SD-WAN Testing of vCPE

The need for increasing service agility and reducing OPEX has motivated the rise of SDN and NFV paradigms and associated technologies. On the SDN side there are multiple protocols southbound and northbound of the SDN controller with proprietary and opens source implementations. In such a scenario, it becomes increasingly important for Service Providers to test the technologies before they pick the appropriate technologies and vendors for deployment. This involves complex and large scale test scenarios that accurately represent real network conditions.

vCPE is one of the early NFV use cases that is seeing increased deployment by Service Providers. SD-WAN and vCPE combined provide a potential to realize centralized provisioning of the VNFs required for vCPE, remote policy configuration and ability to implement policy based routing. These three abilities help the Service Providers to realize the benefits of improved service agility and reduced OPEX.

vCPE deployments can be categorized into three high level areas:

- **Virtual CE or Cloud CPE–**Most of the vCPE functionality such as NAT, Firewall, QOS Policies are deployed in the cloud at the Provider Edge and basic functionality such as forwarding and IP address management (IPAM) supported at customer premises
- **On Premises OTT vCPE–**More functionality such IPAM, NAT, Firewall and QOS Policies are supported by the vCPE VNFs at the customer premises. Customer control plane and data plane traffic is carried over the OTT connection
- **On-premises vCPE–**More functionality such IPAM, NAT, Firewall and QOS Policies are supported by the vCPE VNFs at the customer premises. Customer control plane and data plane traffic is carried over a dedicated link owned by the service provider

Although there are these three broad categories for deployment of vCPE, implementations can have varying amount of functionality in customer premises and in cloud (Service Provider edge).

SD-WAN and vCPE testing can be divided into four high level test scenarios independent of the vCPE deployment configuration:

- Policy validation of vCPE (functional and large scale)
- VNF lifecycle management for vCPE constituent VNFs
- Benchmarking performance and scale of vCPE
- Validation of policy based routing for SD-WAN

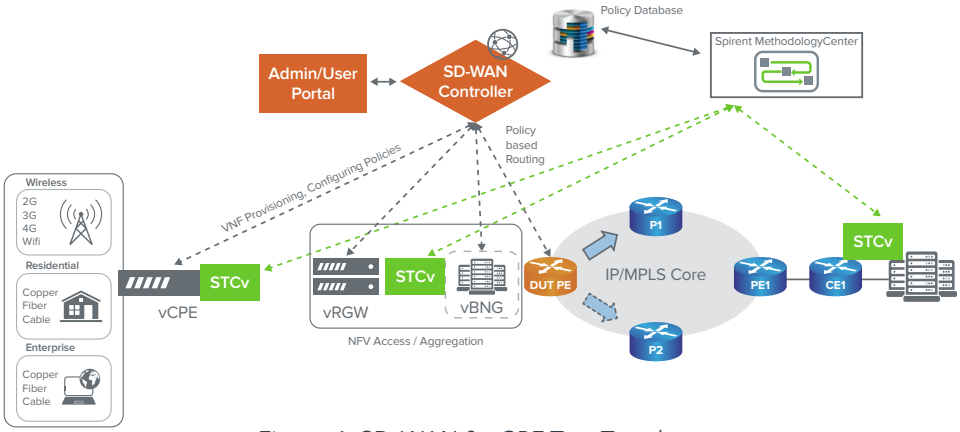

Figure 1. SD-WAN & vCPE Test Topology

SD-WAN Testing of vCPE

vCPE Policy Validation

One of the key benefits of vCPE & SD-WAN technology is the ability to provision policies remotely for residential and business customers. This not only enables service agility but also helps in reducing the OPEX for Service Providers.

One of the key challenges is the validation of policies configured by the SD-WAN controller. SD-WAN controller is expected to maintain an in-built or standalone policy database. The policies may be organized in the policy database on a per customer location basis. Depending on the deployment scenario the policies may be applied to the provider network edge or the customer premises.

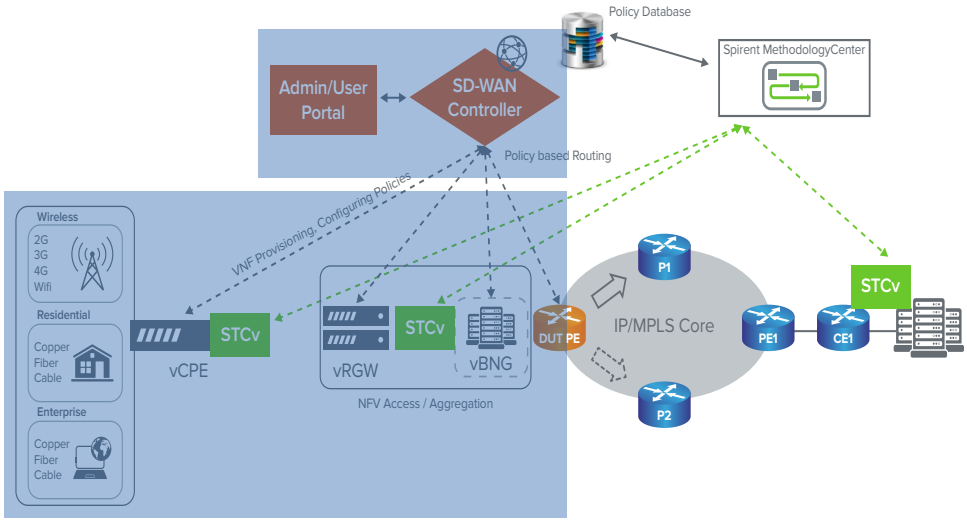

Figure 2. vCPE Policy Validation

The policies may be categorized as:

- **Access Lists:** Port based, VLAN based, L2-L4 based, application or content specific policies
- **Traffic Shaping:** L2 & L3 QoS, DiffServ, Congestion Avoidance, 802.1p

In addition to validating the orchestration and operational aspects of the policies, following test verification are important to evaluate the performance and scalability of policy enforcement at the point of presence:

- Policy validation at max scale and max throughput for each service
- Orchestration of services and associated policies at max scale

If the control plane functionality primarily resides in the provider network (e.g. vCE-CPE scenario) then there may be multiple instances of vE-CPE catering to the individual customer locations. In such a scenario, following two aspects need to be evaluated:

- SD-WAN controller scalability for service orchestration and policy configuration
- Degree of optimization in provisioning of the vCE-CPE instances in the service provider cloud

VNF Lifecycle Management

Independent of where the VNFs required to support the vCPE scenario reside (SP cloud or customer premises), there are metrics associated with the life cycle events of the VNF that impact the overall end user experience, SP OPEX costs and service agility

In summary, the following events related to VNF lifecycle should be examined and benchmarked:

- VNF Instantiation
- VNF Termination
- VNF Autoscaling
- VNF Migration

ETSI NFV TST 001 Clause 7 goes in more detail on the various VNF Lifecycle events and the associated performance metrics that impact the E2E service and end user experience.

vCPE Benchmarking

Each vCPE deployment consists of multiple VNFs providing the desired functionality to achieve functionalities such as IPAM, policy control, traffic shaping, admission control, authentication, routing and access to the desired services. For supporting these functionalities and services VNFs in each vCPE deployment rely on standardized protocols such as DHCP, IGMP/MLD snooping, RIP, BFD, LACP and 802.1X. These control plane protocols are supplemented by static configuration capabilities such as firewall rules and traffic shaping policy rules.

Before the VNFs comprising the vCPE are put into deployment it is important to benchmark the performance and scale of the individual VNFs as well as the VNF service chains.

Broadly, vCPE performance benchmarking may focus on the following protocols and technology aspects:

- Control Plane: PPPoE, DHCP, 802.1x, RIP, OSPF, BFD, LACP, IGMP, MLD, PIM, IGMP Snooping
- Data Plane: MAC based VLANs, Port based VLANs, Multicast VLAN Registration (MVR), LLDP, L3 Forwarding, LAG

Note: The above list for control plane and data plane benchmarking is not intended to be exhaustive but is a representation of functionalities supported by a typical vCPE implementation

Policy Based Routing

Policy based routing involves ability to route the service traffic based on the policies defined by the network operator. These policies are primarily to enforce the SLAs for the service. Additionally, Service Function Chaining (SFC) scenarios require the NSH headers to be added, processed and removed by ingress, egress and intermediate network nodes. Both service function chaining functionality and policy based routing is typically triggered or controlled by SD-WAN control using southbound SDN protocols such as PCEP, NETCONF/YANG, BGP, Openflow, OVSDB and others.

This again brings us to the need for functional, performance and scalability testing of policy based routing and service function chaining.

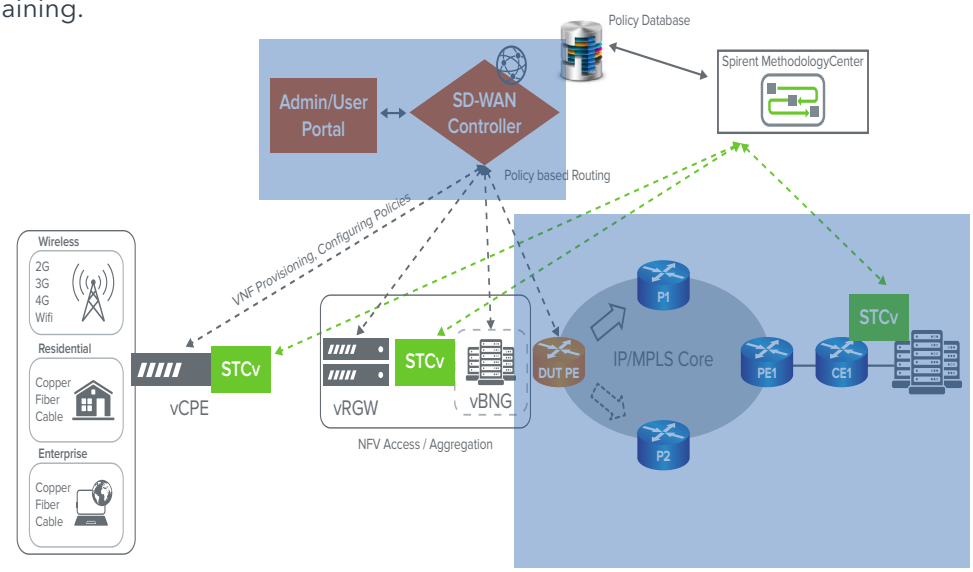

Figure 4. Policy Based Routing Validation

In this test scenario, device under test (DUT) may be the Service Orchestrator or the PE (ingress/egress) device. This further bi-furcates the exact test scenario and puts down certain requirements and capabilities a test tool should support to enable such testing. It also presents the need to define metrics that should be measured to assess the performance of the network entity under test.

Example:
In the above scenario where DUT is a PE device, test tool should be able to emulate core, edge and CE parts of the network and some of the metrics measured may be processing time for installing flows, flow scale supported by PE device, convergence time in the event there is degradation or service unavailability in a certain network path.

About Spirent Communications

Spirent Communications (LSE: SPT) is a global leader with deep expertise and decades of experience in testing, assurance, analytics and security, serving developers, service providers, and enterprise networks.

We help bring clarity to increasingly complex technological and business challenges.

Spirent's customers have made a promise to their customers to deliver superior performance. Spirent assures that those promises are fulfilled.

For more information, visit: www.spirent.com

Spirent Solution

Spirent's SD-WAN test solution can be divided into four parts:

- Comprehensive set of SDN protocols, access network protocols
- Automated test methodologies for policy validation
- VNF Lifecycle Validation methodologies based on ETSI NFV TST 001
- NFVi analytics that enable customers to optimize VNF provisioning, capacity planning and optimizing the performance of VNFs

Spirent's SD-WAN test solution supports a comprehensive set of SDN protocol emulation, automated NFV test methodologies and best in class virtual test agents. Spirent virtual test agent may co-reside as a Test VNF on the server that hosts vCPE or may be deployed on a standalone server.

Spirent is determined to provide comprehensive and effective NFV test solutions to enable NEMs and Service Providers to move to the next stage of NFV deployment with confidence. Spirent's goal is not just to provide test tools but to provide test solutions that help unravel the conundrum surrounding the difficult NFV problems that the industry faces.

For more details on Spirent's SD-WAN/vCPE test solution, please contact your Spirent sales representative or visit www.spirent.com

Contact Us

For more information, call your Spirent sales representative or visit us on the web at www.spirent.com/ContactSpirent.

www.spirent.com

Americas 1-800-SPIRENT
+1-800-774-7368 | sales@spirent.com

Europe and the Middle East
+44 (0) 1293 767979 | emeainfo@spirent.com

Asia and the Pacific
+86-10-8518-2539 | salesasia@spirent.com

Rev B | 09/19