Requirements for MPLS Over a Composite Link
draft-ietf-rtgwg-cl-requirement-01

- Authors: C. Villamizar, Ed.D. McDysan, Ed. S. Ning A. Malis L. Yong
- Contributors: F. Jounay, Y. Kamite
- Acknowledgements: D, Papadimitriou, L. Berger, T. Li, J. Scuder, A. Zinin

Changes since Version 00

- Summary of IETF 77 WG Minutes
  - http://tools.ietf.org/wg/rtgwg/minutes?item=minutes77.html
  - Requirements document should focus on service provider's problem definition
    - Need to prioritize and state what is mandatory vs desirable
  - Describe what needs to be done without saying how
    - Get solutions out of the document
  - "Reboot" (i.e., rewrite) the document, target 7 pages
    - `Discussion in WG about appendix and boilerplate not being included in above page count not in minutes, but clarified separately with WG chairs
  - List of technical topics discussed which draft attempted to cover
    - data plane, label stack encoding, usage
    - latency functional requirements
    - what information is summarized in IGP and how does this scale
    - definition of flow and how this should be handled
    - disruption due to moving LSP
    - scope only MPLS or also including IP
- Summary of WG Mailing List Discussion
  - Curtis documented a list of requirements and discussion thread ensued
    - Primarily Curtis, Dave, Tony Li and John Drake involved
    - Some good discussion on candidate solution approaches, characteristics
    - Non-solution oriented requirements per above WG minutes direction from chairs included in this draft
  - Dave issued a rough draft complete rewrite per WG minutes direction from chairs
    - Written from service provider perspective, added appendix as service provider background
    - Merged in requirements from above thread
    - This was used as basis for draft-01 developed by authors

Rewritten Draft Structure (Minus Boilerplate)

<7 Pages

- 1. Introduction
- 2. Assumptions
- 3. Definitions
- 4. Network Operator Functional Requirements
- 4.1. Availability, Stability and Transient Response
- 4.2. Component Links Provided by Lower Layer Networks
- 4.3. Parallel Component Links with Different Characteristics
- 5. Derived Requirements
- 7. Security Considerations

6 Pages

- Appendix A. More Details on Existing Network Operator Practices and Protocol Usage
- Appendix B. Existing Multipath Standards and Techniques . . . . .
  - B.1. Common Multpath Load Spliting Techniques
  - B.2. Simple and Adaptive Load Balancing Multipath
  - B.3. Traffic Split over Parallel Links
  - B.4. Traffic Split over Multiple Paths
- Appendix C. ITU-T G.800 Composite Link Definitions and Terminology

Assumptions

- Services supported include
  - L3VPN,
  - L2VPN (VPWS, VPLS, VPMS)
  - Internet traffic encapsulated by at least one MPLS label
  - Dynamically signaled MPLS and MPLS-TP LSPs
  - Dynamically signaled pseudowires.
- MPLS LSPs supporting above services may be pt-pt, pt-mpt, or mpt-mpt.
- Requirements context for composite links is a Label Edge Router (LER) or a Label Switch Router (LSR) as defined in RFC 3031 [RFC3031].
- IP DSCP cannot be used for flow identification since L3VPN requires Diffserv transparency (see RFC 4031 5.5.2 [RFC4031])
  - In general, network operators do not rely on the DSCP of Internet packets.

Definitions

- Composite Link (ITU-T G.800 Definitions in Appendix C, translated to IETF terminology in this draft)
  - Multiple parallel links: When multiple parallel component links between a LER/ LSR and another LER/LSR.
  - Multi-layer Component Link: A component link that is formed by other network elements at other layers.
- Component Link:
  - A physical link (e.g., Lambda, Ethernet PHY, SONET/SDH, OTN, etc.) with packet transport capability, or a logical link (e.g., MPLS LSP, Ethernet VLAN, MPLS-TP LSP, etc.)
- Flow:
  - A sequence of packets that must be transferred on one component link.
- Flow identification:
  - The label stack and other information that uniquely identifies a flow.
  - Other information in flow identification may include an IP header, PW control word, Ethernet MAC address, etc.
  - Note that an LSP may contain one or more Flows or an LSP may be equivalent to a Flow.
  - Flow identification is used to locally select a component link, or a path through the network toward the destination.

Network Operator Functional Requirements

- Availability, Stability and Transient Response
  - Limiting unavailability is key to customers and Service Providers
  - SLA objective timeframes range from O(100 ms) (e.g, VPWS) to completely down reporting O(minutes)
  - FR#1 SHALL summarize composite link routing advertisements regarding so that convergence occurs within SLA objective timeframe.
  - FR#2 SHALL aggregate signaling in response to failure for worst case network cross section such that MPLS LSPs are restored within SLA objective timeframe
  - FR#3 SHALL provide path selection for flow across network containing multiple paths (containing composite links) as to automatically distribute load over composite links. SHOULD work similar to case where individual component links characteristics are advertised.
  - FR#4 If extensions/new existing protocols are specified, then SHOULD provide means to migrate an existing deployment in minimally disruptive manner.
  - FR#5 Automatic LSP routing and/or load balancing MUST not oscillate such that an SLA is violated. Since oscillation may cause reordering, MUST control frequency flow placement changes to different component link.
  - FR#6 Management/diagnostic protocols MUST work on composite links.

Network Operator Functional Requirements

- Component Links Provided by Lower Layer Networks
  - Lower (or same) layer networks may change performance characteristics (e.g., latency)
  - Currently no protocol for lower layer network to communicate performance parameters to a higher layer network
  - FR#7 SHALL specify protocol means for lower layer server network to communicate latency to higher layer client network.
  - FR#8 Precision of latency reporting SHOULD be at least 10% of the one way latency for latency of 1 ms or more.
  - FR#9 SHALL limit latency on per LSP basis between nodes to meet an SLA target when path contains one or more composite links.
  - Services may have different SLAs (e.g., loss) for different QoS classes. Overload which violates an SLA parameter (e.g., loss) may occur.
  - FR#10 If traffic flow demand exceeds composite link capacity, SHOULD cause LSPs for some traffic flows to move to other uncongested paths. Preempted LSPs MAY not be restored if there is no uncongested path in the network.

Network Operator Functional Requirements

- Parallel Component Links with Different Characteristics
  - Lower layer networks provide diversity to meet Availability SLAs
  - Many techniques exist to balance flows across composite links or select a path for a flow across a network with composite links (Appendix B)
  - These requirements are in addition to the existing techniques
  - FR#11 SHALL measure traffic for labeled flow and dynamically select component to place this flow to balance load such no component link is overloaded.
  - FR#12 When flow moved between component links in same composite link, MUST be done in minimally disruptive manner.
    - Possibility of reordering when target link latency greater than current
    - Controlling jitter buffer under/overrun important for some flows
  - FR#13 SHALL identify flows needing bound on rearrangement frequency.

Network Operator Functional Requirements

- Parallel Component Links with Different Characteristics
  - FR#14 SHALL communicate whether flows in LSP can be split across multiple component links. SHOULD indicate useable flow identification field(s)
  - FR#15 SHALL indicate flow selection of component link with minimum latency.
  - FR#16 SHALL indicate flow selection of component link with a maximum acceptable latency value as specified by protocol.
  - FR#17 SHALL indicate flow selection of component link with maximum acceptable delay variation value.
  - FR#18 SHALL automatically distribute flows across component links such that SLA objectives are met.
  - FR#19 SHALL provide distribute flows from single LSP across multiple component links to handle case where LSP traffic exceeds largest component link.

Derived Requirements

- Derives high-level protocol specification requirements from functional requirements
  - Captures some mailing list comments, proposals that were technical instead of functional
- DR#1 SHOULD extend existing protocols, develop new protocol only if significant enhancement.
- Vast majority of network operators use L3VPN/L2VPN services over LDP.
- TE extensions to IGP and RSVP-TE viewed as being overly complex.
- DR#2 SHOULD extend LDP capabilities to meet functional requirements (without using TE methods as decided in [RFC3468]).
- DR#3 MUST support coexistence of LDP and RSVP-TE signaled LSPs on composite link.
- DR#4 When nodes connected via a composite link are in the same MPLS network topology, the solution MAY define extensions to the IGP.

Derived Requirements

- DR#5 When nodes are connected via a composite link are in different MPLS network topologies, the solution SHALL NOT rely on extensions to the IGP.
- DR#6 When worst case failure scenario occurs,, links advertised in the IGP causes convergence to occur, causing period of unavailability. The convergence time of the solution MUST meet the SLA objective for unavailability.
- DR#7 SHALL summarize characteristics of component links as composite link. Convergence time MUST be better than advertising individual component links. SHALL represent range of component link capabilities to meet functional requirements SHALL minimize frequency of advertisement updates causing IGP convergence.
- DR#8 EDITORIAL DUPLICATION OF DR#6. WILL REMOVE.
- DR#9 When worst case failure scenario occurs, number of RSVP-TE LSPs resignaled causes period of unavailability. The resignaling time MUST meet SLA objective for unavailability. Resignaling time MUST not increase significantly as compared with current methods.

Proposed Next Steps

- Solicit more working group discussion on the mailing list on this draft to:
  - Agree on assumptions and definitions
  - Clarify/ agree problem statement and functional requirements
  - Clarify/ agree derived protocol requirements
  - Review appendices for clarity and relevance
- Recommend working group discuss/decide on mailing list
  - how best to discuss/decide on candidate solution structure
  - how best to charter/develop any needed protocol specifications