Network Working Group
Internet-Draft
Intended status: Informational
Expires: April 21, 2012

M. Zhang
LF. Zhang
YF. Ji
YB. Xu
BUPT
Y. Wang
CATR

October 19, 2011

Network Survivability Evaluation Metrics in Multi-domain Generalized MPLS Networks
draft-zhangm-ccamp-reroute-02

Abstract

The ubiquitous presence of the internet coupled with the increasing demand for high bandwidth dedicated large scale network has made it imperative that the multi-domain networks are facilitated by the development of GMPLS. In such large scale network, the high performance network survivability is a significant factor to resist the fault service discontinue and interruption even to decrease economic loss and the society impact. This document proposes a series of network survivability evaluation metrics and methodologies that can be used to demonstrate the network survivability performance in single and multi-domain GMPLS networks, more specifically, the network fault restoration performance.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on April 21, 2012.

Table of Contents

1. Introduction

1.1. motivation

Generalized Multi-Protocol Lable Switching (GMPLS) network is a promising choice with the use of optical technology in core networks combined with IP/Multi-Protocol Label Switching (MPLS) solution for the next generation Internet architecture. The ubiquitous presence of the internet coupled with the increasing demand for high bandwidth and dedicated large scale network has made it imperative that the multi-domain networks are facilitated by the development of GMPLS.

Survivability is the capability of the network to maintain service continuity in the presence of faults within the network, at the same time, service influenced could be switched over to free resource. All kinds of intra-domain and inter-domain faults occurs in multi-domain GMPLS Networks, therefore, in such large scale network, the high performance network survivability is a significant factor to resist the fault service interruption even to decrease economic loss and the society impact due to faults. Recovery time is a key factor to measure network survivability performance which has an impact on the link and service evaluation. The long recovery time could increase the traffic delay, packet losses, the resource collision, preemption and service discontinue even the whole network can not reach the level of reliability required by traffic service. The time of every recovery phrase is required to be known by a series of measurement methodologies in order to reduce the fault restoration time. Certain method could be adopted to reduce the every phrase time to achieve the aim of reducing the whole recovery time. Therefore, network survivability evaluation metrics is necessary in multi-domain Generalized MPLS Networks.

This document proposes a series of network survivability evaluation metrics and methodologies that can be used to demonstrate the network survivability performance in single and multi-domain GMPLS networks, more specifically, the network fault restoration performance. The time of every fault restoration phase is measured precisely to evaluate the whole network performance by proposed evaluation metrics.

1.2. Terminology

LSP: Lable Switched Path.

LSR: Label Switched Router.

QoS: Quality of Service.

PSL: Path Switch LSR.

ML: Merge LSR.

NMS: Network Management System.

RSVP: Resource Reserve Protocol.

2. Conventions Used in This Document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].In addition, the reader is assumed to be familiar with the terminology used in [RFC3945], [RFC3471], [RFC3473] and referenced as well as in [RFC4427] and [RFC4426].

3. Overview of Network Survivability Evaluation Metrics

There are two recovery mechanisms (eg. protection and restoration) and the former is outside the scope of this document currently. Network survivability evaluation metric is used to measure precise recovery time which is a key factor during the whole fault recovery process (eg. fault detection, fault location, fault notification, fault recovery and reversion). These phases define the sequence of generic operations that need to be performed when a failure occurs. The evaluation metrics take the time of every phrase into account and give the specific measurement steps and methodologies.

4. Network Survivability Evaluation Metrics

High performance of network survivability has become a key issue to improve and satisfy the increasing requirements of reliability and Quality of Service (QoS) of the whole network. This section defines a network survivability evaluation metric in single and multi-domain Generalized MPLS networks.

4.1. Fault Restoration Time Phases

This section gives several typical definitions of restoration times and durations as shown in figure 1.

Phase 1: Fault detection.

Phase 2: Fault localization and isolation.

Phase 3: Fault notification.

Phase 4: Recovery.

Phase 5: Reversion.

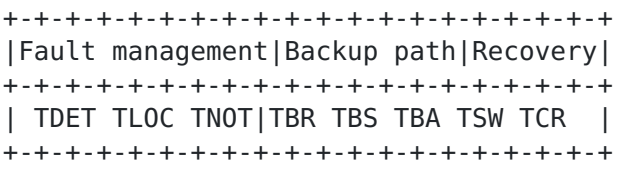

Figure 1: Failure Restoration Time Phases

A detailed analysis and specific definition is provided for each of the restoration phases as identified in [RFC4427] and [RFC4428].

o Fault detection time TDET

Fault detection time is defined as the time between occurrence of fault and detecting the fault and degradation.

TDET depends on several factors pertaining to the link propagation time, link transmission time, node processing time and node queuing time.

o Fault Localization and isolation time TLOC

Fault Localization and isolation time is defined as the time the signal indication information is delivered from fault node to PSL.

o Fault notification time TNOT

Fault notification time is defined as the time to inform the noderesponsible of the switchover that a failure has occurred.

TNOT depends on failure notification delay and the notification method used.

o Backup routing time TBR

Backup routing time is defined as the time for new backup creation, routing (TBR) and signaling (TBS).

TBR depends on the routing method applied.

- Backup signaling time TBS

Backup signaling time is defined as the time that is required to activate the backup path before the switchover.

TBS depends on the signaling method applied.

- Backup activation time TBA

Backup activation time is defined as the time between the settlement of backup path and the switching over the traffic.

TBA depends on the backup path distance and signaling process.

- Switchover time TSW

Switchover time is defined as the time of switching the traffic from the working path through which the traffic is flowing, to the alternative/backup path.

TSW depends on the node technology.

- Restoration completion time TCR

Restoration completion time is defined as the time to complete the fault recovery, i.e. the time it takes the first packet to arrive from the backup path to the ML.

TCR depends on the backup distance.

- The total restoration time

The total restoration time is defined as the sum of TDET, TNOT, TBR, TBS, TBA , TSW and TCR.

4.2. Restoration Schemes and Scenarios

Link restoration could effectively take use of network bandwidth to eliminate faults. The restoration technique is also referred as reroute and fast reroute, for instance, no backup path is established prior to the failure to protect the working path. Therefore, restoration requires dynamic routing algorithms and bandwidth allocation to establish a backup path on demand upon network failure. Once the backup path has been set up, traffic is then switched from the working path.

4.2.1. Fault types

There are three failure types according to the fault level in the optical network, such as service fault, channel failure and fiber failure. We only take channel failure and fiber failure into account.

Service fault : service mistake during the process of the message packaging.

Channel fault: all the services are influenced if a TE link fault occurs in the certain wavelength channel due to transmitter or receiver and so on.

Fiber fault: all the services traversing the link are influenced if a fiber fault occurs due to fiber cut or other external factor and so on.

4.2.2. Faults in single domain

There are two restoration methods in allusion to fault in single domain. Fast reroute mainly provides the local repair function such as span restoration and segment restoration. The start node of span and segment restoration is responsible for backup path computation and traffic switching as the PSL(Path Switch LSR) instead of the source node in reroute scheme.

o Reroute

In the scenario of single domain, detecting entities in transport plane detect related fault information when node or link failure occurs. Failure localization/isolation is triggered immediately after the failure detection. And then the fault indication signaling is sent to the source node through the GMPLS-based signaling or flooding method by the detecting node. In the case of flooding method, intermediate nodes pertaining to the fault end-to-end LSP are informed the fault indication signaling between the upstream node and source node through a notification mechanism. In the signaling-based technique, detecting node sends fault indication signaling such as RSVP-TE to each LSP affected by the failure through different notification mechanism.

After receiving the fault indication signaling, the source node computes a backup path by a series of routing algorithms or route pre-computation scheme and then allocates the bandwidth. Path and RESV signaling are responsible for path establishment and resource reservation respectively for the new backup path. After that, the traffic is switched to the backup path from the working path.

o Fast reroute

In the scheme of fast reroute, failure localization/isolation is triggered immediately after the failure detection. And then the fault indication signaling is sent to the span or segment PSL from the upstream node of failure link through the GMPLS-based signaling or flooding method. These two notification methods are described in reroute part of section 4.2.1. On receiving the fault indication signaling, PSL is computes a new path by a series of routing algorithms and allocates the bandwidth to the backup path bypass the fault LSP. After that, the traffic is switched to the backup path from the working path.

4.2.3. Faults in multi-domain

There are three types of faults in multi-domain network, such as link or node failure within the domain, failure of a link at a domain border and failure of domain border node. Inter-domain and Intra-domain restoration mechanisms are independent with each other.

4.2.3.1. Faults within a domain

When an intra-domain failure occurs, intra-domain restoration mechanism is set up first within a domain and the restoration scheme is similar to that of single domain in the scenario of multi-domain. Inter-domain restoration mechanism would be triggered only if the previous restoration mechanism fails.

o Reroute

Detecting entities in transport plane detect related fault information when node or link failure occurs within a domain. Failure localization/isolation is triggered immediately after the failure detection. And then the fault indication signaling is sent to the source node across intermediate domains through the GMPLS-based signaling or flooding method. After receiving the fault indication signaling, the source node computes a new path by a series of routing algorithms and allocates the bandwidth. Path and RESV signaling are responsible for path establishment and resource reservation respectively for the backup path. After that, the traffic is switched to the backup path from the working path.

o Fast reroute

In the same scenario above, detecting entities in transport plane detect related fault information when node or link failure occurs within a domain. Failure localization/isolation is triggered immediately after the failure detection. And then the fault

indication signaling is sent to the local or segment PSL from the upstream node of failure link through the GMPLS-based signaling or flooding method. These two notification methods are described in section 4.2.1.1. After receiving the fault indication signaling, Path Switch LSR (PSL) is responsible for computing a new path by a series of routing algorithms and allocates the bandwidth to establish the backup path bypass the fault LSP. After that, the traffic is switched to the backup path from the working path.

4.2.3.2. Inter-domain faults

Inter-domain faults comprise inter-domain link fault and border node fault of the domain. Each domain has its own domain border node, and these two border nodes are connected by a TE link. TE link is invalid once the border node fails.

When the LSP traverses multiple domains and inter-domain failure occurs, the process of failure detection and localization/isolation is the same to that of single domain whose detail is described in section 4.2.1. If the fault TE link is the only one between two domains, the restoration mechanism adopts the end-to-end reroute restoration scheme. The fault indication signal is sent to source node by the upstream node along the LSP, and then the source node computes another path and allocates the resource avoiding the domain relative to the fault node and link. Otherwise, the restoration mechanism could adopt either the reroute or the fast reroute scheme if there is more than one link between two domains. Path and RESV signaling are responsible for path establishment and resource reservation respectively between PSL and ML. After that, the traffic is switched to the backup path from the working path.

5. Methodologies

It is difficult to measure Detection time TDEF which depends on the monitoring technique and reversion is a normalization process. Therefore, the methodology of detection and reversion time are outside the scope of this document.

5.1. Fault restoration in single domain network

This section gives two measurement methods of fault restoration which are end-to-end reroute and fast reroute respectively in single domain network. It is assumed that there exits an LSP (1-2-3-4) where data flow is from node 1 to node 4 as an example shown in figure 2 and 3. The link fault occurs between node 2 and node 3.

5.1.1. Reroute

Generally, when the failure occurs the methodology would proceed as follows:

- The node 3 sends Channelstatus Message to node 2 indicating the failure to the corresponding the upstream node.

- Record the timestamp (T1) when the first bit of Channelstatus Message is sent to the node 2 along the LSP.

- When node 2 receives the ChannelStatus message from node 3, it returns a ChannelStatusAck message back to node 3 and correlates the failure locally. When Node 2 correlates the failure and verifies that the failure is clear, it has localized the failure to the data link between node 3 and node 2. At that time, node 2 sends a ChannelStatus message to node 3 indicating that the failure has been localized.

- Then record the timestamp (T2) when the last bit of ChannelStatus message from node 2 is received by node 3.

- The fault localization delay is T2-T1.

- The node 2 sends the notification information to the source node(node 1) of the LSP traversing intermediate nodes. Then record the timestamp (T3) when the first bit of PathErr information is sent out.

- Record the timestamp (T4) when the node 1 receives the last bit of the PathErr Message.

- Notification delay is T4-T3.

- Record the timestamp (T5) after node receives the notification information. Node 1 as the PSL computes a new path through either a series of route algorithms or pre-computed schemes.

- PATH and RESV signaling are responsible for path establishment request and resource reservation respectively for a new backup path. Then the traffic is switched from a working path to the backup path. Record the timestamp (T6) when the first packet of traffic arrives at the ML(node 4) through the backup path.

- Recovery time is T6-T5.

- The total fault restoration time is T2+T4+T6-T1-T3-T5.

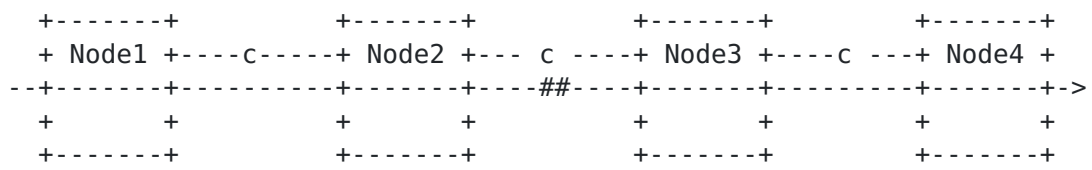

Figure 2: Reroute of fault in single domain (indicated by ## in the figure)

5.1.2. Fast Reroute

Generally, when the failure occurs, the methodology would proceed as follows:

- The process of fault localization is similar to that of reroute restoration in single domain network which is described in section 5.1.1.
- The fault localization delay is also T2-T1.
- PathErr information is sent to different PSL that differs from fast reroute restoration scheme. Node 2 is the PSL as the ingress node of backup path if the span recovery scheme is adopted. Otherwise, consider other PSL as the ingress node of backup path if segment restoration scheme is implemented.
- Then record the timestamp (T3) when the first bit of notification information is sent out by the node 2 to the PSL which is responsible for switching over the traffic.
- Record the timestamp (T4) when the PSL receives the last bit of the notification information.
- Notification delay is T4-T3.
- Record the timestamp (T5) after PSL receives the PathErr Message. The PSL computes a new path through either a series of route algorithms or pre-computed scheme (eg. 1-2-5-3-4).
- PATH and RESV signaling are responsible for path establishment request and resource reservation respectively for the backup path. Then the traffic is switched from a working path to the backup path. Record the timestamp (T6) when the first packet of traffic arrives at the ML(node 3) through the backup path.

- Recovery time is T6-T5.

- The total fault restoration time is T2+T4+T6-T1-T3-T5.

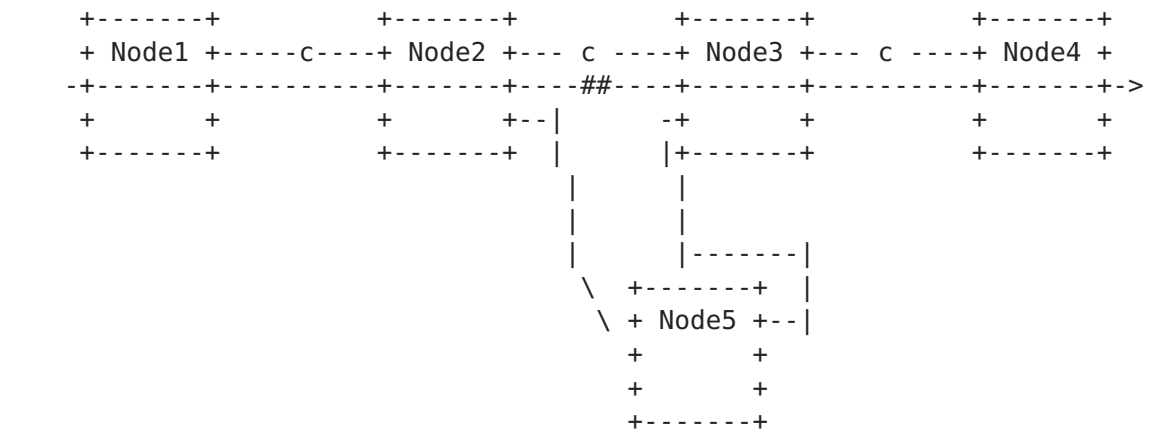

Figure 3: Fast reroute of fault in single domain (indicated by ## in the figure)

5.2. Fault restoration within a domain in multi-domain network

5.2.1. Reroute

Figure 4 describes the node connection situation. As illustrated node 1 and node 4 are in domain A and B respectively and node 2 and 3 are all in domain B. Generally, when the failure occurs, the methodology would proceed as follows:

- The node 3 sends Channelstatus Message to node 2 indicating the failure to the corresponding upstream node.

- Record the timestamp (T1) when the first bit of Channelstatus Message is sent to the node 2 along the LSP.

- When node 2 receives the ChannelStatus message from node 3, it returns a ChannelStatusAck message back to node 3 and correlates the failure locally. When Node 2 correlates the failure and verifies that the failure is clear, it has localized the failure to the data link between Node 3 and node 2. At that time, Node 2 sends a ChannelStatus message to Node 3 indicating that the failure has been localized.

- Then record the timestamp (T2) when the last bit of ChannelStatus message from node 2 is received by node 3.

- The fault localization delay is T2-T1.

- Node 2 sends the notification information to the source node of the LSP(node 1) traversing intra-domain nodes and border nodes. Notification time depends on whether the source and the destination node are in the same domain or not. Then record the timestamp (T3) when the first bit of notification information is sent out.

- Record the timestamp (T4) when the node 1 receives the last bit of the notification information.

- Notification delay is T4-T3.

- Record the timestamp (T5) after node 1 receives the PathErr Message. As the PSL, node 1 finds a new path through either a series of route algorithms or pre-computation scheme.

- PATH and RESV signaling are responsible for path establishment request and resource reservation respectively for a new backup path. Then the traffic is switched from a working path to the backup path. Record the timestamp (T6) when the first packet of traffic arrives at the destination node (node 4) through the backup path.

- Recovery time is T6-T5.

- The total fault restoration time is T2+T4+T6-T1-T3-T5.

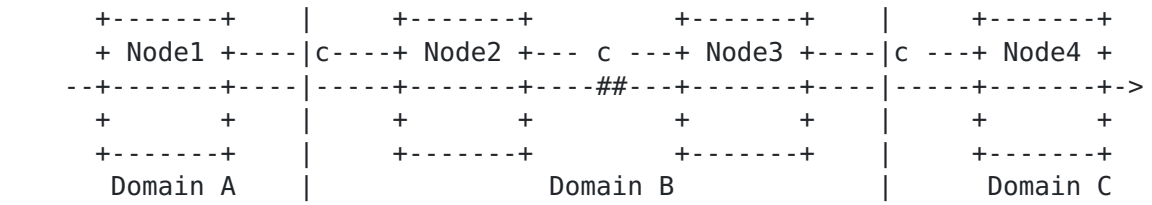

Figure 4: Reroute of fault within a domain in multi-domain network(indicated by ## in the figure)

5.2.2. Fast Reroute

Figure 5 describes the node connection situation that is node 1 and node 4 are in domain A and B respectively and node 2 ,3 and 5 are all in domain B.

Generally, when the failure occurs between node 2 and 3 in domain B, the methodology would proceed as follows:

- The process of fault localization is similar to that of reroute restoration in single domain network which is described in section 5.1.2. The fault localization delay is also T2-T1.

- Notification information is sent to different PSL that differs from fast reroute restoration scheme. Node 2 is the PSL as the ingress node of restoration path if the span recovery scheme is adopted. Otherwise, consider other PSL as the ingress node of restoration path if segment recovery scheme is implemented.

- Then record the timestamp (T3) when the first bit of notification information is sent out by the node 2 to the PSL which is responsible for switching over the traffic.

- Record the timestamp (T4) when the PSL receives the last bit of the PathERR message.

- Notification delay is T4-T3.

- Record the timestamp (T5) after PSL receives the PathErr Message. The PSL finds a new path through either a series of route algorithms or pre-computed schemes.

- PATH and RESV signaling are responsible for path establishment request and resource reservation respectively for a new backup path. Then the traffic is switched from a working path(2-3) to the backup path(2-5-3). Record the timestamp (T6) when the first packet of traffic arrives at the ML(node 3) through the backup path.

- Recovery time is T6-T5.

- The total fault restoration time is T2+T4+T6-T1-T3-T5.

- If the intra-domain fast reroute mechanism fails, reroute restoration is triggered whose methodology is illustrated in section 5.2.1.

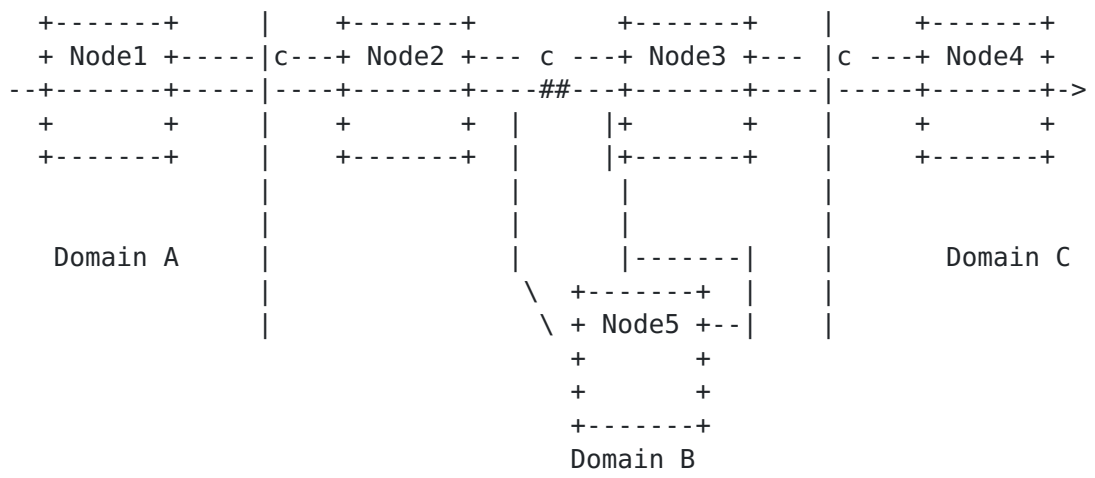

Figure 5: Fast reroute of fault within a domain in multi-domain network(indicated by ## in the figure)

5.3. Inter-domain fault restoration in multi-domain network

Figure 6 describes the node connection situation. As illustrated node 1 and node 4 are in domain A and C respectively and node 2,3 and 5 are all in domain B.

Generally, when the failure between domain A and B occurs, the methodology would proceed as follows:

- The node 4 sends Channelstatus Message to node 3 indicating the failure to the corresponding upstream node.

- Record the timestamp (T1) when the first bit of Channelstatus Message is sent to the node 3 along the LSP.

- When node 3 receives the ChannelStatus message from node 4, it returns a ChannelStatusAck message back to node 4 and correlates the failure locally. When Node 3 correlates the failure and verifies that the failure is clear, it has localized the failure to the data link between Node 3 and node 4. At that time, Node 3 sends a ChannelStatus message to Node 4 indicating that the failure has been localized.

- Record the timestamp (T2) when the last bit of ChannelStatus message from node 3 is received by node 4.

- The fault localization delay is T2-T1.

- Measurement method of notification delay is the same to that of fault reroute restoration within a domain in multi-domain network as described in section 5.2.1.

- Notification delay is T4-T3.

- Record the timestamp (T5) after node 1 receives the PathErr Message. Node 1 as the PSL computes a new path through either a series of route algorithms or pre-computed scheme. Consider to choose a backup path bypass the upstream domain of fault link if the fault link is the only link between domain B and domain C.

- PATH and RESV signaling are responsible for path establishment request and resource reservation respectively for a new backup path. Then the traffic is switched from a working path to the backup path. Record the timestamp (T6) when the first packet of traffic arrives at the destination node (node 4) through the backup path.

- Recovery time is T6-T5.

- The total fault restoration time is T2+T4+T6-T1-T3-T5.

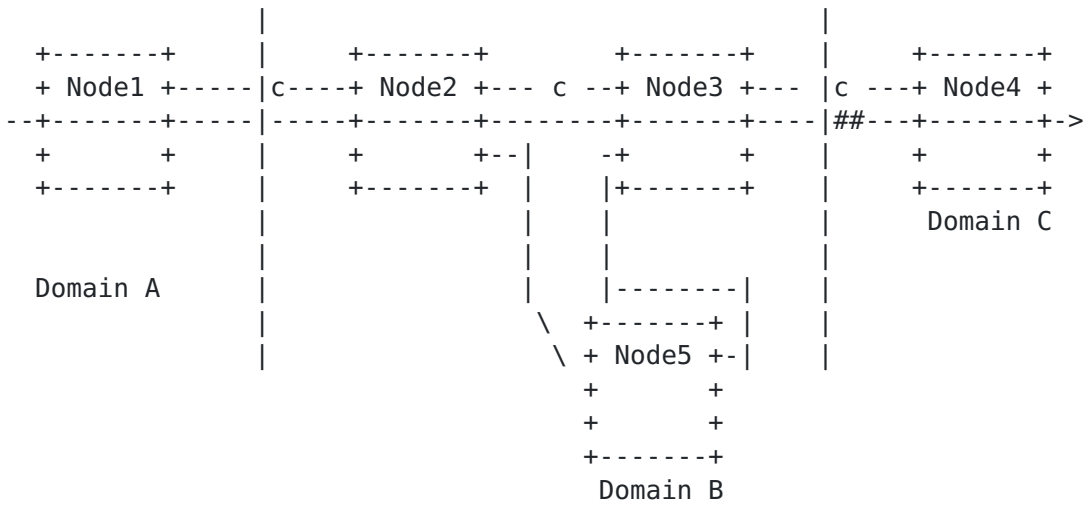

Figure 5: Inter-domain fault in multi-domain network(indicated by ## in the figure)

6. Protocol Extension Requirements

It is assumed that clock of every control node is synchronous during the process of measurement. Control plane reports different time to NMS(Network Management System) which is responsible for computing the sum of different fault restoration duration time. LMP and RSVP extensions are required in order to record precise the start and end time in every restoration phrase.

In the process of fault location measurement, detection entities send alarm information to upstream neighbor node through signaling of LMP when it detects the fault in control plane. It is necessary to extend LMP by adding a FAULT_TIMESTAMP object as a timestamp in the ChannelStatus Message. The FAULT_TIMESTAMP Object could be used to record the time when the signaling is sent and received to measure the precise fault location notification time. Then when the fault notification is implemented, the fault indicating signal is delivered to the PSL through the PathErr signal of RSVP. SEND_ERR_TIMESTAMP and RECEIVE_ERR_TIMESTAMP Objects are added in PathErr signal and defined to record the time of notification signal sent and received by upstream node next to the fault and PSL respectively.

7. Security Considerations

As this document is solely for the purpose of providing metric methodology and describes neither a protocol nor a protocol implementation, there is no security considerations associated with this document.

8. Acknowledgments

We wish to thank Jiuyu Xie, Yongli Zhao and Shengwei Meng for their comments and help.

The RFC text was produced using Marshall Rose's xml2rfc tool.

9. Normative References

[RFC3473] Berger, L., "Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource Reservation Protocol-Traffic Engineering (RSVP-TE) Extensions", RFC 3473, January 2003.

[RFC4090] Pan, P., Swallow, G., and A. Atlas, "Fast Reroute Extensions to RSVP-TE for LSP Tunnels", RFC 4090, May 2005.

[RFC4204] Lang, Jonathan P., "Link Management Protocol (LMP)", RFC 4204, October 2005.

[RFC4426] Lang, Jonathan P., "Generalized Multiprotocol Label Switching (GMPLS)Recovery Functional Specification", RFC 4426, March 2006.

[RFC4427] Mannie, E. and D. Papadimitriou, "Recovery (Protection and Restoration) Terminology for Generalized Multi-Protocol Label Switching (GMPLS)", RFC 4427, March 2006.

[RFC4428] Papadimitriou, D. and E. Mannie, "A Backward-Recursive PCE-Based Computation (BRPC) Procedure to Compute Shortest Constrained Inter-Domain Traffic Engineering Label Switched Paths", RFC 4428, March 2006.

Appendix A. Other Authors

1. Haiyi Zhang

MIIT

No.52 Hua Yuan Bei Lu,Haidian District

Beijing 100083

P.R.China

Phone: +861062300100

Email: Zhanghaiyi@mail.ritt.com.cn

Authors' Addresses

Min Zhang
BUPT
No.10,Xitucheng Road,Haidian District
Beijing 100876
P.R.China

Phone: +8613910621756
Email: mzhang@bupt.edu.cn
URI: http://www.bupt.edu.cn

Lifang Zhang
BUPT
No.10,Xitucheng Road,Haidian District
Beijing 100876
P.R.China

Phone: +8615210889041
Email: capricorn7111@hotmail.com
URI: http://www.bupt.edu.cn/

Yuefeng Ji
BUPT
No.10,Xitucheng Road,Haidian District
Beijing 100876
P.R.China

Phone: +8613701131345
Email: jyf@bupt.edu.cn
URI: http://www.bupt.edu.cn/

Yunbin Xu
BUPT
No.52 Hua Yuan Bei Lu,Haidian District
Beijing 100083
P.R.China

Phone: +8613681485428
Email: xuyunbin@mail.ritt.com.cn
URI: http://www.catr.cn/

Yu Wang
CATR
No.52 Hua Yuan Bei Lu,Haidian District
Beijing 100083
P.R.China

Phone: +8613651161646
Email: wangyu@mail.ritt.com.cn
URI: http://www.catr.cn/