OPSA Working Group
Internet-Draft
Intended status: Informational
Expires: January 19, 2017
July 18, 2016

H. Deng
China Mobile

Requirements of Composed VPN Service Model
draft-deng-opsawg-composed-vpn-sm-requirements-01

Abstract

The operator facing data model is valuable to reduce the operation and management. This document describes requirements of the composed VPN service model for operators to deploy end to end PE-based VPN services across multiple autonomous systems.

Requirements Language

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 RFC 2119 [RFC2119].

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 January 19, 2017.

Copyright Notice

Copyright (c) 2016 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction

Internet Service Providers (ISPs) have significant interest on providing Provider Edge (PE) based virtual private network (VPN) services, in which the tunnel endpoints are the PE devices. In this case, the Customer Edge (CE) devices do not need to have any special VPN capabilities. Customers can reduce support costs by outsourcing VPN operations to ISPs and using the obtained connectivity.

Typically, customers require either layer 2 or layer 3 connectivity services to exchange traffic among a collection of sites. The ISP gets the requirement and deploys the end to end VPN across multiple autonomous systems (AS) with an orchestrator.

The model described in [I-D.ietf-l3sm-l3vpn-service-model] is used for communication between customers and network operators. It facilitates customers to request the layer 3 VPN service while concealing many provider parameters they do not know.

However, the network operators have a different view of the managed network. An operator facing model is required to reduce the operation and management while still having reasonable control on the network. So that the operators can verify and optimize the VPN deployment based on the existing network.

This document describes requirements of the generic VPN model from the operators’ view for the PE-based VPN service configuration. It aims at providing a simplified configuration on how the requested VPN service is to be deployed over the shared network infrastructure. This model is limited to PE-Based VPNs as described in RFC 4110 [RFC4110] with the combination of layer 2 and layer 3 VPN services in multiple ASes.

2. Definitions

- Segment VPN service: The VPN service deployed for one segment which is usually an AS.

- Composed VPN service: The VPN service deployed within the ISP administrative domain across one or more segments. It could be a combination of layer 2 and layer 3 VPN services for each segment.

3. Use Cases and Usage

In practice, ISP may have various scenarios for the end to end VPN service deployment depending on the network infrastructure and the customer sites connectivity requirements. It will consequently generate requirements of the generic composed VPN service model design. The composed VPN service data model described in this document covers the following scenarios:

- Multi-AS VPN Service: Customer sites are located in different autonomous systems(AS). ISP need to deploy the VPN service across multiple ASes.

- Composed L2 and L3 VPN Service: Although the customer may request either layer 2 or layer 3 VPN service, the network infrastructure among customer sites may require different VPN service in the corresponding AS. So, an end to end VPN service within the ISP domain may be a composition of multiple segmental layer 2 and layer 3 VPN services.

- Dynamic Site Insertion: The customer site that is not in the previously provisioned VPN can be quickly included.

A typical usage of this operator facing model is as an input for an orchestration layer which will be responsible to translate it to segment VPN information for the configutation of domain controllers. As shown in the following figure, while, for example, users may send highly abstracted layer 3 VPN service requests to the application (e.g. BSS), it’s not enough for operators to deploy an end to end VPN service. The operator facing interface enables configuration of VPN deployment by introducing more network knowlegde and garvenance policies. For example :

- o Optimize the VPN deployment of the customer’s requests based on the exiting networking, e.g. deploy the L3VPN request from the customer to multiple VPN segments (IPRAN, PTN, IPCore) in the end to end environment.

- o Add the operation requirements, e.g. operation visualization, monitoring, diagnosis.

- o Manage various policies for different customers.

```
                                   +
       Customer Facing Interface   |
                            +------v-------+
                            | Application  |
                            +------+-------+
       Operator Facing Interface   |
                            +------v-------+
                            | Orchestrator |
                            +----+---+-----+
                                 |   |
                       +---------+   +-----------+
                       |                         |
                +------+------+            +------+------+
                | Controller1 |            | Controller2 |
                +------+------+            +------+------+
                       |                         |
             +---------+-----------+  +----------+----------+
             |      AS1 L2VPN      |  |      AS2  L3VPN     |
  +-------+  | +------+   +------+ |  | +------+   +------+ |  +-------+
  | Site1 +----+ PE11 +---+ PE12 +------+ PE21 +---+ PE22 +----+ Site2 |
  +-------+  | +------+   +------+ |  | +------+   +------+ |  +-------+
             +---------------------+  +---------------------+
```

4. Design Requirements

The PE-based VPN service is modeled with a recursive pattern as shown in the following figure. The VPN service deployed within each AS is modeled as a Segment VPN object including the VPN description information within this AS and the Access Points (AP) that are used to connect to the peered device or AS. As an end to end VPN service within the ISP domain, it’s then modeled as a Composed VPN object with the overall VPN information and the APs that are used to connect to the peered customer sites.

```
                        AP1 +---------------+ AP4
                    +-------+  ComposedVPN  +-------+
                            +----+-----+----+
                                 |     |
                       +---------+     +---------+
                       |                         |
             AP1 +-----v-----+ AP2     AP3 +-----v-----+ AP4
          +------+  SegVPN1  +-------------+  SegVPN2  +------+
                 +-----------+             +-----------+
  +--------------------------------------------------------------------+
             +---------------------+  +---------------------+
             |        AS1          |  |        AS2          |
  +-------+  | +------+   +------+ |  | +------+   +------+ |  +-------+
  | Site1 +----+ PE11 +---+ PE12 +------+ PE21 +---+ PE22 +----+ Site2 |
  +-------+  | +------+   +------+ |  | +------+   +------+ |  +-------+
             +---------------------+  +---------------------+
```

Generic PE-based VPN Modeling

The composed VPN model can be structured as in the following figure. The Composed VPN top container contains VPN basic information, a list of segment VPN information, and a list of access point information.

The Basic Information here includes overall description for this composed VPN service. I.e., all the properties (e.g., topology, service type) in this object describe the overview that the customer want, no matter with any segment VPN information.

The Access Point List in the Composed VPN container describes a list of APs that are used to connect to the peered customer sites. However, the AP is modeled with generic Access Point Information provided by the PE either in the composed VPN view or in the segment VPN view. The AP contains:

- the basic information that is relatively static, no matter which exact peer AP is going to connect.

- the information about the routing protocol that is used to exchange the routing information with the remote peer. This object is extensible with any posible routing protocols. The BGP and static routing listed are examples to show how these two widely used solutions are described.

- the QoS description. There can be two kinds of QoS configuration. The AP based QoS: describes the QoS requirements on the access point. For example, the CAR (committed access rate) definition on the inbound or outbound ports. The flow based QoS: describes the

QoS requirements on a flow. This enables the fine grained QoS control with the capability of identifying the flow.

A composed VPN includes one or more segment VPN desribed by the Segment VPN List. Each Segment VPN Information is only described from the segment point of view. I.e., the description here takes care about how the segment VPN looks like and how it can communicate with peered devices outside this segment VPN. The segment information is composed of the basic information and a list of APs. The set of APs in the description are interfaces that customer sites or other segment VPNs can attach. In different scenarios, each segment VPN could be a layer 2 VPN, or layer 3 VPN.

```
                      +--------------+
                      | Composed VPN |
                      +---+----------+
                          |
                          |  +-------------------+
                          +--+ Basic Information |
                          |  +-------------------+
                          |      +--Topology
                          |      +--Service Type
                          |      +--...
                          |
                          |  +-------------------+
                          +--+ Access Point List |
                          |  +-------------------+
                          |      +--Basic Information
                          |      +--QoS
                          |      +--Routing Protocol
                          |      +--...
                          |
                          |  +------------------+
                          +--+ Segment VPN List |
                             +------------------+
                                 +--Basic Information
                                 +--Access Point List
                                 +--...
```

Composed VPN Model Structure

5. IANA Considerations

TBD

6. Security Considerations

TBD

7. Acknowledgements

TBD

8. References

8.1. Normative 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>.

[RFC4110] Callon, R. and M. Suzuki, "A Framework for Layer 3 Provider-Provisioned Virtual Private Networks (PPVPNs)", RFC 4110, DOI 10.17487/RFC4110, July 2005, <http://www.rfc-editor.org/info/rfc4110>.

8.2. Informative References

[I-D.ietf-l3sm-l3vpn-service-model] Litkowski, S., Shakir, R., Tomotaki, L., Ogaki, K., and K. D’Souza, "YANG Data Model for L3VPN service delivery", draft-ietf-l3sm-l3vpn-service-model-12 (work in progress), July 2016.

Authors’ Addresses

Hui Deng
China Mobile
No.32 Xuanwumen West Street
Beijing 100053
China

Email: denghui02@hotmail.com