

Routing Area Working Group
Internet-Draft
Intended status: Informational
Expires: January 5, 2015

T. Huang
Z. Li
S. Hares
Huawei Technologies
July 4, 2014

Use Cases for an Interface to MPLS TE
draft-huang-i2rs-mpls-te-usecases-02

Abstract

Network services based on Virtual Networks (VN) or Virtual Circuits (VC) may be run over MPLS-TE links, and support network configurations such as hub-spoke, service routing, or on-demand networks. An MPLS Traffic Engineering (TE) network is typically configured and the results of its operation analyzed through network management interfaces (CLI, SNMP or NETCONF). These interactions control each of the MPLS TE links, and diagnose operations issues concerning link configuration, MPLS TE protection, and traffic switching-over. The network management functions also monitor MPLS TE links and provide fault detection.

The Interface to the Routing System (I2RS) (draft-ietf-i2rs-architecture) programmatic interface to the routing system provides an alternative way to control the configuration and diagnose the operation of MPLS links. I2RS may be used for the configuration, manipulation, polling, or analyzing MPLS TE. This document describes a set of use cases for which I2RS can be used for MPLS TE. It is intended to provide a base for a solution draft describing I2RS information models and protocol functions that will support virtual networks that utilize MPLS TE.

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 5, 2015.

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. I2RS Requirements from the MPLS TE Use cases	3
3. MPLS TE Configuration	5
3.1. Static CR-LSP Configuration	5
3.2. RSVP-TE Policy Configuration	6
4. MPLS TE Protection	6
5. MPLS TE Traffic Switch Overs	7
5.1. Failure Detection	7
5.2. Network Upgrading	7
5.3. Handling Node Overload	8
6. Monitoring of MPLS TE	8
6.1. Performance Monitoring	8
6.2. Fault Monitoring	9
6.3. LSP Monitoring	9
7. IANA Considerations	10
8. Security Considerations	10
9. References	11
9.1. Normative References	11
9.2. Informative References	11
Authors' Addresses	12

1. Introduction

Network services based on Virtual Networks (VN) or Virtual Circuits (VC) may be run over MPLS-TE links, and support network configurations such as hub-spoke, service routing, or on-demand networks. Typically, MPLS TE networks are configured and results of its operation analyzed through network management interfaces (CLI, SNMP or NETCONF). These interactions to control MPLS TE links and

diagnose their operation encompass: MPLS TE configuration, MPLS TE protection, traffic switching-over, traffic detection, and fault detection.

The I2RS architecture and protocol as defined in [[I-D.ietf-i2rs-architecture]] may be used to control network protocols like MPLS TE using a set of programmatic interfaces. These programmatic interfaces allow one I2RS client to control the MPLS TE network by analyzing its operational state and TE LSP data, plus manipulating TE LSP's configuration to achieve various goals. I2RS is not intended to replace any existing network management or configuration mechanisms, (E.g. Command Line Interface or NETCONF). Instead, I2RS is intended to augment these existing mechanisms by defining a standardized set of programmatic interfaces to enable easier configuration, interrogation, and analysis of the protocol.

This document describes set of use cases for which I2RS's programmatic interfaces can be used to control and analyze the operation of MPLS TE. The use cases described in this document cover the following aspects of MPLS TE: MPLS TE configuration, MPLS TE protection, MPLS TE traffic switch-over, monitoring of MPLS TE and fault detection. The goal is to increase the community's understanding of where the I2RS MPLS TE extensions fit within the overall I2RS architecture. It is intended to provide a basis for the solutions draft describing the set of Interfaces to the MPLS TE.

2. I2RS Requirements from the MPLS TE Use cases

This section summarize the requirements from the MPLS TE use cases. Each of these requirements has been given an ID number of MPLS-TE-REQ-*nn* for ease of reference. While this summary provides a handy reference, the reader is advised to review the full details of the MPLS TE scenario.

The requirements from the Traffic Steering use case are:

- o MPLS-TE-REQ-01: Network programming software managing the static CR-LSP devices may incorporate an I2RS Client along with a path calculation entity, a label management entity, and a bandwidth management entity. The I2RS Client should be able to communicate the static configuration to the network nodes, and monitor the status of the CR-LSPs.
- o MPLS-TE-REQ-02: The I2Client should be able to synchronously send the configuration for all of the network nodes from egress node to ingress node via the I2RS Agents attached to each node, and be able to delay the final ingress node configuration until all the

I2RS AGents on all other nodes toward the egress have denoted a successful path set-up.

- o [MPLS-TE-REQ-03:] MPLS TE defines abundant constraints such as explicit path, bandwidth, affinity, SRLG, priority, hop limit, and others. The I2RS Client Agent exchange should be able to signal concurrent local path calculation could obtain an optimized result and allow more services to be held in a TE network. The I2RS Agent should be able to trigger a global concurrent re-optimization at a specific time on multiple nodes by communicating with each node's I2RS agent.
- o [MPLS-TE-REQ-04:] The I2RS client should be able to manually calculate a re-optimization of the the MPLS TE network and send the new constraints including the calculated path to each node via the I2RS agent with an indication to re-signal the TE LSPs with make-before-break method.
- o [MPLS-TE-REQ-05] With I2RS, the node's I2RS agent should be able to send to an I2RS client a status notification that not enough resources exist for a back up LSP and TE tunnel. Upon receiving this notification the I2RS client should be able to trigger concurrent calculation for the failed path calculation of the backup LSP or TE tunnel and send the updated paths to I2RS agents with a command to re-signal the TE LSPS with make-before-break Method.
- o [MPLS-TE-REQ-06] With I2RS, upon receipt the failure notification from an I2RS Agent, the I2RS client would create a global concurrent optimization to handle the failure event. This would occur by the I2RS client signalling the I2RS agents on all nodes to: a) trigger a new concurrent calculation of the backup LSP or TE tunnel via failed path calculation, and b) re-signal updates to the TE LSPs process with a make-before-break method.
- o [MPLS-TE-REQ-07] Upon receiving a signal an upgrade event signal (from operator), the I2RS client could calculate another path for the affected TE tunnels to deviate traffic away from the resource being upgraded, and then send the request to I2RS agents on the appropriate nodes to move the traffic. After the upgrade completes, the I2RS client can simply remove I2RS configurations causing the traffic to revert to the original path. Or, the I2RS can re-optimize the TE tunnels for another pathways (E.g. as a part of a sequence of upgrades).
- o [MPLS-TE-REQ-08] I2RS agents can notify I2RS Clients of impending or existing MPLS TE overload conditions that might cause TE LSP

rejections. This overload conditions include: due to CPU, memory, LSP label space, or LSP numbers.

- o [MPLS-TE-09] Automatic bandwidth adjustment applications can also be linked to the I2RS clients need to monitor the traffic on TE tunnels in order to provide traffic analysis. The I2RS client should be able to read the TE Tunnel topology and the bandwidth analysis in order to automatically calculate a new path for the TE tunnel if it is needed. The I2RS Client also needs to be able to the I2RS agents in the nodes to install the new TE Tunnels with the make-before-break option.
- o [MPLS-TE-REQ-10] With I2RS, the node failure or link failure can be part of the notification stream sent by an I2RS Agent to an I2RS Client on a centralized server gathering information.
- o [MPLS-TE-REQ-11] The I2RS client can notify the I2RS agents on specific nodes (or devices) to re-signal TE LSPs one by one if there is a resource dependency. [MPLS-TE-REQ-12] The I2RS Client can gather the TE LSPs' state from I2RS Agents on all nodes in order to coordinate such handling of LSP resources.
- o [MPLS-TE-REQ-13] The I2RS Clients collecting information from I2RS Agents can be arranged in a hierarchy to provide scaling of collections. An application hosting an I2RS client collecting information from I2RS Agents on nodes can have an I2RS Agent that reports combined information to a single location.

3. MPLS TE Configuration

There are two types of TE LSP: static CR-LSP and dynamic TE LSP created by protocol of RSVP-TE or CR-LDP. Static CR-LSP is configured with forwarding items such as interface, label and bandwidth, etc. node by node. Dynamic TE LSP is configured with MPLS TE parameters which are used to calculate path and set up TE LSP by protocol. Both configurations are complex.

The following cases will introduce how to improve configuration efficiency with I2RS and I2RS client.

3.1. Static CR-LSP Configuration

Currently, nodes and interfaces to be configured with a Static CR-LSP are assigned label and bandwidth values before the static CR-LSP is configured through some network management configuration interface (e.g. CLI or NETCONF). Due to this complex configuration, Static CR-LSP is only used in small, simple topologies with few services.

[MPLS-TE-REQ-01] Network programming software managing the static CR-LSP devices may incorporate an I2RS Client along with a path calculation entity, a label management entity, and a bandwidth management entity. The I2RS Client will communicate the static configuration to the network nodes, and monitor the status of the CR-LSPs.

Currently the downloading of CR-LSP forwarding is processed node by node. When an ingress node finishes download before all other nodes have completed, the forwarding path will not be set-up and the traffic will be lost.

[MPLS-TE-REQ-02] With I2RS, the I2RS client may send the configuration for all of the network nodes from egress node to ingress node. The final ingress node configuration may be delayed until all other nodes toward the egress have denoted a successful path set-up.

3.2. RSVP-TE Policy Configuration

MPLS TE defines abundant constraints such as explicit path, bandwidth, affinity, SRLG, priority, hop limit, and others. A local path calculation entity would calculate an appropriate path according to the constraints. It is common knowledge that the calculated results are closely related with the request order, different calculation order may have different results. Concurrent calculation could obtain an optimized result and allow more services to be held in a TE network.

[MPLS-TE-REQ-03:] With I2RS, an I2RS client could trigger global concurrent re-optimization at a specific time on multiple nodes by communicating with each node's I2RS agent.

[MPLS-TE-REQ-04:] Alternatively, the I2RS client could manually re-optimize the MPLS TE network and send the new constraints including the calculated path to each node via the I2RS agent with an indication to re-signal the TE LSPs with make-before-break method.

4. MPLS TE Protection

There are many kinds of protection for MPLS TE, such as TE tunnel protection, TE LSP protection and TE FRR protection. Further, each protection may have two methods: 1:1 and 1+1 protection. FRR may have another two methods: link and node protection. With I2RS, I2RS client can define the protection mode according to the service requirement and transmit to the I2RS agent on each node.

In addition, typically when one node's calculations determine that there is not enough resource for the backup LSP or TE tunnel, it is usually not true in the distributed network. If the existing LSP or TE tunnel could be adjusted to bypass some links or nodes, the necessary resources will be released to provide the backup LSP or TE tunnel.

[MPLS-TE-REQ-05] With I2RS, the node's I2RS agent can send to an I2RS client the status notification of not enough resources for back up LSP and TE tunnel. Upon receiving this notification the I2RS client could trigger concurrent calculation for the failed path calculation of the backup LSP or TE tunnel and send the updated paths to I2RS agents with a command to re-signal the TE LSPS with make-before-break Method.

5. MPLS TE Traffic Switch Overs

This section describes use cases for the MPLS TE traffic switch over caused by failure detection, network upgrading, overloading, and schedule traffic movements.

5.1. Failure Detection

There are many failure detection technologies such as Ethernet OAM/ BFD/ OAM/RSVP Hello. When a failure is detected, traffic will be switched over to the backup path. Re-optimization of the TE tunnel may fail for insufficient resource.

[MPLS-TE-REQ-06] With I2RS, upon receipt the failure notification from an I2RS Agent, the I2RS client would create a global concurrent optimization to handle the failure event. This would occur by the I2RS client signaling the I2RS agents on all nodes to: a) trigger a new concurrent calculation of the backup LSP or TE tunnel via failed path calculation, and b) re-signal updates to the TE LSPs process with a make-before-break method.

5.2. Network Upgrading

When upgrades in a network are planned (e.g., for maintenance purposes), some graceful mechanisms can be used to avoid traffic disruption by gracefully shutting down MPLS-TE or GMPLS-TE resources. The resources include TE links, component links within bundled TE links, label resources, and an entire TE node. Typically IGP or RSVP-TE protocol is extended to notify ingress node to bypass the shut down point.

[MPLS-TE-REQ-07] With I2RS, the operator signals the upgrade event to the application associated with the I2RS client. The I2RS client

could calculate another path for the affected TE tunnels to deviate traffic away from the resource being upgraded. The I2RS client would then communicate with I2RS agents on the appropriate nodes to move the traffic. After the upgrade completes, the I2RS client can simply remove I2RS configurations causing the traffic to revert to the original path. Or, the I2RS can re-optimize the TE tunnels for another pathways (E.g. as a part of a sequence of upgrades).

5.3. Handling Node Overload

When a node with MPLS TE support becomes overloaded due to the usage exceeding maximums of CPU, memory, LSP label space, or LSP number space, the setup of new TE LSPs should be rejected. The overload condition may also impact existing LSPs, and even cause flapping of MPLS TEs. Typically, a threshold value is set to avoid the overload condition so that existing TE LSPs will not be impacted. Normally, IGP protocols or RSVP-TE would be extended to notify all other nodes of the overload condition. This notification allows ingress nodes to bypass the overloaded node.

[MPLS-TE-REQ-08] I2RS agents can notify I2RS Clients of impending or existing MPLS TE overload conditions that might cause TE LSP rejections. This overload conditions include: due to CPU, memory, LSP label space, or LSP numbers.

6. Monitoring of MPLS TE

6.1. Performance Monitoring

Typically, performance measurement such as traffic statistics is done in the ingress node of TE tunnel. Applications such as traffic analysis or traffic forecasts depend on these traffic statistics being reported to centralize site for processing

With I2RS, the I2RS client can be attached to the application as gather the traffic statistics from I2RS agents running on the ingress nodes.

[MPLS-TE-REQ09] Automatic bandwidth adjustment applications can also be linked to the I2RS clients that monitor the traffic on TE tunnels and provide analysis. The I2RS client can read the TE Tunnel topology and the bandwidth analysis in order to automatically calculate a new path for the TE tunnel if it is needed. The I2RS Client would then signal the I2RS agents in the nodes to install the new TE Tunnels with the make-before-break option.

6.2. Fault Monitoring

When node or link failure happens, traffic will be switched over to the backup path. At the same time, the failure information will be reported and recorded. Network operators will process network management and maintenance based on the failed information.

[MPLS-TE-REQ-10] With I2RS, the node failure or link failure can be part of the notification stream sent by an I2RS Agent to an I2RS Client on a centralized server gathering information.

6.3. LSP Monitoring

In the global concurrent re-optimization process in section 2.2, an LSP update may depend on another LSP to release resources for it.

[MPLS-TE-REQ-11] The I2RS client can notify the I2RS agents on specific nodes (or devices) to re-signal TE LSPs one by one if there is a resource dependency. [MPLS-TE-REQ-12] The I2RS Client can gather the TE LSPs' state from I2RS Agents on all nodes in order to coordinate such handling of LSP resources.

[MPLS-TE-REQ-13] The I2RS Clients collecting information from I2RS Agents can be arranged in a hierarchy to provide scaling of collections. An application hosting an I2RS client collecting information from I2RS Agents on nodes can have an I2RS Agent that reports combined information to a centralized service as shown in the figure 1 below

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

[I-D.hares-i2rs-use-case-vn-vc]

Hares, S. and M. Chen, "Use Cases for Virtual Connections on Demand (VCoD) and Virtual Network on Demand (VNoD) using Interface to Routing System", draft-hares-i2rs-use-case-vn-vc-02 (work in progress), February 2014.

[I-D.ietf-i2rs-architecture]

Atlas, A., Halpern, J., Hares, S., Ward, D., and T. Nadeau, "An Architecture for the Interface to the Routing System", draft-ietf-i2rs-architecture-04 (work in progress), June 2014.

[I-D.ietf-i2rs-problem-statement]

Atlas, A., Nadeau, T., and D. Ward, "Interface to the Routing System Problem Statement", draft-ietf-i2rs-problem-statement-04 (work in progress), June 2014.

[I-D.ietf-i2rs-rib-info-model]

Bahadur, N., Folkes, R., Kini, S., and J. Medved, "Routing Information Base Info Model", draft-ietf-i2rs-rib-info-model-03 (work in progress), May 2014.

[I-D.ietf-mpls-ldp-dod]

Beckhaus, T., Decraene, B., Tiruveedhula, K., Konstantynowicz, M., and L. Martini, "LDP Downstream-on-Demand in Seamless MPLS", draft-ietf-mpls-ldp-dod-09 (work in progress), July 2013.

[I-D.ietf-mpls-ldp-ip-pw-capability]

Raza, K. and S. Boutros, "Controlling State Advertisements Of Non-negotiated LDP Applications", draft-ietf-mpls-ldp-ip-pw-capability-07 (work in progress), April 2014.

[I-D.ietf-mpls-seamless-mpls]

Leymann, N., Decraene, B., Filsfils, C., Konstantynowicz, M., and D. Steinberg, "Seamless MPLS Architecture", draft-ietf-mpls-seamless-mpls-07 (work in progress), June 2014.

- [RFC4364] Rosen, E. and Y. Rekhter, "BGP/MPLS IP Virtual Private Networks (VPNs)", RFC 4364, February 2006.
- [RFC4447] Martini, L., Rosen, E., El-Aawar, N., Smith, T., and G. Heron, "Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)", RFC 4447, April 2006.
- [RFC4762] Lasserre, M. and V. Kompella, "Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling", RFC 4762, January 2007.
- [RFC5036] Andersson, L., Minei, I., and B. Thomas, "LDP Specification", RFC 5036, October 2007.
- [RFC5283] Decraene, B., Le Roux, JL., and I. Minei, "LDP Extension for Inter-Area Label Switched Paths (LSPs)", RFC 5283, July 2008.

Authors' Addresses

Tieying Huang
Huawei Technologies
Huawei Bld., No.156 Beiqing Rd.
Beijing 100095
China

Email: Huangtieying@huawei.com

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

Email: lizhenbin@huawei.com

Susan Hares
Huawei Technologies
7453 Hickory Hill
Saline, MI 48176
USA

Email: shares@ndzh.com