1. Introduction

In the last couple of decades, Internet service providers (ISPs) have adopted new technologies to provide better end-to-end services to customers. They started with Interior Gateway Protocols (IGP) metric controlled dedicated lines (using T1s and T3s) in the 90's, and then came the ATM networks (using OC-3s and OC-12s) during the mid 90's (Soricelly et al., 2003, p.475-p.478). The inability of IGP controlled dedicated lines to provide higher speeds and inefficient control over traffic led to the coming of ATM technology which eliminated both these drawbacks by introducing Private Virtual Circuits (PVCs), allowing the separation of customer traffic from physical end-to-end dedicated lines to logical end-to-end virtual circuits. (Soricelly et al., 2003, p.478). Later on, Multiprotocol Layer Switching (MPLS) was introduced in order to consolidate the ATM, Frame Relay, Voice and IP networks into a single unified network infrastructure (De Ghein, 2007, p. xxiv). Given the fact that MPLS was created based on the knowledge of the IP protocol, most ISPs have deployed it in their backbone network to support mission critical data like voice, video and core business services (Capello et al., 2005, p.1).

Historically, MPLS have been deployed in a logical fully meshed fashion, having the core devices to maintain unidirectional paths of each and every traffic destination (Yasukawa, et al., 2009, p.2). These paths are called Labeled Switch Paths (LSPs). LSPs are created dynamically in an end-to-end fashion on a per customer basis. However, Yasukawa, Farrel and Komolafe (2009) suggest that, as customers connect to the MPLS cloud, ISPs deploy more and more of these unidirectional links (p.16). This presents a scalability factor especially in memory management and node re-convergence after link failure when all the paths using the link have to be re-signaled through an alternative path.

Our paper aims to address these concerns by replicating the most common implementation architecture used by ISPs to confirm the existence of network performance degradation based on LSP re-signaling process. At the same time, this research project will evaluate one of the most viable solutions to alleviate the process of path re-signaling.

2. Literature Review

MPLS forwards traffic based on the labels attached to the IP packets (Osborne, 2002, p.6). The advantage of MPLS is the fact that MPLS labels are used to forward the packets, eliminating the need of IP destination address lookup, speeding up the forwarding process (De Ghein, 2007, p. 5). The operation of MPLS requires unidirectional LSPs to be established (Soricelly et al., 2003, p.480). MPLS LSPs can be signaled using either Resource Reservation Protocol (RSVP) or Label Distribution Protocol (LDP). RSVP reserves capacity between two end hosts by establishing unidirectional flows across the ISP backbone (Soricelly et al., 2003, p.488). LDP is used for the creation, exchange and
advertisement of labels across the MPLS network by establishing TCP sessions between the peer devices (De Ghein, 2007, p. 67). However, both signaling methods have different features. RSVP provides traffic engineering capabilities by establishing the LSPs using traffic engineering attributes rather than using the IGP shortest path alone (Soricelly, 2004, p 499). This feature of RSVP permits ISPs to manipulate traffic on their own will. LDP is more scalable than RSVP because LSPs are signaled on a per hop basis rather than on an end-to-end basis like in RSVP (Soricelly, 2004, p 500). Moreover, LDP is simpler to operate since it does not require a full mesh of LSPs to be configured manually between routers (Alcatel Lucent, 2009, p.185). One limitation of LDP is that it does not provide traffic engineering and traffic protection features like RSVP (Alcatel Lucent, 2009, p. 184).

Today, most of the ISPs implement end-to-end traffic engineered RSVP tunnels in their core networks in order to provide differentiated services on a per customer basis (Adami et al., 2005, p.1). In an ISP’s backbone network, outages even for a small period of time are detrimental for customers who are using the mission critical traffic (Apostolopoulos, 2007, p.1). With more services being offered by ISPs, along with the increasing number of customers moving to a MPLS based services for remote connectivity, this implementation places significant amount of information on the core router’s database as they have to maintain the state of a large number of LSPs (G. Mundle., R. Moreno, interview, September 23, 2010). According to Yasukawa, Farrel and Komolafe (2009), the number of LSPs in the backbone network should be reduced for several reasons, the most important being, the increase in time taken by routers to re-signal those LSPs in case of a link or node failure. In the current MPLS implementation, this process of re-signaling causes a significant amount of packet loss. The number of LSP states maintained by the core routers is calculated by the formula N*(N-1) where N is the number of edge boxes connected to the core routers, hence, every router added increases the number of LSP states to be maintained by the CORE router by 2(N-1) where N is the Nth edge router added (Yasukawa, et al., 2009, p.16). To the best of our knowledge, network operators and ISPs are looking for solutions which are more viable to mitigate this problem.

There are existing implementations that alleviate packet loss and decrease convergence time in an ISP MPLS backbone network. They are Border Gateway Protocol Label-Unicast (BGP-LU) and LDP over RSVP tunneling. BGP-LU alleviates restoration capabilities on an ISP network by dividing it into multiple IGP regions, preventing them from exchanging signaling and routing information. That way, the core routers will only have to maintain LSP states with neighboring routers reducing the MPLS overhead (Juniper, 2010, p. 3). However, the ISPs are moving away from this solution because they do not prefer implementing BGP protocol on their core routers which is required by BGP-LU for label exchange (J. Wacaser, interview, October 4, 2010). Another existing solution is the implementation of LDP over RSVP tunneling. Here end-to-end LDP LSPs are used to connect the edge boxes and then a common single RSVP LSP in the core is used to carry the LDP LSPs. This feature is very beneficial for deployment of large scale MPLS based networks because it would not require full mesh of RSVP LSPs between PE routers (Alcatel Lucent, 2009, p.194). Apostolopoulous (2007) emphasizes that LDP over RSVP combines simplicity and scalability benefits of LDP with RSVP’s traffic engineering and traffic protection capabilities (p.1). LDP over RSVP is easier to deploy when compared to BGP-LU and can co-exist with current end-to-end RSVP implementation. It is supported by most vendors including Cisco, Juniper and Alcatel Lucent (J. Wacaser, interview, October 4, 2010). LDP over RSVP tunneling is preferred in large networks which have over 100 edge boxes where simply using end-to-end RSVP tunnels will have inferior performance (Alcatel Lucent, 2009, p.194).

The review of the related literature shows that there is critical concern for network performance degradation for ISPs who are implementing end-to-end traffic engineered RSVP MPLS network as they seek to provide more services and increase their number of customers. There are a few existing solutions out of which LDP over RSVP tunneling is the most promising in reducing the re-signaling
process required during link failure. In this research, a basic ISP MPLS backbone will be replicated using real equipment and setup and then this research will confirm how LDP over RSVP tunneling can alleviate packet loss during link failure. Moreover this research will provide correlation between the increasing number of LSPs and respective packet loss for end-to-end RSVP tunnels and LDP over RSVP tunnels. This analysis will be beneficial for ISPs and network designers who want to improve performance on their MPLS network.

3. Research Problem

3.1 The statement of the problem and sub-problems

In an ISP MPLS backbone network implemented using end-to-end RSVP tunnels, the increasing number of LSPs that need to be re-signaled in the core routers during link failure is causing significant packet drops. Our research aims to determine how, during link failure between two core routers, LDP over RSVP tunneling improves link convergence in terms of packet drops than end-to-end RSVP tunnels.

**Sub-problem 1:** To model the ISP's MPLS backbone network using end-to-end RSVP tunnels and determine the number of packets dropped during link restoration between two core routers as the number of LSPs increase gradually.

**Sub-problem 2:** To model the ISP's MPLS backbone network using LDP over RSVP tunneling and determine the number of packets dropped during link restoration between two core routers as the number of LSPs increase gradually.

**Sub-problem 3:** To correlate the increasing number of LSPs and respective packet drops for end-to-end RSVP tunnels (existing implementation) and LDP over RSVP tunneling (solution).

**Sub-problem 4:** To confirm that LDP over RSVP architecture alleviates the packet loss.

3.2 Hypothesis

LDP over RSVP tunneling method will provide a better performance in alleviating the problem of packet drops during link failure between two core routers than end-to-end RSVP tunnels while providing the same end-to-end services. This hypothesis is supported by the fact that the number of LSPs maintained by the core devices in case of LDP over RSVP tunneling is significantly reduced in the core routers which only have to maintain the state of the LSPs signaled between directly connected core routers (G. Mundle., R. Moreno, interview, September 23, 2010). In the case of end-to-end RSVP tunnels the core routers have to maintain a full mesh of LSPs throughout the entire topology of the MPLS network (De Ghein, 2007, p 281).

3.3 Delimitations

a) The scope of this research is limited to study the performance of both end-to-end RSVP and LDP over RSVP implementations during link failure only between core routers.

b) In event of a link failure facility backup (link-protection) method is used that uses a single backup LSP sufficient to protect multiple LSPs. One-to-one link-protection (described in RFC 4090) method has not been used as it creates one backup LSP per LSP (Pan, et al., 2005, p.7).
3.4 Assumptions

This research replicates a portion of an ISP backbone network in a lab environment by incorporating comparable hardware and transport technologies used by ISPs on a day-to-day basis. The figure A below represents the minimum lab setup needed in order to test the re-convergence after link failure.

a) These experiments are implemented using industry grade equipment. These devices are a combination of Juniper MX960, MX480, T640 and M320 for Provider Edge (PE) and Core (P) devices that are commonly used in ISP’s production networks. The IGP used was ISIS and all devices were connected with a flat hierarchy that is ISIS-Level 2. The IGP metrics were manipulated for the test traffic to flow through the Device Under Test (DUT).

b) Spirent Test Center, which is a carrier grade tool used by ISPs for performance testing purposes, is used to simulate customer traffic. Each LSP carries uniform size packets to prevent the packet size from being a variable affecting the experiments.

c) Any person who can replicate this testing environment with commercial off the shelf devices configured with vendor standards and comparable hardware will be able to get similar results.

4. Methodology

4.1 Network Diagram

The below network diagram shown in Figure B is the basic building unit of the ISP’s MPLS backbone network consisting of Provider Edge (PE) and CORE (P) devices. This network was used for our experiments with end-to-end RSVP and LDP over RSVP tunneling implementation. PE routers are devices that serve as an aggregation point and interface between the customer routers and the ISP’s network. Generally, they have lower capacity and processing speed than P routers. PE routers push
MPLS labels when the IP packets enter the MPLS domain and also remove labels when the packets exit the MPLS domain. P routers are high capacity and high speed transit devices that perform label switching for forwarding MPLS traffic. Core Router B referenced as Device Under Test (DUT) in the diagram was used in the experiments for evaluating the re-convergence performance.

**Figure B. Network Diagram**

![Network Diagram](image)

**4.2 Experiment I: end-to-end RSVP implementation**

For end-to-end RSVP implementation multiple RSVP LSPs were established between Router A and Router D. Figure 1 below shows the flow of multiple RSVP LSPs before the link failure event. Each individual LSP is completely independent from each other and requires a unique RSVP label. The intermediate routers perform the forwarding process based on these labels. The link between core Routers B and C actually carries all the individual RSVP LSPs. We are forcing all the individual LSPs to follow the path from Router A – Router B – Router C – Router D.

In the case of link failure between core Routers B and C, ISPs have to maintain end-to-end connectivity. This can be obtained by using link protection mechanism. One way is using one-to-one backup method (described in RFC 4090) where each LSP is protected by one backup LSP (Pan, et al. 2005, p.7). However, this doubles the number of LSP states on core routers and is not recommended (J. Wacaser, interview, October 4, 2010). In this experiment, we implemented link protection using Facility backup method (described in RFC 4090). In Facility backup, multiple LSPs going through a common link are protected using a single backup LSP (Pan, et al., 2005, p.7). As shown in Figure 2 below, in the event of link failure between core Routers B and C, the LSPs are redirected to a new path (Router A – Router B – Router E – Router F – Router D). When the link fails, the backup LSP protecting the individual RSVP LSPs immediately takes control and diverts the entire traffic through the new path. At the same time the Point of Local Repair (PLR) Router B informs Router A that the old
path (Router A – Router B – Router C – Router D) is no longer available, requiring Router A to re-signal all the individual RSVP LSPs through the new path. Router A needs to re-signal all RSVP LSPs as each one of them can have different characteristics for providing differentiated services to customers. This re-signaling involves Router A sending RSVP messages simultaneously to establish the path for all RSVP LSPs. Packet drops are observed in each LSP during re-signaling process due to the delay involved in establishing path for each individual RSVP LSP.

For the purpose of this research, the experiment focuses on packet drops due to re-signaling. First 1000 RSVP LSPs were established from Router A to D and equivalent traffic was passed through each LSP using Spirent. Then the link between core Routers B and C was manually disabled as shown in Fig. 2 and packet drops due to re-signaling in each LSP were recorded. The above procedure was repeated as the number of LSPs was incrementally expanded; and respective packet drops were documented. While running the experiments enough time was provided to the network and protocols to detect and restore it services.
4.3 Experiment II: LDP over RSVP tunnel implementation

As mentioned earlier, LDP over RSVP tunneling is changing the way labels are managed by core routers by breaking a single uniform domain into multiple regions. This implementation has two different variations.

a) RSVP full mesh LSPs in the P region and LSPs established by LDP in both the PE regions.

b) Another variation is LDP enabled on all routers with RSVP full mesh LSPs in P region between P routers and RSVP full mesh LSPs in both PE regions between PE and P routers.

With the first variation, LSPs established by LDP alone in PE regions do not support Traffic Engineering (TE) and Traffic Protection (TP) (Soricelli, 2004, p. 499). For end-to-end service provisioning, TE and TP are two key features that ISPs require. Hence the second variation is the most viable for ISP’s network as it will provide TE and TP capabilities in all regions, and will be used in these experiments.

As shown in Figure 3 below, RSVP LSPs are established between PE and P routers on a per customer basis in PE Regions 1 and 3. However, a single RSVP LSP is established between P Routers B and C in P Region 2. The intention of this solution is to transport more than one customer LSP from PE Region 1 using a single label in P Region 2. Figure 3 below shows how multiple LDP labels are aggregated below a common RSVP label for the single inter-core LSP established between the P Routers B and C. This effectively reduces the number of LSP states that the P Router B has to maintain. Also, the RSVP LSPs are segregated back on a per customer basis in PE Region 3. The end-to-end connectivity is attained by enabling LDP on all routers.

In terms of restoration, during link failure between P routers B and C, single inter-core LSP is protected by a single backup LSP. As shown in Figure 4 below, the point of local repair Router B in this case re-signals a single RSVP LSP through the new path (Router B – Router E – Router F – Router C) alleviating the re-signaling on a per customer basis. RSVP LSPs in PE Region 1 and 3 are not affected by the link failure in the P Region 2 as they are not part of the restoration process. The advantage of using this design is that multiple RSVP LSPs in PE region are tunneled inside a single RSVP LSP in the P region providing end-to-end connectivity with traffic engineering and traffic protection capabilities in all regions.

For this experiment, we followed the exact same procedure as in step 4.2 Experiment I except we established a single RSVP LSP in the P region 2 and multiple RSVP LSPs in PE Regions 1 and 3.
5. Results

5.1 Graph for End-to-end RSVP tunnel implementation.

For end-to-end RSVP implementation, the data showed a wide spread range of packet drops during link failure. Therefore we represented the data for two cases: The best case and the worst case scenario for each data set. In Figure 5 below, the lower curve represents our best case scenario which is based on the minimum amount of packets dropped. The upper curve represents our worst case scenario which is based on the maximum amount of packets dropped. We plotted the following curves explaining how, as the number of LSPs increase, the number of packets dropped also increase in both scenarios.
5.2. Graph for LDP over RSVP tunnel implementation.

For LDP over RSVP implementation, the data showed uniform number of packet drops for each of the LSPs during link failure. We plotted the following curve shown in Figure 6 below explaining how, as the number of LSPs increase, the number of packets drops also increased.
5.3. Graph for End-to-end RSVP versus LDP over RSVP.

![Graph](image)

The above curves in figure 7 show that End-to-end RSVP implementation dropped significantly higher number of packets when compared to LDP over RSVP tunneling implementation during link failure.

5.4 Interpretation

Generally, in an ISP MPLS backbone network, the busiest link between core routers carries approximately 4000 active LSPs (J. Wacaser, interview, October 4, 2010). The equations resulting from the curves show in Figure 8 below, predict the number of packet drops when 8000 LSPs have to be maintained by the core routers during link failure. Refer Appendix B for calculations. Table 1 shows the values predicted:

<table>
<thead>
<tr>
<th>Implementation</th>
<th>Accuracy (%)</th>
<th>Number of packets dropped</th>
</tr>
</thead>
<tbody>
<tr>
<td>Best case for end-to-end RSVP</td>
<td>99.87</td>
<td>15,630</td>
</tr>
<tr>
<td>Worst case for end-to-end RSVP</td>
<td>99.91</td>
<td>20,829</td>
</tr>
<tr>
<td>LDP over RSVP</td>
<td>99.97</td>
<td>1,418</td>
</tr>
</tbody>
</table>

In LDP over RSVP tunneling implementation, multiple LSPs are being carried by a single RSVP LSP having the core router to re-signal only one RSVP LSP in the event of link failure reducing the number of packets, thereby improving convergence time. In this scenario, the number LSPs have an effect, but are significantly lesser when compared to end-to-end RSVP implementation.
LDP over RSVP presents an accurate predictability of packet loss since only a single RSVP LSP needs to be re-signaled by the core router. In this implementation, a single RSVP LSP dropped the same number of packets during link failure every time it had to be re-signaled. This is different for end-to-end RSVP where the number of packets dropped by each LSP during link failure, is variable, therefore very difficult to predict.

5.5 Caveat

End-to-end RSVP provides greater granularity in core region for differentiated services to customers than LDP over RSVP tunneling since ISPs are able to control the packet flows on a per customer basis by manipulating traffic engineering attributes for each individual RSVP LSP. This is different for LDP over RSVP where all edge RSVP LSPs are tunnelled into a single RSVP label in the core, preventing this solution to control packet flows on a per customer basis. However, this issue can be addressed by using more than one RSVP labels in the core to tunnel groups of RSVP LSPs from edge region. This can provide flexibility to group customers and provide differentiated services to customers with the same need. In this approach, still the effective number of LSP states that the core routers have to maintain will be less than in the case of end-to-end RSVP tunnels.
6. Conclusion

We have confirmed that LDP over RSVP tunneling gives a better performance than end-to-end RSVP tunnels in terms of packet loss during link failure between core routers. Besides the loss of granularity in core region for differentiated services on a one-to-one customer basis, we found no technical and operational difficulties for this solution. It is simple to implement, scalable, supported by all vendors and can co-exist with end-to-end RSVP LSPs without any issues. End-to-end RSVP just by design will have detrimental effect on the ISP network, as it faces scalability and performance degradation with ISPs adding more and more customers/services. LDP over RSVP tunneling proves to be an efficient solution for mitigating the packet loss and providing the same end-to-end services that are available with end-to-end RSVP tunnels. ISPs currently using end-to-end RSVP tunnels should consider adopting LDP over RSVP tunneling as it is worth their time and effort to transition to this new design.
7. References


8. APPENDIX:

A. Use of Spirent Test Center to generate traffic and document results

Spirent which is a carrier grade tool that is used by most service providers for performance testing was used for these experiments. Traffic was passed through each LSP at 100 frames per second with each IP packet having a frame size of 128 bytes, IP header of 20 bytes and data payload of 90 bytes. This combination ensured that even with large number of LSPs the traffic never exceeds link capacity during the testing. Frame size of 128 bytes was specifically chosen as it is generally used by ISPs for performance testing (J. Wacaser, interview, October 4, 2010). These packets were chosen to be uniform as we did not want to introduce any other variables for our testing. Command Sequencer in Spirent was used to automate the test procedures so that they are constant for all our experiments. Also, the Results Reporter was used to document all packet drops for each LSP under test.

B: Calculations.

Equations

Here $R^2$ value indicates the reliability of the trend and accuracy of the forecast. Values of $R^2$ close to 1 are highly accurate. The equations are as follows:

1) End-to-end RSVP equations:
   
a) Best Case $\rightarrow$ $y = 0.0003x^2 - 0.955x + 4070$
   $\quad R^2 = 0.9987$
   
b) Worst Case $\rightarrow$ $y = 0.0001x^2 + 0.5507x + 10023$
   $\quad R^2 = 0.9991$

2) LDP over RSVP equation:
   
   Equation $\rightarrow$ $y = 2E-05x^2 + 0.0022x + 120.5$
   $\quad R^2 = 0.9997$

Extrapolation

The number of packet drops obtained by extrapolating the number of LSPs to 8000 in above equations:

1) End-to-end RSVP equations:
   
a) Best Case $\rightarrow$ $y = 0.0003(8,000)^2 - 0.955(8,000) + 4070 = 15,630$
   
b) Worst Case $\rightarrow$ $y = 0.0001(8,000)^2 + 0.5507(8,000) + 10023 = 20,829$

2) LDP over RSVP equation:
   
   $y = 2E-05(8,000)^2 + 0.0022(8,000) + 120.5 = 1,418$
C. Definition of terms


BGP-LU (BGP Label Unicast): Advertises route information between inter-region routers.

Egress LSR: Strip off the label on a packet to further perform an IP lookup.

End-to-End Services: Provide services like data, video and VoIP for customers from one end to another.

FEC (Forward Equivalence Class): All packets that are treated the same manner in an MPLS domain.

Ingress LSR: Inserts a label in a non-labeled IP packet and sends it through the data link.

IGP metric controlled dedicated lines: Metric of Interior gateway protocols are changed to control traffic flows between links.

ISP (Internet Service Provider): A telecommunications company who has the capability of selling internet services.

LDP (Label Distribution Protocol): Protocol in charge of discovering LSRs running LDP; session establishment; maintenance and advertising of label mappings.

LSR (Label Switch Router): A router that participates in the exchange of MPLS labels.

LSP (Label Switch Path): Sequence of LSRs that switch a labeled packet through an MPLS network.

MPLS (Multiprotocol Label Switching): This protocol uses labels attached to IP packets to forward packets.

RSVP (Resource Reservation Protocol): Protocol that reserves resources across a network.

T1: Leased lines which have speed of 1.544 Mbps.

T3: Leased lines which have speed of 44.736 Mbps.