Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 5, 2012

X. Fu
M. Betts
Q. Wang
ZTE
D. McDysan
A. Malis
Verizon

July 4, 2011

Framework for latency and loss traffic engineering application
draft-fuxh-ccamp-delay-loss-te-framework-00

Abstract

Latency and packet loss is such requirement that must be achieved according to the Service Level Agreement (SLA) / Network Performance Objective (NPO) between customers and service providers. Latency and packet loss can be associated with different service level. The user may select a private line provider based on the ability to meet a latency and loss SLA.

The key driver for latency and loss is stock/commodity trading applications that use data base mirroring. A few milli seconds and packet loss can impact a transaction. Financial or trading companies are very focused on end-to-end private pipe line latency optimizations that improve things 2-3 ms. Latency/loss and associated SLA is one of the key parameters that these "high value" customers use to select a private pipe line provider. Other key applications like video gaming, conferencing and storage area networks require stringent latency, loss and bandwidth.

This document describes requirements to communicate latency and packet loss as a traffic engineering performance metric in today's network which is consisting of potentially multiple layers of packet transport network and optical transport network in order to meet the latency/loss SLA between service provider and his customers.

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/.

Copyright Notice

Table of Contents

1. Introduction

Current operation and maintenance mode of latency and packet loss measurement is high in cost and low in efficiency. The latency and packet loss can only be measured after the connection has been established, if the measurement indicates that the latency SLA is not met then another path is computed, setup and measured. This "trial and error" process is very inefficient. To avoid this problem a means of making an accurate prediction of latency and packet loss before a path is establish is required.

This document describes the requirements and control plane implication to communicate latency and packet loss as a traffic engineering performance metric in today's network which is consisting of potentially multiple layers of packet transport network and optical transport network in order to meet the latency and packet loss SLA between service provider and his customers.

1.1. Conventions Used in This Document

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].

2. Latency and Loss Report

This section isn't going to say how latency or packet loss is measured. How to measure has been provided in ITU-T [Y.1731], [G.709] and [ietf-mpls-loss-delay]. It's purpose is to define what it is sufficiently clear that mechanisms could be defined to measure it, and so that independent implementations will report the same thing. If control plane wish to define the ability to report latency and packet loss, control plane must be clear what it are reporting.

Packet/Frame loss probability is expressed as a percentage of the number of service packets/frames not delivered divided by the total number of service frames during time interval T. Loss is always measured by sending a measurement packet or frame from measurement point to its reception and recception sending back a response.

The link of latecny is the time interval between the propagation of an electrical signal and its reception. Latency is always measured by sending a measurement packet or frame from measurement point to its reception. In some usages, latency is measured by sending a packet/frame that is returned to the sender and the round-trip time is considered the latency of bidirectional co-routed or associated LSP. One way time is considered as the latency of unidirectional

LSP. The one way latency may not be half of the round-trip latency in the case that the transmit and receive directions of the path are of unequal lengths.

Control plane should report two components of the delay, "static" and "dynamic". The dynamic component is caused by traffic loading. What is reporting for "dynamic" portion is approximation.

Latency on a connection has two sources: Node latency which is caused by the node as a result of process time in each node and: Link latency as a result of packet/frame transit time between two neighbouring nodes or a FA-LSP/Composit Link [CL-REQ]. The average latency of node should be reported. It is simpler to add node latency to the link delay vs. carrying a separate parameter and does not hide any important information. Latency variation is a parameter that is used to indicate the variation range of the latency value. Latency, latecny variation value must be reported as a average value which is calculated by data plane.

3. Requirements Identification

End-to-end service optimization based on latency and packet loss is a key requirement for service provider. This type of function will be adopted by their "premium" service customers. They would like to pay for this "premium" service. Latency and loss on a route level will help carriers' customers to make his provider selection decision. Following key requirements associated with latency and loss is identified.

- REQ #1: The solution MUST provide a means to communicate latency, latency variation and packet loss of links and nodes as a traffic engineering performance metric into IGP.

- REQ #2: Latency, latency variation and packet loss may be unstable, for example, if queueing latency were included, then IGP could become unstable. The solution MUST provide a means to control latency and loss IGP message advertisement and avoid unstable when the latency, latency variation and packet loss value changes.

- REQ #3: Path computation entity MUST have the capability to compute one end-to-end path with latency and packet loss constraint. for example, it has the capability to compute a route with X amount bandwidth with less than Y ms of latency and Z% packet loss limit based on the latency and packet loss traffic engineering database. It MUST also support the path computation with routing constraints combination with pre-defined priorities,

e.g., SRLG diversity, latency, loss and cost.

- REQ #4: One end-to-end LSP may traverses some Composite Links [CL-REQ]. Even if the transport technology (e.g., OTN) implementing the component links is identical, the latency and packet loss characteristics of the component links may differ. In order to assign the LSP to one of component links with different latency and packet loss characteristics, the solution SHOULD provide a means to indicate that a traffic flow should select a component link with minimum latency and/or packet loss, maximum acceptable latency and/or packet loss value and maximum acceptable delay variation value as specified by protocol. The endpoints of Composite Link will take these parameters into account for component link selection or creation.

- REQ #5: One one end-to-end LSP may traverse a server layer. There will be some latency and packet loss constraint requirement for the segment route in server layer. The solution SHALL provide a means to indicate FA selection or FA-LSP creation with minimum latency and/or packet loss, maximum acceptable latency and/or packet loss value and maximum acceptable delay variation value. The boundary nodes of FA-LSP will take these parameters into account for FA selection or FA-LSP creation.

- REQ #6: The solution SHOULD provide a means to accumulate (e.g., sum) of latency information of links and nodes along one LSP across multi-domain (e.g., Inter-AS, Inter-Area or Multi-Layer) so that an latency validation decision can be made at the source node. One-way and round-trip latency collection along the LSP by signaling protocol and latency verification at the end of LSP should be supported. The accumulation of the delay is "simple" for the static component i.e. its a linear addition, the dynamic/ network loading component is more interesting and would involve some estimate of the "worst case". However, method of deriving this worst case appears to be more in the scope of Network Operator policy than standards i.e. the operator needs to decide, based on the SLAs offered, the required confidence level.

- REQ #7: Some customers may insist on having the ability to re-route if the latency and loss SLA is not being met. If a "provisioned" end-to-end LSP latency and/or loss could not meet the latency and loss agreement between operator and his user, The solution SHOULD support pre-defined or dynamic re-routing to handle this case based on the local policy. The latency performance of pre-defined protection or dynamic re-routing LSP MUST meet the latency SLA parameter.

- REQ #8: If a "provisioned" end-to-end LSP latency and/or loss performance is improved because of some segment performance promotion, the solution SHOULD support the re-routing to optimize latency and/or loss end-to-end cost.

- REQ #9: As a result of the change of latency and loss in the LSP, current LSP may be frequently switched to a new LSP with a appropriate latency and packet loss value. In order to avoid this, the solution SHOULD indicate the switchover of the LSP according to maximum acceptable change latency and packet loss value.

4. Control Plane Implication

- The latency and packet loss performance metric MUST be advertised into path computation entity by IGP (etc., OSPF-TE or IS-IS-TE) to perform route computation and network planning based on latecny and packet loss SLA target. Latency, latecny variation and packet loss value MUST be reported as a average value which is calculated by data plane. Latency and packet loss characteristics of these links and nodes may change dynamically. In order to control IGP messaging and avoid being unstable when the latency, latency variation and packet loss value changes, a threshold and a limit on rate of change MUST be configured to control plane. If any latency and packet loss values change and over than the threshold and a limit on rate of change, then the change MUST be notified to the IGP again.

- Link latency attribute may also take into account the latency of a network element (node), i.e., the latency between the incoming port and the outgoing port of a network element. If the link attribute is to include node latency AND link latency, then when the latency calculation is done for paths traversing links on the same node then the node latency can be subtracted out.

- When the Composite Links [CL-REQ] is advertised into IGP, there are following considerations.

  * The latency and packet loss of composite link may be the range (e.g., at least minimum and maximum) latency value of all component links. It may also be the maximum latency value of all component links. In these cases, only partial information is transmited in the IGP. So the path computation entity has insufficient information to determine whether a particular path can support its latency and packet loss requirements. This leads to signaling crankback. So IGP may be extended to advertise latency and packet of each component link within one

Composite Link having an IGP adjacency.

- One end-to-end LSP (e.g., in IP/MPLS or MPLS-TP network) may traverse a FA-LSP of server layer (e.g., OTN rings). The boundary nodes of the FA-LSP SHOULD be aware of the latency and packet loss information of this FA-LSP.

  * If the FA-LSP is able to form a routing adjacency and/or as a TE link in the client network, the total latency and packet loss value of the FA-LSP can be as an input to a transformation that results in a FA traffic engineering metric and advertised into the client layer routing instances. Note that this metric will include the latency and packet loss of the links and nodes that the trail traverses.

  * If total latency and packet loss information of the FA-LSP changes (e.g., due to a maintenance action or failure in OTN rings), the boundary node of the FA-LSP will receive the TE link information advertisement including the latency and packet value which is already changed and if it is over than the threshold and a limit on rate of change, then it will compute the total latency and packet value of the FA-LSP again. If the total latency and packet loss value of FA-LSP changes, the client layer MUST also be notified about the latest value of FA. The client layer can then decide if it will accept the increased latency and packet loss or request a new path that meets the latency and packet loss requirement.

- Restoration, protection and equipment variations can impact "provisioned" latency and packet loss (e.g., latency and packet loss increase). The change of one end-to-end LSP latency and packet loss performance MUST be known by source and/or sink node. So it can inform the higher layer network of a latency and packet loss change. The latency or packet loss change of links and nodes will affect one end-to-end LSP's total amount of latency or packet loss. Applications can fail beyond an application-specific threshold. Some remedy mechanism could be used.

  * Pre-defined protection or dynamic re-routing could be triggered to handle this case. In the case of predefined protection, large amounts of redundant capacity may have a significant negative impact on the overall network cost. Service provider may have many layers of pre-defined restoration for this transfer, but they have to duplicate restoration resources at significant cost. Solution should provides some mechanisms to avoid the duplicate restoration and reduce the network cost. Dynamic re-routing also has to face the risk of resource limitation. So the choice of mechanism MUST be based on SLA or

policy. In the case where the latency SLA can not be met after a re-route is attempted, control plane should report an alarm to management plane. It could also try restoration for several times which could be configured.

5. Security Considerations

The use of control plane protocols for signaling, routing, and path computation of latency and loss opens security threats through attacks on those protocols. The control plane may be secured using the mechanisms defined for the protocols discussed. For further details of the specific security measures refer to the documents that define the protocols ([RFC3473], [RFC4203], [RFC4205], [RFC4204], and [RFC5440]). [GMPLS-SEC] provides an overview of security vulnerabilities and protection mechanisms for the GMPLS control plane.

6. IANA Considerations

This document makes not requests for IANA action.

7. References

7.1. Normative References

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

[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.

[RFC3473] Berger, L., "Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions", RFC 3473, January 2003.

[RFC3477] Kompella, K. and Y. Rekhter, "Signalling Unnumbered Links in Resource ReSerVation Protocol - Traffic Engineering (RSVP-TE)", RFC 3477, January 2003.

[RFC3630] Katz, D., Kompella, K., and D. Yeung, "Traffic Engineering (TE) Extensions to OSPF Version 2", RFC 3630, September 2003.

[RFC4203] Kompella, K. and Y. Rekhter, "OSPF Extensions in Support

of Generalized Multi-Protocol Label Switching (GMPLS)", RFC 4203, October 2005.

7.2. Informative References

[CL-REQ] C. Villamizar, "Requirements for MPLS Over a Composite Link", draft-ietf-rtgwg-cl-requirement-02 .

[G.709] ITU-T Recommendation G.709, "Interfaces for the Optical Transport Network (OTN)", December 2009.

[Y.1731] ITU-T Recommendation Y.1731, "OAM functions and mechanisms for Ethernet based networks", Feb 2008.

[ietf-mpls-loss-delay] D. Frost, "Packet Loss and Delay Measurement for MPLS Networks", draft-ietf-mpls-loss-delay-03 .

Authors' Addresses

Xihua Fu
ZTE

Email: fu.xihua@zte.com.cn

Malcolm Betts
ZTE

Email: malcolm.betts@zte.com.cn

Qilei Wang
ZTE

Email: wang.qilei@zte.com.cn

Dave McDysan
Verizon

Email: dave.mcdysan@verizon.com

Andrew Malis
Verizon

Email: andrew.g.malis@verizon.com