ITC19/ Performance Challenges for Efficient Next Generation Networks 1787-1796
LIANG X.J. and XIN Z.H.(Editors)
V.B. IVERSEN and KUO G.S.(Editors)
Beijing University of Posts and Telecommunications Press

# Packet Layer Routing Stability Analysis for GMPLS-based IP Backbone Network

Atsushi Tagami, Teruyuki Hasegawa and Toru Hasegawa

KDDI R&D Laboratories
2-1-15 Ohara, Kamifukuoka-shi, Saitama 356-8502, Japan
E-mail: tagami@kddilabs.jp

**Abstract** GMPLS (Generalized Multi-Protocol Label Switching) is a promising technology for constructing and managing next-generation ISP (Internet Service Provider) backbone networks. As optical and packet layer signaling and routing protocols are integrated at the control plane, this vertical integration gives us a common network operation environment that supports quick optical path arrangement corresponding to traffic demand, and provides fast recovery from optical path failures. However, such vertical coordination may cause serious problems on packet layer routing stability due to parameter mismatches and functional similarities between the packet and optical layers. The mismatch is caused by the fact that time granularity of optical path state changes is faster than that of the packet layer routing protocol; i.e., OSPF (Open Shortest Path First). In this paper, we analyzed the packet layer routing instability due to the mismatch based on simulation, and proposed a guard time for concealing the mismatch.
**Keywords** GMPLS, Next Generation Internet, OSPF, RSVP, Routing, Optical Internet

## 1. INTRODUCTION

With the continuous growth of the Internet traffic volume and widespread emergence of new applications with different traffic characteristics, many ISPs (Internet Service Providers) are facing continual problems with accommodating such tremendous IP traffic and optimizing network topology suitable for current traffic trends based on simple integrated network architecture.

GMPLS (Generalized Multi-Protocol Label Switching) is a promising technology for constructing and managing next-generation ISP backbone networks in terms of both high bandwidth adaptability and flexibility on changing logical network topology. Conceptually the data plane in GMPLS-based IP networks is composed of 2 independent layers: PSC (Packet Switching Capable, *packet* for short) and non-PSC (we call it *optical*) [1]. In contrast, these 2 layers closely cooperate with each other at the control plane. This vertically integrated architecture gives us a common network operation environment that supports a quick optical path arrangement between packet layer nodes (i.e. IP routers) corresponding to traffic demand, provides fast recovery from some optical path failure events, and so forth.

However such vertical coordination may cause serious problems with network stability due to parameter mismatches and functional similarities, between the packet and optical layers [2]. For example, some restoration facility at the optical layer may interfere with IP

routing stability at the packet layer. We then indicated a timing mismatch issue between OSPF (Open Shortest Path First), a de-facto intra-domain IP routing protocol, and GMPLS-based optical path management procedures [3].

In GMPLS-based IP backbone networks, the packet layer connectivity (i.e. OSPF link) at the data plane is mainly provided by an optical path logically established through multiple optical layer nodes, e.g. OXCs (Optical Cross Connects) and WDM (Wavelength Division Multiplexing) systems, in addition to conventional physically connected links. These optical paths that are used as OSPF links have different characteristics from conventional paths. First, optical path failures may be recovered using some proprietary function inside the optical layer, though recovery time is inconstant. Second, the IP router may accommodate optical paths passing through both common and disjointed routes in the optical layer, so that the router can receive optical path failure notifications at quite different timings when some common link or node goes down. In contrast, OSPF has a mechanism for suppressing OSPF link state fluctuations, but it does not assume such timing variations on detecting OSPF link state changes as described above. This mismatch may degrade OSPF routing stability.

In order to construct a well-coordinated intra-domain IP backbone based on GMPLS architecture, this paper shows our detailed analysis for this timing mismatch problem under some practical scenarios, and our novel proposal for preserving OSPF routing stability using a simulation approach.

The remainder of this paper is organized as follows. Section 2 describes a GMPLS-based IP backbone structure and timing mismatch problem. Section 3 proposes a guard time for concealing the mismatch to avoid packet layer routing instability. Section 4 describes simulation analysis both on routing instability due to the mismatch and on the effects of guard time. Finally, Section 5 discusses analysis results.

## 2. MULTILAYER INCONSISTENCY ON GMPLS-BASED IP BACKBONE

### 2.1 GMPLS-based Internet Backbone

A GMPLS-based IP backbone physically consists of routers, OXCs, WDM systems and links. It logically consists of the control and data planes [1] as shown in Fig. 1-(1). At the control plane, an IPCC (IP Control Channel) is set up between neighbor nodes such as OXCs and routers. The data plane consists of optical and packet layers as shown in Fig. 1-(2). At the data plane, many links are used to constitute optical paths. An optical path is established between routers by concatenating links at the optical layer. OXCs only switch incoming and outgoing links without packet processing, and routers forward packets on the established optical path.

The most probable scenario for introducing GMPLS is that routing and signaling protocols of the two layers are integrated at the control plane. Routing protocols of the two layers, i.e., OSPF [4] of the packet layer and OSPF-TE (Traffic Engineering Extensions to OSPF) [5] of the optical layer constitute a single OSPF backbone area, i.e., area 0 of OSPF [4]. A signaling protocol of the optical layer, RSVP-TE (Resource ReserVation Protocol-Traffic Engineering) [6,7], also runs at the control plane.

Vertical coordination of the two layers takes place at routers in the following manner. A router directly initiates establishing an optical path to another router using RSVP-TE. We call a router initiating the establishment a *head router*, and the *other router* a tail router.

coordination scenarios depending on whether or not the packet layer is notified of an OSPF link down. Figure 2-(1) and 2-(2) show vertical coordination sequences of optical and packet layers at the head router.

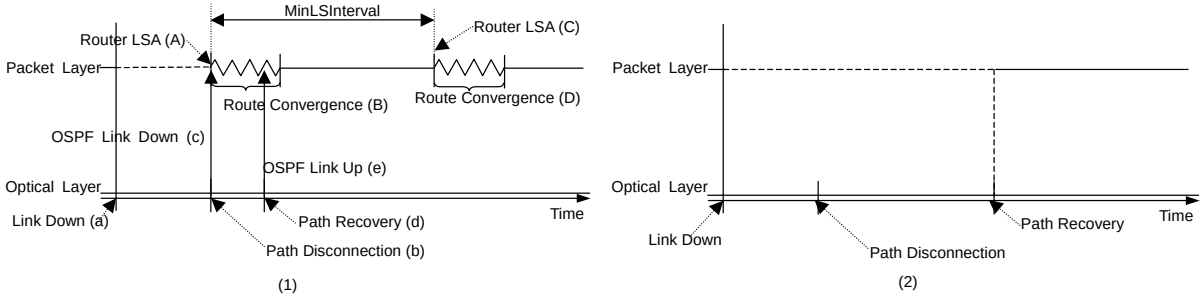


**Figure 2-(1) Time Sequence with Path Disconnection Notification**
**Figure 2-(2) Time Sequence without Path Disconnection Notification**

The first scenario is shown in Fig. 2-(1). After a link becomes down ((a) of Fig. 2-(1)), an OXC sends a PathErr message to the head router. When the head router receives the PathErr message ((b) of Fig. 2-(1)), the packet layer ((c) of Fig. 2-(1)) is notified of the corresponding OSPF link down by the optical layer. Then the optical layer starts disconnecting the optical path by sending a *PathTear* message and then starts re-establishing an optical path by sending a *Path* message. At the same time, at the packet layer, the head router originates and floods a Router LSA that informs the other routers ((A) of Fig. 2-(1)) of the OSPF link down, and routing tables of all routers take some time to converge ((B) of Fig. 2-(1)). Packet layer routing is unstable during the convergence.

Then an optical path is re-established when receiving a Resv message ((d) of Fig. 2-(1)), and the packet layer ((e) of Fig. 2-(1)) is notified of the OSPF link up. However, if MinLSInterval does not elapse, the Router LSA informing the OSPF link up cannot be originated. The problem is that a re-established optical path is not utilized for MinLSInterval even if it is alive. Moreover, after MinLSInterval elapses, the LSA is flooded ((C) of Fig. 2-(1)) which again causes packet layer instability ((D) of Fig. 2-(1)). Namely, the first scenario causes two problems in terms of new optical path utilization and double the packet layer routing instability.

The second scenario is shown in Fig. 2-(2). In the second scenario, the packet layer is not notified of an OSPF link down. Even if the packet layer routing instability does not occur, all packets are lost until the optical path is re-established.

**(2) Simultaneous Path Disconnections**

A similar problem occurs when common links or OXCs whose head or tail routers are the same go down as shown in Fig. 3. In Fig. 3, two links of the data plane, Link1 and Link2, go down simultaneously due to OXC failure. Then the neighbor OXCs send PathErr messages to the same head router, Router 1, at the control plane, and send ResvErr messages to the tail routers. Since the two PathErr messages for Path A and Path B take different routes to Router 1, as shown in Fig. 3, they arrive at Router 1 at different timings.

The arrival time difference may cause a problem at the head router as shown in Fig. 4. After Path A disconnection due to Link 1 down is notified by RSVP-TE ((a) of Fig. 4), the optical layer of Router 1 immediately notifies the packet layer ((b) of Fig. 4) of OSPF link

- **Restoration** reserves a resource for a backup path and calculates the route in advance, but it does not establish a backup path. It establishes a back up path using a signaling mechanism, and then switches a working path to the backup path after the working path failure. The restoration period must be less than 200 milliseconds for the 1st restoration target range that prevents voiceband disconnects according to ANSI [9]. In this paper, we use this value as the restoration period.
- **Re-routing** recalculates a new path after a working path fails without reserving any resource. The re-routing period depends on network sizes. It is reported that the re-routing period is from a few seconds to several minutes [8].

Taking into account the above re-establishment periods, we considered appropriate GuardTime values for the above recovery mechanisms. First, the appropriate GuardTime value is about 200 milliseconds for optical paths of protection and restoration. Second, on the contrary, GuardTime is not required for optical paths of re-routing according to the following reasons. The re-routing period is not predicted because it depends on network sizes, unreserved network resources (unreserved links), conditions of link downs, and so forth. Moreover, the rerouting period is almost the same order as MinLSInterval. In the worst case, rerouting fails due to resource shortage.

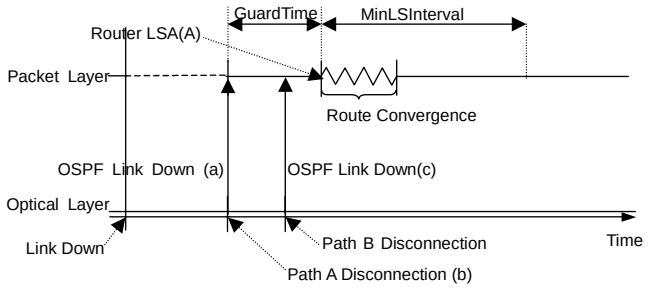


**Figure 5 Time Sequence with GuardTime**

**(2) Simultaneous Optical Path Disconnections**

When multiple optical paths, whose head or tail routers are the same, are simultaneously disconnected as shown in Fig. 3, the router should wait for the last PathErr or ResvErr message. As each PathErr / ResvErr message passes along the same route as that of the optical path at the data plane, PathErr / ResvErr messages normally take different routes. They reach head and tail routers at different times. A period from the first message receipt to the last receipt corresponds to the difference between the shortest and longest routes. Therefore, the GuardTime value should be equal to the difference. However, as the difference depends on where and how link and node failures occur and on a network size, it is not determined in advance. Therefore, in the remainder of this paper, we analyze the period on a network simulation basis.

## 4. SIMULATION ANALYSIS ON PACKET LAYER ROUTING STABILITY

### 4.1 Simulator Implementation

Simulation of OSPF, OSPF-TE and REVP-TE message exchanges is required in order to precisely measure PathErr / ResvErr propagation periods. We have chosen *ns2* (The

simulation starts in the following manner. First, an optical path is set up between any pair of routers. In other words, an optical path is established between Router $i$ and Router $j$ ($\forall i, j \mid i \neq j$). Then, taking into account the diversity of optical path routes, an additional path is established between Router 1 and Router 2. If this additional path were not established, optical paths would be distributed in a uniform way. As a result, 15 optical paths connect every pair of routers in a full mesh manner, and an additional optical path connects Router1 and Router2. Finally, all optical paths are installed in the packet layer as OSPF links.

As an explicit route mechanism is not supported so far by the simulator, every intermediate OXC calculates a next hop using CSPF on hop-by-hop basis. Therefore, the routes of individual paths depend on the order of path establishments.

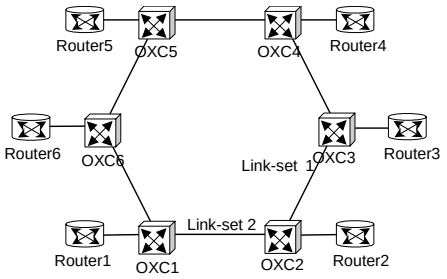


**Figure 6 Simulation Network Topology**

In order to measure PathErr / ResvErr propagation periods, we analyze the control plane behavior when two sets of links, i.e., Link-set 1 and Link-set 2, go down due to OXC2 failure. OXC2 fails at the 10th second in the simulation time.

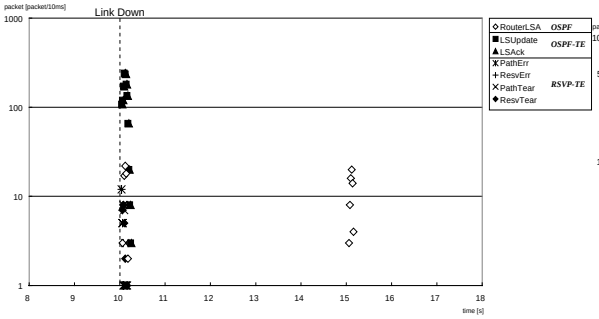


**Figure 7 Numbers of Messages Received by All Routers Every 10 milliseconds**

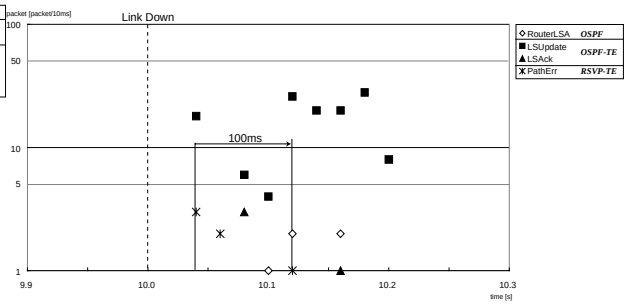


**Figure 8 Numbers of Messages Received by Router1 Every 10 milliseconds**

First, we analyze the total transferred message numbers. Figure 7 shows the numbers of messages which all nodes received every 10 milliseconds. In this figure, the numbers are counted for individual messages. At the 10th second, Link-set 1 and Link-set 2 go down simultaneously. Just after that, many Opaque LSAs of OSPF-TE and Router LSAs of OSPF are transferred. After MinLSInterval (5 seconds) elapses, many Router LSAs are transferred at about the 15th second. This is due to the problem shown in Fig. 4. Some routers whose paths pass OXC2 receive multiple PathErr / ResvErr messages at about the 10th second. At this time only the Router LSAs corresponding to the first PathErr / ResvErr message are originated and flooded. Then at about the 15th second, the LSAs informing the other OSPF

[13]. Neighbor routers detect an OSPF link down within 1 second or 2 seconds by exchanging HELLO messages at an interval of hundreds of milliseconds. However, as the proposed GuardTime is about 300 milliseconds, the optical path disconnection notification with GuardTime provides much faster packet layer recovery than sub-second HELLO.

## 5. **CONCLUSION**

In this paper we showed that packet layer routing on a GMLPS-based IP backbone becomes unstable due to a mismatch between the packet layer MinLSInterval time and the fast optical path state changes. We developed a simulator for the GMPLS-based IP network control plane in order to quantitatively analyze the instability. From the analysis results of a 12-node environment, we obtained the following results. First, we proposed a guard time that prevents the packet layer routing instability by suppressing early optical path notifications from the optical layer to the packet layer. We also showed that an appropriate guard time value is around 300 milliseconds for a medium-sized IP backbone that provides protection and restoration mechanisms. Second, the developed simulator is useful for analyzing the detailed control plane behavior so that PathErr / ResvErr propagation periods are precisely measured. As the propagation periods depend on network topologies, advanced route selection functions of OXCs and so forth, we are measuring the periods on more complicated network topologies and implementing advanced functions to improve the simulator.

## **REFERENCES**


1. “Generalized Multi-Protocol Label Switching Architecture,” RFC3945, October 2004.
2. “Hierarchy & Multilayer Survivability,” RFC3386, November 2002.
3. A. Tagami, T. Hasgegawa and T. Hasegawa, “Multi-Layer Timer Interruption on GMPLS Network,” Proc. of IEICE Society Conference, September 2003 (in Japanese).
4. “OSPF Version 2,” RFC2328, April 1998.
5. “Traffic Engineering (TE) Extensions to OSPF Version 2,”RFC3630, September 2003.
6. “Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions,” RFC3473, January 2003.
7. “RSVP-TE: Extensions to RSVP for LSP Tunnels,” RFC3209, December 2001.
8. “Analysis of Generalized Multi-Protocol Label Switching (GMPLS)-based Recovery Mechanisms (including Protection and Restoration).” draft-ietf-ccamp-gmpls-recovery-analysis-05, April 2005.
9. “Enhanced Network Survivability Performance,” ANSI T1.TR.68-2001, February 2001.
10. “The Network Simulator (ns) 2,” http://www.isi.edu/nsnam/ns/
11. “Link Management Protocol (LMP),” draft-ietf-ccamp-lmp-10.txt, October 2003.
12. “The OSPF Opaque LSA Option,” RFC2370, July 1998.
13. A. Basu and J. Riecke, “Stability Issues in OSPF Routing,” Proc. of SIGCOMM 2001, August 2001.