White Paper

Enterprise
Universal Customer Premises Equipment

Cloudify, RAD Develop Reference Stack for Mass uCPE Deployment

Combining Cloudify orchestrator with RAD's vCPE-OS (and RADview domain orchestrator) on Intel® architecture uCPE enables convergence of communication, information, and operational technology services at network and customer edges

Corporate wide area networks (WAN) were well-planned systems that connected branch offices back to the corporate headquarters for access to email, databases, and other enterprise/IT business services. These networks were known to be very secure thanks to dedicated multiprotocol label switching (MPLS) network connections that were secured by the telecommunication network. These networks served companies well until the rise of the cloud. Accessing cloud services by connecting to the corporate office and then out to the cloud via the internet or even separate dedicated connections was frustratingly slow. The massive amount of cloud hosted data being exchanged across the network swamped MPLS connections.

Branch offices then bought broadband data connections and small routers to bypass the enterprise headquarters' WAN to access cloud services faster. These ad hoc network changes led to network security challenges and increased tech support calls. What saved companies from this chaotic scenario was software-defined WAN (SD-WAN) and universal customer premises equipment (uCPE), a type of virtualized CPE (vCPE) with compute, storage, and networking features sized appropriately for regional headquarters, branch offices, or small office networks.

SD-WAN provided a hybrid approach to branch networking with application traffic intelligently distributed over broadband, LTE, and traditional MPLS and carrier Ethernet connections. uCPE is complementary in that it enables hosting of a variety of functions, including SD-WAN and firewalls as virtual networking functions (VNFs) that can be on-boarded, service chained, and even replaced as needed to provide for all the networking functions required without the costs associated with maintaining and updating multiple appliances at remote locations.

Many communications service providers (CoSPs) began trials and soon network functions virtualization (NFV) found a home in branch office networking. NFV is exciting because it holds the promise of scalable network services, remote service deployment, and reduced costs as virtual network functions (VNFs) can be deployed and consolidated on Intel® architecture-based commercial off-the-shelf (COTS) servers instead of dedicated appliance hardware.

NFV is a great concept but there have been some implementation challenges. VNFs are often still implemented in a monolithic software instantiations that self-contain all of their services. This results in great isolation for VNFs, allowing multiple networking functions and applications to run on the same server. And while VNFs boost network service deployment agility, the monolithic nature of VNFs and their accompanying virtual machine infrastructure can be resource heavy.

Enter a new way to virtualize network functionality called containers. Containerized networking functions (CNFs) utilize container software distributed as software images that are managed using container-management tools such as Kubernetes or Docker. CNFs break apart a virtualized application into microservices that can be separately scaled and deployed. This enables fast delivery, network agility, portability, modernization, and lifecycle management.

Table of Contents

Containers work with stateless microservices, however; and not every network function lends itself to a stateless microservices approach. For example LAN or WAN interfaces will still be suitable for a VNF approach with the driver support and 24x7 operation model. Even with CNFs growing in popularity, both CNFs and VNFs will co-exist in the CoSP network for a long time; this is just a nature of the complex supplier chain model. This situation adds a new dimension to orchestration programs that manage the application lifecycle.

To demonstrate an orchestration service for both containers and VNFs, Intel® Network Builders ecosystem partners Cloudify and RAD have collaborated with Intel to design an open uCPE reference architecture for service-assured cloud access. The reference design uses RAD vCPE-OS operating system and RADview domain orchestrator combined with Cloudify's orchestrator. Using an open source architecture, the reference design shows how multiple, single-use appliances can be replaced with an operationally efficient and multi-functional uCPE.

uCPE Reference Design Components

To create the reference design, Cloudify has integrated with RAD's RADview domain orchestrator (see Figure 1) so that it can orchestrate microservices/containers as well as VNFs at the enterprise edge. RAD's vCPE-OS operating system offers security features and provides high performance networking and virtualization infrastructure to host VNFs and CNFs.

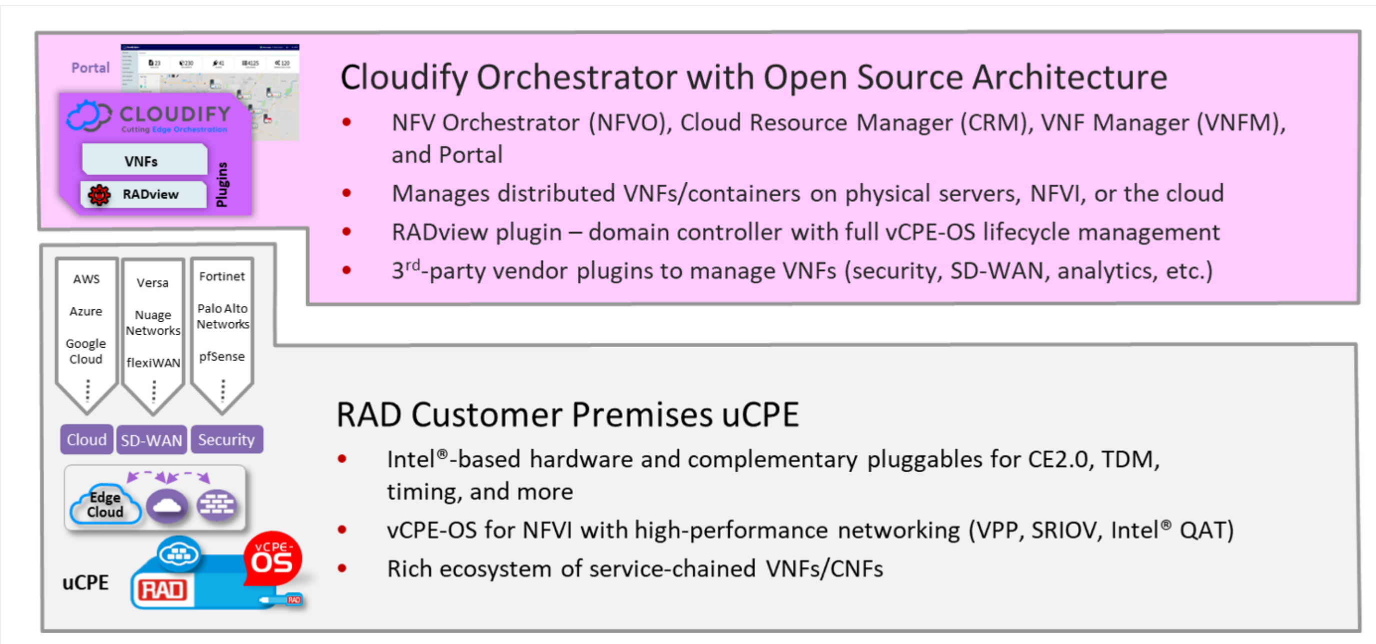

Figure 1. Key features of Cloudify orchestrator and RAD uCPE.[1]

Cloudify Network Automation and Orchestration

Cloudify is a cloud-native open management and orchestration (MANO) solution that allows enterprises to model, implement, and scale networks efficiently from core to edge. Cloudify provides modeling, management, and orchestration capabilities to SD-WAN and uCPE-based networks.

Figure 2 shows the following key features of the software:

- **vCPE/SD-WAN Manager:** This software module contains the vCPE/SD-WAN domain logic and allows network managers to adapt or create Cloudify Blueprints using Topology and Orchestration for Cloud Applications (TOSCA) models. The module also holds all configurations required to provision the overlay networks, and all the VNFs participating in the service chain. This module collects data from Cloudify's remote agents and agentless monitoring nodes on infrastructure. It then analyzes this application health information from the network nodes and compares it to key performance indicators (KPIs). Understanding the differences between performance and KPIs enables real-time network automation.
- **Open Source Orchestrator:** This orchestration engine manages the lifecycle of all vCPE and SD-WAN nodes in the network, including onboarding, instantiation, day 2 changes and updates, and termination. Using Netconf, the orchestrator is notified when a new device is added to the network and begins the onboarding process using predefined day 0 and day 1 configurations, and day 2 policies.
- **vCPE/SD-WAN GUI (Cloudify Console):** This flexible user interface (UI) is used for designing and deploying applications and services and also for single-pane monitoring and management of all deployments running within the vCPE/SD-WAN Manager. The UI lets network managers take action—either automated or manual—when it detects anomalous network events.

These modules allow Cloudify to automate a branch office network that provides a wide range of services, allowing services to be modeled once and then provisioned and configured across the network. CoSPs can integrate any external cloud native service, such as Netconf or Kubernetes, with all major public and private cloud infrastructures.

RAD Operating System and Device Management

RAD is providing its vCPE-OS and RADview Domain Orchestrator to the joint RAD/Cloudify/Intel reference design.

RAD vCPE OS

RAD's secure vCPE-OS is a Linux-based operating system and virtualization platform for white box servers as well as RAD's uCPE systems. The software combines powerful networking capabilities with virtualization for hosting SD-WAN and any other value-added VNF/CNF applications from other vendors.

RAD vCPE-OS provides a high-performance networking and NFV infrastructure to host VNFs/CNFs with full lifecycle management and APIs for interoperability with third-party orchestrators, such as Cloudify. The OS is designed to be light on resources with minimal usage of expensive RAM and disk usage while also providing an accelerated data plane for great performance with less CPU usage.

Figure 3 shows a block diagram of the vCPE-OS and how it works as an Intel architecture-based uCPE. VNFs plug into the hypervisor/KVM layer, and these services can then access optional, value-added functionality, including security, performance monitoring, or tunneling. Connecting to the hardware layer at the bottom are the transport layer services, including routing and Linux services along with Ethernet network interface device services.

Across all those layers is a comprehensive management and control functionality using Netconf, CLI, and/or simple network management protocol (SNMP). The management functionality also features a zero-touch provisioning (ZTP) capability that allows for plug-and-play device deployment. Finally, an OpenStack API is also available in the system.

RADview

RADview is a comprehensive and modular network management suite for planning, provisioning, and monitoring of networks and services that utilize RAD technologies. RADview can be used for both physical and virtual network resources, and it provides network planning, service provisioning, performance monitoring, and management. RADview is carrier class in terms of redundancy and support of important CoSP features such as ITU-T FCAPS compliance and security management.

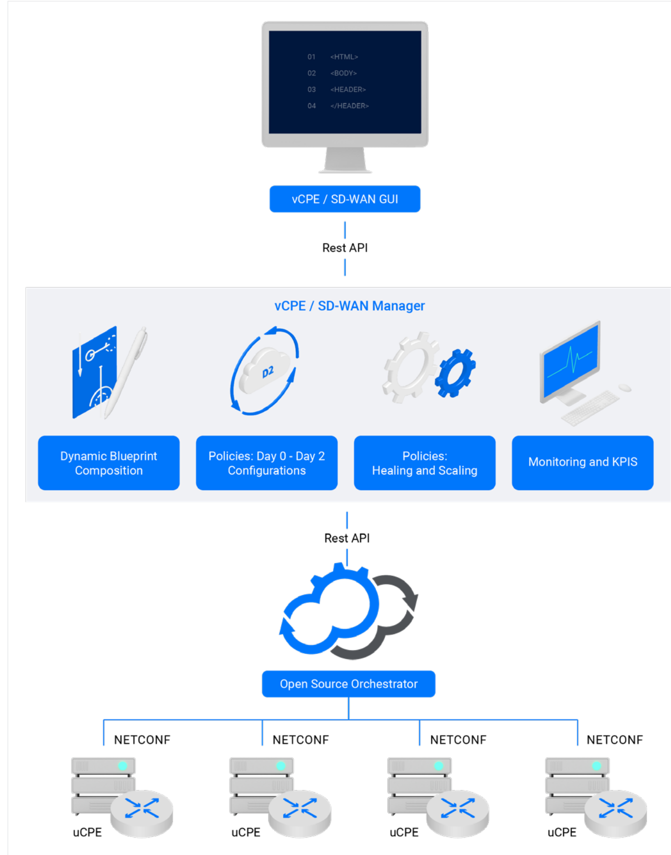

Figure 2. Cloudify orchestration services and architecture.

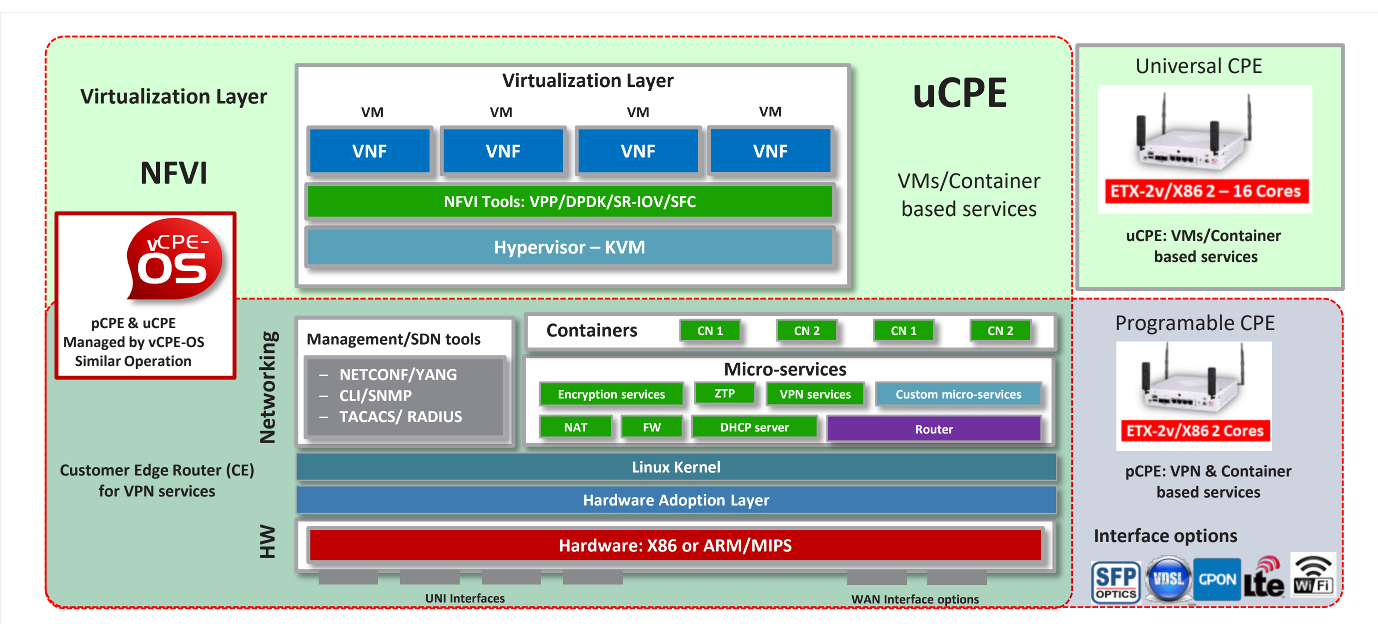

Figure 3. vCPE-OS block diagram describing virtualization and OS services.

RADview can be used as an end-to-end service manager for carrier Ethernet services, a performance monitoring portal for ongoing monitoring of Ethernet and IP services, a D-NFV orchestrator for virtual machines and application services at the customer edge, and a network planner for resource optimization and capacity planning.

Powered by Intel® Technology

The reference design specifies processors and accelerators from Intel. For enterprise headquarters or CoSP locations, Intel® Xeon® Scalable CPUs provide hardware-enhanced security and dynamic service delivery. The CPUs support hybrid cloud infrastructure and the most demanding applications—including in-memory analytics, artificial intelligence, autonomous driving, high performance computing (HPC), and network transformation.

uCPE devices can be based on either Intel® Xeon® D processors or Intel Atom® processors. Intel Xeon D processors deliver workload-optimized performance in space- and power-constrained environments at the network's edge. These innovative, system-on-a-chip processors support high-density, single-socket network, storage, and cloud edge computing solutions with a range of integrated security, network, and acceleration capabilities.[2]

Another option for uCPE applications are Intel Atom processors, which are compact and energy-efficient. These processors support security features, including biometric passwords, and they deliver advanced technology and processing capabilities onto an ultra-thin and lightweight design.[3]

Another important Intel technology for uCPE applications is Intel® QuickAssist Technology (Intel® QAT). Intel QAT accelerates encryption and decryption performance in cloud, networking, big data, and storage applications for data in motion and at rest. Intel QAT improves performance across applications and platforms.[4] That includes symmetric encryption and authentication, asymmetric encryption, digital signatures, RSA, DH, and ECC, and lossless data compression.

Pulling It All Together: The Open uCPE Software Reference Design

The open uCPE reference design combines Cloudify and RAD software to create a complete management and orchestration stack that is available for white box uCPE servers powered by Intel architecture CPUs. The reference design provides the following benefits to CoSPs and their customers:

- Simplifies migration from a collection of single-use appliances to operationally efficient and multi-functional CPE that offers networking, voice, security, cloud, IoT, and other services.
- Leverages CNF/VNF ecosystem to deliver dynamic value-added services at the network edge where they are needed and where a lack of management and orchestration can drive up costs.
- Leverages disaggregation to ensure optimal software and hardware without vendor lock-in.
- Complements IoT, 5G, and cloud native networks and strategies, and can implement a service provider's secure access service edge (SASE) service.

An example of such services is the automatic orchestration of an internet of things (IoT) service with the full CNF/VNF life cycle orchestration including provisioning, collection of the data, and the establishment of a communication tunnel to the cloud or an on-premises data center.

The orchestration of this service spans from edge to core, including the lifecycle management of all the components at the edge, communication and provisioned cloud services, as well as the creation of a service chain between these components.

This reference design could be a solution for companies that need to connect multiple remote locations like small offices or branches utilizing a secured connection to a central service or HQ.

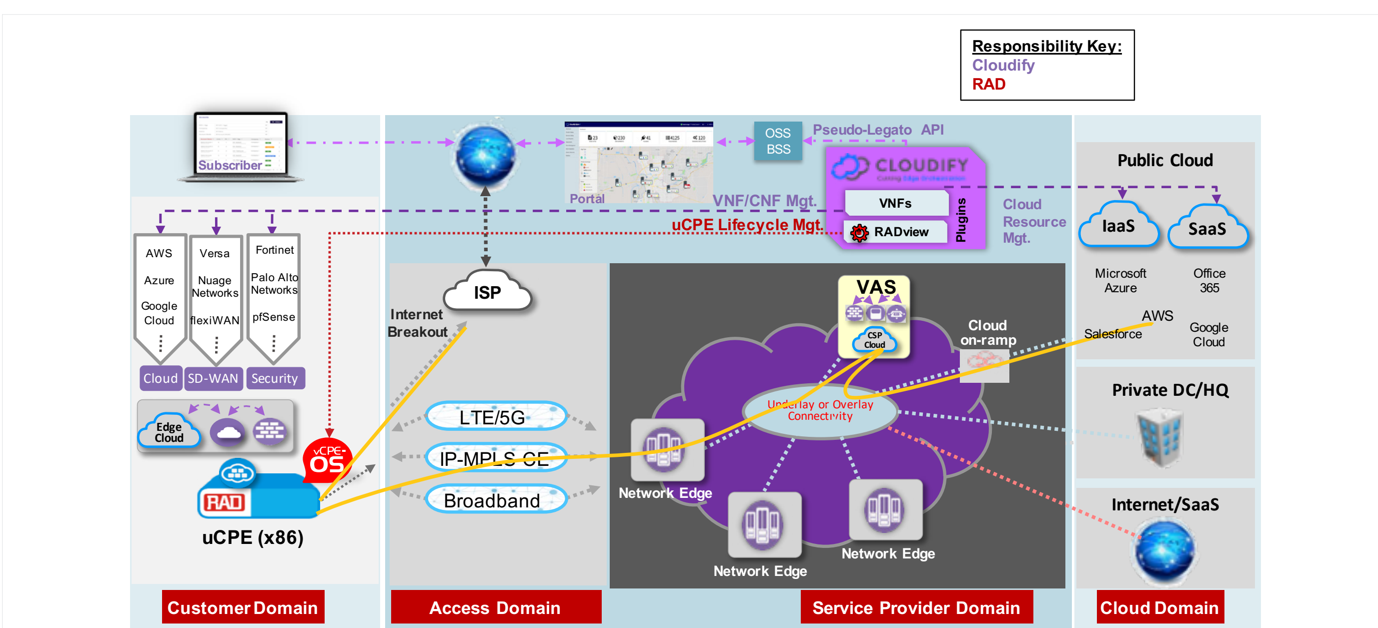

Figure 4. uCPE software stack secure device installation demonstration.

With the reference design in place, the companies organized a demonstration to show how the technologies work together to initiate a secure cloud service. Figure 4 shows the network that was created for the demonstration. The hardware used was the RAD ETX-2v powered by an Intel Atom processor and an optional RAD MINID, a network interface device and probe that utilizes Cyclone® V GX field programmable gate array (FPGA).

The first step shown on the left side of Figure 4 is the configuration of the uCPE, including VNF onboarding and service function chaining. Once these are onboarded, the Cloudify orchestrator manages the distributed VNFs and containers hosted at the uCPE, edge data centers, or in the cloud.

The next step is establishing connectivity to the cloud and to corporate resources. If required, the uCPE can also provide local internet breakout. The reference architecture supports multi-link traffic distribution for failover, load balancing, and traffic steering over a range of access options, including carrier Ethernet, IP VPNs, broadband services, and/or wireless 4G/5G services.

Once the data traffic reaches the CoSPs, they can provide supplemental value-added services at the customer premises via edge data centers or both.

Conclusion

The popularity of cloud access has forced enterprises to revisit their entire WAN architecture, replacing the collection of networking appliances with a flexible uCPE solution offering many virtualized network services. The right uCPE software platform includes advanced virtualization, orchestration, and management capabilities that streamline and automate the service provisioning and the lifecycle of the server. By joining forces on a uCPE software reference design, Cloudify, Intel, and RAD have an integrated solution providing a complete foundation that meets next generation uCPE requirements.

Learn More

Intel® Network Builders

Intel® Xeon® D Processors

Intel® Xeon® Scalable Processors

Cloudify

RAD vCPE-OS

RADview Network Management

Notices & Disclaimers

[1] Images provided courtesy of RAD and Cloudify.
[2] https://www.intel.com/content/www/us/en/products/details/processors/xeon/d.html
[3] https://www.intel.com/content/www/us/en/products/details/processors/atom.html
[4] https://www.intel.com/content/www/us/en/architecture-and-technology/intel-quick-assist-technology-overview.html

0421/DO/H09/PDF ♻ Please Recycle 346832-001US