

Performance Analysis of the Impact on Both the use of Redundant Equipment and Link Failure Repair Paths in Convergence Mobile IP Transactions Utilizing MPLS

M. Asante and R. S. Sherratt
Signal Processing Laboratory, School of Systems Engineering,
The University of Reading, UK

Abstract - High availability of IP/MPLS networks is a prerequisite to offer reliable and profitable carrier-class services and also enhances convergence where voice, video and data are transmitted along the same medium. A well-designed network element, such as a router, facilitates the building of highly available networks and reduces the capital expenditure and operational expenditure associated with redundant network infrastructures. An effective network design seeks to satisfy service reliability and availability objectives at the minimum network equipment and operational cost and will fully improve a Convergent Mobile Internet Protocol (MOIP) transmissions. The use of redundant hardware components, including line cards, switching fabric, control processor cards, physical interfaces and link failure repairs reduces unplanned hardware-related downtime. This paper discusses three types of redundancy schemes and the effect of link failures on prioritized and non prioritized routes. In particular, this paper outlines mechanisms for reducing network downtime in Mobile IP transactions.

Keywords: Multi-Protocol Label Switching (MPLS), Internet Protocol (IP), Mobile Internet Protocol (MOIP), Quality of Service (QoS), Convergence

1. Introduction

The availability of a backup or “redundant” component in the event of a component failure will prevent the loss of service and be provided via software, hardware, or combination of the two. Network-level fault tolerance relies on software or hardware to quickly detect the failure and switch to a known backup path/link. The backup paths may be provided at multiple transport layers, including *Wavelength-Division Multiplexing* (WDM), Synchronous Optical Network/Synchronous Digital Hierarchy (SONET/SDH), and Multi Protocol Label Switching (MPLS). Mobile IP (MOIP) enables users to keep the same IP address regardless of its location in which case data packets can be re-routed if the user moves to a different position on the Internet. In the traditional way, IP tunneling is the method used by Home Agents (HAs) to transmit packets that are meant for a Mobile Node (MN) [1]. This method appears to be inefficient especially if more than one MN from the same HA but attached to different foreign networks are all transmitting or receiving signals. In this situation the Quality of Service (QoS) will be compromised in the transmission of voice, video and data through the tunnel since no priority is assigned to any particular type of data and also a failure of the ingress router to a home network will not work well for MOIP transmissions. As a result, there will be congestion loss of data and the Mobile Node will not be able to communicate with the Home Agent (HA). In effect MOIP convergence will be fully enhanced as a result of the implementation. The use efficient transfer of packets utilizing MPLS together with redundant equipments as a standby in case of failure will eliminate a lot of these shortfalls and enhance the transfer of voice, video and data. With MPLS, there are no permanent virtual connections between sites. Instead, secure and logical paths are set up through the network as and when there

is traffic to be delivered using the best route available at the time. This means that users, sites or devices can be added to the network at any time without reconfiguration and without affecting security and reliability.

MPLS system is a label tagging technology designed to remove the setback in IP technology. Before a packet enters an MPLS network, each packet is classified (based on source/destination address, port number and service types) into different Forward Equivalent Classes (FEC) and assign a label. Packets with the same labels are routed along the same route, or Label Switch Path (LSP) [2].

MPLS also support new QoS guaranteed services such as DiffServ, Intserv model and also the MPLS resource management server can decide if there are sufficient resources for a particular demand or not based on the status of the network[3]. The main objective of any network operator is to maximize throughput in order to service many demands whenever they are needed in which case any route which satisfies demand constraints such as bandwidth, hop count/administrative constraints is considered to be a “best route”. Traffic demands can either be permanent or on-request. Permanent traffic demand such as Virtual Private Network (VPN) is usually determined in advance and various off-line algorithms can be used to control the routing procedures.

2. Reliability and Availability of a Network

The reliability of a system or network its ability to perform its intended function without failure over a given period of time. A commonly used measure of reliability is known as Mean Time Between Failures (MTBF), which is the average expected time between failures. A service outage caused by a failure is represented as a Mean Time To Repair (MTTR), that is the average time required to restore a system from a failure. MTTR includes time required for failure detection, fault diagnosis, and actual repair. Availability is related to MTBF and MTTR as follows:

$$\text{Availability} = \text{MTBF} / (\text{MTBF} + \text{MTTR}) \quad (1)$$

This relationship shows that increasing MTBF and decreasing MTTR improves availability. This means that the availability of a router can be improved by increasing the reliability of its hardware and software components [4]. Similarly, improving the reliability of its constituent elements such as routers, switches, and transport facilities can enhance the availability of a network as illustrated in figure1. Therefore using redundant components and link failure repairs, system downtime can be reduced by orders of magnitude and get closer to the carrier-class goal of high availability while keeping the MTBF and MTTR the same. The effectiveness of a redundancy and link failure repair schemes depends on its switchover success rate. Redundancy and link failure repairs is therefore some of the key building blocks for improving high availability and do not only prevent equipment failures from causing service outages, they can also provide a means for in-service planned maintenance and upgrade activities. Redundant network elements add to the overall network cost of equipments but the effective services provided by these redundant equipments is money well spent. This allows alternative routers and paths to be quickly established and used in the event of a failure. In the core, additional routers and links are used to provide fault tolerance. In contrast, on the edge, often thousands of customers are connected through a single router, and the edge router usually represents a single point of failure that can cause considerable delay in the network as illustrated in Figure 2. From figure 2, the failure of the nodes D1,D5,D8,D9 and the links such as R25, R13, R14, R11, R12, R15, R18, R22, R23 etc will cause a considerable delay in packet transmission within the network because all these nodes can be ingress/egress nodes [5].

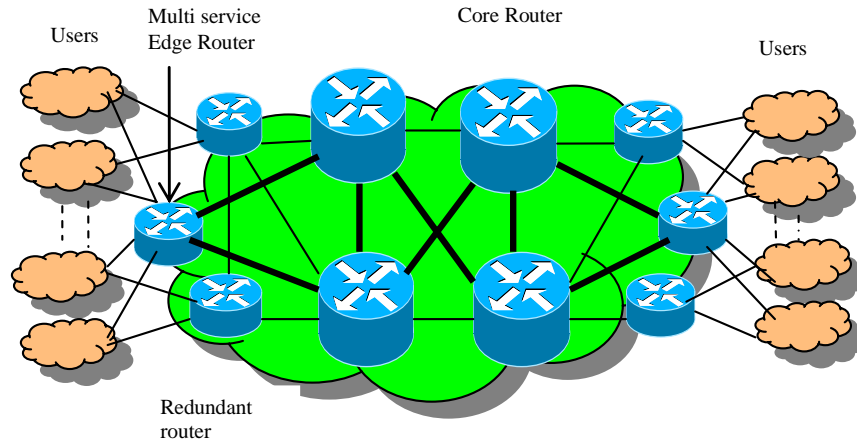


Figure 1: IP/MPLS Network

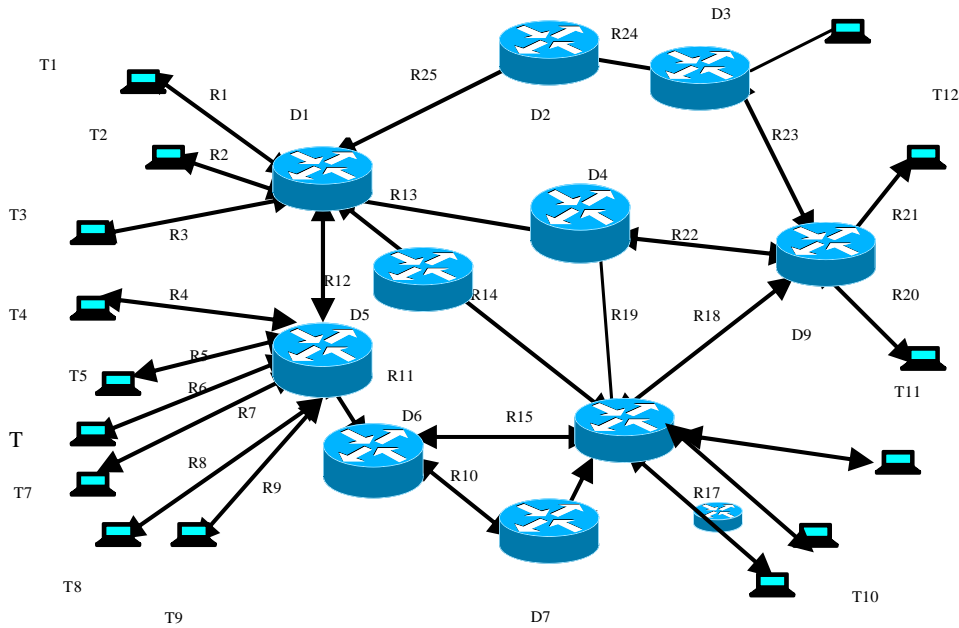


Figure 2: Transmission routes within a network

4. Simulation

A simulation was carried using the network in figure 2 based on One-for-N (1:N), One-for-one (1:1) and One-plus-one (1+1) all in the presence of link failures along all the routes. The delay along all the routes based on the specifications were recorded.

The packets were further classified into grades or in order of priority. The first one being the High priority LSP (H-LSP) for voice, the second being Medium priority LSP(M-LSP) for video and the third being the Low priority LSP (L-LSP) for Data, were established between each IP router pair located at the edge of an MPLS cloud. The delay on all the links D1-D6 along R12-R11, R14-R15 and D6 to D9 along R10-R16-R18 and T10 to D9 along R17-R18 including all the other links were determined based on prioritized and non-prioritized packets within a single /double link failure and multi-link failure repair paths. The results of the simulation is shown in figure 3 and figure 4.

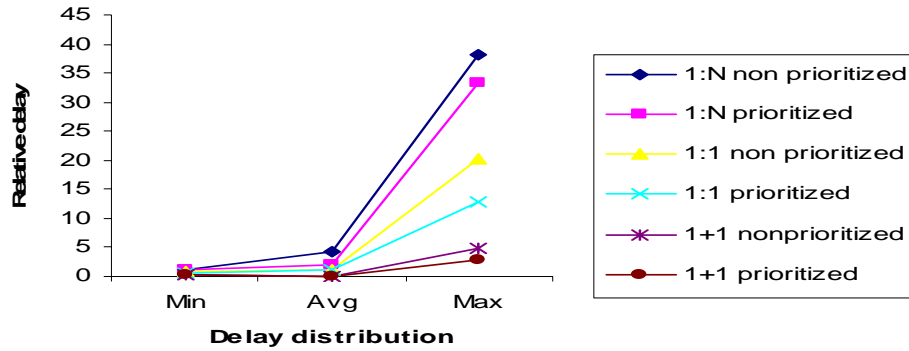


Figure 3: Delay along selected links within repair paths for single/double link failure repair path

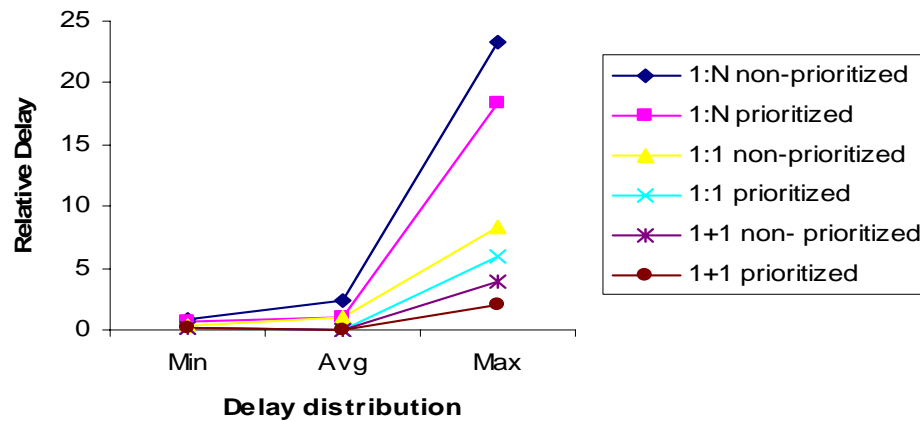


Figure 4: Delay along selected links within repair paths of a multi-link failure repair path

5. Results

The mean delays due to the movement of prioritized and non prioritized packets along the routes R12-R11,R14-R15,D6 to D9 along R10-R16-R18 and T10 to D9 along R17-R18 and all other routes with a single/double link failure and without failure were measured and compared with that of multiple link failure in the same manner. Results are illustrated in Figure 3&4.

It can be inferred from the two figures that creating multi-repair paths and prioritizing packets in the presence of redundant equipment reduces delay and increases throughput better than in a single/double repair paths as illustrated in Figure 4. In this case the delays at the ingress/egress LSPs were low in the decreasing in the order of 1:N, 1:1 and 1+1 in the presence standby nodes, non-prioritized and prioritized. We also found out from our analysis that there was a slight increase in delay in the presence of the redundant nodes as each added equipment was expected to add a fraction of delay (internal delay due processing within an added equipment) to the overall delay. There will still be some setbacks when transmitting Voice, Video and Data as the quality of service will be compromised in the case of voice when the delay at the ingress/egress LSPs/Node is high as a result of interference from numerous remote signals.

6. Conclusion

It is apparent that reliability and stability of router hardware and software are absolutely crucial for building reliable and available IP/MPLS networks in which case preventing the occurrence of a network breakdown is better than repairing a break down.

In general, to offer network services securely and reliably, security and fault-tolerance mechanisms must be built in to IP and MPLS networks. Examples of common defensive techniques against network security threats include data encryption, authentication, packet filtering, firewalls, separation of control and forwarding planes, intrusion detection and intrusion prevention can be put in place to prevent any network breakdown. This paper has analyzed the importance of link failure repairs, the need to prioritized data packets involving voice, video, data (when all three are being transmitted through a single medium) and the use of redundant components as a means to increase the quality of service of a network.

References

- [1] Perkins, C., "Mobile Networking through Mobile IP", IEEE Internet Computing, Vol. 2(1), 1998, pp. 58-69
- [2] Saleh, A., "Mobile IP Performance and Internetworking Architecture in 802.11", 2nd Annual Conference on Communication Networks and Services Research, 19-21 May 2004, pp.75-79
- [3] Marzo, J.L., Calle, E., Anjali, T., "Adding Quality of Service Protection in order to Enhance MPLS Quality of Service Routing", IEEE International Conference on Communications, 11-15 May 2003, Vol. 3, pp. 1973-1977
- [4] Heavy Reading Analysts, "2004 Survey of Carrier Attitudes Toward IP/MPLS Backbones and VPNs," Heavy Reading Report, Vol. 2(4), 2004.
- [5] Nelakuditi, S., Zhang, Z.L., Tsang, R.P., "Adaptive Proportional Routing: A localized QoS routing approach.", IEEE/ACM Transactions on Networking, Vol. 10(6), 2002, pp. 790-804
- [6] Ahuja, A., F. Jahanian, C. Labovitz, "Experimental Study of Internet Stability and Wide-Area Backbone Failures", 29th International Symposium on Fault-Tolerant Computing, June 1999.
- [7] Kodialam, M., Lakshman, T.V., "A Minimum Interference Routing with application to MPLS traffic Engineering", 19th Annual Joint Conference of the IEEE Computer and Communications Societies, Tel-Aviv, Israel, March 2002, Vol.2, pp. 884-893
- [8] Fang, L., "Security Framework for Provider Provisioned Virtual Private Networks", IETF work in progress, July 2004.
- [9] Akar, N., Atik, M., Karasan, E., "A Re-ordering-free Multi-path Traffic Engineering Architecture for Diffserv MPLS Networks", 3rd IEEE Workshop on IP Operations and Management, 1-3 Oct. 2003, pp. 107-113