Area Scoped LSP Restoration for MPLS with Differentiated Resilience QoS

Yuh-Wen Yang and Huei-Wen Ferng

Department of Computer Science and Information Engineering,
National Taiwan University of Science and Technology,
Taipei 106, Taiwan, R.O.C.

E-mail: yuhwen_yang@anet.net.tw; hwfern@mail.ntust.edu.tw

Abstract

The quality of service (QoS) on tunnel resilience of the label switch path (LSP) for the multiple protocol label switching (MPLS) technology has drawn much research attention recently. To address the relevant issue, we propose an architecture/mechanism of the area scoped LSP restoration for MPLS incorporating different classes of resilience QoS in this paper. We first define four QoS classes by a proper modification based on the draft of RSVP-TE fast reroute extension. Then, according to these QoS classes, two different scopes of area for the LSP recovery are designed to achieve each QoS requirement. We show that the proposed MPLS recovery mechanism is more scalable and can reduce latency of the LSP restoration.

Keywords: Quality of service, Resilience, Restoration, MPLS, Area scoping.

I. Introduction

The emerging real-time multimedia applications over Internet protocol (IP) network such as voice over IP (VoIP) and video on demand (VoD) etc. raise the issue of network availability to the Internet service providers (ISPs). To further improve performance and network resource utilization for the IP network, MPLS technology has been proposed. As for MPLS traffic engineering, it focuses not only on the QoS issue for a lasting connection, but also on the resilience requirements when the connection is abruptly broken, e.g., recovery time [1]. Resilience requirements differ from applications. For example, VoIP has a stringent requirement for the recovery time (less than 100ms), while a loose requirement of the recovery time (about a few seconds) is claimed for the web-browsing. To reduce the recovery time, it can be done via suitable design on the recovery scope, trigger event, and resource reservation etc. when defining different resilience requirements [2].

In the literature, resource reservation protocol - traffic engineering (RSVP-TE) and constraint-based (LSP) setup using label distribution protocol (CR-LDP) are two up-to-date MPLS signaling protocols for traffic engineering. However, the LSP recovery schemes defined for these two signaling protocols only support LSP re-setup when link or node failures occur. Moreover, the LSP restoration time intimately depends on the network scope and resource availability. This may results in not guarantee for resilience QoS of a LSP tunnel without area scoping. To greatly reduce the recovery time, one may employ the fast reroute scheme in which the alternative LSP is pre-established. But such scheme wastes much of network bandwidth. For RSVP-TE protocol, the fast reroute extension has been proposed, see [3].

If we want to incorporate area scoping into consideration, then we should determine the scope of recovery area. We first notice that most ISPs’ networks are hierarchical and divided into multiple interior gateway protocol (IGP) areas, or even multiple autonomous systems (ASs). Then, several problems will be encountered for the QoS requirement when the LSPs cross multiple IGP areas. For example, the LSP setup failure caused by the unavailable explicit route calculated by ingress label edge router (LER). Moreover, the lack of complete QoS information of other areas from the area border router (ABR) causes the ingress LER difficult to calculate an available end-to-end explicit route for setting up the LSP. The above discussion suggests that the area within an IGP area between two ABRs is a possible choice of area besides the whole scope of a network and a segment between two nodes. In this paper, such scopes of area are used to achieve QoS requirement.

Different schemes on the resilience-related issue in the literature have been proposed, e.g., [4]—[8]. They are now briefly reviewed as follows. The resilience-differentiated QoS (RD-QoS) is introduced based on different requirements of recovery time in [4], where four types of RD-QoS classified by the LSP recovery time and the associated recovery schemes are roughly defined. It is proven that the total resource usage will be drastically reduced by service-differentiation. However, no detailed description of implementation on LSPs’ resilience QoS has been given there. In [5], the reverse notification tree (RNT) architecture for reducing failure notification messages is proposed. The point to multipoint LSP tree in the opposite direction of the protected LSPs is established accompanying with the setup of the protected LSPs. Once some links or nodes fail, the node detecting the fault will issue a failure notification message on the RNT to enforce all the ingress head-ends of LSPs affected by the link- or node-fault to recover the failed LSPs. In [6], a fast reroute architecture which does not need failure notification is proposed to guarantee zero packet loss during the LSP recovery. But the approach introduces packet disordering during LSP rerouting phase. Then another scheme proposed in [7] solved the disordering problem for the scheme in [6] but it is not scalable. In [8], the IETF draft suggests that the computation of the explicit route of LSP tunnel should be devolved to the intermediate nodes such as the area border node to improve the validness of the explicit route. Hence, three types of scope for LSP restoration, i.e., end-to-end, ABR, and segment rerouting are suggested for traffic engineering.

Therefore, we proposed an LSP restoration architecture/mechanism for MPLS from RSVP-TE, in which the restoration scope is limited to the IGP area and the differentiated resilience QoS are incorporated into this paper.
The rest of the paper is organized as follows. In Section II, we classify resilience QoS. Then we describe the proposed recovery mechanism in Section III. In Section IV, a comparison of our scheme with other schemes previously proposed in the literature is made. Finally, Section V concludes the paper.

## II. QoS Classes of Resilience

Four resilience classes (RC) of LSP QoS have been defined in [4]: RC1, RC2, RC3, and RC4 (See Table 1). In this paper, we refine the resilience QoS definition and propose an MPLS recovery scheme supporting the resilience QoS in the later sections. Shown in Table 1 (the fields in gray are the refined parts) are the aspects of each resilience QoS which is explained in the following.

<table>
<thead>
<tr>
<th>Service Class</th>
<th>RC1</th>
<th>RC2</th>
<th>RC3</th>
<th>RC4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resilience Requirement</td>
<td>High</td>
<td>Medium</td>
<td>Low</td>
<td>None</td>
</tr>
<tr>
<td>Recovery Time</td>
<td>10-100ms</td>
<td>100ms-1s</td>
<td>1s-10s</td>
<td>N.A.</td>
</tr>
<tr>
<td>Recovery Scheme</td>
<td>Fast Reroute</td>
<td>Fast Reroute</td>
<td>Rerouting</td>
<td>Preemption</td>
</tr>
<tr>
<td>Path Setup</td>
<td>Pre-Established</td>
<td>Pre-Established</td>
<td>On-Demand</td>
<td>None</td>
</tr>
<tr>
<td>Recovery Scope</td>
<td>Segment Rerouting</td>
<td>ABR Rerouting</td>
<td>ABR Rerouting</td>
<td>None</td>
</tr>
<tr>
<td>Fault Notification Scheme</td>
<td>Physical Layer Alarm</td>
<td>Path Err/MPLS Ping</td>
<td>Path Err/MPLS Ping</td>
<td>None</td>
</tr>
<tr>
<td>Resource Allocation</td>
<td>Pre-Reserved</td>
<td>Pre-Reserved</td>
<td>On-Demand</td>
<td>Available</td>
</tr>
<tr>
<td>QoS after Recovery</td>
<td>Extra Latency Induce (Under Some Upper Bound)</td>
<td>Equivalent</td>
<td>On-Demand</td>
<td>(if Available)</td>
</tr>
</tbody>
</table>

### A. Resilience Class RC1

This class includes real-time applications such as VoIP, video conferencing, and virtual leased line, which need the highest resilience requirement. It employs the fast reroute recovery scheme with segment rerouting, i.e., rerouting is limited to any two adjacent nodes on the route of the LSP. The operation of switching over from the primary LSP to the backup LSP is triggered by alarms of the physical layer without fault notification. Since the backup LSP may degrade the QoS of other LSPs, the backup LSP will revert to the primary LSP while the link failure on the primary LSP is restored. Note that only the links between adjacent nodes are protected for RC1 class due to the segment recovery scope under the assumption that nodes are more reliable than links. However, once a node is down, the LSP is rerouted by establishing the alternative backup LSP on-demand at the Ingress LER.

### B. Resilience Class RC2

Class RC2 is defined for the critical data service such as virtual private network and symmetric remote data facility etc. Its QoS is guaranteed by high-level service level agreement (SLA). Again, the fast reroute scheme is applied but in the scope between two ABRs. This means that the ABRs are responsible for the establishment of the backup LSP and switching the primary LSP over to the backup LSP while a node or a link fails. For RC2, the fault notification is needed to enforce the ABR to reroute the failed LSP using path error message of control plane or MPLS OAM ping of data plane [9].

### C. Resilience Class RC3

Data applications such as FTP and web browsing etc. fall into the RC3 class. The recovery scope is also between ABRs. Therefore, the alternative backup LSP is established by the upstream ABR while a node/link fault notification (using methods similar to those of RC2) message arrives. It is possible to fail to establish the alternative backup LSP due to the lack of network resource.

### D. Resilience Class RC4

RC4 applications do not need any failure recovery while LSPs fail. And the higher resilience classes LSPs can preempt the resource reserved by RC4 LSP.

## III. Proposed MPLS Recovery Mechanism

Before explaining how the proposed architecture works, we first introduce the LSP restoration scheme in RSVP-TE (Subsection A). Then we roughly describe the fast reroute support for RSVP-TE in the IETF draft [3] (Subsection B). Finally, the detail of the proposed architecture is described (Subsections C and D).

### A. LSP Tunnel Recovery in RSVP-TE

In the RSVP-TE protocol [10], path messages periodically refresh the soft states of the LSP tunnels. If some intermediate node/link fails, its upstream LSR will issue the path error message towards the ingress LER. When the ingress LER receives the path error message, it learns the link/node failure of the LSP and reissues another path message which includes the sender template object (STO) with new LSP identifier to recovery the failed LSP. As shown in Fig. 1, the path A-B-C-E-F is the original LSP tunnel. If the link between LSR B and C fails, the LSR B will issue a path error message to enforce the ingress LER A to recovery the LSP. The LER A calculates the explicit route (A-B-D-E-F) of the alternative LSP by its local traffic engineering base (TE-Base) and issues another path message which contains the new LSP ID in STO. Besides the explicit route object and STO, all the other objects are the same as the original path message. For the paths that are still available in the original LSP, such as A-B and E-F, the same tunnel ID in the session object will refresh the state of the original LSP path. But for the nodes in the alternative path, the new path message will enforce the nodes to establish the alternative path. The LSP failures are on-demand recovered by The RSVP-TE protocol with the end-to-end scope. Hence there exists the scalability
problem which causes long recovery time.

Fig. 1. LSP recovery by inserting the new STO.

B. LSP Recovery in Fast Reroute Extension of RSVP-TE

The IETF draft [3] proposed the fast reroute extension for RSVP-TE to automatically pre-establish the alternative LSP between the intermediate LSRs to protect the primary LSP path of the same head-end. Two fast reroute schemes are proposed: “one-to-one backup” which establishes an alternative detour LSP for each protected LSP and “facility backup” in which one bypass tunnel LSP is established to protect multiple LSPs between the same intermediate LSRs.

Shown in Fig. 2 is the one-to-one backup scenario, two new RSVP-TE objects, fast reroute object (FRO), and detour object are defined for the pre-establishment of the alternative backup LSP. FRO in the path message on the primary LSP specifies which fast recovery scheme is applied and the associated QoS constraints. The intermediate LSRs on the primary LSP determine whether or not to establish the detour LSP with their local TE-Base according to FRO.

The FRO does not identify which intermediate LSR should establishes the alternative LSP which implies that all available LSR will establish the alternative detour LSP using segment scope between any two intermediate LSP peers. However, not all applications need the fast reroute protection of segment rerouting.

C. The New RSVP-TE Objects

By modification of the one-to-one backup scheme mentioned above, we introduce the architecture of LSP tunnel recovery for MLPS to incorporate the resilience classes. As shown in Fig. 3, two new RSVP-TE objects are defined: the modified FRO and resilience differential object (RDO). Using RDO, the resilience class (RC1~RC4) of the associated LSP can be identified. Then each intermediate router determines the protection method of the LSP depending on the RC value. Besides the resilience class, the revertible option of protected LSP is also defined in the RDO. The revertible attribute value determines whether the protected LSP should revert to the primary LSP when the failures are restored.

In the FRO, we add the point of local repair (PLR) and merging point (MP) IP address pairs information to specify the path segment between the PLR and MP to pre-establish the detour LSP for fast reroute recovery at PLR nodes.

D. The Proposed Recovery Architecture

In the proposed recovery architecture, three types of area scoped LSP restoration schemes with differentiated resilience classes are introduced. As shown in Fig. 4, the LSPs of resilience QoS are established from the LSP ingress node to the egress node crossing multiple IGP areas. The ingress node will issue the path message containing the RDO to inform each LSR on the route of the protected LSP resilience requirement (RC1~RC3). The LSRs will protect the LSP appropriately according to the RC value of the RDO. All the LSP restoration is limited to the IGP area. For LSPs of RC1, the detour LSPs between any pairs of the back-to-back intermediate LSRs of the protected LSP are pre-established for fast rerouting when links fail. For LSPs of RC2, the detour LSPs between any pairs of ABRs of the protected LSP are pre-established for fast rerouting when links or nodes between the ABR pairs fail. Finally, for the LSPs of RC3, the upstream ABR before the failed link/node will reroute the failed LSPs on demand. We shall explain the LSP restoration schemes for each resilience class later.
Fig. 4 The area scoped LSP restoration schemes.

When any link fails, the immediate upstream PLR node detects the failure and reroute the traffic to the detour LSP for recovery of the failed LSP. Due to no fault notification, the critical resilience requirement can be achieved with the shortest restoration time.

As the revertible attribute value in RDO of RC1 is always enable, the PLR will revert the detour LSP to the primary LSP when the link failure is restored.

2) MPLS Fast Reroute Scheme for Resilience Class RC2:

ABR scope is used for RC2. The detour LSP is pre-established from one ABR to the immediate downstream ABR. When receiving the LSP path message with RDO of RC2, the ABR inserts the FRO which specifies itself as the PLR node and the immediate downstream ABR as the mapping MP node. And then the PLR ABR establishes the detour LSP along the available route to the MP router by its local TE-Base. The route calculation should consider the path diversity from the protected primary LSP.

Similar to the RC1 fast reroute scheme, the lifetime of the FRO is also within the IGP area. As shown in Fig. 6, the ABR A inserts the FRO of PLR A and MP D into the LSP setup path message. And then the ABR A establishes the detour LSP A-E-F-D by its local TE-Base.

When any link or node fails in the primary LSP, the PLR ABR will detect the failure by receiving the path error message or the expiration of the OAM ping timer and switch the failed LSP over to the detour LSP. When the link/node failure is restored, it is optional for the PLR ABR to revert the detour LSP back to the primary LSP depending on the service policy of the service provider.

3) MPLS Reroute On-demand Scheme for Resilience Class RC3:

Because of the looser resilience requirement of RC3, it is not necessary to pre-establish the backup path for RC3 LSPs. However, the restoration scope is still limited to the area for the higher success probability and the scalability of rerouting of the failed primary LSP. As shown in the Fig. 7, when link C-D in area 0 fails, the ABR A will receive a path error message and re-establish the alternative LSP path from ABR A to the immediate downstream ABR D by its local TE-Base.

When the link/node failure is restored, it is up to the ABR
to revert the alternative LSP back to the primary LSP depending on the service policy of the service provider.

Fig. 7. LSP reroute on-demand with ABR scope.

IV. Comparison

Through a simple comparison with the IETF draft of the fast reroute extension of the RSVP-TE [3] as shown in Table 2, we show that the proposed MPLS LSP restoration architecture has the following advantages:

1) Scalability: Using of the IGP area scoping improves the scalability of the LSP recovery.

2) Flexibility: Differentiated resilience QoS arrangement causes the network resource utilization to be improved. This aspect has been proven in [4]. That is to say, differentiated resilience QoS improves the flexibility of the product line for ISPs.

3) Performance: As the limited length of the alternative LSPs by limiting the scope of restoration, the LSP setup will speed up and the recovery time will be reduced which improve the performance of the LSP.

Table 2. Comparisons of LSP restoration architectures.

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Fast Reroute Extension of RSVP-TE</th>
<th>Proposed MPLS LSP Restoration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scalability</td>
<td>End-to-End Scope</td>
<td>Scope within ABRs</td>
</tr>
<tr>
<td>Flexibility</td>
<td>Simple Resilience Class</td>
<td>Differentiated Resilience QoS</td>
</tr>
<tr>
<td>Performance</td>
<td>Longer Recovery Time</td>
<td>Shorter Recovery Time</td>
</tr>
</tbody>
</table>

V. Conclusion

In this paper, we propose the architecture/mechanism of area scoped MPLS recovery with differentiated resilience QoS classes. First making a modification based on the draft of fast reroute extension of RSVP-TE, four differentiated resilience QoS classes are clearly defined. Furthermore, by limiting the LSP recovery scope to the IGP area, our MPLS recovery mechanism becomes more scalable. Moreover, the LSP recovery time and the resource utilization are improved.

VI. References