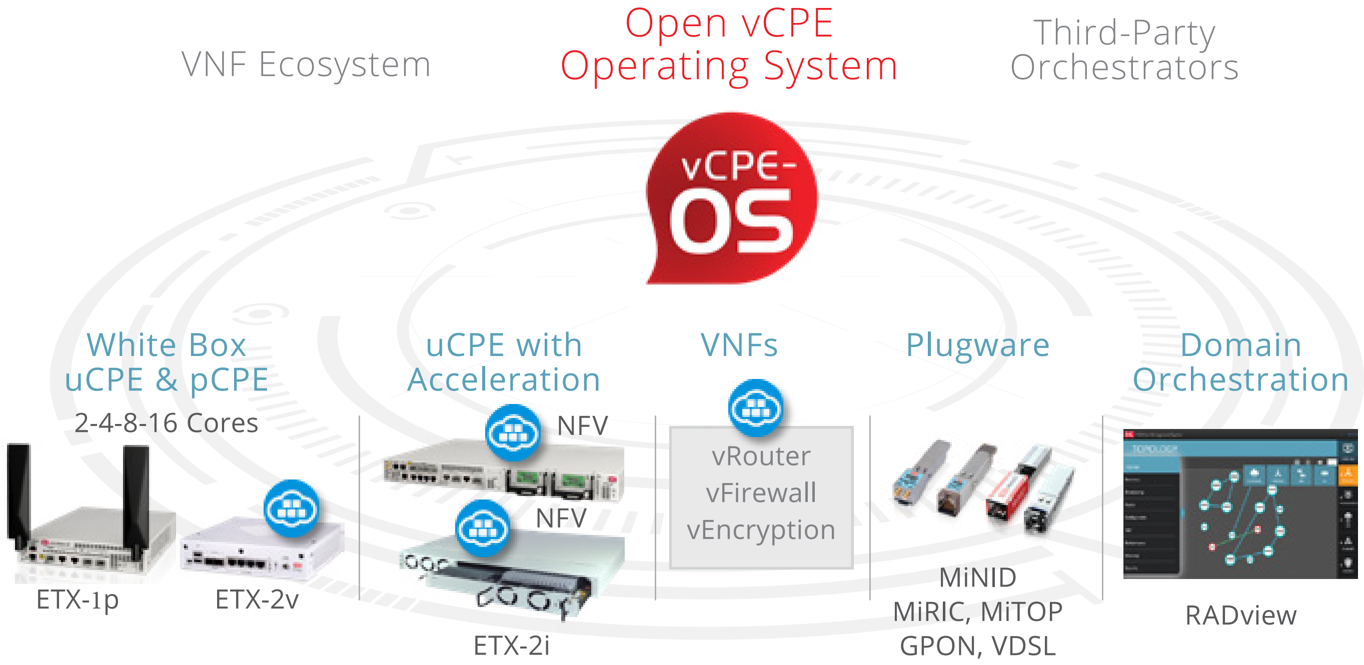
✓ **Health**
Monitoring of performance (PM, FM) and resource utilization in real time, diagnostics, troubleshooting, and self-healing/recovery (SH/SR) on every level: vCPE, NFVI and individual VNFs.

✓ **Automation**
Zero-touch provisioning, VNF onboarding, instantiation and chaining, as well as maintenance, updates, rollback/reconfiguration, and tear down.

✓ **WAN connectivity**
Ubiquitous service look & feel over PON, Carrier Ethernet, xDSL, LTE, and even TDM access. Such variety of WAN connections and interfaces enables a unified global deployment for any NFV (VAS).

RAD's Service Assured vCPE Toolbox

RAD, the industry pioneer of network edge virtualization, provides the comprehensive **vCPE Toolbox** offering everything CSPs need to roll out carrier-grade, service assured vCPE-based services **today**.



VNF Ecosystem

Open vCPE Operating System

Third-Party Orchestrators

vCPE-OS

White Box uCPE & pCPE

2-4-8-16 Cores

ETX-1p

ETX-2v

uCPE with Acceleration

NFV

NFV

ETX-2i

VNFs

vRouter
vFirewall
vEncryption

Plugware

MiNID
MiRIC, MiTOP
GPON, VDSL

Domain Orchestration

RADview

MEF AWARDS 2018
Technology Solution of the Year
NFV

What We Have

The vCPE Toolbox meets carrier needs vis-à-vis current gaps and includes the following:

- vCPE-OS that runs on any white box platform
- Plugware adding connectivity, acceleration options to third-party white boxes
- RADview Domain Orchestrator with standard APIs
- Networking, security and IT VNFs

RAD's Service Assured vCPE Toolbox

Open vCPE Operating System

vCPE-OS

White Box uCPE & pCPE

2-4-8-16 Cores

ETX-1p

ETX-2v

uCPE with Acceleration

ETX-2i

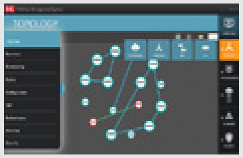
VNFs

vRouter
vFirewall
vEncryption

Plugware

MiNID
MiRIC, MiTOP
GPON, VDSL

Domain Orchestration



RADview

Powerful, **open vCPE-OS operating system** capable of running on any hardware platform

White box and pCPE platforms with distributed and centralized virtualization capabilities

Universal CPE including Carrier Ethernet NIDs (EADs) and IP routers with pluggable x86 server modules to provide service-assured WAN communications for on-net service provider VPNs, off-net public IP and hybrid networks

Virtualized network functions (VNFs), including vRouter, vFirewall, vSD-WAN, vEncryption and more

D-NFV Alliance: Pre-tested VNFs and apps

Plugware adding a broad spectrum of interface, connectivity, conversion and hardware offload/ acceleration capabilities to any white box

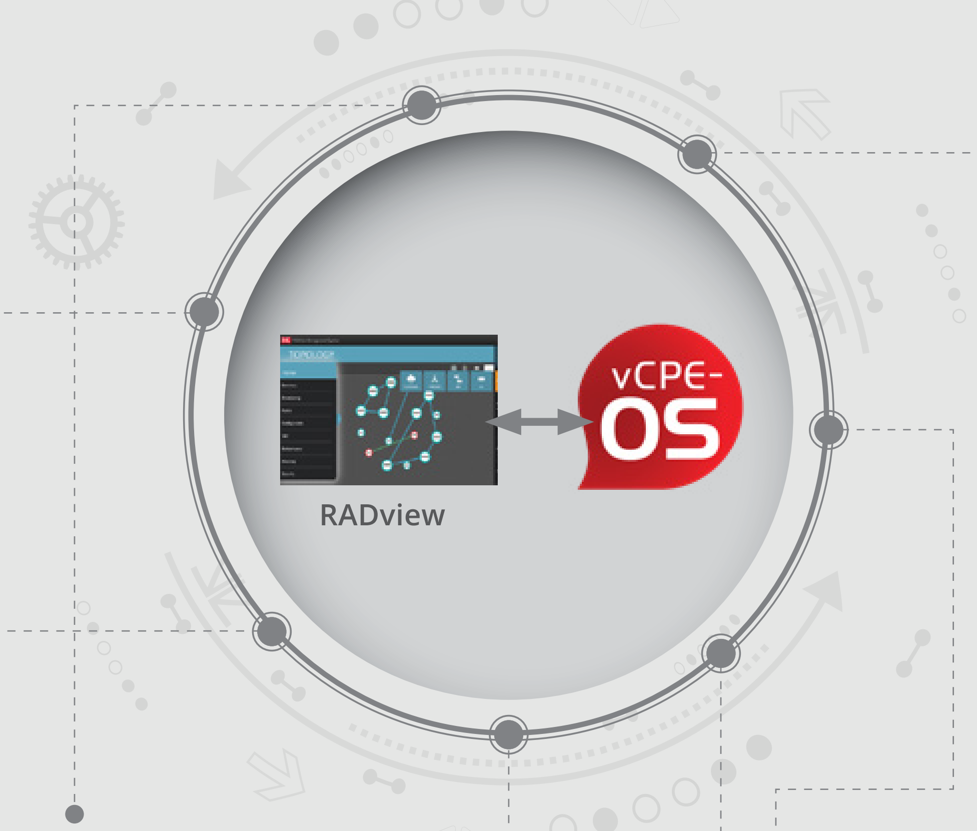
RADview management and domain orchestration with standard APIs for quick service rollout and easy migration to third-party orchestrators

What can **you** do with it?

The vCPE Toolbox is modular and open to fit any vendor solution component – VNFs, hardware platforms and orchestrators. Service providers can change elements as their needs change and employ consistent network and VNF service chain monitoring using vendor-independent OAM capabilities.

In addition, the vCPE Toolbox offers hardware acceleration and specialized functions, including MEF CE2.0, PTP Grandmaster timing and wire-speed L2/L3 switching, as well as forwarding, traffic analysis and encryption.

The vCPE Toolbox enables service providers to manage the entire service lifecycle with intuitive, automated tools:



vCPE Deployment
Zero-touch, secure management channels

VNF Onboarding
VNF certification, network service design

VNF Provisioning
NFV instantiation and chaining, Day 1 VNF configuration

Service Assurance
vCPE/NFVI/VNF analytics, vCPE fault management

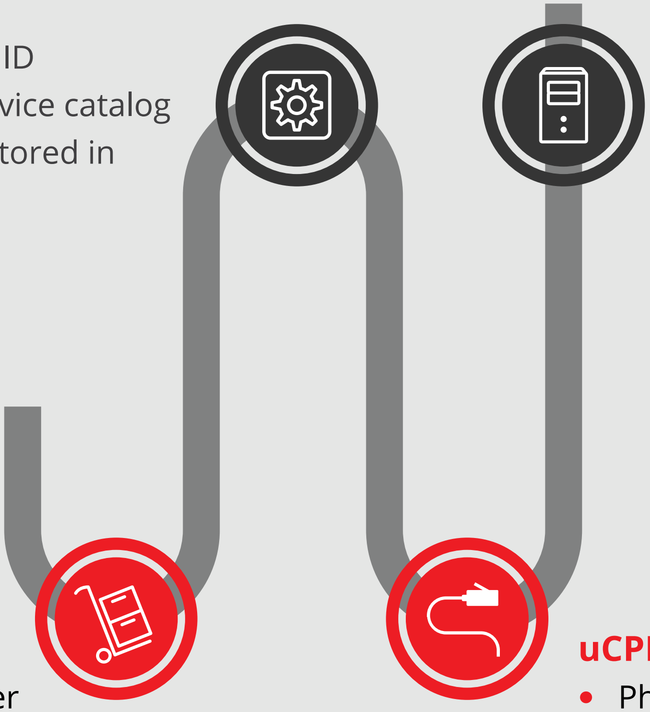
Modification
Remove/replace VNFs, flexible service chains

SW Maintenance
vCPE SW updates/rollback, VNF SW updates/rollback

Service Continuity
vCPE backup/restore, VNF SW backup/restore

True zero-touch deployment –
How it works

- Faster, simpler rollouts
- No on-site technicians
- Immediate revenues



ZTP Preparation at NOC

- Assign CPE ID to customer ID
- Select CPE profile from service catalog
- CPE profile automatically stored in bootstrap server

Pre-Staging

- By RAD or service provider
- Install ZTP SW and certificates
- Label CPE/carton with CPE ID

uCPE Shipped to End-user

- Physical installation by end-user
- Connect CPE to power & networks

uCPE "Call Home" Process

Fully automatic process:

- Connects securely to bootstrap server
- Downloads CPE profile/SW
- Connects securely to RADview for lifecycle management and monitoring

Assured Virtual Services

with vCPE Toolbox

Service Monitoring

- TWAMP
- UDP and ICMP echo
- Responder Agnostic Delay Measurement (RADM)

VM Monitoring

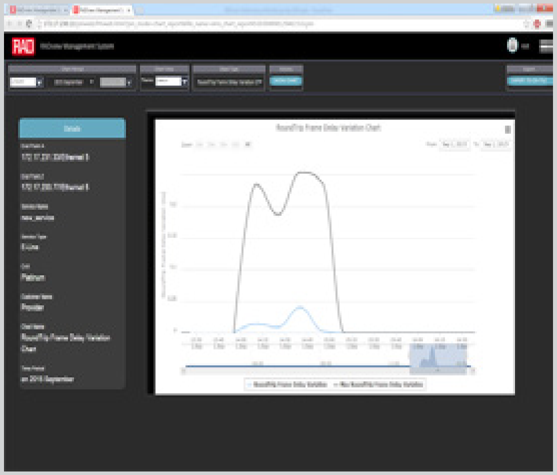
- Monitor and analyze VMs
- Self-healing for “hung” VNFs
- Core pinning for performance scaling

Hardware Monitoring

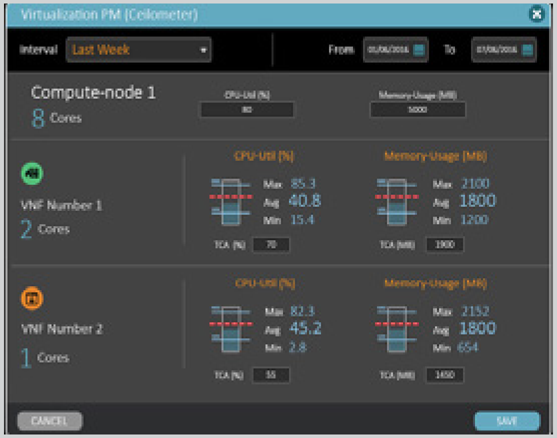
- All interfaces including ETH, LTE, VDSL, Smart SFPs
- Link-Loss Carry Forward
- Fault propagation

NFVI Monitoring

- Service chain monitoring for NFVI
- Troubleshooting provided by virtual interface counters



SLA Monitoring



Virtualization PM (Ceilometer)

Interval: Last Week

Compute-node 1
8 Cores

CPU-Util (%): 80
Memory-Usage (MB): 5000

VNF Number 1
2 Cores

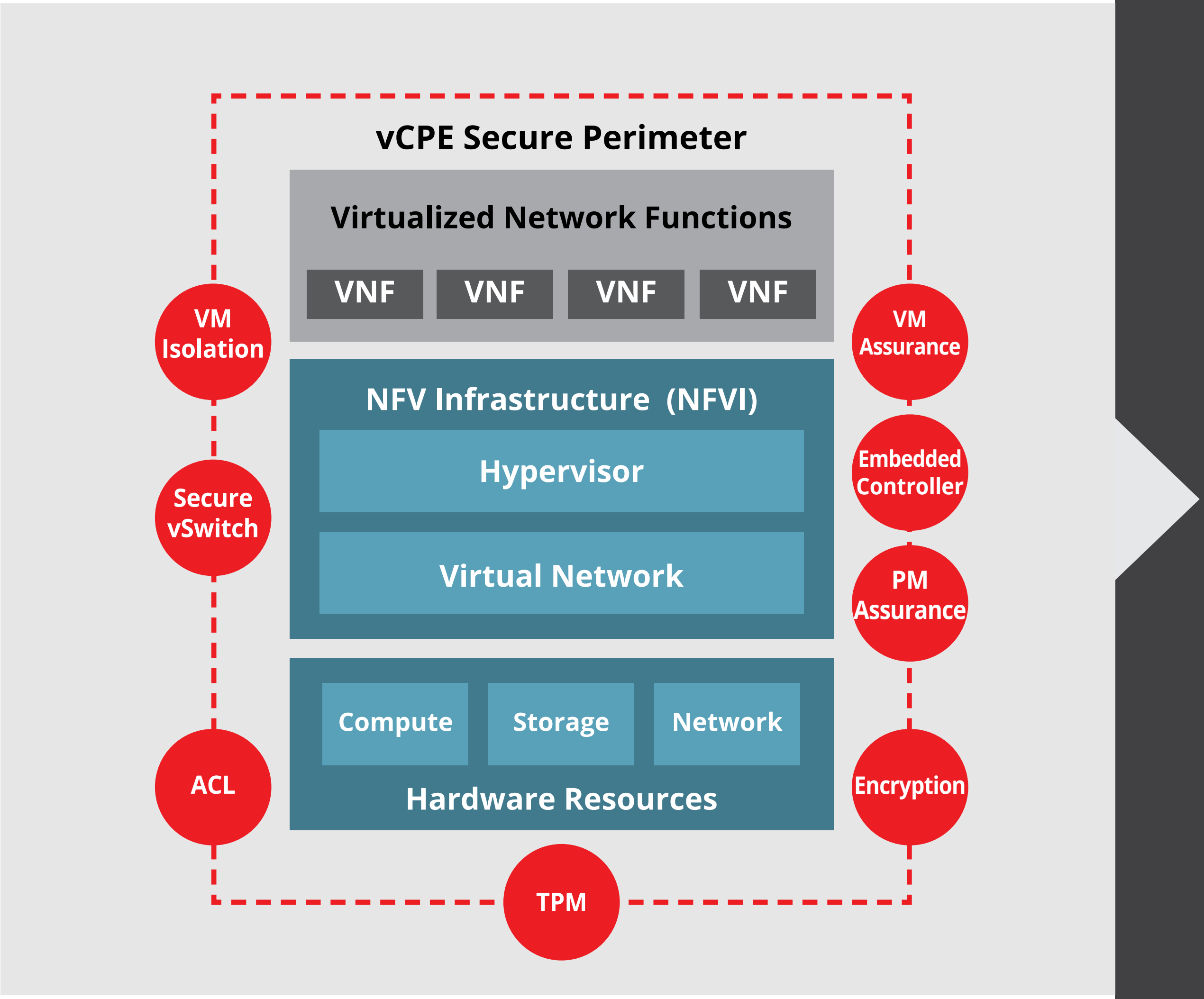
CPU-Util (%): Max 85.3, Avg 40.8, Min 15.4, TCA (%) 70
Memory-Usage (MB): Max 2100, Avg 1800, Min 1200, TCA (MB) 1900

VNF Number 2
1 Cores

CPU-Util (%): Max 82.3, Avg 45.2, Min 2.8, TCA (%) 55
Memory-Usage (MB): Max 2152, Avg 1800, Min 654, TCA (MB) 1450

NFVI Health Monitoring

vCPE Toolbox
provides multi-layered security



- **Secure Console Access (ACLs):** Credentials with complex password enforcement and physical console access control
- **Secure Remote Management Access:** IPsec/SSL encryption
- **Tampering protection:** Trusted Platform Module (TPM) supporting secure boot
- **Security-hardened virtual switch** featuring high isolation between tenants at L2/L3
- **Embedded virtualization controller in CPE** simplifies operation over public network
- **Identity management:** Device ID bind to certificate authority (CA)-signed certificate
- **Health measurement** with fault propagation

Deployment Scenarios and Use Cases

Leading Tier 1 Service Providers all around the globe benefit from the advanced features offered by RAD's vCPE Toolbox. These are the typical use cases:

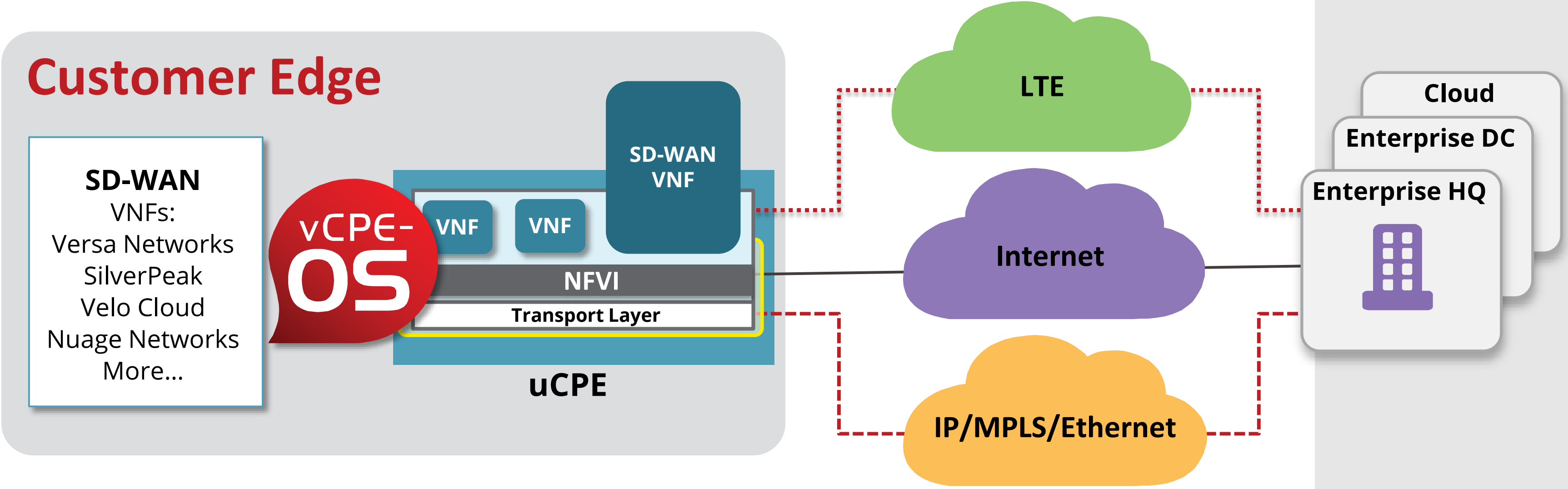
The following video shows various vCPE flavors & deployment scenarios using RAD's vCPE Toolbox:

Use Case 1: vSD-WAN

Enhancing virtualized SD-WAN with more NFV-based VAS, for instance firewall and WAN optimization. In addition, enabling flexibility with the possibility of adding or replacing VNF as service requirements evolve over time.

RAD's offering includes:

- ETX-2v white box portfolio
- vCPE-OS for global deployment and hosting of third-party VNFs
- Tightly-integrated Versa vSD-WAN VNF, or any other vSD-WAN offering

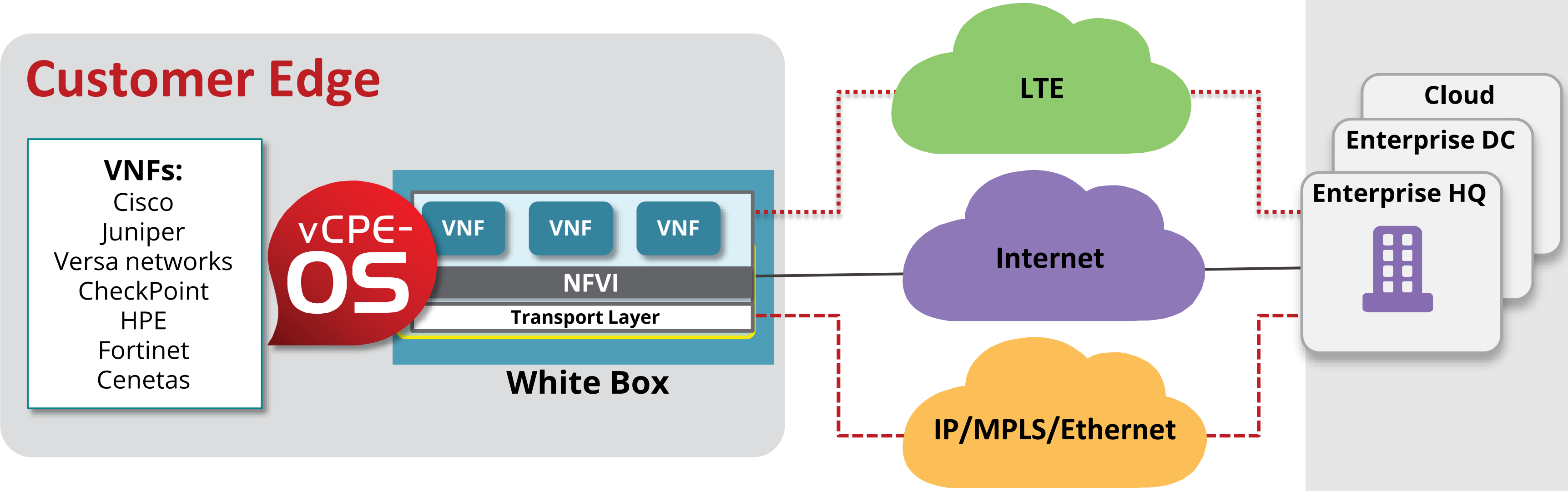


Use Case 2: L3 VPN Services

IP VPNs have become too costly for many enterprise customers who no longer perceive the value of this connectivity-only service as justifying its cost. vCPE allows service providers to add premium offerings – or VAS - on top of the Layer 3 service. These can be virtual firewalls, virtual routers and even IT services, which, until now were not part of a typical business service offering. Such upgraded bundles help CSPs move up the value chain, penetrate into new market segments and, as a result, protect their revenues.

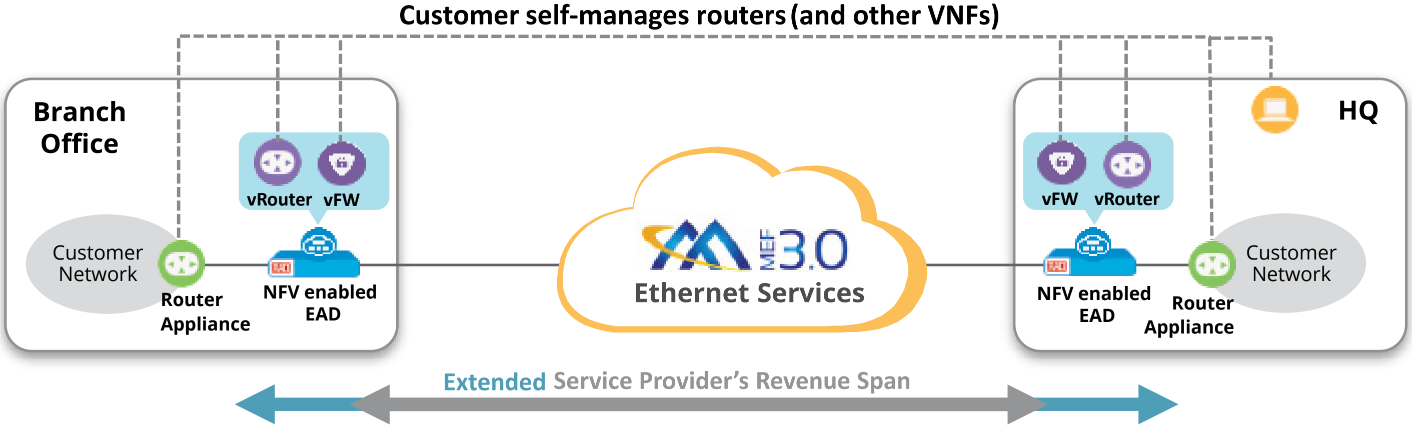
RAD provides:

- Wide portfolio of ETX-2v white boxes host any VNF
- RAD's plugware to connect the white boxes over any access (LTE, WiFi, xDSL, TDM)
- Carrier-grade vCPE-OS
- RADview domain orchestrator



Use Case 3: L2 VPN for Business and Wholesale Services

vCPE presents an opportunity for L2 divisions within CSPs to move up the value chain. Instead of offering "pipes-only" Carrier Ethernet VPN SLAs for connectivity between enterprise branches and/or to the data center, they can now introduce new services, such as hosted virtual routers, firewalls, etc. from their end, their customers can save on the deployment and operational costs that are associated with hardware appliances.

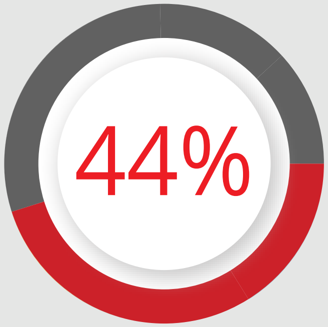


RAD is providing the following:

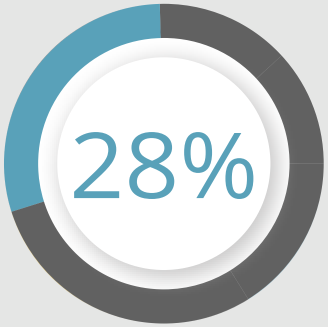
- MEF-certified ETX-2i uCPE with full EAD functionality
- Pluggable x86 module for "pay as you grow" flexibility
- Carrier-grade vCPE-OS operating system with open NFVI to allow hosting and chaining of any VNF
- RADview NMS + domain orchestrator
- Self-managed VNFs, e.g., vRouter, vFirewall, vEncryption, etc.

vCPE Survey

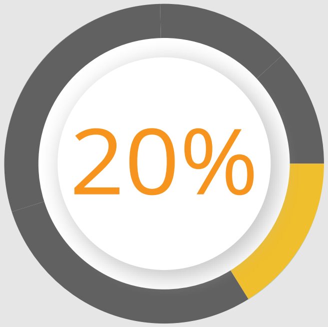
In a poll we conducted during a **RAD webinar**, we asked participants which was the most compelling use case for vCPE. Here are the results:



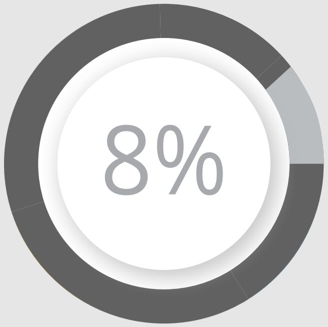
believed that
vSD-WAN was the best vCPE use case



voted for
L3 VPN with VAS



thought
Carrier Ethernet business and wholesale offerings with VAS that present the most popular use for vCPE



chose
“other” use case/s

The results of the poll mirror RAD’s own insights based on our extensive conversations with CSPs over the last few years. They illustrate the extent of market transformation brought on by the fact that the technology behind the disaggregated architecture has reached a level of maturity that allows it to make a true impact. They also shed light on the driving forces behind them: The most compelling use case is driven by the biggest external competitive threat to CSPs’ business model (SD-WAN), while the others present opportunities to upgrade CSPs’ business services and offer more value to their customers.

What do you think?

Take the Poll

Where do we go from here?

vCPE technology is changing our market. This is true for vendors and CSPs alike as it affects product and service offerings, the competitive landscape and growth strategies.

Some enterprise customers prefer on-site VAS to control and manage their own applications, so that they can meet IT policy requirements and address security issues. CSPs, on the other hand, prefer to offer SMBs centralized solutions to benefit from economies of scale and simplicity in duplicating service packages in mass quantities. That is where multi-tenant service models and cost effective deployments come into play.

Other service models are required to address different customer constraints and CSP priorities. As digital transformation is evolving, we’re likely to see growing demand for solutions that offer True Openness with a wealth of options and flexibility. CSPs are not likely to embrace vCPE until they’re allowed to avoid vendor lock-in and choose best-of-breed elements that optimally suit their business needs.

Want to learn more on Service-Assured vCPE?

Check out RAD’s resources:

Webinar
vCPE Market Trends, Drivers and Use Cases

Video
AT&T Labs’ Elie Francis Presents MEF18 PoC – Boosting uCPE with SDN/NFV/Legacy Capabilities

Blog
Distributed NFV and Multi-access Edge Computation

RAD

Your Network’s Edge®

There’s plenty more

www.rad.com

or

contact us