Analysis of MPLS Signaling Protocols and Traffic Dissemination in OSPF and MPLS

Sang-Chul Kim^{O} and Jong-Moon Chung
Department of Computer Science, Kookmin University
sckim7@kookmin.ac.kr
School of Electrical Engineering, Yonsei University
jmc@yonsei.ac.kr

Abstract

This paper analyzes MPLS signaling protocols for traffic engineering, shows the capability of providing traffic engineering in MPLS compared to the conventional routing protocol, and explains the MPLS LSR operations based on the basic LSR functionality of classification, queue, and scheduling. CR-LDP, RSVP and RSVP-TE are summarized and analyzed based on how to set up LSP for TE with help of protocol messages. In addition, the comparisons of CR-LDP, RSVP, and RSVP-TE are conducted based on the aspects of LSP reliability and LSP adaptability. A performance metric such as throughput is adopted in order to measure the capability of MPLS traffic engineering based on computer-based simulation.

1. Introduction

The explosive growth of the Internet over past a few years has made the IP protocol suite the most predominant networking technology. Furthermore, the convergence of voice and data communications over a single network infrastructure is expected to happen over IP-based networks. Traditional IP networks offer little predictability of service, which is unacceptable for applications such as telephony, as well as for emerging and future real-time applications. One of the primary goals of traffic engineering is to enable networks to offer predictable performance.

As recent history tells us, the upper limit of transmittable bandwidth doubles and sometimes quadruples every nine to twelve months. Already transmission of tens of tera bits-per-second over a single optical fiber is possible and matching data transferring topologies as well as improved system reliability are currently needed. Based on the above facts, two major candidates that are in competition to become the dominant future network protocol and network architecture are differential services (DS) and multiprotocol label switching (MPLS) [1]. In the competition of DS and MPLS, MPLS has been emerging as the protocol of the future for the following reasons. Realizing the features provided by MPLS makes it an easy choice. First, it is a true "multiprotocol architecture" utilizing a simple label switching mechanism, which is where its versatility in application exists, e.g., MPLS over ATM, frame relay (FR), etc. Second, through utilizing classification, queue, and scheduling (CQS) traffic-engineering topologies MPLS is capable of providing controllable quality of service (QoS) features [2]. Third, MPLS provides a solution to scalability and enables significant flexibility in routing. Fourth, the connection oriented architecture and QoS reliability features easily enable high quality end-to-end service features that are necessary in applications such as virtual private networks (VPN) [3]. These benefits of MPLS networking are made possible through traffic engineering. Currently, the constraint-based routing label distribution protocol (CR-LDP) and the resource reservation protocol (RSVP) are the signaling algorithms used for traffic engineering. In this paper, we compare the signaling procedures of the CR-LDP and RSVP algorithms and discuss the appropriateness of the applications in MPLS traffic engineering networks. Applying MPLS is truly a protocol architecture matter where the software over the routers/gateways and switches/bridges need to be reconfigured to include label edge router (LER) and label switching router (LSR) functionalities. This means that the existing network architecture can be utilized as MPLS architecture without digging out cables and replacing whole new devices. Although systems that highly depend on hardware functionality will unfortunately have to be replaced to include MPLS architecture. Conventional IP networks reflect

Proceedings of the First Asia International Conference on Modelling & Simulation (AMS'07)
0-7695-2845-7/07 $20.00 © 2007 IEEE

the unpredictable and undifferentiated packet loss and jitter characteristics of traditional best-effort routers. Queuing introduces latency and the potential for packet loss if a queue overflows. In order to provide a solution to this, this research plan investigates the requirements of MPLS networking for predictable differentiated loss, latency, and jitter characteristics to traffic classes of applications. Also, this paper provides the construction methods of restoration to MPLS router for the network facility failures in operating high speed. This paper is organized as follows: Section 2 introduces the operation of MPLS LSR. Sections 3 and 4 explain a detailed explanation of the CR-LDP and RSVP-TE signaling respectively. Section 5 compares MPLS signaling protocols based on LSP reliability and LSP adaptability. Section 6 yields the numerical experiments and results in detail. Finally, Section 7 summarizes our work and concludes this paper.

2. MPLS LSR OPERATION

The LSR that conducts the differential services is required to conduct a three-step procedure to enable traffic engineering. These three basic steps are classification, queue, and scheduling (CQS). As label attached packets arrive at the input ports, the input label is used to identify the forwarding equivalent class (FEC) and the corresponding output label. The output label will replace the input label of the packet. Then, based on the output label and FEC, the packet will be sent to the corresponding output queue where the scheduling multiplexer will decide on the output order, timing, and the output port for the packet to be sent out. The setup of the LSR is done by the signaling protocols (CR-LDP, RSVP-TE). The functional diagram of a LSR is provided in Fig. 1 [4].

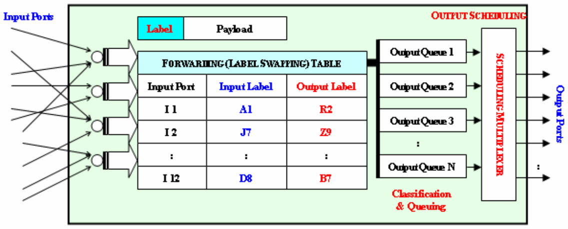


FIG. 1. FUNCTIONAL DIAGRAM OF THE LSR CLASSIFICATION, QUEUE, AND SCHEDULING (CQS) OPERATION.

3. BASIC CR-LDP SIGNALING

CR-LDP standards attempt to enable the LDP protocol to work over an explicit route, transporting various traffic parameters for resource reservation as well as the options for CR-LSP robustness features [5]. Both LDP and CR-LDP are hard state protocols, where signaling messages are transmitted once without any refreshing-information requirements. The transport mechanism for peer discovery is UDP, while TCP is used for session, advertisement, notification, and LDP messages. To setup an explicit route, a LABEL REQUEST message containing a list of nodes along the constraint-based route to be traversed is sent. The signaling message will be sent to the destination following the selected path, and if the requested path is able to satisfy the requirements, labels are allocated and distributed by means of LABEL MAPPING messages starting with the destination and propagating in the reverse direction back to the source. Assuming that resources are available, the LSP setup is completed after a single round-trip of the signaling message. CR-LDP is capable of establishing both strict and loose path setups with setup and holding priority, path preemption, and path re-optimization. The procedure for reporting failures in CR-LDP is based on ingress and egress router's TCP layer transport operations. CR-LDP enables multiprotocol operations by using an opaque FEC, which allows core LSRs to be indifferent with respect to the type of traffic being transported across the network. The opaque FECs are also used for security purposes as well, not enabling the LSRs to know the transport data services identity.

4. BASIC RSVP SIGNALING

Based on RFC 2205 [6], the RSVP signaling protocol standard published by the IETF is intended for soft state resource reservation focusing on enterprise networks to support integrated services [7]. RSVP inherently is a soft state protocol that uses PATH and RESV commands to establish a LSP. In RSVP, based on the destination IP address and protocol ID, packets are transferred based on raw IP datagram routing. The ingress LSR uses a PATH message to inform every router along the selected LSP to acknowledge that this is a desired LSP to be established. Following this, the receiving LSR will use the RESV message with traffic and QoS parameters traversing upstream to reserve the resources on each node along the desired LSP. The node along the LSP will install the reservation for the related state by creating an entry on the label-forwarding table. At every node along the path, the PATH and RESV messages are used periodically to refresh the path and reservation states. Problems in resource reservation can result based on the RSVP soft state mechanism and the merging points along the selected LSP. Overall, there is no guarantee that the resources will be reserved based on the end-to-end request.

RSVP-TE has been made and proposed to support ER-LSP as well as provide additional features to RSVP [8]. Since the RSVP protocol was proposed to support MPLS LSP setups, a considerable amount of modifications and extension have been made to the original protocol to cope up with the traffic engineering requirements. The major modifications and extensions fall into the areas of adding traffic engineering capabilities and resolving scalability problems. The revised RSVP protocol has been proposed to support both strict and loose explicit routed LSPs (ER-LSP). For the loose segment in the ER-LSP, the hop-by-hop routing can be employed to determine where to send the PATH message. Thus, RSVP also supports hop-by-hop downstream-on demand ordered mode.

5. COMPARISON OF SIGNALING PROTOCOL TOPOLOGIES

In this section, the signaling protocols of MPLS traffic engineering are compared. The signaling protocols in comparison are the CR-LDP, original RSVP, and the RSVP-TE. The features of the three signaling protocols are organized in Table 1 [4].

Table 1. A COMPARISON OF CR-LDP, RSVP, AND RSVP-TE

Protocol / Categories	CR-LDP	RSVP	RSVP-TE
Protocol Objective	Created to enable LSP setup for reliable end-to-end differentiated services in MPLS networks.	Established to support soft state resource reservation of integrated services of IP networks.	Proposed with modifications to support differentiated services with RSVP for MPLS networks.
Network Positioning	Designed for carrier backbone networks.	Designed for edge and host services.	Revised design for backbone networks.
Differentiated Services	Supported	Not Supported	Supported
Routing Types	Strict, Loose, Pinned	Strict, Loose, No Pinning	Strict, Loose, Pinning
Scalability	Good	Poor	Marginal
User Security	Low	Low	Low
LSP Features			
LSP State	Hard	Soft	Soft
LSP State Refresh	None	Periodic, All Nodes	Periodic, All Nodes
Resource Request	By sending LER	By Receiving LER	By receiving LER
LSP Setup Action	Forward, Downstream	Backwards, Upstream	Backwards, Upstream
LSP Architecture	Sink Tree	Source Tree	Source Tree
Reliability			
LSP Failure Detection	Reliable	Unreliable	Unreliable
LSP Failure Recovery	Local & Global	Local & Global	Local & Global
LSP Failure Recovery Traffic	Low	High, All Nodes	High, All Nodes
Multiple Connection Support			
Multipoint LSP Merging	Yes	Yes	Yes
Multicasting LSP Setup	No	Yes	No
Adaptability			
Loop Prevention	Yes	Yes	Yes
Path Rerouting	Yes	Yes	Yes
Path Preemption	Yes	Yes, but not reliable.	Yes, but not reliable.

CR-LDP was created to enable LSP setup for reliable end-to-end differentiated services in MPLS networks. Compared to this, RSVP was established to support soft state resource reservation of integrated services over IP networks. RSVP was created before CR-LDP with originally a different intension of where it would be used. Therefore, it is not surprising that RSVP is not suitable for traffic engineering in MPLS networks. The RSVP-TE contains several specifications to support differentiated services with RSVP for MPLS traffic engineering networks, although some of the key components of the architecture are the same. For example, the original protocol base of using the internetworking protocol (IP) is the same, also the hop-by-hop soft state refreshing algorithms are basically the same (although somewhat modified), as well as the reverse upstream LSP setup topology remains the same. Several features of CR-LDP, that were not a part of RSVP, are now possible by the RSVP-TE.

As in terms of scalability, CR-LDP is a hard state protocol, and due to this, it inherently possess better scaling properties in terms of the volume of signaling traffic in the network as the number of CR-LSPs increase. One of the significant drawbacks of RSVP is its scalability when there are a large number of paths passing through a node. This is due to the soft state characteristics of RSVP and RSVP-TE, which require periodical refreshing of the state for each path.

5-1. LSP RELIABILITY

In RSVP and RSVP-TE signaling for traffic engineering, the failure notification process contains several problems. Relying on raw IP creates possible problems that RSVP may not be able to quickly inform the edge routers that the connectivity between them has failed. RSVP-TE does have explicit tear down messages, but due to relying on raw IP transporting they are not sent reliably enough. As a result, the edge LSRs may not start to re-route traffic until the expiration of the timeout interval. Based on the recommendations of RFC 2205 [6], 30 seconds of a refresh interval and 90 seconds of a cleanup timeout interval have been proposed. These values are significantly too large for backbone network operations. If the timing intervals were reduced, the traffic load due to the refresh operations would create more scalability problems.

Additionally, to handle loop detection, RSVP-TE uses the RECORD REROUTE OBJECT, which provides route information of a certain LSP for route diagnostic purpose. In order to solve scalability problems due to the soft state characteristics, RSVP-TE allows aggregation of the refresh messages to reduce the total number of transmissions. To reduce the processing load of these refresh messages on a node, a MESSAGE ID is introduced with the intentions of letting the receiving node quickly identify a state change. However, the use of the ID needs very careful management of the ID numbers and messages by the nodes to avoid many possible errors, such as a mismatch or a duplicate, which imposes other overheads. The RSVP-TE standards also suggest the nodes to completely suppress the refreshes. In RSVP-TE, the LSRs are proposed to use the HELLO protocol to detect the loss of neighboring routers or link states. On the other hand, the soft state design does provide some robustness to the signaling system mechanism. By occasional rechecks, failures in neighboring routers or link states can be detected early.

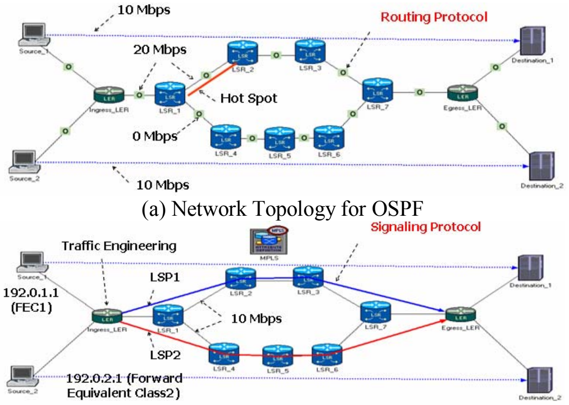
In comparison to this, the TCP end-to-end connection oriented controlling mechanism of the CR-LDP relies on the ingress and egress LSRs to manage the LSP. Based on the fact that the CR-LDP is a hard state protocol, scalability is not an issue to consider. If a link is to fail, the TCP process will detect this and the ingress LSR will determine the procedures to take. In this case, the LSP options of being strict, loose, or pinned will define the options to take.

5-2. LSP ADAPTABILITY

In RSVP, the shared explicit (SE) reservation style is used to set up alternative paths through "make-before-break" procedures. This requires a session to be established before leaving the previously used path. The newly selected LSP will have a different tunnel ID compared to the original one. In RSVP-TE, the protocol does have explicit tear down messages, although if this were to fail under high traffic pressure, the old LSP will be left to timeout (without being refreshed to stay alive) and will eventually be terminated. This possible scenario could result in serious problems for the network. First, the timeout period is much too long for backbone networks to be waiting for path termination, which results in a significant waste of bandwidth. Second, the remaining LSP may cause looping problems or other confusions to the LSRs, which is most undesirable.

For the case of path preemption, RSVP uses setup and holding priorities to determine if a new path can preempt an existing path. Transport mechanism of RSVP, which is on raw IP, may cause problems again for this feature support. Because preemption is often required when the network is running short of resources, the RSVP signaling messages may get lost in this case. Then the path preemption feature would not be executed at all. Compared to this, CR-LDP relies on TCP, which shields the signaling protocol by continuously checking errors as well as the sequence of the data sessions executed. The rerouting capability in RSVP may be used to re-optimize the path, which is executed by all participating nodes exchanging local traffic information to reselect the new path. The standards for RSVP do not have the pinning option included, although the RSVP-TE does contain the pinning option as an additional feature. In CR-LDP, path re-optimization is conducted by the ingress LSR, which is the most proper method to stably control the rerouting. The process is governed by the ingress LSR where end-to-end checking of the sequence of operation commands is protected by the TCP layer mechanism.

6. EXPERIMENT AND OBSERVATION



(a) Network Topology for OSPF

(b) Network Topology for MPLS

FIG.2. NETWORK TOPOLOGIES FOR MPLS AND OSPF.

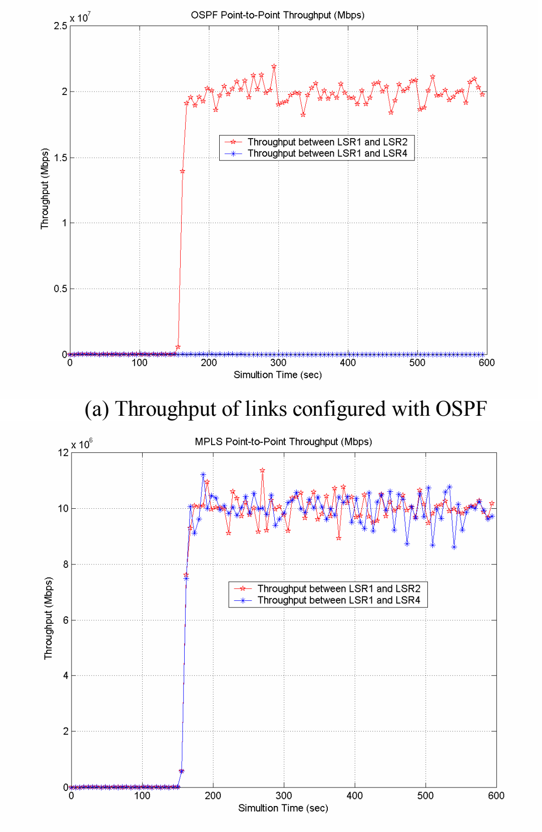
For simple example to show the TE property of MPLS, Open Shortest Path First (OSPF) may be compared with MPLS. OSPF routing protocol can provide traffic load balance when multiple paths have equal costs to the destinations. However, if the multiple paths have different costs to the destinations, OSPF chooses a shortest path first. Therefore, traffic is not evenly distributed to the multiple paths and it may increase network traffic load. MPLS-TE can be used in this case. MPLS uses signaling protocols to disseminate the traffic to multiple paths and to do QoS and DS by installing LSP among the multiple paths. Therefore, the traffic load at each path can be divided based on the LSP's traffic dissemination parameters.

Fig. 2 shows the network topologies that were used to simulate the MPLS TE in OPNET. Figs. 2(a) and (b) contain two sources, two destinations, and two traffics (data flows) where the traffic requires 10 Mbps (bits/sec) from a source to a destination. Between a source and a destination, Figs. 2(a) and (b) include several LSRs where LSRs in Fig. 2(a) have been composed of OSPF and LSRs in Fig. 2(b) have been composed of with MPLS signaling protocols such as CR-LDP and RSVP-TE. In order to perform the traffic engineering, the topology has been constructed as follows. Ingress LER has two input traffics from two sources and one output traffic to

LER1. One data flow follows a route (let's say *route A*) from LER1 LSR2, LSR3 to LSR7. The other data flow follows a route (let's say *route B*) from LSR1, LSR4, LSR5, LSR6, to LSR7. It is assumed that there is no other background traffic in LSRs. Since all LSRs in Fig. 2(a) are configured with OSPF, the data flow of 20 Mbps from Ingress_LER follows the *route A* since the *route A* provides the shortest path compared the *route B* following LSR1, LSR4, LSR5, LSR6, and LSR7. However, all LSRs in Fig. 2(b) are configured with MPLS signaling protocols such as CR-LDP and RSVP-TE, the data flow of 20Mbps is separately divided into two data flows of 10Mbps and *route A* and *route B* service each data flow 10Mbps separately. Two LSPs are setup in the *route A* and the *route B*. Figs 3 (a) and (b) show the graphs of simulation results. In both figures, *x* axis shows the simulation time in second unit and *y* axis shows the throughput between LSR1 and LSR2 and the throughput between LSR1 and LSR4. Based on the results, it can be expected that in the case of OSPF, the link between LSR1 and LSR2 causes the problem of hot-spot; however, the link between LSR1 and LSR4 is idle during the simulation time since it is not used. In the case of MPLS, the link between LSR1 and LSR2 has no more problems of hot-spot and the link between LSR1 and LSR4 is moderately used compared to its throughput.

7. CONCLUSION

This paper explains the MPLS LSR operations based on the basic LSR functionality of classification, queue, and scheduling. In addition, MPLS signaling protocols such as CR-LDP, RSVP and RSVP-TE are summarized and analyzed based on how to set up LSP for TE with help of the protocol messages. CR-LDP is a hard-state protocol and capable of establishing both strict and loose path setups with setup and holding priority, path preemption, and path re-optimization. RSVP inherently is a soft state protocol that uses PATH and RESV commands to establish a LSP. RSVP-TE has been proposed to support ER-LSP as well as provide additional features to RSVP and contains several specifications to support differentiated services with RSVP for MPLS traffic engineering networks. Based on comparison of signaling protocols, it can be found that RSVP has drawback in its scalability when there are a large number of paths passing through a node due to the periodical refreshing of the state for each path. In the simulation, when MPLS signaling protocols were implemented in a MPLS network of TE, the traffic in hot spot can be reduced and the traffic is moderately distributed into several LSPs, which is not able to achieve in the conventional routing protocol.



(a) Throughput of links configured with OSPF

(b) Throughput of links configured with MPLS

FIG.3. THROUGHPUT COMPARISON FOR MPLS AND OSPF.

8. ACKNOWLEDGMENT

This research was supported by the Seoul R&BD program of Korea.

9. REFERENCES

[1] E. Rosen, A. Viswanathan, and R. Callon, "Multiprotocol Label Switching Architecture," RFC 3031, Jan. 2001.

[2] J. L. Marzo, E. Calle, C. Scoglio, and T. Anjali, "QoS on-line routing and MPLS multilevel protection: a survey," *IEEE Commun. Mag.*, vol. 41, pp. 126-132, Oct. 2003.

[3] J.-M. Chung, E. Marroun, H. Sandhu, and S.-C. Kim "VoIP over MPL S Networking Requirements," *Proceedings of IEEE International Conference on Networking 2001 (IEEE ICN'01),* Colmar, France, July 11-13, 2001.

[4] J.-M. Chung, "Analysis of MPLS Traffic Engineering," *Proceedings of the IEEE Midwest Symposium on Circuits and Systems 2000 Conference* (IEEE MWSCAS'00), East Lansing, MI, USA, Aug. 8-11, 2000.

[5] B. Jamoussi *et al*, "Constraint-Based LSP Setup using LDP," IETF RFC 3212, Jan. 2002.

[6] L. Zhang *et al*, "Resource ReSerVation Protocol (RSVP)," IETF RFC 2205, Sep. 1997.

[7] J. Wroclawski, "The Use of RSVP with IETF Integrated Services," IETF RFC 2210, Sep. 1997.

[8] D. Awduche *et al*, "RSVP-TE: Extensions to RSVP for LSP Tunnels," IETF RFC 3209, Dec. 2001.