MPSL Traffic Protection

Svetlin Petrov

Abstract: *The paper discusses Multiprotocol Label Switching (MPLS) traffic protection approaches and their advantages and disadvantages.*

Key words: *Multiprotocol Label Switching (MPLS), traffic engineering, QoS*

INTRODUCTION

The main task of the MPLS recovery approaches is controlling the traffic flow in the network and finding the best way for backup path in the event of network failure. The main idea of the different traffic recovery approaches is rerouting the traffic using an alternative paths. Below are discussed some of the existing MPLS recovery approaches which ensure the MPLS traffic protection.

MPLS TRAFFIC PROTECTION

Makam suggested one of the first methods for MPLS recovery [1] and this is the reason this method to be known as Makam's. The main idea of the method is to ensure end-to-end protection of MPLS LSP by establishing a global recovery path connecting the ingress and egress LSR. If a failure occurs a fault information message is send to the path switch LSR which function is to reroute the traffic using the backup path.

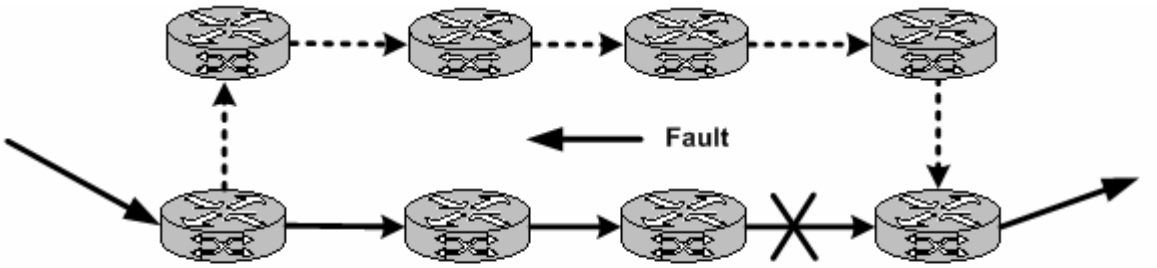

Figure 1: Makam's end-to-end LSP Protection

Figure 1 illustrates the sending of the fault message to the upstream LSRs during the process of the discovery of a failure in the MPLS network.
The Makam's LSP protection can use protection switched and dynamically created recovery path. The protection switched path is the preferred approach and is more frequently used due to the fact that the process of dynamically creation of recovery path is slower.
It is possible several LSPs to be connected using the same connection to LSP because the LSP setup is unidirectional. This approach has several advantages. In the case of network problems the corresponding LSR must be informed which neighbour LSR should receive the fault message. In most of the cases the Makam's LSP protection can handle the network failures but the process of sending the fault message to the upstream LSR can be optimized using the so called Reversed Notification Tree.

When a fault event occurs it can be characterized as global or local. If it is local recovery the recovery operation is performed by the node which detected the failure. The scenario with the global protection is more complicated - the node responsible for the recovery operation must be informed by the node which discovered the failure event. Due to the unidirectional connection used by LSP the failure message must be sent in some way to

the upstream device. It is important to be noticed that if there is setup using merging LSPs then several nodes responsible for the recovery operation must be informed.

The Reverse Notification Tree described in [2] is another mechanism used in the MPLS based LSP protection. Its main idea is the creation of a notification tree in segmented or global protected environment offering one to one protection. The node responsible for the recovery operation is the root of a multipoint tree which is used by the reverse notification tree protection. The reverse notification tree allows merging of the MPLS labels and thus several network paths can be merged in a multipoint to point tree.

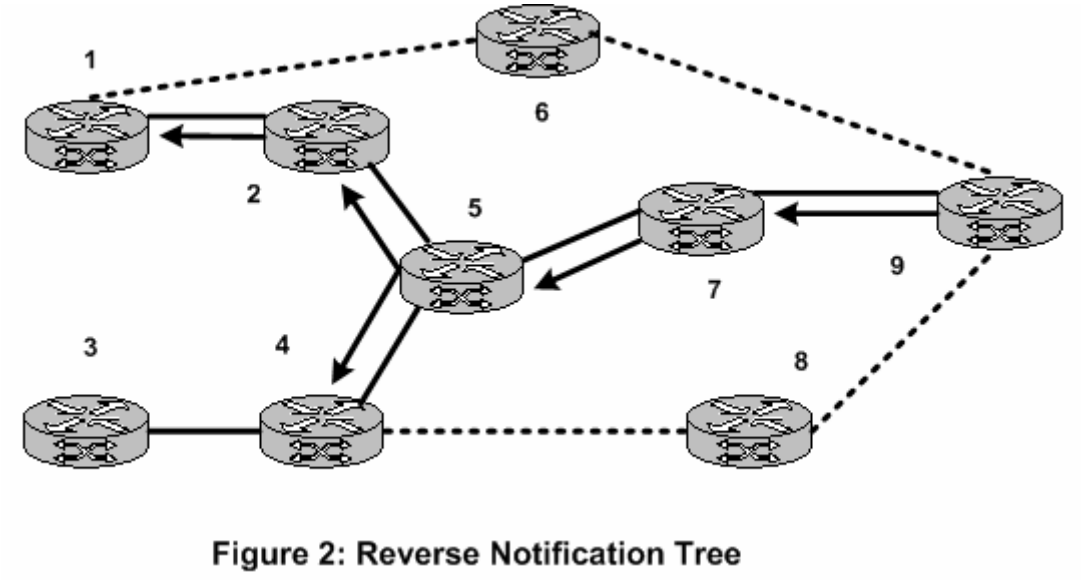

Figure 2: Reverse Notification Tree

Figure 2 shows that the path (5, 7, 9) is a result of the merging of 1, 2, 5, 7, 9 LSP and 3, 4, 5, 7, 9 LSP. One of the recovery paths is 1, 6, 10 and the other recovery path is 4, 8, 9. The node responsible for the recovery operation never mind which recovery path will be used is 9.

The reverse notification tree determines in which way the failure signal will be send upstream in the case of networking problems between path 5 – 9. If LSR 5 is notified with a failure signal by LSR 7 it must send two notification signals to 2 and 4.

Another recovery approach is the reverse backup. Its main idea is to reverse the traffic back to the node which is responsible for the recovery operation. In the case of failure detection by some LSR it starts to redirect the traffic to an operating LSR which is configured in the reverse direction of the working path. The reversed traffic is forwarded to a global protection path when it reaches the node responsible for the recovery operation.
The reverse backup recovery was described by Haskin [3] and due to this is known with the Haskin name.

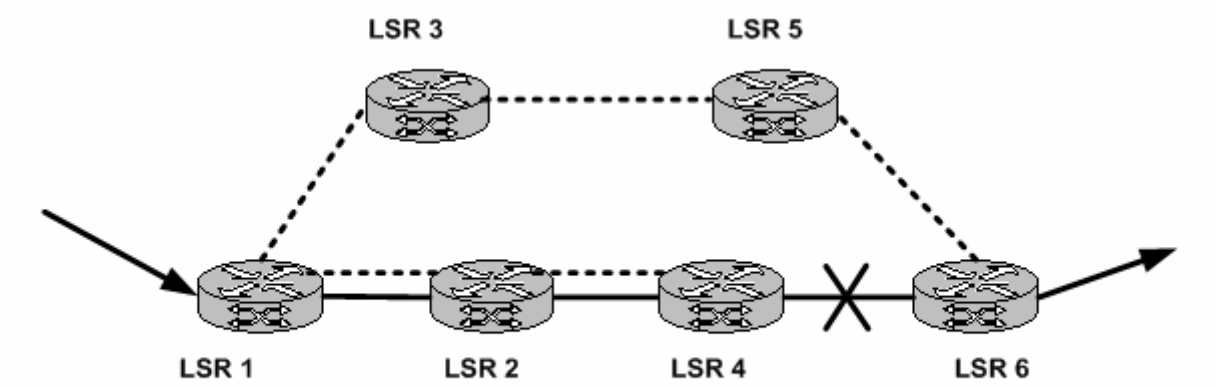

Figure 3: Reverse Backup

Figure 3 shows a scheme of the reverse backup. The global protection is used for the working and recovery paths and in addition a reverse path is established between the ingress LSR 1 and LSR 4. In the case of network failure it is discovered by LSR 4 and it forwards the traffic back to the ingress LSR using the reverse backup LSP and to the global recovery path.

One of the main disadvantages of the Haskin's approach is the inefficient resources usage because of the fact that in most of the cases the length of the recovery path is longer then the original path which is used. On the other hand this approach for MPLS path recovery is the low package loss in the case of network problems. This is due to the fact that no notification message is necessary when the traffic itself from the reverse backup is used as notification message to the node responsible for the recovery operation.

Another recovery approach is suggested by Hundressa [4]. Its main goal is to offer better functionality compared to the reverse backup. In the case of network problems they are detected by a LSR and the packets that would normally be forwarded using the path with the problem are returned to the node responsible for the recovery operation using the dedicated backup route. The difference compared to the fast recovery is that the initial packet which contains the message for the network problems is accepted at the upstream LSR and it tags the next packet it sends to the network and the next received packets which are from the same path are buffered. The buffer keeps the packets until the tagged packet is received using the reversed backup path and forwarded on the reverse backup path. After the last packet which was sent by the node responsible for the recovery operation using the failed path is received from the reversed path then all of the packets are send to the global recovery path. The advantage of this approach is that it is not necessary the packets to be reordered and the forwarding operations using the network path with the problem are reduced.

Another approach for MPLS recovery is the fast reroute one-to-one. The mail idea is the usage of so called detour LSP which is a backup LSP for every LSR in the protected path.

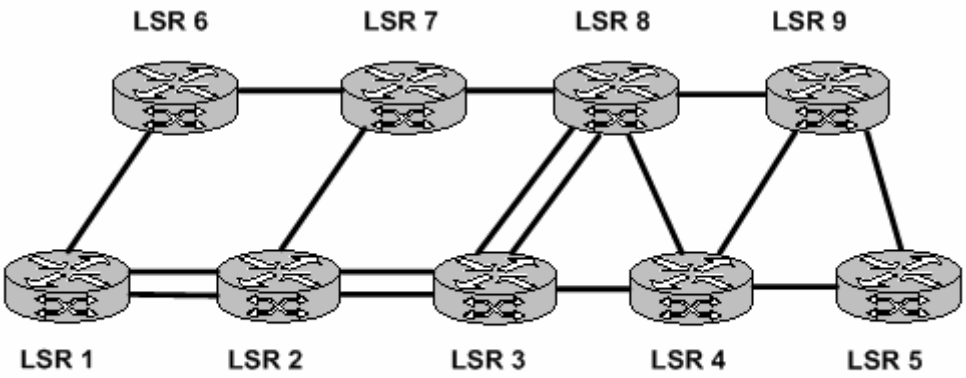

Figure 4: Fast Reroute One-to-one

Figure 4 shows the protected 1, 2, 3, 4, 5 LSP has four detour LSPs. In the case of network problem in the protected path the LSP which discovers the problem can redirect the traffic to some available backup path without sending a failure notification signal.

It is clear that the approach of fast reroute one-to-one is not optimal from resource usage point of view – many LSRs are dedicated to a backup event. In some of the cases even double reservations exist. Avoiding this can be achieved by using merging in the scenario (Figure 5) when two or more reservations are backup for some working path and the next detour hop in the downstream is the same.

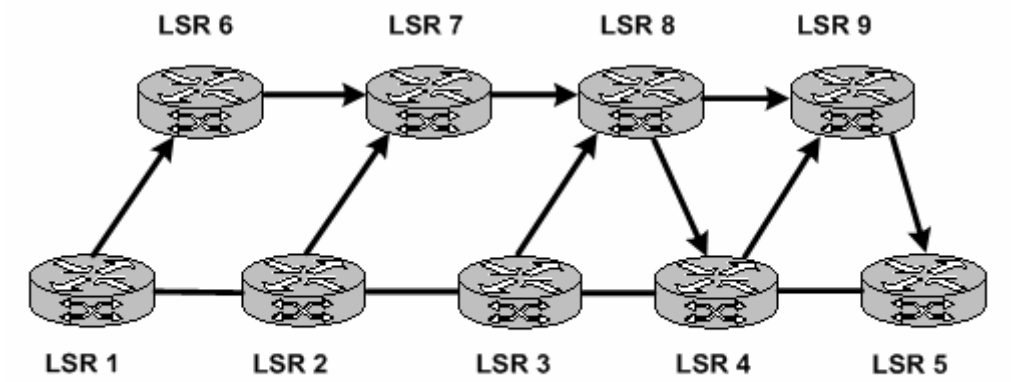

Figure 5: Fast Reroute One-to-one with Merging

When using reservations it is important that the reservation can be available on the backup path which is shortest one to the egress of the protected LSP. In the case of several paths which meet this condition exist then the path which contains nodes which should not be used by some traffic is not selected.

CONCLUSIONS AND FUTURE WORK

In general most of the approaches which are used for MPLS recovery and protection are already implemented in some degree in the existing other network layers thus raising the question if they are really needed. The fact that the MPLS functionality is based on the techniques and protocols which work between layer 2 and 3 of the OSI standard allows it to use the recovery approaches which already exist in these layers. On other hand MPLS can be implemented in different network environments using different technologies so having its own recovery capabilities is an advantage of the MPLS real life usage.

Choosing the most appropriate MPLS recovery mechanism depends on the network usage requirements. Using recovery approaches which are lower layers based offer good

speed but they suffer from poor network utilization and lack of transparency for the higher network layers. On the other hand the rerouting based recovery approaches are slower but offer less resource usage compared to the lower level recovery mechanisms.

The high priority traffic should be protected using fast recovery mechanisms with minimal failure recovery time in the case of a network problems and the rerouting based protection are better when less resource usage is required for recovery.

REFERENCES

[1] S.Makam, V.Sharma, K.Owens, C.Huang "Protection/Restoration of MPLS Networks" draft-makam-mpls-protection-00.txt October 1999

[2] C. Huang, V. Sharma, K. Owens, S.Makam "Building Reliable MPLS Networks Using a Path Protection Mechanism" IEEE Communications Magazine
March 2002

[3] D. Haskin, R.Krishnan "A Method for Setting an Alternative Label Switched Paths to Handle Fast Reroute" draft-haskin-mpls-fast-reroute-05.txt November 2000

[4] L.Hundessa, J.Pascual "Fast Rerouting mechanism for a protected label switched path" Proceedings of the IEEE International Conference on Computer Communications 01
October 2001

ABOUT THE AUTHOR

Msc. Svetlin Petrov, Department of Computer Systems, University of Rousse, Phone: +359 82 888 685, E-mail: SPetrov@ecs.ru.acad.bg