Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: September 15, 2016

B. Pularikkal
Cisco Systems
Q. Fu
H. Deng
China Mobile
G. Sundaram
S. Gundavelli
Cisco Systems

March 14, 2016

Virtual CPE Deployment Considerations
draft-pularikkal-virtual-cpe-00

Abstract

Broadband Service Provider Industry has been gearing towards the adoption of Virtual CPE (vCPE) solutions. The concept of vCPE is build around the idea that the physical CPE device at the customer premises can be simplified by moving some of the key feature functionalities from the physical CPE device to the Service Provider Network. This document starts discussing the drivers behind vCPE adoption followed by Solution level requirements. Two key Architecture models for vCPE, which can address the service provider and subscriber requirements, are covered in this reference document. Document also touches up on some of the key deployment considerations, which can influence the adoption of the vCPE architecture models.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on September 15, 2016.

Table of Contents

1. Introduction

Broadband Service Providers are constantly looking for opportunities to generate additional revenue streams from their existing broadband infrastructure. In order to achieve this, new value added services need to be created for the end customers. Customer retention is another key focus area for broadband subscribers, where they have been facing competition from Internet content providers on home multi-media services such as broadcast video, video on demand and voice. There is a need to improve the overall end user experience on an ongoing basis to reduce the subscriber churn. In order to achieve these business goals, Broadband Service Providers are starting to

consider the deployment of Virtual CPE based Architectures. There are several factors, which are driving the adoption of vCPE-based solutions. Also the recent technological advancements in cloud computing and software defined networking are expected to further accelerate the adoption vCPE based architectures.

The key aspect of the vCPE solutions is the simplification of the physical CPE device. Such a simplification allows minimizing the feature dependency on CPE vendors for the roll out of new service offerings. Also it reduces the complexities around service provisioning, Service Upgrade Troubleshooting etc. There are multiple architecture options being considered by the industry for vCPE solutions.

Objective of this draft is to serve as a reference material for Broadband Service Operators who are interested in migrating to vCPE based architectures. The document starts with going over some of the key drivers for vCPE solution adoption. Also it covers typical solution level requirements, which needs to be considered while selecting the right architecture models. Document also touches up on some of the key deployment considerations, which can influence the adoption of the vCPE architecture models.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

3. Solution Requirements for vCPE

This section provides a high level summary of solution requirements, which needs to be addressed by Virtual Connected Home Architecture Models. The solution requirements can be broadly classified under the following categories:

(1) Subscriber side requirements: Subscriber in the context of this documentation refers to a homeowner with Broadband connection. These requirements primarily map to the end user experience for a home subscriber in terms of connectivity, quality of experience and value added services.

(2) Broadband Operator side requirements: Operator is the broadband service provider such as Cable MSOs, DSL providers etc. These requirements primarily maps to the business aspects which needs to be covered in the solution in terms of CAPEX, OPEX reduction, service velocity, new revenue generation opportunities etc.

High level requirements under the above two categories are summarised in the table below:

Subscriber Side Requirements	Operator Side requirements
1) Private Home Network	1) Service Velocity
2) Zero Touch Provisioning	2) Simplified CPE
3) Local Bridging	3) Per UE Visibility
4) Local Routing	4) Community Wi-Fi
5) NAT, FW, IDS, Parental Control	5) IP Address Persistence
6) Home Network Analytics	6) UE Attachment/ Detachment detction
7) Self Service Portal	7)Usage based billing
8) Dynamic IP address Assignment	8)Quality of Service
9) Home Network Remote Access	9) NAT Traversal

Figure 1: VCPE Requirements

4. Architecture Models for vCPE

In this document three different architecture models are covered for the Virtual CPE based solutions. This section starts with a definition of what represents a virtual CPE and then gets into the details of the Architecture options, which are available for the implementation of the same.

4.1. Virtual CPE Definition

A virtual CPE (vCPE) is a logical representation of classical CPE functions performed by a physical CPE device. In other words, business logic and feature functionalities which are traditionally embedded in a CPE device is separated from the hardware device and runs in the Service Providers cloud. Concepts of vCPE has basis on the Network Function Virtualization. The business logic and feature functionalities of a CPE device are virtualized and runs as NFV in the cloud. Each simplified physical CPE would have a corresponding virtual CPE function running in the cloud. There are several ways to realize this vCPE instance in the cloud. One approach is to have separate vCPE instance running as a Linux container or micro-VM corresponding to each physical CPE instance. The vCPE may also be implemented as a representational state on aggregation platforms such as broadband network gateways (BNGs). A third approach may rely on a

combination of the BNG representational state and Service function chaining to represent the vCPE instance in the cloud. These Architecture models are covered in the subsequent sub-sections.

4.2. Virtual CPE Architecture Model-01

This model is build around the concept of separate virtualized instance per physical CPE device. In this model Virtual CPE instance handles the control plane as well as the data plane. Each micro VM represents an NFV element of CPE with integrated control and data plane. All feature functionalities get implemented on the NFV element itself. This model does not leverage the dynamic service function chaining capabilities.

A high level Architecture view of this model is provided in figure-below:

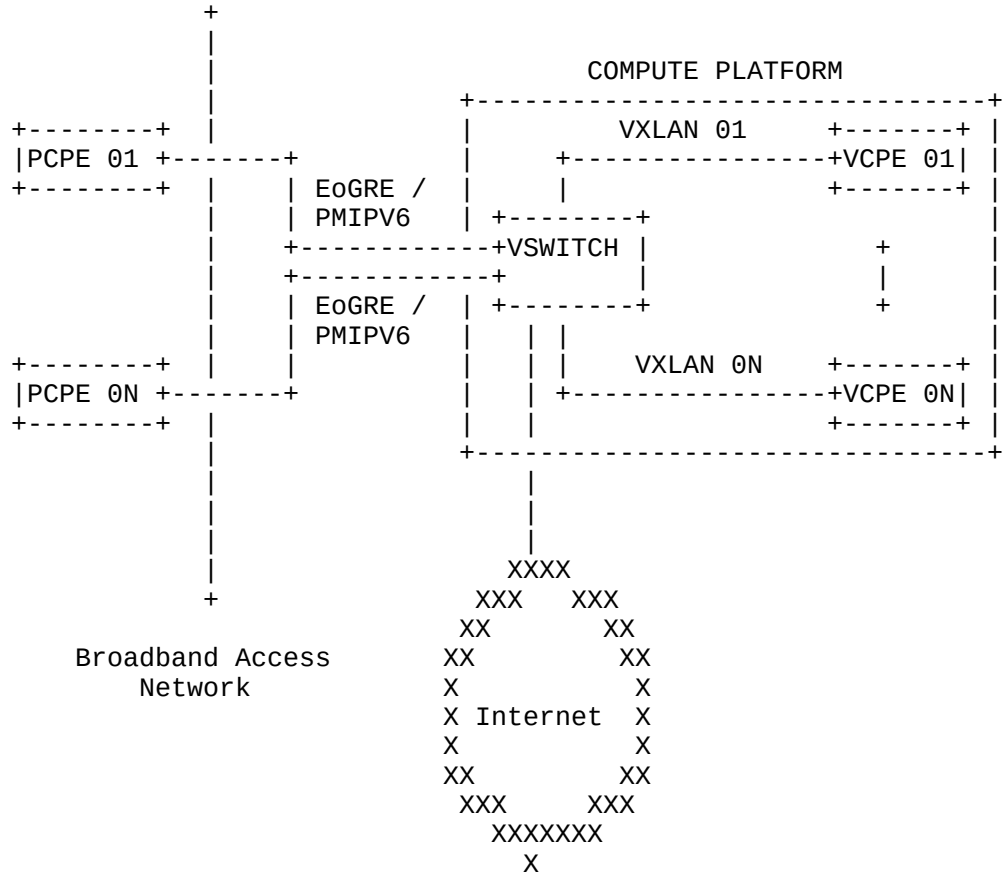

Figure 2: VCPE deployment model-01

P-CPE device performs just the bridging function where the layer-2 traffic between directly connected devices will be simply bridged by the P-CPE. Any layer-3 traffic will be transparently forwarded to the cloud over the tunnel.

In this model all the key cloud based components run on virtualized platforms. These virtual components are deployed on standalone virtual platforms rather than on large scale virtual DC of Service providers. Therefore, the tunnel will be terminated on the vSwitch rather than a tunnel termination GW located at the boarder of the DC.

An implementation could leverage either a vendor specific vSwitch or an Open vSwitch.

Tunnel end points are uniquely identified with the IP address of the P-CPE. The vSwitch maps the de-encapsulated traffic from the tunnels to unique VXLANs and will forward to the corresponding Micro VM instances. Micro VM instances will be responsible for supporting the key functions traditionally performed on physical CPE devices. After the feature processing, V-CPE instance will send the traffic back to the v-Switch over VXLAN tunnels and vSwitch will forward it to external network.

4.3. Virtual CPE Architecture Model-02

In this model vCPE in the cloud is corresponding to each physical CPE is realized by a representational state on a tunnel aggregation platform such as BNG. A provisioned physical CPE in run state is expected to have at least one tunnel established between the physical CPE and the BNG. As long as the PCPE is in run state there will be a CPE session on the BNG which represents the CPE itself. Some of the key CPE features will be running on the BNG while supplementary features and services can be deployed using dynamic service function chaining functions.

A high level Architecture view of this mode2 is provided in figure-below:

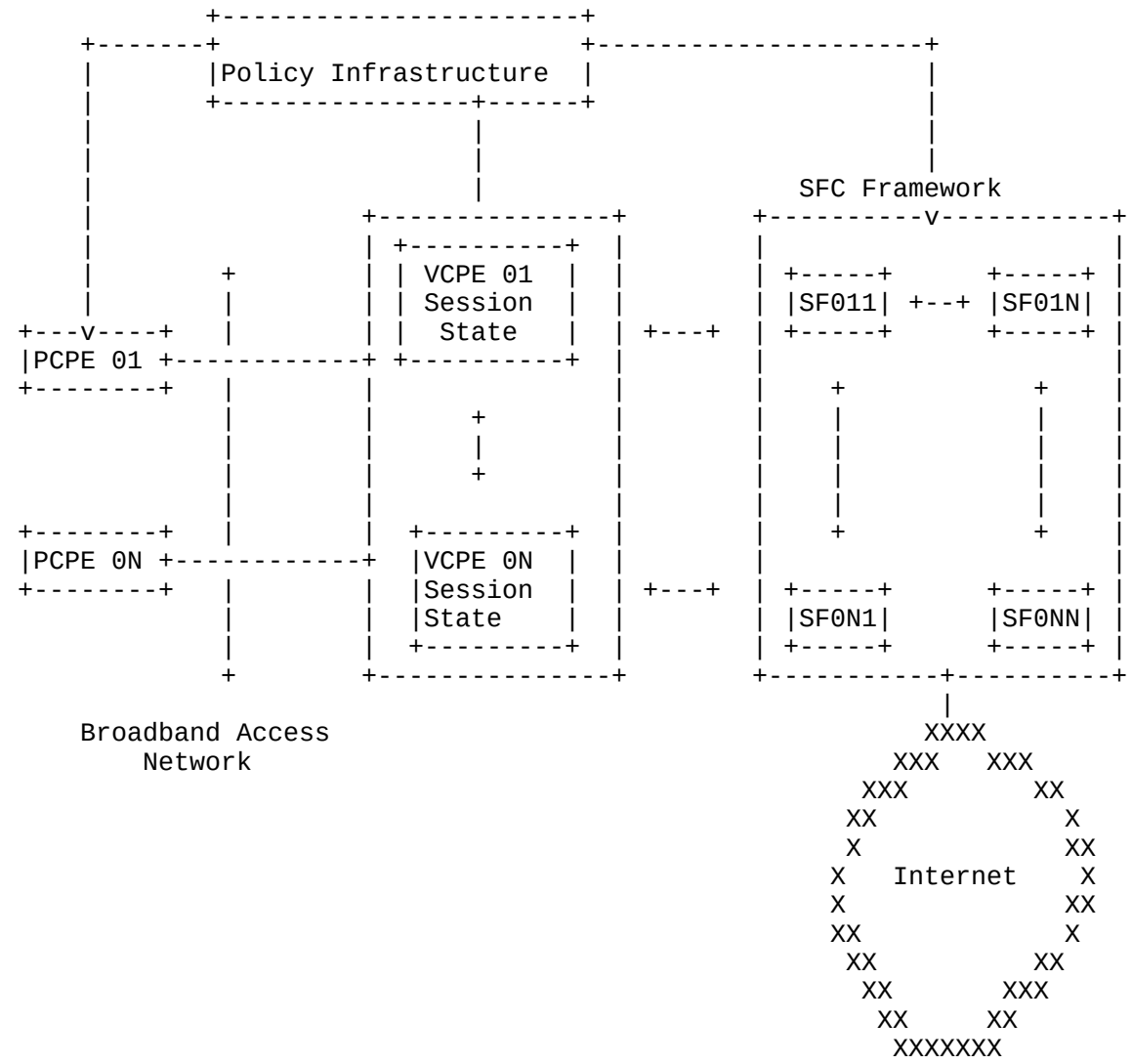

Figure 3: VCPE deployment model-02

In this model as well, P-CPE device performs just the bridging function where the layer-2 traffic between directly connected devices will be simply bridged by the P-CPE. Any layer-3 traffic will be transparently forwarded to the BNG over the tunnel.

There is no need for pre-configuration of the tunnels on BNG. When a P-CPE device become active and gets provisioned it will try to

establish an EoGRE tunnel session with V-CPE. Up on detecting a new P-CPE end point, the BNG would invoke an authorization process for the tunnel end point. It is up to the implementation to decide whether an out of band authentication mechanism is required before establishing v-CPE state on the BNG. If the access network is untrusted, the service provider may decide to overlay the EoGRE tunnel with IPSec encapsulation.

BNG will need to uniquely tag the subscriber flows before forwarding to the SFC framework. This can be accomplished by using some scalable tagging mechanisms such as VXLAN.

4.4. Virtual CPE Architecture Model-03

This is similar to model-02 but leverages split architecture for control plane and data plane for the BNG. This model introduces the concept of a BNG controller, which essentially carries out the control plane functions. Data plane component of the BNG can be a purpose built hardware optimized for scaleable tunnel termination, data encryption and data forwarding. Control plane intelligence of each vCPE resides as a session state on the BNG controller and the data plane intelligence including tunnel termination of each vCPE resides on the BNG-DP system. BNG-CP will leverage the FPC (Forwarding Policy Configuration) interface which is being defined in the DMM working group to instruct the BNG-DP system to establish V-CPE DP states with relevant configuration.Role of FPC interface in this solution is described in the sub-section below. In this model, all basic and supplementary subscriber features will be implemented using a dynamic service function-chaining framework.

A high level Architecture view of this mode3 is provided in figure-below:

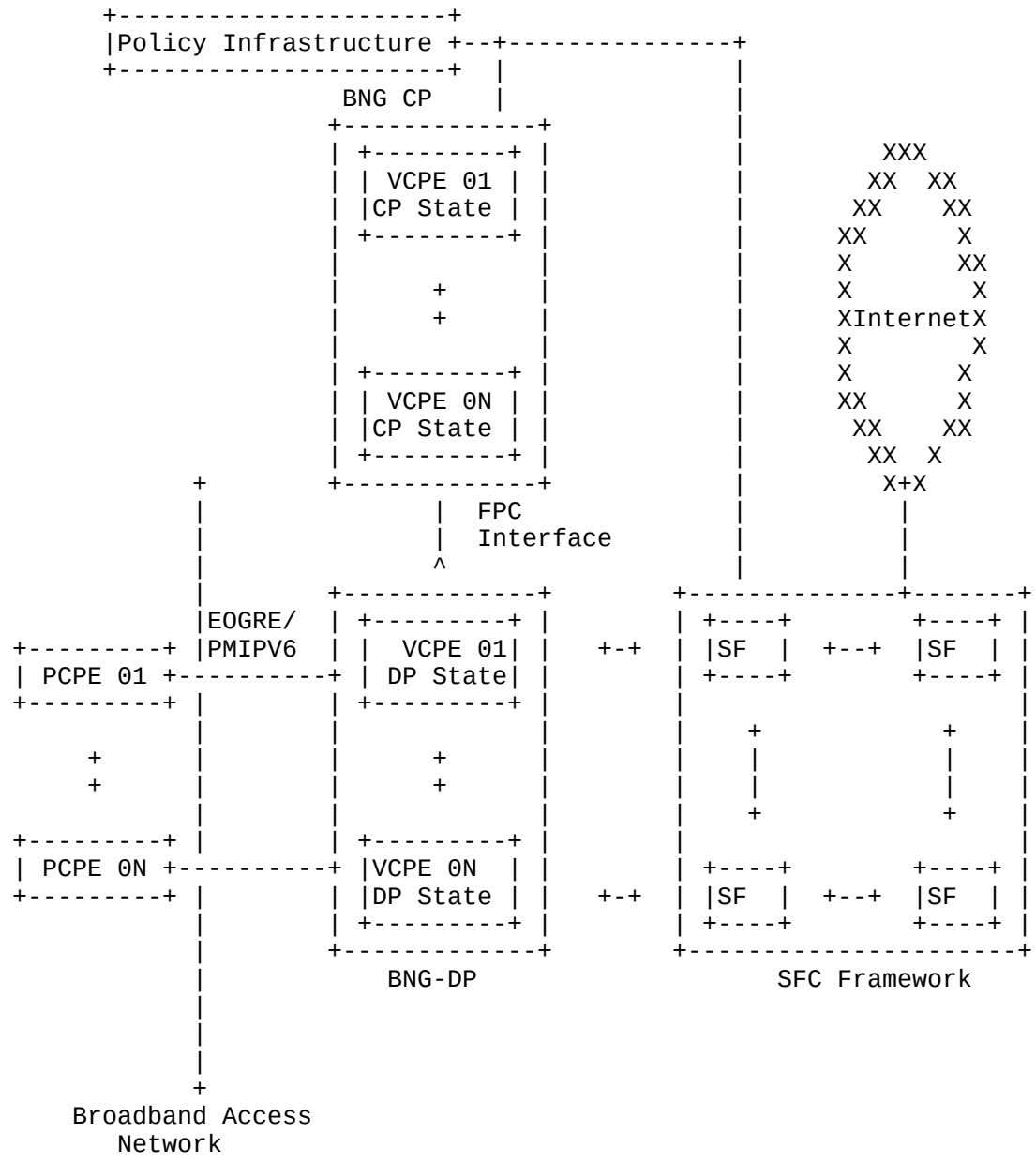

Figure 4: VCPE deployment model-03

4.4.1. Forwarding Policy Configuration (FPC) Interface

FPC Protocol interface defined in the DMM working group enables DMM use cases with Control Plane and data plane separation. In vCPE solution model-03, FPC protocol is applied to the interface between BNG-CP and BNG-DP. FPC interface consists of a client function which resides on the Control Plane System (BNG-CP in this case) and an agent function which resides on the Data Plane System (BNG-DP in this case). FPC defines a standard set of protocol semantics to exchange configuration information from the client to the agent. Agent processes the protocol semantics and translates them into configuration commands as per BNG-DP system technology. FPC client function residing on BNG-CP device will leverage FPC Protocol semantics to provision activate or deactivate the V-CPE DP states on BNG-DP with desired features.

5. Deployment Considerations for vCPE

This section at a high level touches up on some of the key deployment charecteristics which needs to be considered while selecting the right vCPE architecure

5.1. Multi-tenancy

vCPE represents the abstraction of key functions and features typically performed by classical device into service provider cloud. In order for such a solution to be operationally feasible and profitable, it is important for vCPE architecture to support multi-tenancy. This multi tenancy support needs to scale of the order of hundreds of thousands. From the context of vCPE deployments, the multi-tenancy refers to the logical separation of vCPE instances, which are housed in a common backend infrastructure. This backend infrastructure could consist of virtual elements on a compute platform or physical networking components. It could very well be a combination of virtual and physical components in the service provider cloud. Few of the key areas where multi-tenancy model will have an implication on the operational efficiency of the solution are listed below:

Overlapping IP addressing: Typically home networks are configured with RFC 1918 private address space 192.168.0.0/24. A vCPE solution, which deals with IP address management of the private home network, must support address overlap for these private home subnets.

Tunnel scale: Tunnel termination points in the service provider must support tunnel scale of the order of hundreds of thousands. A vCPE implementation must implement some form of unique tunnel id per

physical CPE to support saleable multi-tenancy for tunnel termination.

Overlapping SSID naming: vCPE framework must be flexible enough to allow home subscribers to configure private SSID names of their choice. Possibility of overlapping SSID names cannot be ruled out as subscribers randomly decide up on their private SSID names. Multi-tenancy solution for a vCPE framework must take into consideration this.

5.2. Tunneling

In a vCPE solution, the end subscriber data must be tunneled from the physical CPE towards the vCPE instance in the cloud. Typical home broadband deployments may have community Wi-Fi SSID enabled in addition to subscribers private home SSID. For such cases, the tunnel must be capable of carrying both private and community Wi-Fi SSID traffic in a secured manner. Today there are various tunneling methods being used for community Wi-Fi deployments. Two of the most common tunneling methods in use are EoGRE and PMIPv6. EoGRE is a layer-2 tunneling technology and it does not have a control plane of its own. PMIPv6 is a layer-3 tunneling technology with a well-defined control plane for tunnel management and session management. Either of these tunneling options can be leveraged to carry the private SSID traffic from the home towards the cloud-based vCPE. And both are capable of carrying community Wi-Fi and private home SSID traffic. The choice of the tunneling technology may be influenced by various factors such as simplicity, need for IP address persistence with client roaming, layer-2 forwarding in the data plane to the cloud as opposed to layer-3 forwarding etc.

5.3. Security

The classical home broadband deployments based up on intelligent physical CPE devices typically provide data privacy and security for the end subscriber content as it gets carried over the access network. A security framework for a vCPE network has to account for the following key aspects:

Subscriber Authentication

Protection against spoofing attacks

Data privacy

Prevention of eaves dropping between subscribers

Security considerations go hand in hand with multi-tenancy requirements as data and meta data from multiple subscribers will be handled by the backend systems.

5.4. Dynamic Service Chaining

One of the key motivation behind a cloud based connected home solution is to find additional revenue generation opportunities through rapid deployment of new services. The implementation of these new services requires a combination of system and network level functions to be applied to the end user traffic flows. Some of these functions may be enabled, by leveraging system level features on the CPE Device Anchor. But in many cases, it makes more sense to offload the feature processing to network function elements, which are external to the CPE Device Anchor (CDA).

Service function chaining (SFC) refers to a collection of network elements connected in a serialized fashion through which a traffic flow will be diverted prior to forwarding to the intended destination. Traditionally these service chains are hard connected there by causing challenges around flexibility and scale.

With dynamic service function chaining approach, the network elements, which perform various service functions, are arranged in grid model. Logical connectivity is established on a per traffic flow basis between the network elements to establish SFC pipeline for a qualified traffic flow. Dynamic SFC addresses the scale and flexibility limitations of the traditional chaining model. A vCPE solution must support the deployment of dynamic service function chaining.

5.5. NAT Traversal

Some vCPE deployments may leverage third party access networks and offer the solution as an overlay. In such cases, there may be requirement to bring up P-CPE behind a NAT router. The vCPE service provider may not have direct control over the NAT router, which is managed by the access network provider. In such cases, a tunnel transport mode, which can traverse NAT, needs to be selected.

EoGRE tunnels do not support NAT traversal, since there is no UDP layer in the encapsulation header. PMIPv6 can support NAT traversal if the right data encapsulation option is selected. If a layer tunneling technology is desired for the implementation where NAT traversal is a requirement, then tunnel transport mechanisms such as L2TPV3 may be explored.

6. Conclusion

In this document, the concept of VCPE is illustrated in detail. The basic concept of VCPE is to shift the complicated functions from the pCPE at the customer side to the VCPE at the service provider side. The motivation of such shifting can be concluded as providing quick launched customer defined services, reducing the Capex and Opex of the pCPE, and simlify the maintainance of both pCPE and VCPE. A use cases of community Wi-Fi is proposed for VCPE, which is a typical scenario for DMM. Three models are then discussed for the field deployment of VCPE. And CP/DP interface is suggested to be utilized in the deployment models.

7. Informative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

Authors' Addresses

Byju Pularikkal
Cisco Systems
170 West Tasman Drive
San Jose
United States

Email: byjupg@cisco.com

Qiao Fu
China Mobile
Xuanwumenxi Ave. No.32
Beijing
China

Email: fuqiao1@outlook.com

Hui Deng
China Mobile
Xuanwumenxi Ave. No.32
Beijing
China

Email: denghui@chinamobile.com

Ganesh Sundaram
Cisco Systems
170 West Tasman Drive
San Jose
United States

Email: gsundara@cisco.com

Sri Gundavelli
Cisco Systems
170 West Tasman Drive
San Jose
United States

Email: sgundave@cisco.com