

Network Working Group
Internet-Draft
Intended status: Informational
Expires: January 4, 2015

L. Zheng
Z. Li
S. Aldrin
Huawei Technologies
B. Parise
Cisco Systems
July 3, 2014

Performance Monitoring Analysis for L3VPN
draft-zheng-l3vpn-pm-analysis-03

Abstract

To perform the measurement of packet loss, delay and other metrics on a particular VPN flow, the egress PE need to tell to which specific ingress VRF a packet belongs to. But for L3VPN, multipoint-to-point network model applies, flow identifying is a challenge. This document summarizes the current performance monitoring mechanisms for L3VPN in MPLS networks, and analyzes various solutions and challenges for measuring performance metrics within these networks. This document also identifies various key points which needs to be taken in consideration when designing L3VPN performance monitoring mechanisms. Performance measurements within non-MPLS L3VPN networks is not within the scope of the document.

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 4, 2015.

Internet-Draft

PM Analysis for L3VPN

July 2014

Copyright Notice

Copyright (c) 2014 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	2
2.	Requirement of L3VPN Performance Monitoring	3
3.	Overview of Current Mechanisms for MPLS Networks	4
3.1.	Packet Loss and Delay Measurement for MPLS Networks	4
3.2.	Synthetic Measurements	4
3.3.	Real packet Measurements	5
3.4.	Profile for MPLS-based Transport Networks	5
4.	Challenge for L3VPN Performance Monitoring	5
5.	Design Consideration	7
5.1.	P2P Pseudo Connection	7
5.2.	Hierarchy L3VPN	7
5.3.	Control Plane	7
5.4.	Data Plane	7
5.5.	MPLS OAM	7
5.6.	QoS	8
5.7.	ECMP	8
6.	Manageability Consideration	8
7.	Security Considerations	8
8.	IANA Considerations	8
9.	References	9
9.1.	Normative References	9
9.2.	Informative References	9
	Authors' Addresses	9

[1.](#) Introduction

Level 3 Virtual Private Network (L3VPN) [[RFC4364](#)] service is widely deployed in the production network. It is deployed to provide enterprise interconnection, Voice over IP (VoIP), video, mobile, etc. services. Most of these services are sensitive to the packet loss and delay. The capability of performance metrics measurement for

packet loss, delay, as well as related metrics is essential for performance monitoring and Service Level Agreement (SLA). The requirement for SLA measurement for MPLS networks has been documented in [[RFC4377](#)].

One popular deployment of L3VPN nowadays is in mobile backhaul networks. When deploying MPLS-TP in mobile backhaul networks, due to the scaling issue with PWs, L3VPN is used either for end-to-end service delivery, or L2VPN and L3VPN are used in hybrid networking. The measurement capability of L3VPN provides operators with greater visibility into the performance characteristics of their networks, and provides diagnostic information in case of performance degradation or failure and helps for fault localization.

To perform the measurement of packet loss, delay and other metrics on a particular VPN flow, the egress PE need to tell to which specific ingress VRF a packet belongs. But for L3VPN, there multipoint-to-point (MP2P) network model applies, flow identifying is a challenge. This document summarizes the current performance monitoring mechanisms for MPLS networks, and analyzes the challenges for L3VPN performance monitoring. This document also discuss the key points need to be taken into consideration when designing L3VPN performance monitoring mechanisms. All references to L3VPN in the document refers to MPLS L3VPN networks.

[2.](#) Requirement of L3VPN Performance Monitoring

The specific user's traffic is usually transported by the VPN of the service provider. The performance monitoring needs to be done on the aggregation flow between a pair of VRFs which belong to the same VPN for a specific user. And the corresponding performance monitoring report should be provided against the Service Level Agreement (SLA) by the service provider. For example, in the following figure, the VRF11 and VRF12 belongs to VPN1 which is used to bear the service traffic for the specific user USER1, and the VRF21 and VRF22 belongs to VPN2 which is used to bear the service

traffic for the specific user USER2. Then the performance monitoring needs to be implemented on the aggregation traffic flow between VRF11 and VRF12 for the USER1. And the performance monitoring needs to be implemented on the aggregation traffic flow between VRF21 and VRF22 for the USER2.

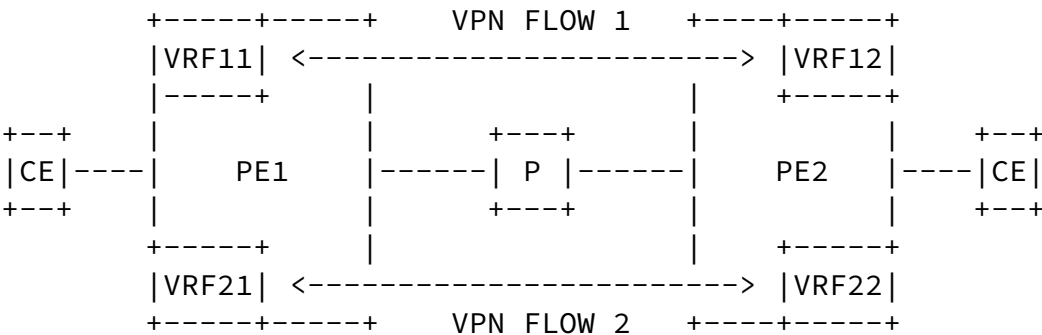


Figure 1: Performance Monitoring between VRFs

- In order to facilitate the description, we introduce two terminologies in this document:
- VPN flow: a VPN flow is the aggregate traffic flow between an ingress VRF and an egress VRF belongs to the same VPN.
 - L3VPN Performance Monitoring (PM): L3VPN PM means the performance mornitoring on a VPN flow.

3. Overview of Current Mechanisms for MPLS Networks

3.1. Packet Loss and Delay Measurement for MPLS Networks

[RFC6374]defines procedure and protocol mechanisms to enable the efficient and accurate measurement of packet loss, delay, as well as related metrics in MPLS networks.

The Loss Measurement (LM) protocol can perform two distinct kinds of loss measurement. In inferred mode, it can measure the loss of specially generated test packets (in order to infer the approximate data-plane loss level). In direct mode, it can directly measure data-plane packet loss. Direct mode measurements provide perfect loss accounting, but may require specialized hardware support and is only applicable to some LSP types. Inferred measurement provides only approximate loss measurements but is generally applicable. The LM and Delay Measurement (DM) protocols are initiated from a single node. A query message may be received either by a single node or by multiple nodes; i.e. these protocols provide point-to-point or point-to-multipoint measurement capabilities.

[3.2.](#) Synthetic Measurements

Performance measurements are done using synthetic packets sent over the network. Metrics like response time, jitter, packet loss could be inferred using these synthetic packet measurements. In order to

perform inferred measurements, the crafted packets have to behave like data packets and take the same path as data packets.

[3.3.](#) Real packet Measurements

Measurements of actual data packets is resource intensive and requires special way of accounting for the measurements. Counters within the network devices are primarily used to measure various metrics. Various technologies like Netflow, IPFIX, etc are used to collect the data and process it offline to derive performance measurements. When the data is aggregated, collecting per flow or per VPN customer traffic data becomes complex.

[3.4.](#) Profile for MPLS-based Transport Networks

Procedures for the measurement of packet loss, delay, and throughput in MPLS networks are defined in [\[RFC6374\]](#). [\[RFC6375\]](#) describes a profile, i.e. a simplified subset, of procedures that suffices to meet the specific requirements of MPLS-based transport networks [\[RFC5921\]](#) as defined in [\[RFC5860\]](#). This profile is presented for the convenience of implementers who are concerned exclusively with the transport network context.

LM session is externally configured and the values of several protocol parameters can be fixed in advance at the endpoints involved in the session, so that inspection or negotiation of these parameters is not required.

4. Challenge for L3VPN Performance Monitoring

To perform the measurement of packet loss, delay and other metrics on a particular VPN flow, the egress PE need to tell to which specific ingress VRF a packet belongs.

The above mentioned existing mechanisms for MPLS networks provide either point-to-point or point-to-multipoint measurement capabilities. For a specific receiver, it could easily identify a specific flow by the label stack information, when LDP is not used and Penultimate Hop Pop (PHP) function is disabled.

But in the case of L3VPN, multipoint-to-point network model applies , it makes the identification of a flow a challenge, for packet loss and delay measurement. According to the label allocation mechanisms of L3VPN, a private label itself cannot uniquely identify a specific VPN flow. That is, when the egress PE allocates VPN label for a specific prefix of a VPN, the same label will be advertised to all its peers. Given a VPN flow, the egress PE cannot tell which ingress

VRF is from based on the private label it carries. As a result, it's not feasible to perform the loss or delay measurement on this flow.

Some people may argue this could be solved by using " tunnel label + private label" for flow identification, but it is not true. In L3VPN when LDP LSP applies[RFC5036], the LSPs may be merged at any intermediate nodes along the LSP. The egress PE cannot derive a unique identifier of the source PE from label stack. The tunnel label cannot help for flow identification due to the LSP merge. When TE LSP applies [[RFC3209](#)] in L3VPN, the ingress VRF could be identified by the " tunnel label + private label" only if no extranet exist. The egress PE cannot tell which specific VRF a packet belongs to, when extranet (If the various sites in a VPN are owned by different enterprises) exist on ingress PE. Figure 1 shows an example of extranet VPN. In the extranet VPN, both Site 11 and Site

[illegible]

The current label allocation mechanism of L3VPN makes the flow identification a challenge for L3VPN performance monitoring, as a result the current performance monitoring mechanisms for MPLS networks cannot be applied to L3VPN networks. Without any backward compatible extensions or alteration to current label allocation

5. Design Consideration

This section discuss the key points need to be taken in consideration when designing L3VPN performance monitoring mechanism.

[5.1.](#) P2P Pseudo Connection

As analyzed above, to perform the packet loss or delay measurement on a specific VPN flow, it is critical for the egress PE to uniquely identify the ingress VRF, i.e. to establish the Point-to-Point pseudo connection between the two VRFs. Current allocation mechanism may need extension or alteration to help build up the Point-to-Point pseudo connection. Once the Point-to-Point pseudo connection is built up, current measurement mechanisms may be applied to L3VPN .

[5.2.](#) Hierarchy L3VPN

There are flexible hierarchy L3VPN deployment scenarios such as inter-AS, carrier's carrier, etc. [[RFC4364](#)]. The the design of LM and DM mechanisms should take these scenarios into account.

[5.3.](#) Control Plane

In L3VPN, BGP is used to distribute a particular route, as well as an MPLS label that is mapped to that route [[RFC4364](#)]. The label mapping information for a particular route is piggybacked in the same BGP Update message that is used to distribute the route itself. In order to setup the Point-to-Point pseudo connection between ingress and egress VRFs the current label distribution mechanism may be altered. For compatibility, this alteration SHOULD NOT change the current label distribution mechanism dramatically.

[5.4.](#) Data Plane

Same as for control plane, for compatibility reason, the data plane should as far as possible be compatible with the current L3VPN forwarding procedure.

[5.5.](#) MPLS OAM

[[RFC6374](#)], [[RFC6375](#)] defines procedure and protocol mechanisms to enable the measurement of packet loss, delay, as well as related metrics for MPLS networks. These mechanisms SHOULD be reasonably reused in L3VPN networks. The addressing of source and destination of

to be changed to identify the measured VRF.

LSP ping and trace based on [[RFC4379](#)] are used to perform various metric measurement which includes jitter etc. Most of the measurements like response time, jitter, etc., are inferred measurements with synthetic measurements and not necessarily the true representation of the data packets traversing the network, especially with respect to packet loss measurements.

[5.6.](#) QoS

Performing the packet loss or delay measurement in L3VPN network, either proactive or on-demand, SHOULD NOT impact the customer QoS experience.

[5.7.](#) ECMP

Performance measurements within ECMP networks poses a bigger challenge. When the data packet traverse the network, the logic of hashing on to a ECMP path is a local decision based on the header information it is carrying. Number of labels, IP header, UDP header could play a role in considering which path the packet traverses. When PM is measured with synthetic packets, the crafted packets have to be constructed to ensure various ECMP paths are measured. This poses a big challenge for the source, which generates these packets, to reflect the behavior of the actual data traffic and measure the metrics. [[RFC4379](#)] provides various mechanisms to perform LM and DM measurements over ECMP networks.

[6.](#) Manageability Consideration

[RFC6374] describes manageability consideration of packet loss and delay measurement for MPLS network. The defined mechanisms should be reused for L3VPN PM.

[7.](#) Security Considerations

This document does not change the security properties of L3VPN.

[8.](#) IANA Considerations

This document makes no request to IANA.

[9.](#) References

[9.1.](#) Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.

[9.2.](#) Informative References

- [RFC3209] Awduche, D., Berger, L., Gan, D., Li, T., Srinivasan, V., and G. Swallow, "RSVP-TE: Extensions to RSVP for LSP Tunnels", [RFC 3209](#), December 2001.
- [RFC4364] Rosen, E. and Y. Rekhter, "BGP/MPLS IP Virtual Private Networks (VPNs)", [RFC 4364](#), February 2006.
- [RFC4377] Nadeau, T., Morrow, M., Swallow, G., Allan, D., and S. Matsushima, "Operations and Management (OAM) Requirements for Multi-Protocol Label Switched (MPLS) Networks", [RFC 4377](#), February 2006.
- [RFC4379] Kompella, K. and G. Swallow, "Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures", [RFC 4379](#), February 2006.
- [RFC5036] Andersson, L., Minei, I., and B. Thomas, "LDP Specification", [RFC 5036](#), October 2007.
- [RFC5860] Vigoureux, M., Ward, D., and M. Betts, "Requirements for Operations, Administration, and Maintenance (OAM) in MPLS Transport Networks", [RFC 5860](#), May 2010.
- [RFC5921] Bocci, M., Bryant, S., Frost, D., Levrau, L., and L. Berger, "A Framework for MPLS in Transport Networks", [RFC 5921](#), July 2010.
- [RFC6374] Frost, D. and S. Bryant, "Packet Loss and Delay Measurement for MPLS Networks", [RFC 6374](#), September 2011.
- [RFC6375] Frost, D. and S. Bryant, "A Packet Loss and Delay Measurement Profile for MPLS-Based Transport Networks", [RFC 6375](#), September 2011.

Authors' Addresses

Internet-Draft

PM Analysis for L3VPN

July 2014

Lianshu Zheng
Huawei Technologies
Huawei Building, No.156 Beiqing Rd.
Beijing 100095
China

Email: vero.zheng@huawei.com

Zhenbin Li
Huawei Technologies
Huawei Building, No.156 Beiqing Rd.
Beijing 100095
China

Email: lizhenbin@huawei.com

Sam K. Aldrin
Huawei Technologies

Email: aldrin.ietf@gmail.com

Bhavani Parise
Cisco Systems

Email: bhavani@cisco.com

