International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in

Vol.3., Issue.4., 2015
(July-Aug)

REVIEW ARTICLE

ISSN: 2321-7758

A SURVEY ON MULTIPLE ROUTING CONFIGURATIONS AGAINST NODE AND LINK FAILURES

SAMIKSHA CHATARE[1], RAVE SINGH PIPPAL[2]

[1]Department of computer science and technology, Radharaman College of Engineering, Bhopal

[2]Department of computer science and technology, Radharaman College of Engineering, Bhopal

ABSTRACT

As the Internet takes an increasingly central role in our communications infrastructure; the slow convergence of routing protocols after a network failure becomes a growing problem. Internet plays a vital role in our day to day activities such as online banking, online shopping, online transactions and some other type of communications infrastructure; due to slow convergence of routing protocols after network failure becomes the massive problem for communication network. A recovery technique name Multiple Routing Configurations (MRC) is used to guarantee fast recovery from link and node failure in networks. In the communication network if the communication is done from the different nodes to transfer the data from source node to destination node, if the communication nodes are damaged or the communication link is broken due to some interference, then network stop and data may lost in this process. So recovery of the data from the network and keep the network functional even if the nodes in the network are failed is the most important for the communication network. So in this paper a detail review on multiple routing configurations (MRC) is done.

Key Words— Multiple Routing Configuration (MRC), Re-convergence, Routing Instability, Proactive Mechanism, Failure Recovery.

I.INTRODUCTION

In last few decades the Internet has been transformed from a special purpose network to a ubiquitous platform for a wide range of applications used for communication. In last decade availability and reliability of the internet have been increased very rapidly. If the node in the communication networks are failed or like is broken it will affect hundreds of thousands of TCP connections or phone conversations, with obvious adverse effects. The ability to recover from failures has always been a central design goal in the Internet. IP networks are automatically robust, since IGP routing protocols like OSPF are designed to update the forwarding information based on the changed topology after a failure [1].

This re-convergence assumes full distribution of the new link state to all routers in the network domain. When the new state information distrusted over the network, every router on the network calculates new valid routing tables. This network-wide

IP re-convergence is a very lengthy process and required large time node failure is followed by a period of routing by making it

frequently occurred. To optimize the convergence of IP routing many different efforts are developed, i.e., detection of non functional nodes, dissemination of information and shortest path calculation, but time required for convergence is still more for applications with real time requirements. The main problem is instable. At this time, data packets may be dropped due to invalid routes in the network. This concept is studied in both IGP and BGP context, and has an adverse effect on real-time applications. Events leading to a re-convergence have been that since most network failures very short, it occurs very fast and because of this re-convergence process can cause route flapping and increased network instability [1].

Multiple Routing Configurations is a proactive and local protection mechanism that allows recovery in the range of in very short time. Multiple Routing Configurations allows packet forwarding to continue over preconfigured alternative next-hops immediately by detecting failure in the system. MCR can be very effectively used against network failures. In this process the normal IP convergence process can be put on hold till system recover. Because no re-routing is performed, fast failure detection mechanisms like fast hellos or hardware alerts can be used to trigger MRC without compromising network stability [3]. Recovery from any single node or link failure is guaranteed by MRC, which constitutes a large majority of the failures experienced in a network. MRC makes no assumptions with respect to the root cause of failure, e.g., if the packet transferring is disrupted due to a failed link or a failed router.

Multiple Routing Configurations [MRC] [2] is a proactive and local protection mechanism that allows fast and good recovery from failure. The shifting of recovered traffic to the alternative link may lead to congestion and packet loss in parts of the network [4]. Ideally, a proactive recovery scheme should not only guarantee connectivity after a failure, but also do so in a manner that does not cause an unacceptable load distribution. This requirement has been noted as being one of the principal challenges for pre-calculated IP recovery schemes [5]. MRC is a proactive routing mechanism, and it improves the fastness of the routing but it does not protect network from multiple failures. It can protect only from the single link/node failures.

The main idea of MRC is to use the network graph and the associated link weights to produce a small set of backup network configurations. MRC assumes that the network uses shortest path routing and destination based hop-by-hop forwarding. The shifting of traffic to links bypassing the failure can lead to congestion and packet loss in parts of the network. This limits the time that the proactive recovery scheme can be used to forward traffic before the global routing protocol is informed about the failure, and hence reduces the chance that a transient failure can be handled without a full global routing re-convergence.

In this paper we are going to review the work done by different authors to improve the multiple routing configurations. The structure of the paper is as follows: Section I gives the brief introduction about the MRC and how it will implemented in the communication networks to recover the failure of the network. Section II gives the literature review. In this section we study the work done by different authors in the field of MRC. Section III giver the brief over view about the MRC and finally section IV and section V gives the conclusion and future work respectively.

II. RELATED WORK

Each IP router normally maintains a primary forwarding port for a destination (prefix). When a failure occurs, some of the primary ports could point to the damaged link/node and become unusable. The idea of IPFRR is to proactively calculate backup ports that can be used to replace primary ports temporarily until the subsequent route recalculation is completed. Figure 1 shows an example with node 1 as the A simple scheme related to IPFRR is equal cost multi-paths (ECMP), where a number of paths with the same cost are calculated for each source/destination pair [6]. The failure on a particular path can be handled by sending packets along an alternate path. This approach has been implemented in practical networks.

However, an equal cost path may not exist in certain situations (such as in a ring), thus ECMP cannot guarantee 100% failure recovery [7]. The condition ensures that packets do not loop back to *S*. Similar to ECMP; this scheme does not guarantee 100% failure recovery since a node may not have such a neighbor. In [8], a scheme is proposed to set up a tunnel from node *S* to node *Y* that is multiple hops away. The alternate path to a destination D is from S to Y then to D. This guarantees 100% failure coverage. The extra cost is the maintenance of many tunnels and potential fragmentation when the IP packet after encapsulation is longer than the maximum transmission unit (MTU) [9]. Removing any of these links forces the packets to go back to *S*. Therefore, the failure of any key links can be inferred by *S* at a deflected packet. To provide an alternate path, FIR removes the key links and runs shortest path routing from *S* to *D*. FIR also supports ECMP. Our scheme and FIR share similar ideas. The difference is: we develop a different algorithm that does not have any assumptions on the primary paths (E.g., the primary paths can be either shortest or non-shortest); and our algorithm supports generic multi-path routing where the paths could have different costs.

Author Mohamed AEL-Seraty and Ahmed M Elsayed [10] proposed a use of multiple routing configurations (MRC) IP fast reroute recovery process for the datacenter disaster recovery. In this paper author shows how the recovery scheme can be used to recover the data from the datacenter. In this paper author implemented a new technique that's uses unequal weight load balance inside open shortest path first (OSPF) and it is used with MRC. This technique achieves good load distribution.

Author Gowthan Gajala presented a paper on "Multiple Routing Configuration in Fast IP Network Recovery" [1]. In this paper proposed scheme guarantees recovery in all single failure scenarios in the communication network, using a single mechanism to handle both node and link failures. MRC is many used as connectionless network, and assumes only destination based hop-by-hop forwarding. MRC is based on keeping additional routing information in the every router in the network, because of this it allows packet forwarding to continue on an alternative output link immediately ones the failure is detected. With some minor changes it can be implemented to existing solutions. In this paper author present multiple routing configurations architecture, and analyze its performance with respect to backup path lengths, scalability, performance and load distribution after a failure. Author also shows how an estimate of the traffic demands in the network can be used to improve the distribution of the load traffic, and when MRC is used it reduce the chances of congestion.

With MRC, the link weights are set individually in each backup configuration. It provides more flexibility with to recovered traffic from the route and how it mange. The backup configuration used after a failure is selected based on the failure instance, and thus can choose link weights in the backup configurations that are well suited for only a subset of failure instances. MRC is based on providing the routers with additional routing configurations, allowing them to forward packets along routes that avoid a failed component. MRC guarantees recovery from any single node or link failure in an arbitrary bi-connected network.

Another author T. K. Rajesh presents a paper "Fast IP Network using MRC" [11]. In the proposed method author present a new scheme for handling link and node failures in IP networks. MRC is based on providing the routers with additional routing configurations, allowing them to forward packets along routes that avoid a failed component. MRC guarantees recovery from any single node or link failure in an arbitrary bi-connected network. By calculating backup configurations in advance, and operating based on locally available information only, MRC can act promptly after failure discovery. MRC operates without knowing the root cause of failure, i.e., whether the forwarding disruption is caused by a node or link failure. This is achieved by using careful link weight assignment according to the rules we have described. The link weight assignment rules also provide basis for the specification of a forwarding procedure that successfully solves the last hop problem [11].

Author Pondugala Bhaskar Rao presented a new recovery scheme for fast IP networks to handle both link and node failure [12]. According to author if IP to become a full-fledged carrier grade transport technology in the communication network a native IP failure-recovery scheme is necessary that can correct failures in the order of milliseconds. The proposed method in this paper IP Fast Reroute (IPFRR) intends to provide fast, fill this gap, local and proactive handling of failures right in the IP layer of communication network. Building on extensive measurement and experiences results collected with a prototype implementation of the proposed technique by author, not-via, in this paper author identify high address management burden and computational complexity as the major causes of why commercial IPFRR deployment still lags behind. MRC guarantees recovery from any single node or link failure in an arbitrary bi-connected network. By calculating backup configurations in advance, and operating based on locally available information only, MRC can act promptly after failure discovery.MRC operates without knowing the root cause of failure, i.e., whether the forwarding disruption is caused by a node or link failure. This is achieved by using careful link weight assignment according to the rules we have described. The link weight assignment rules also provide basis for the specification of a forwarding procedure that successfully solves the last hop problem. The performance of the algorithm and the forwarding mechanism has been evaluated using simulations. We Have shown that MRC scales well: 3 or 4 backup configurations are typically enough to isolate all links and nodes in our test topologies.

III. MRC OVERVIEW

MRC is based on constructing a small set of back-up routing configurations that are used to route recovered traffic on alternate paths after a failure. The backup routing configurations differs from the normal routing configuration in which link weights are set so as to avoid routing traffic in certain parts of the network. We examine that if all links attached to a node are given sufficiently high link weights, traffic will never be routed through the particular node. The failure of that node will affect traffic that is sourced at or destined for the node itself. Similarly, to eliminate a link (or a group of links) from taking part in the routing, we assign it infinite weight. The link can then fail out without any consequences for the traffic. Our approach (MRC) is Threefold. First we create a set of backup configurations, so that every network component is isolated in one configuration. Second, for each configuration, a standard routing algorithm like OSPF is used to calculate configuration specific shortest path trees and create forwarding tables in each router, based on the configurations. The use of a standard routing algorithm guarantees loop free forwarding within one configuration. Finally, we design a forwarding process that takes advantage of the backup configurations to provide fast recovery from a component failure [11] [12].

In basic system the backup configurations such that for all links and nodes in the network, there is a configuration where that link or node is not used to forward traffic. Thus, for any single node or link failure, there will exist a configuration that will route the traffic to its destination on a route that avoids the failed element. Also, the backup configurations must be created so that all nodes are accessible in all configurations, i.e., there is a valid path with a finite cost between each node pair. Using a specific shortest path calculation, each router generates a set of configuration-specific forwarding tables. For the ease of, so that a packet is forwarded according to a routing configuration, meaning that it is forwarded using the forwarding table calculated based on that configuration. In this paper we have a separate forwarding table for each configuration, but more proficient solutions can be found in a practical implementation. It is important to note that MRC does not affect the failure-free original routing, i.e., when there is no failure, all packets are forwarded according to the original configuration, where all link weights are normal. On the detection of a failure, only traffic reaching the failure will change configuration. All other traffic is forwarded according to the original configuration as usual.

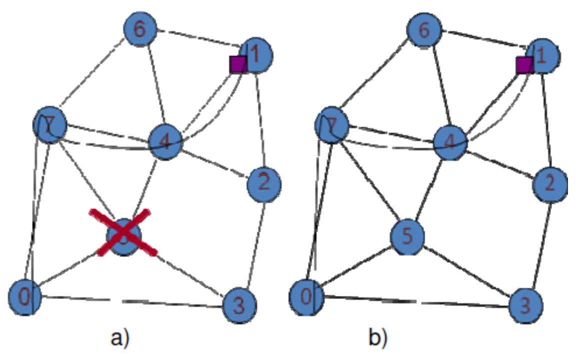

Figure 1 Selection of routes in MRC a) At the time of failure occurrence in MRC b) After the failure recovery in MRC [12].

Figure 1 shows the simple route selection schema used for the different conditions. Figure 1 (a) shows the selection of routes at the time of failure occurrence in MRC and figure 1 (b) shows the selection of routes at the time.

IV. CONCLUSION

In this paper we try to attempt the review a significant number of papers to cover the recent development in the field of Multiple Routing Configuration (MRC). Present study reveals that various author proposed different methods to improve the multiple routing configuration technique. This paper also reviews the basic multiple routing configuration concept. The list of references to provide more detailed understanding of the approaches described is enlisted. Apologize to all the researchers whose important contributions may have been overlooked.

V. FUTURE WORK

In the paper the analytic review on the different Multiple Routing Configuration technique used to recover the failure in the communication network is done. In future work we are going to implement Multiple Routing Protocol to recover the route of the communication in case of failure in the network.

REFERENCES

[1]. Gowtham Gajala, Nagavarapu Sateesh, "Multiple Routing Configurations for Fast IP Network Recovery" at international Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 4, April 2013.

[2]. A. F. Hansen, T. Cicic, S. Gjessing, A. Kvalbein, and O. Lysne. (April 2009). "Multiple Routing Configurations For Fast IP Network Recovery," IEEE/ACM Trans. Netw. 17(2), pp. 473-486. DOI=10.1109/TNET.2008.926507. [June. 25, 2010]

[3]. S. Nelakuditi, S. Lee, Y. Yu, Z.-L. Zhang, and C.-N. Chuah. (April 2007). "Fast local rerouting for handling transient link failures," IEEE/ACM Trans. Netw. 15(2), pp. 359-372. DOI=10.1109/TNET.2007.892851. [Aug. 25, 2010]

[4]. S. Ayer, S. Bhattacharyya, N. Taft, and C. Diot. "An approach to alleviate link overload as observed on an IP backbone." in Proc. IEEE INFOCOM, 2003, pp. 406–416.

[5]. S. Rai, B. Mukherjee, and O. Deshpande. (Oct. 2005). "IP resilience within an autonomous system: Current approaches, challenges, and future directions." IEEE Commun. Mag. 43(10), pp. 142–149.

[6]. Markopoulou.A G. Iannaccone, Bhattacharyya, C.-N. Chuah, and C. Diot, "Characterization of failures in an IP backbone network," in Proceedings INFOCOM, Mar. 2004.

[7]. S. Gjessing, A. Kvalbein, and O. Lysne. (April 2006). "Multiple Routing Configurations For Fast IP Network Recovery," IEEE/ACM Trans. Netw. 17(2), pp. 473-48.

[8]. Przygienda.T N. Shen, and N. Sheth, "M-ISIS: Multi topology (MT) routing in IS-IS," Internet Draft (work in progress), Oct. 2005, draft iet f-isis-wg-lti-topology-11.txt.

[9]. Rai.S, B. Mukherjee, and O. Deshpande, "IP resilience within an autonomous system: Current oaches, challenges, and future directions," IEEE Communications Magazine, vol. 43, no. 10, pp. 142–149, Oct. 2005.

[10]. Mohamed AEL-Seraty and Ahmed M Elsayed, "Multiple Routing Configurations for Datacenters Disaster Recovery Applicability and Challenges" at IEEE 5th international conference on computer & communication engineering, 2014.

[11]. T.K Rajesh, N. Sreenivasulu, K.V.Ragavender, "Fast IP Network Recovery using MRC" at international Journal of Research in Computer Science ISSN 2249-8257 Volume 1 Issue 1 (2011) pp. 75-88.

[12]. Pondugala.Bhaskar Rao, U. Nanaji,"A New Recovery Scheme for Handling Both Link And Node Failure in The Fast IP Networks" at International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622, Vol. 2, Issue 1, Jan-Feb 2012, pp.108-113.