International Journal of Electrical and Computer Engineering (IJECE)
Vol.1, No.2, December 2011, pp. 151~160
ISSN: 2088-8708

Comparison Analysis of Recovery Mechanism at MPLS Network

Mohammad Yanuar Hariyawan
Politeknik Caltex Riau
Jl. Umbansari 1, Rumbai, Pekanbaru, Riau, +62-761-9023094
yanuar@pcr.ac.id

Abstract

Multi-protocol Label Switching (MPLS) has become an attractive technology of choice for Internet backbone service providers. MPLS features the ability to perform traffic engineering and provides support for Quality of Service traffic provisioning. To deliver reliable service, MPLS requires a set of procedures to provide protection for the traffic carried on Label Switched Paths (LSP). In this case Lable Switched Routers (LSR) supports recovery mechanism when failure happened in the network.This paper studied about performance from usage of different techniques that can be used to reroute traffic faster then the current IP rerouting methods in the case of a failure in a network. Local rerouting, Fast Reroute one to one backs up, Haskin, PSL oriented path protection and 1+1 path protection recovery mechanism was compared by given of aggregate traffic which has self-similarity character. Packet drop, rejection probability, recovery time, service disruption time and pre-reserved resources backup will be made as comparator parameter with various bitrate and different position of link failure. Packet loss, rejection probability, recovery time and service disruption time at five recovery mechanisms influenced by position of link failure to ingress. 1+1 path protection mechanism has least packet drop, but costliest way to do recovery in the case of usage resources, as traffic is sent simultaneously in two paths which disjoint. Fast Reroute one to one backup is quickest way to operate protection switching recovery after 1+1 path protection mechanism.

Keywords*: MPLS, recovery, rerouting, self-similar traffic, protection switching*

1. Introduction

In the globalization era, the speed and quality of service in communication becomes an important factor. Some sources in the network may have failed. To provide high availibility appropriate network, network providers must be able to predict and plan for this failure. Link failure is a common cause service interruption in computer networks. When the channel on the network fails, all communication channels that fail to use it to temporarily be interrupted. When done in handling low-level communication layer, rerouting can be done quickly but are expensive because it requires additional hardware. On the other hand, it is possible to reroute traffic at a higher layer using software mechanisms, but results are slow.

Internet is a datagram packet switching network where data is carried in IP packets. Multiprotocol Label Switching (MPLS) carry IP packets through a virtual circuit, which combines the advantages datagram packet switching and virtual circuit switching to meet the need for reliability, speed and efficiency in handling link failures. In terms of handling damage to the network, MPLS network has a method of protection against traffic, where the method of protection is part of the quality of services provided MPLS to provide certainty in the validity of transmitted data. The ability of a network protection in MPLS-TE requires recovery mechanisms to handle failure will occur so that the rate of traffic in fixed networks can be done without losing traffic data to be transmitted.

Some recovery mechanism [1], [2], [3], [4], [5], [6], [7] has been developed to overcome the problem of sending data packets through the MPLS network, including the local rerouting [1] , Haskin [6], Fast Reroute one-to-one backup [3], [7], 1 +1 path protection [5] and the Path Switch LSR-Oriented Path protection [2], [3]. Each technique has advantages and disadvantages for each development priority on certain parameters. If the speed of recovery be given top priority, then the model of protection switching was to be used, while if the network efficiency less advanced than the speed for any reason, then the rerouting model with the scope of local recovery into a fairly logical choice for service providers. Some comparative analysis [8], [9], [10], [11], [20] ,[22],[23], have been made to see performance of recovery mechanisms in MPLS networks using a single source that has a **constant bit rate** (CBR).

This paper will analyze comparative performance of Local Rerouting mechanism, Haskin, Fast Reroute One-to-One Backup, 1 +1 path protection and the Path Switch LSR-Oriented Path protection by giving aggregate traffic which has **self-similarity** character, using comparison criteria:

- Packet loss during recovery process
  Packets discarded by the router or lost when the way to the destination. Measurement of packet loss is used as a parameter reliability comparison.
- Rejection probability
  Rejection probability is the probability of a data packet having dropped when sent from source to destination.
- Service disruption time

Received Sep 6th, 2011; Revised Nov 11th, 2011; Accepted Nov 21th, 2011

Long service interruption is the time between the last bit transmitted before the failure occurred and the event is received when the first bit of data using a back up the path to the receiver, is used as a parameter of the speed ratio.

- Recovery time
  Recovery time is the time it takes the backup path for the active and start carrying packets of data after the failure. Recovery time also marks the time between failure detection and the time when the packet is passed through the backup LSP. The calculation is done by comparing the recovery time between the time when a link failure occurs until the recovery process is completed. Mark with the transfer of packets from an upstream node that detects a link failure to the backup path that has been provided.
- Pre-reserved resources
  Total resources available for backup traffic on the network before the failure occurred.

2. Research Method

Recovery mechanism simulation will be done by using the Network Simulator (NS) 2.26 version with MPLS Network Simulator (MNS). This simulation involves several stages:

a. Aggregate traffic source modelling yielding pattern self-similar with clauses of parameter value hurst : $1/2 \leq H \leq 1$
b. MPLS network modelling
c. Scheme of simulation Local Rerouting, Fastreroute One-to-One Backup, Haskin, 1+1 path protection, PSL-Oriented Path protection
d. Giving of additional traffic at network MPLS

2.2.1. Aggregate Traffic Source Modeling

Self Similar traffic generated by performing aggregation of a number of sources, where each source release package with a fixed size, while the probability of occurrence time of these packages follow a Pareto distribution [18], where the variables contained there in is the shape parameter (α), can be seen in Figure *1*. Three variables that can affect characteristics of traffic generated, among others, shape parameters, the number of source and size of the package at [19] concluded that the addition of the source does not eliminate the bursty nature of self-similar traffic, therefore it is not absolutely require a large amount of source, design of traffic source used 15 sources.

Shape parameter

Changing shape parameter affects the shape of the resulting Pareto distribution, generally will affect mean and variance. There is a relationship between shape parameter and the Hurst parameter, namely:

$$H = (3-\alpha)/2 \quad (1)$$

Self-similar traffic has a Hurst parameter value requirements: $2 \leq H \leq 1$. To meet these requirements, then the shape parameter $1 \leq \alpha \leq 2$ value ranges.

Based on research that has been done [19], stated that traffic would have self-similar characteristic if has $1/_2 \leq H \leq 1$. By looking at the equation of the relationship between shape parameter and the Hurst parameter (eq. 1), then the design of self-similar traffic source will be used an alpha value of 1.2 to produce H of 0.9.

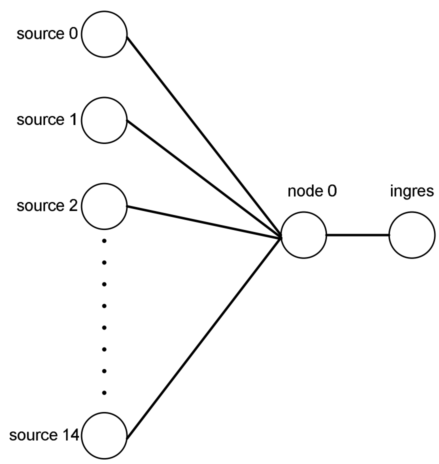

Figure 1. Aggregate Traffic Generation Topology

Number of Source
Theoretically, the number of sources will affect self-similar bursty characteristic. The design of aggregate traffic sources will be used 15 sources, based on [19].

2.2.2. Scheme of Recovery Mechanism Simulation at MPLS Network

Mechanism simulationof Local Rerouting, Fast Reroute One-to-One Backup, Haskin, 1+1 Path Protection and PSL-Oriented Path Protection simulation by using network simulator version 2.26 has been installed MNS module is comprising modules MPLS using LDP and CR-LDP.

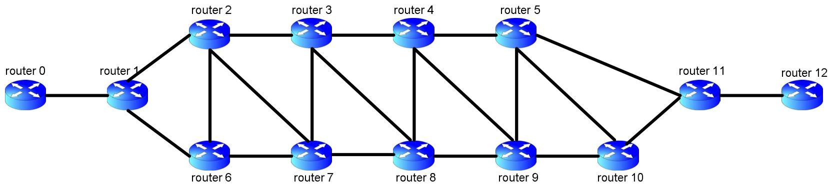

Figure 2. Network Topology

Partial mesh topology used to simulate the performance of recovery in MPLS as shown in Figure 2, where there are several MPLS routers that are connected to each other and there is also a normal IP router as the agent sender and receiver package.

3.1. Recovery Local Rerouting Mechanism Design

Local rerouting is rerouting mechanism with a combination of local repair model [17]. Recovery LSP will be set up dynamically when there is fault on the LSP. Each LSR has the ability to detect errors ranging from up to form a new LSP. As was explained earlier that the rerouting model has the advantage of saving network resources but lacking in speed recovery, and that's why local rerouting mechanism is developed, to minimize recovery time by giving them the ability on each LSR to be able to quickly establish itself after the recovery LSP detected a fault, Figure 3 explains Local Rerouting mechanism.

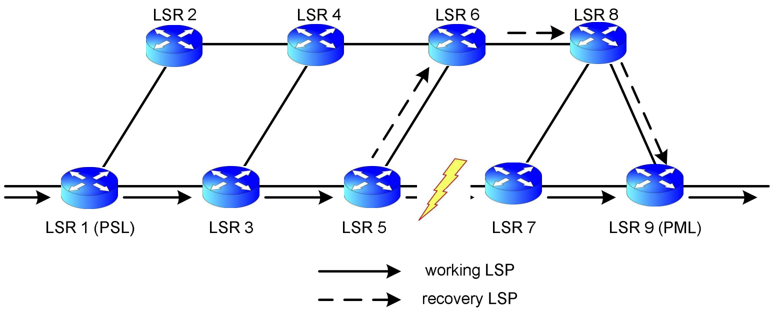

Figure 3. Local Rerouting Mechanisme [17]

At local rerouting mechanism use ”simple-dynamic" routing model, meaning that from the beginning there was no formation of LSP for backup purposes, but dynamically. In the event of fault on the working LSP, the LSR that detect it (LSR upstream) will soon run the algorithm to find the shortest route from the leading to the egress LSR and then put the traffic from the working LSP to the new route, if the fault occurs on link 3-4, the protection given on LSR3. MPLS LSR will also enable the flow protection with intervals 0.01 seconds toward node 12.

3.2. R*ecovery Fastreroute One-to-One Backup* Mechanism Design

Fastreroute One-to-One Backup is a process whereby data recovery in MPLS networks can be directly transferred to the backup path without requiring the signaling process when the failure occurs [5]. No such protection switching, where it is the repair point is failure detection point. So there is no requirement to notify an error or disturbance to the repair point by using the signaling protocol. Figure *4* describes the Fastreroute One-to-One Backup mechanism.

Fastreroute one-to-one mechanism back-up, uses dynamic routing protocols “Distance Vector” in simulation. This protocol will be used in the transfer of information between LSRs for updating to each other its routing table and make the process of transferring traffic if the recovery process have been accomplished. Initial process of the simulation is establish network topology including nodes, links, and the agent which used, then each agent such as UDP and IP routing will have to initialize. In handling a link failure that occurred on the network, then established an alternative route as a backup that will transfer data packets from the LSP which face a link failure, go back to the

LSP in different paths, in order to be sent back toward the destination. This alternative path is formed at each node that is on the LSP (One-to-One Backup) to overcome every possible link failure will happen in all the links on the LSP.

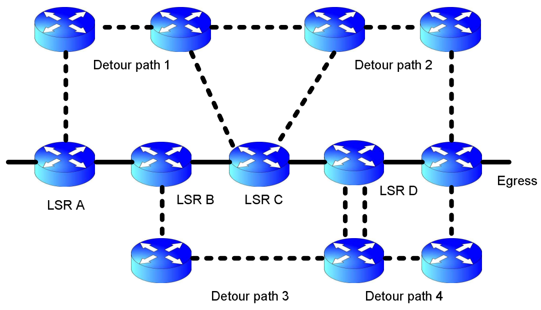

Figure 4. Detour Fastreroute One-to-One Backup [5]

3.3. Haskin Mechanism Design

Haskin mechanism is a method to do setting-up alternative LSP in handling fast rerouting traffic, at the time of the happening of failure in working LSP MPLS network [6]. Since it provide mechanism of protection fast rerouting, hence LSP alternative is made before the happening of failure.

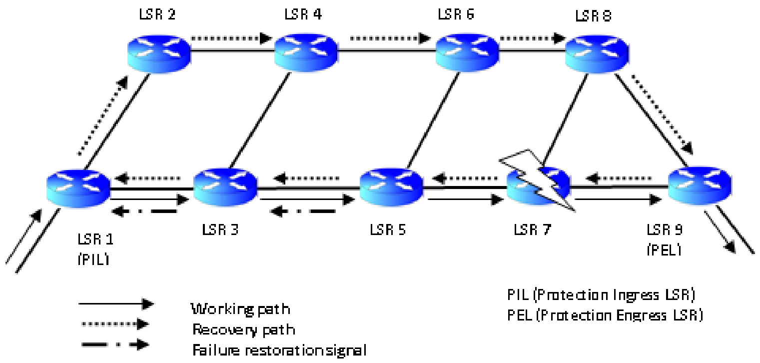

Figure 5. Haskin Recovery Mechanisme [17]

At Haskin mechanism, method applied based on global of repair where protection of network is done in end-to-end by using protection switching method. Protection switching is a form of protection building recovery path before the happening of failure at working path. On the happening of failure at LSR, data package will be returned to part of ingress LSR applies reverse LSP. Ingress LSR will look for path to return to through alternative LSP as data delivery route, as shown in **Error! Reference source not found.**. Initial process in implementing simulation of this recovery equal to mechanism process before all is forming of network topologies covering node, link, and agent applied. Then each agent like UDP and protocol routing will do inisialisation. Message request sent from ingress LSR towards egress LSR. After the request message sent is received by the egress LSR, the egress LSR will send a reply to the ingress LSR which contains important information that will be delivered to each node that dialuinya as well as the information required in the establishment of an LSP.

3.4. PSL-Oriented Path Protection Mechanism Design

PSL-Oriented Mechanism Path Protection was developed to support the 1:1 path protection mechanism is a mechanism whereby in normal condition, protected traffic passing through the working path will be moved to a recovery path when a fault occurs on the working path [20]. Switching action is performed by the PSL, and therefore this mechanism is also referred to as the PSL-oriented. Established recovery path is not specified as a backup, but still available for traffic with low priority. Protected traffic moved to the recovery path will occupy the low-priority traffic found on the recovery path. This method is slightly improved efficiency in resource usage, Figure *6* shows the mechanism of PSL-Oriented Path Protection.

Procedure PSL-Oriented Path mechanism, similar protection with other recovery mechanisms procedures and the establishment of an MPLS LSP and additional modules have in common, which distinguishes it from others that is in the process of transferring traffic to the recovery LSP. When the PSL has received FIS is working LSP stated fault so that the process of moving traffic to the recovery LSP is immediately run. The procedure is called by functions that have been applied to the LDP agent for the case of FIS reception by a node. Type of recovery mechanism used is 'notify-prenegotiated' means that do is a notification signal transmission mechanism FIS and the process of moving traffic from the working LSP to the recovery LSP. 'Notify-prenegotiated' is used for the case of fault on the links 2-3, 3-4, and 5-11, while for the case of fault on link 1-2 does not require the same mechanism as LSR1 is a PSL that does not require notification process again. Therefore, for the case of fault on link 1-2 ‘notify-prenegotiated’ should be replaced with ‘drop’.

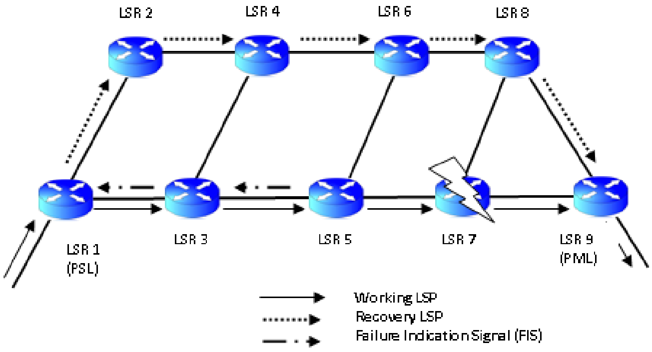

Figure 6. PSL-Oriented Path Protection Mechanisme

As with other mechanisms, initiall procedure is the process of formation of the working LSP, then the establishment of LSP recovery, after the occurrence of a fault in one of the links on the working LSP. Establishment of working LSP begins with a label-request process where LSR1 or ingress will send a signal LDP for label-request to LSR11 or egress. After receiving the signal-LDP label request, immediately send the signal egress LDP for label-mapping to the ingress where its function is to map the labels on each LSR that will be passed by the packages will use the working LSP. The second is the formation process of recovery LSPs are disjoint to the working LSPs. After receive the label request, the egress to do a label-mapping by sending a signal back through the LSR 11-10-9-8-7-6-1 LDP. Thus has prepared a working LSP and backup when a fault current occurs on the working LSP.

3.5. 1 +1 Path Protection Mechanism Design

The purpose of the use of path protection, or specifically in the 1 +1 path protection is to protect the working path of destruction a link or node on that path [1]. Because in this scheme a recovery path made a separate (not connected) with the protected working path, so if there is damage to either the node or link on the working path will not affect the employment recovery path, as shown in Figure *7*.

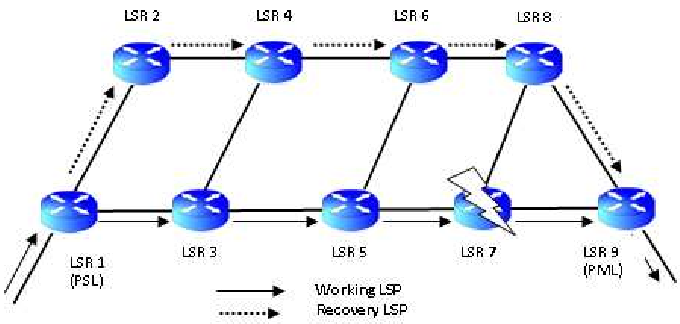

Figure 7. Recovery 1+1 Path protection Mechanism [1]

1 +1 path protection mechanism procedure similar to other procedures for recovery mechanisms and the establishment of an MPLS LSP and additional modules have in common, except that in this mechanism was raised two times the aggregate traffic sources (2 x 15 sources = 30 sources). This is due to MPLS node in NS2 simulator does not support packet duplication function. In 1 +1 path protection mechanism is formed of two LSP (working path and backup path), where the second LSP will submit the package are identical to each other to the same destination. So when there is a failure on the working path line, the destination still receive data packets in their entirety.

3. Result and Discussion

In the following section will discuss the comparison of different mechanisms in the position of a link failure and packet delivery rate is different.

3.1. Packet Drop

Comparison of packet drop in five mechanisms can be seen in Figure *8*, the mechanism of 1 +1 path protection, traffic on the working path has a duplicate of which is always sent through the path to recovery regardless of whether an interruption in the delivery of traffic on the working path or not. With these conditions, then the packet drop in this mechanism does not indicate the number of packets discarded in the working path for any damage, because traffic on the working path is not protected by this recovery mechanism.

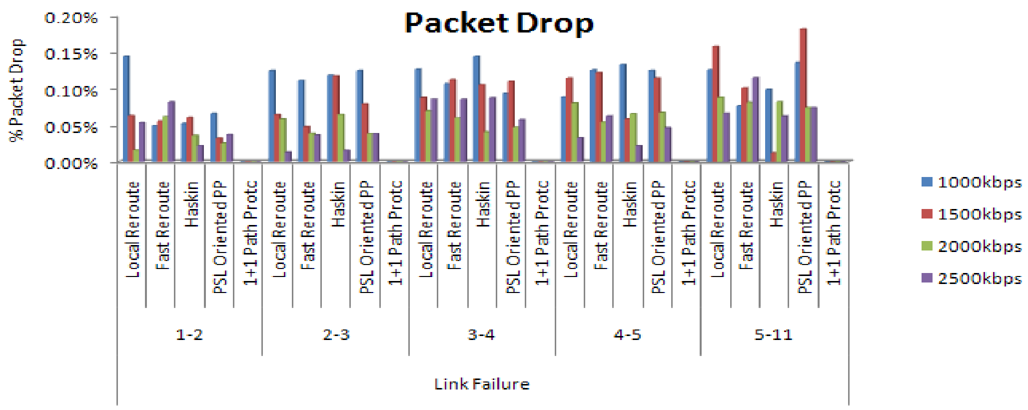

Figure 8. Comparison of packet drop at the five mechanisms

Packet data on the working path will be left is wasted because it already has a duplicate traffic sent through other channels that are not affected by damage to the link on the working path. Packages that are ignored by the receiver when not working path of damage was also not included in the category of packet drop. These packages are not categorized as a packet drop due to the loss of the package does not affect the reception of information by the receiver.

On the local rerouting mechanism the packet drop tends to increase at the location of the link fault is increasingly distant from the ingress, while the Fast Reroute mechanisms drop packets at all positions relative link has the same amount, it is in because of the lack of backup path calculation mechanism to find the shortest path toward the egress LSR. In Haskin mechanism does not form a specific pattern in the packet being dropped, but the link failure has the most distant from the ingress packet drop at most. The amount of packet drop in the mechanism of PSL-Oriented Path Protection tended increasingly to the location of the link failure is increasingly distant from the PSL. This is caused by the FIS to be sent back to the PSL before traffic can be routed to the recovery LSP, so that the location of the link fault is increasingly distant from the PSL, the FIS delivery process will stay longer and cause more and more packets are still delivered on the working LSP before it is transferred to the recovery LSP.

3.2. Rejection Probability

Rejection probability is the probability of a data packet having dropped when sent from source to destination. In the fifth recovery mechanism (can be seen in Figure *9*), rejection probability does not form a specific pattern in cases where a link failure occurs, but tends to rise when a link failure away from the ingress. Rejection probability depends on the number of packets sent and the number of packets dropped, while the number of packets generated in each simulation is different, this will affect the number of packets dropped.

PSL oriented on average have the highest probability of rejection at any rate that is used compared to other mechanisms. While the mechanism of 1 +1 path protection has 0% probability for all packets received at the destination.

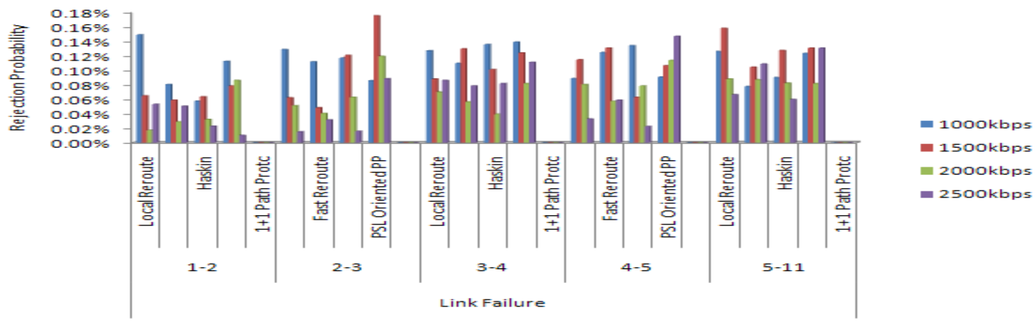

Figure 9. Comparison of rejection probability at the five mechanisms

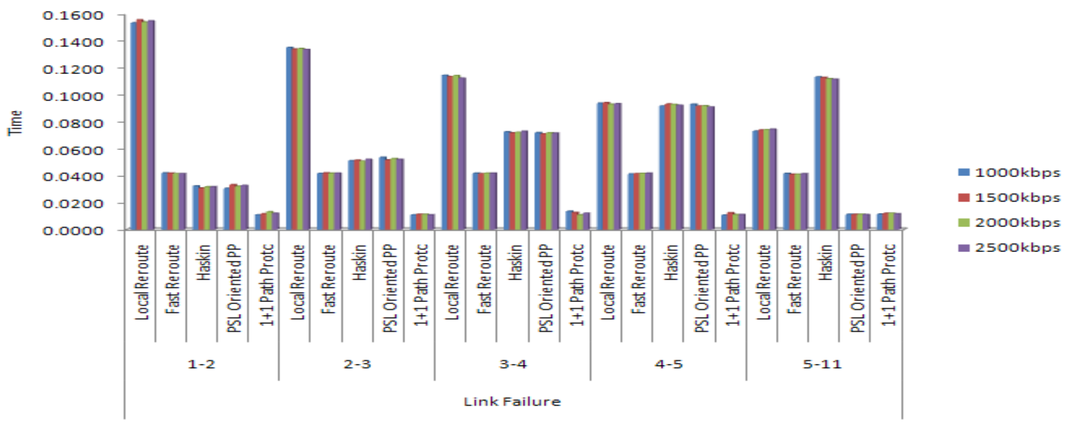

Figure 10. Comparison of the service disruption time in the five mechanisms

3.3. Service Disruption Time

Service disruption times, is the length of time of the package that arrived at the destination node is calculated based on the difference of time from last packet entering the destination node after a link failure occurs until the first packet into the destination node after recovery mechanism is complete. Basically the service disruption time calculation was done in order to see how long it took the arrival of the packet back to the destination node after an interruption in the network. In applications that are real time, such as voice applications over IP (VoIP) and video transmission, the time of this disturbance can only be tolerated for much less than 60 ms [5], so between the two mechanisms are compared in the task of recovery this end, it is known recovery mechanisms which are capable of serving applications that are real time. Figure *10* shows the rejection probability of the five mechanisms.

In the Fast Reroute service disruption time is relatively constant as the node that detects a failure of nodes to switch traffic to the backup path and not take time to set up the backup path before failure occurs. Service disruption time on the PSL mechanism oreiented Haskin and will increase for both models when the link failure away from the ingress node, this is due to FIS or reversed traffic should be sent upstream to the ingress before it can be routed to the global recovery path, these results also occur when the MPLS network is loaded with CBR[8], [9], [10], [11], [21]. In 1 +1 path protection is needed the most rapid recovery compared with other mechanisms, where the average time required by 0.01167s.

The amount of service disruption time on a 1 +1 path protection is a time interval of receipt of successive packets from the working path and the recovery path, so that wherever the location of the damage link has same time, succesive packets interval from the working path and the recovery path will remain. Service disruption time on the Local Reroute mechanisms will decrease when a link failure occurs away from the ingress node, with different Haskin mechanisms and PSL oriented, this is due to the mechanism of local route, the distance between the site of a link failure with the destination node is very influential. Closer distance between the site of a link failure to the egress LSR mean length of backup paths are also shorter, then the recovery process is done faster.

3.4. Recovery Time

The calculation is done by comparing the recovery time between the time when a link failure occurs until the recovery process was completed, which is marked by the transfer of packets from an upstream node that detects a link failure to the backup path that has been provided. Local rerouting requires an average recovery time is longer than the other mechanisms. On the Fast Reroute and Haskin mechanism, recovery time was not influenced by the position of a link failure, whereas the other mechanisms recovery time influenced by the position where the link failure occurs, , these results are similar when the MPLS network is loaded with CBR [8], [9], [10], [11], [21]. On the local rerouting and 1+1 path protection mechanism, when a link failure recovery time away from the ingress will increase, while during the recovery mechanism PSL oriented path protection, when link failure close to the ingress, then the recovery time needed will be more rapid. This is caused by the FIS to be sent back to the PSL, so that the location of the link fault is increasingly distant from the PSL, the FIS delivery process will stay longer. But the recovery time required by the three mechanisms above is still much faster recovery time period required by the mechanism of Fast Reroute and Haskin mechanism. In the Fast Reroute One to One Backup and Haskin mechanisms, recovery time is not affected where the position of a link failure occurs and both have almost the same recovery time of about 0.010565 seconds, Fast Reroute mechanism requires an average recovery time of about 0.01059 seconds, while the Haskin mechanism requires average recovery time of about 0.01054 seconds. Figure *11* shows the comparison of the five recovery mechanism. For CBR load, Haskin mechanism [8] need recovery time about 0.01 – 0.0148 seconds and Fast Reroute One to One Backup mechanism [9] about 0.0118-0.0136 seconds.

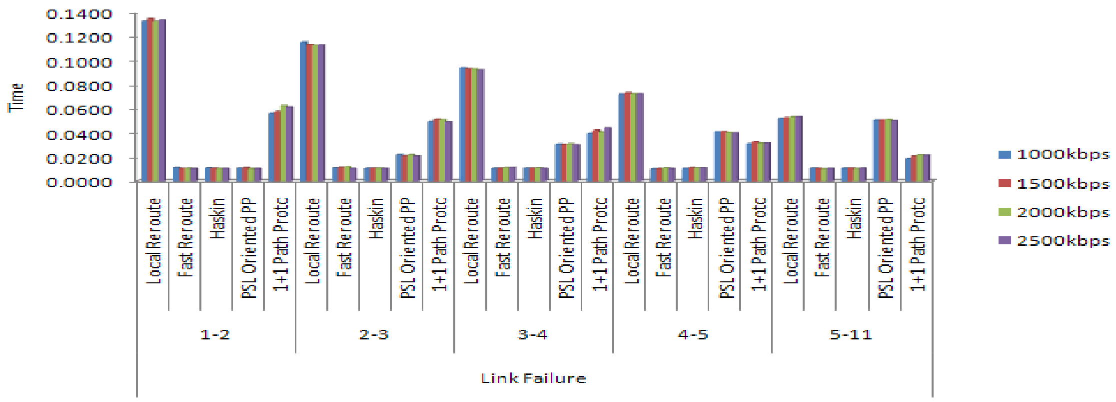

Figure 11 Comparison of recovery time from the five mechanisms

3.5. Pre-reserved Resources Backup

Figure 2.11 shows the amount of resources reserved for backup traffic on the network before the failure occurred. Local rerouting model setup the backup path on demand after the failure occurred. Fast rereoute one to one backup requires ten global resources reserved for backup paths. Haskin requires six global resources for backup paths and three reversed path, with a total ten resources reserved. PSL oriented path protection and 1 +1 path protection takes 6 reserved backups. The number of reserved resources depends on the topology of the network.

Haskin and PSL oriented path protection depends on both the global recovery path, Haskin will always require more resources than the PSL oriented path protection because of the Haskin requires reverse backup path in addition to the global recovery path.

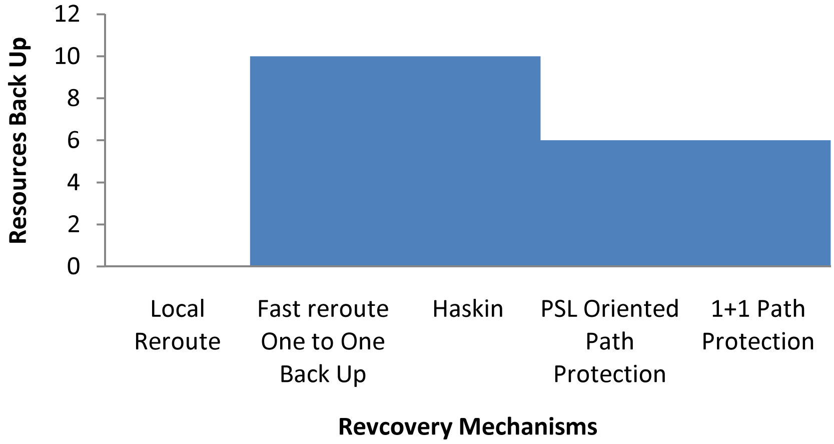

Figure 12. Pre-reserved Backup Resources

From the results of discussions which have been carried out on all the mechanisms and performance parameters, obtained results on performance comparison table mechanism which can be seen in Table 1.

4. Conclusion

Self-similar traffic, can be generated using aggregate traffic consisting of 15 distributed pareto traffic source with α=1.2, which produces an average Hurst parameter 0.67148. Rerouting mechanism will have the service disruption time is higher than the protection switching, since the time rerouting path computation and path setup and this is not needed on protection switching. The mechanisms that have the least service disruption time is 1 +1 path protection. With this mechanism, failure notification, the calculation of the recovery path or recovery path setup is not required. Fast Reroute one to one backup is the fastest way to perform the protection switching operation recovery after a 1 +1 path protection mechanism and more possible to be realized. Pre-reserved resources become attention when protection switching is used, because rerouting is not provided for a number of resources before starting the recovery process. Rerouting is the best option in terms of the use of pre-reserved resources. For high priority traffic, protection switching is the best mechanism to use. The quickest way to recovery with the fewest dropped packets on the network is through protection switching with 1+1 protection, but this approach is the most expensive way to do recovery in the use of resources, when the flow of traffic are sent simultaneously on two disjoint paths. Haskin and Fast Reroute mechanism requires the which is briefest recovery time if it is compared to other mechanisms and does not depend on position of link failure.

Refferences

[1] Ahn G, *et* al., "An efficient rerouting scheme for MPLS-Based Recovery and its Performance Evaluation," *Telecommunication Systems*, 481–496, 2002.
[2] Owens, et al., "A path protection/restoration mechanism for MPLS networks," *Internet Draft*, 2001
[3] Huang C *et al*., "Building reliable mpls networks using a *path protection* mechanism," *Communications Magazine, IEEE*, 40(3): 156–162, 2002.
[4] Pan P, *et al.*, "A. Fast Reroute Extensions to RSVP-TE for LSP Tunnels", *Internet Draft*, draft-ietf-mpls-rsvp-lsp-fast*reroute*-06.txt. 2004
[5] Harrison, E,"Protection and Restoration in MPLS Network," *Data Connection White Paper*. 2001
[6] Haskin, D. and Krishnan, R, "A Method for Setting an Alternative Label Switched Paths to Handle Fast Rerouter, "Draft-Haskin-mpls-fast-*reroute*-05.txt. 2004
[7] Nagarajan, *et al*.,"A packet 1+1 path protection service for MPLS networks," *IETF Internet Draft*. 2002
[8] Afrinaldi, Z,"Penggunaan Mekanisme Recovery Haskin pada Jaringan MPLS," *Final Project*, Surabaya: Teknik Telekomunikasi Multimedia, Teknik Elektro, Institut Teknologi Sepuluh Nopember; 2006.
[9] Heriansyah, D, "Penggunaan Mekanisme Recovery Fast Reoute One to One Backup pada Jaringan MPLS,"Surabaya:Teknik Telekomunikasi Multimedia, Teknik Elektro, Institut Teknologi Sepuluh Nopember;2006.
[10] Nugroho, H,"Penggunaan Mekanisme Recovery 1+1 *Path protection* pada Jaringan MPLS," Surabaya: Teknik Telekomunikasi Multimedia, Teknik Elektro, Institut Teknologi Sepuluh Nopember; 2006.
[11] Setiawan, W,"Penggunaan Mekanisme PSL *Path protection* pada Jaringan MPLS," Surabaya: Teknik Telekomunikasi Multimedia, Teknik Elektro, Institut Teknologi Sepuluh Nopember; 2006.
[12] Rosen, E et al., "Multiprotocol Label Switching Architecture," *RFC3031, IETF*. 2001.
[13] Kuhn, R,"*Source*s of failure in the public switched telephone network," *IEEE Computer*. 1997
[14] Network Strategy Partners, LLC. Reliable IP Nodes,"A Prerequisite To Profitable IP Services," *Whitepaper*. 2002
[15] Sharma, V. and Hellstrand, F,"Framework for MPLS-Based Recovery," *IETF RFC 3469*. 2003
[16] Bartos, R. and Raman, M,"A heuristic approach to service restoration in MPLS networks," *IEEE International Conference on ommunications (ICC)*, Helsinki, Finland. 2001
[17] Yoon, S,"An efficient *recovery* mechanism for MPLS-based protection LSP," *Joint 4th IEEE Internat. Conf. on ATM (ICATM)*, 75–79, . 2001.
[18] Crovella, M.E. and Bestavros,"A. Self-similarity in world wide web traffic: evidence and possible causes," *ACM SIGMETRICS'96*, Philadelphia, USA, 160-169, . 1996.
[19] Setijadi, Eko,"Rancang Bangun Pembebanan Trafik Self Similar pada Testbed Jaingan MPLS over IP di Jaringan Telekomunikasi Elektro ITS," *Tesis*. Surabaya: Institut Teknologi Sepuluh Nopember; 2006.
[20] Banerjee, A.*et al*.,"Generalized multiprotocol label switching: An overview of routing and management enhancements," *IEEE Communications Magazine*, vol. 39, no. 1, 144–150, 2001.
[21] Johan M.O. Petersson,"MPLS Based Recovery Mechanisms," *Master Thesis*. Oslo: University of Oslo; 2005
[22] Yimin Qiu, et al.,"MPLS-based Network Fault Recovery Research," *International Journal of Intelligent Engineering and Systems, Vol.3, No.4*, 2010.
[23] El Kamel Ali and Youssef Habib,"An efficient hybrid recovery mechanism for MPLS-based networks," *Computers and Communications IEEE Symposium, ISCC* 2009.

Bibliography of authors

Mohammad Yanuar Hariyawan received Bachelor and Magister degrees in Telecommunication Multimedia from the Sepuluh Nopember Institute of Technology Surabaya, Indonesia, in 2001 and 2007 respectively.
He is Lecturer and Member of Wireless Communication Research Group at Telecommunication Department, Polytechnic of Caltex Riau.

Table 1 Recovery Mechanism Comparison Table

Parameter	**Recovery Mechanism**				
	Local Reroute	**Fastreroute One to One backup**	**Haskin**	**PSL Oriented Path Protection**	**1+1 path protection**
Packet Drop	• increases when the position of a link failure and the farther from the ingress. • increases when there is additional traffic load	• does not depend on the position of a link failure. • increases when there is additional traffic load.	• increases when the position of a link failure and the farther from the ingress. • increases when there is additional traffic load.	• increases when the position of a link failure and the farther from the ingress. • increases when there is additional traffic load.	there is no packet drop
Rejection Probability	• does not depend on the position of a link failure. • decreases on the rate of 2000k and 2500k. increases when there is additional traffic load	• does not depend on the position of a link failure. • decreases on the rate of 2000k and 2500k. increases when there is additional traffic load	• does not depend on the position of a link failure. • decreases on the rate of 2000k and 2500k. increases when there is additional traffic load	• does not depend on the position of a link failure. • decreasases on the rate of 2000k and 2500k. increases when there is additional traffic load	0% because there is duplication of packets sent through a recovery path
Service Disruption Time	more rapidly when the position of a link failure the farther from the ingress, max = 0.115569s, min = 0.07301s	does not depend on the position of a link failure, average of 0.04157643s	more slowly when the position further away from the ingress link, max = 0.11156s, min = 0.03227s	more slowly when the position further away from the ingress link, max = 0.112128s, min = 0.0304956s	does not depend on the position of a link failure, an average of 0.01167s
Recovery Time	more rapidly when the position of a link failure the farther from the ingress, max = 0.13469s, min = 0.05221s	does not depend on the position of a link failure, an average of 0.01059s	does not depend on the position of a link failure, an average of 0.01054s	more slowly when the position of a link failure and the farther from the ingress, max = 0.051031s, min 0.0102262s	more rapidly when the position of a link failure the farther from the ingress, max = 0.6234s, min = 0.1859s
Pre-reserved backup	0	10	10	6	6

Received Sep 6th, 2011; Revised Nov 11th, 2011; Accepted Nov 21th, 2011