ISSN:0975-9646
Aditi Thakkar / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (6) , 2014, 8221-8224

# Multiple Routing Configurations for Fast IP Network Recovery

Aditi Thakkar

*Department of Computer Engineering*
*MCT's Rajiv Gandhi Institute Of Technology*
*Andheri(W), Mumbai-53, India.*

***Abstract*— Internet has become the nerve centre of today's age. Be it online transactions, online shopping, or other related applications, internet plays a vital role. But there exists a problem of slow convergence of routing protocols after a network failure, which gives slow reaction and fosters instability. Thus to ensure fast recovery from link and node failures in IP networks, this paper presents a recovery scheme called Multiple Routing Configurations (MRC). The proposed scheme guarantees recovery in all single failure scenarios, using a single mechanism to handle both link and node failures, and without knowing the root cause of the failure. MRC is strictly connectionless, and assumes only destination based hop-by-hop forwarding. MRC is based on keeping additional routing information in the routers, and allows packet forwarding to continue on an alternative output link immediately after the detection of a failure.**

*Keywords*— **MRC, internet, single and multiple link failures.**

## I. INTRODUCTION

**T**he ever-increasing demand on the Internet is because it is transformed from a special purpose network to a common platform for many online services such as online transactions, entertainment and for other e-commerce applications. Internet suffers from slow convergence of routing protocols after a network failure. The central goal in the Internet is the ability to recover from failures. Generally in IP networks, when a node/link failure occurs, the IGP routing protocols like OSPF are used to update the forwarding information based on the changed topology and the updated information is distributed to all routers in the network domain and each router individually calculates new valid routing tables. This network-wide IP re-convergence is a time consuming process, and a link or node failure is typically followed by a period of routing instability, which can result into dropping of packets due to invalid routes. This phenomenon has been studied in both IGP and BGP context , and has adverse effects on real-time applications.

Many attempts have been made for optimizing the different steps of the convergence of IP routing, i.e., detection, dissemination of information and shortest path calculation. But still the convergence time is still too large for applications with real time demands.

Moreover, the IGP convergence process is slow because it is reactive and global, i.e., it reacts to a failure after it has occurred, and it involves all the routers in the domain. In this paper we present a scheme for handling single link and node failures in IP networks. Multiple Routing Configurations (MRC) is a proactive and local. This protection mechanism allows recovery in the range of milliseconds. This approach of MRC can be used as a first line of defence against network failures, with which the normal IP convergence process can be put on hold. This process is then initiated only as a consequence of non-transient failures. Since no global re-routing is performed, fast failure detection mechanisms like fast hellos or hardware alerts can be used to trigger MRC without compromising network stability. MRC guarantees recovery from any single link or node failure, 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., whether the packet forwarding is disrupted due to a failed link or a failed router.

## II. LITERATURE SURVEY

The Internet has seen tremendous growth in the past decade and has now become the critical information infrastructure for both personal and business applications. It is expected to be always available as it is essential to our daily commercial, social and

cultural activities. Service disruption for even a short duration could be catastrophic in the world of ecommerce, causing economic damage as well as tarnishing the reputation of a network service provider. In addition, many emerging services such as Voice over IP and virtual private networks for finance and other real-time business applications require stringent service availability and reliability. Unfortunately, failures are fairly common in the everyday operation of a network due to various causes such as link failures etc.

The main idea of MRC is to create a small set of backup network configurations using the network graph and the associated link weights. The link weights in these backup configurations are manipulated so that the node that detects the failure can safely forward the incoming packets towards the destination on an alternate link. 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. 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 precalculated IP recovery schemes. The link weights, in case of MRC are set individually in each backup configuration.This gives great flexibility with respect to how the recovered traffic is routed.

The backup configuration used after a failure is selected based on the failure instance, and thus we can choose link weights in the backup configurations that are well suited for only a subset of failure instances.

## III. COMPARITIVE STUDY

| Sr. No | Papers | Concept Used | Detection Type | Publication Year | Resources |
|---|---|---|---|---|---|
| 1 | Multiple Routing Configurations for Fast IP Network Recovery | MRC | Single Node/Link Failures | 2009 | IEEE |
| 2 | Fast recovery from dual-link or single-node failures in IP networks using tunneling | IP Tunneling | Upto dual node/link failures | 2010 | ACM |
| 3 | Fast IP Network Recovery using MRC | MRC | Single Node/Link Failures | 2011 | IJORCS |
| 4 | Enhanced Multiple Routing Configuration For Fast IP Network Recovery From Multiple Failures | EMRC | Multiple link failures | 2011 | IJCN |
| 5 | Fast and Efficient IP Network Recovery using Multiple Routing Configuration | MRC | Single Node/Link Failures | 2012 | IJCTA |

## IV. MRC OVERVIEW & BACKUP MECHANISM

MRC is based on building a small set of backup routing configurations that are used to route recovered traffic on alternate paths after a failure. The backup configurations differ from the normal routing configuration in that link weights are set so as to avoid routing traffic in certain parts of the network. We observe that if all links attached to a node are given sufficiently high link weights, traffic will never be routed through that node. The failure of that node will then only affect traffic that is sourced at or destined for the node itself. Similarly, to exclude a link (or a group of links) from taking part in the routing, we give it infinite weight. The link can then fail without any consequences for the traffic.

This MRC approach is threefold. First, we create a set of backup configurations, so that every network component is excluded from packet forwarding in one configuration. Second, for each configuration, a standard routing algorithm like OSPF is used to calculate configuration specific shortest paths 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.

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. The link weights in these backup configurations are manipulated so that for each link and node failure, and regard less of whether it is a link or node failure, the node that detects the failure can safely forward the incoming packets towards the destination on an alternate link. MRC assumes that the network uses shortest path routing and destination based hop-by-hop forwarding. It is important to stress 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. Upon detection of a failure, only traffic reaching the failure will switch configuration. All other traffic is forwarded according to the original configuration as normal. If a failure lasts for more than a specified time interval, a normal re-convergence will be triggered. MRC does not interfere with this convergence process, or make it longer than normal. However, MRC gives continuous packet forwarding during the convergence, and hence makes it easier to use mechanisms that prevent micro-loops during convergence, at the cost of longer convergence times. If a failure is deemed permanent, new configurations must be generated based on the altered topology.

### 1. *A. Normal Configuration*

In Normal Configuration Packet is forwarded according to configuration, i.e. packet is forwarded using the forwarding

table. In this process routers are selected randomly and packets are reached to the destination.

### 2. *B. Router Recovery*

When we send the packet from source to destination if one of router get down, then packet will not reach to destination. In order to avoid to this situation we have a mechanism that is router recovery, in our MRC router will recover back in milliseconds.

### 3. *C. Backup Configuration*

When a router detects that a neighbour can no longer be reached through one of its interfaces, it does not immediately inform the rest of the network about the connectivity failure. Instead, packets that would normally be forwarded over the failed interface are marked as belonging to a backup configuration, and forwarded on an alternative interface towards its destination. This process is

called backup configuration. The number and internal structure of backup configurations in a complete set for a given topology may vary depending on the construction model.

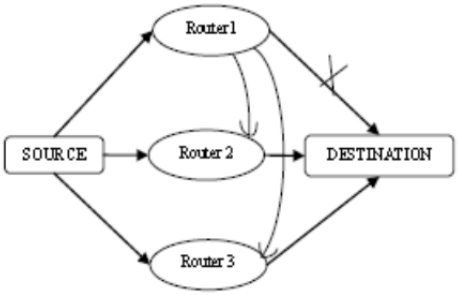


Fig. 1

If more configurations are created, fewer links and nodes need to be isolated per configuration, giving a richer (more connected) backbone in each configuration. On the other hand, if fewer configurations are constructed, the state requirement for the backup routing information storage is reduced. However, calculating the minimum number of configurations for a given topology graph is computationally demanding. One solution would be to find all valid configurations for the input consisting of the topology graph G and its associated normal link weights w0, and then find the complete set of configurations with lowest cardinality. Finding this set would involve solving the Set Cover problem, which is known to be NP-complete. Instead we present a heuristic algorithm that attempts to make all nodes and links in an arbitrary bi-connected topology isolated.

Our algorithm takes as input the directed graph G and the number n of backup configurations that is intended created. If the algorithm terminates successfully, its output is a complete set of valid backup configurations. The algorithm is agnostic to the original link weights w0, and assigns new link weights only to restricted and isolated links in the backup configurations. For a sufficiently high, the algorithm will always terminate successfully. This algorithm isolates all nodes in the network, and hence requires a bi-connected as input. Topologies where the failure of a single node disconnects the network can be processed by simply ignoring such nodes, which are then left unprotected.

### *4. D. Load Distribution*

Whenever there is a heavy traffic (load) on the links or on routers traffic is shifted to alternate links or routers so as to avoid the congestion. This process is called load distribution. Time consumption to send a message to the destination through single router which uses a single channel is more. Load distribution reduces the time consumption. Here, load distribution delivers the data such that the data is shared among the routers.

*Algorithm :* Load Distribution.
i← ith router failed
Ri← Router failed // for all i Є N
if (Ri failed) {
if (Load distribution) {
divide Msg into n-1 parts such that
Msgtotal=Msg1+Msg2+ . . . +Msgn-1
}
for (i =0; i<n-1; i++) {
end Msgi through Ri
}
}

The requirements that must be put on the backup configurations used in MRC, we propose an algorithm that can be used to automatically create such configurations. The algorithm will typically be run once at the initial start-up ofthe network, and each time a node or link is permanently added or removed. The backup configurations so 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 link or node failure, there will exist a configuration that will route the traffic to its destination on a path that avoids the failed element. Also, the backup configurations must be constructed so that all nodes are reachable in all configurations, i.e., there is a valid path with a finite cost between each node pair. Shared Risk Groups can also be protected, by regarding such a group as a single component that must be avoided in a particular configuration.

## V. PERFORMANCE EVALUATION

MRC requires the routers to store additional routing configurations. The amount of state required in the routers is related to the number of such backup configurations. Since routing in a backup configuration is restricted, MRC will potentially give backup paths that are longer than the optimal paths. Longer backup paths will affect the total network load and also the end-to-end delay.

Full, global IGP re-convergence determines shortest paths in the network without the failed component.Here performance is used as a reference point and evaluate how closely MRC can approach it. It must be noted that MRC yields the shown performance immediately after a failure, while IP re-convergence can take seconds to complete.

## VI. CONCLUSION & FUTURE ENHANCEMENT

Multiple Routing Configurations as an approach to achieve fast recovery in IP networks. 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. With MRC, the link weights are set individually in each backup configuration. This gives great flexibility with respect to how the recovered traffic is routed.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 provides basis for the specification of a forwarding procedure that successfully solves the last hop problem. MRC thus achieves fast recovery with a very limited performance penalty.

MRC is a proactive routing mechanism, and it improves the fastness of the routing but it does not protect network from multiple failures. But it can protect only from the single link/node failures. Hence, future research can be carried out to generate Enhanced Multiple Routing Configurations for fast multiple nodes/links failure recovery.

## REFERENCES


[1] D. D. Clark, "The design philosophy of theDARPAinternet protocols," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 18, no. 4, pp. 106–114, Aug. 1988.

[2] A. Basu and J. G. Riecke, "Stability issues in OSPF routing," in *Proc. ACM SIGCOMM*, San Diego, CA, Aug. 2001, pp. 225–236.S. Zhang, C. Zhu, J. K. O. Sin, and P. K. T. Mok, "A novel ultrathin elevated channel low-temperature poly-Si TFT," *IEEE Electron Device Lett.*, vol. 20, pp. 569–571, Nov. 1999.

[3] C. Labovitz, A. Ahuja, A. Bose, and F. Jahanian, "Delayed internet routing convergence," *IEEE/ACM Trans. Networking*, vol. 9, no. 3, pp. 293–306, Jun. 2001.

[4] C. Boutremans, G. Iannaccone, and C. Diot, "Impact of link failures on VoIP performance," in *Proc. Int. Workshop on Network and Operating System Support for Digital Audio and Video*, 2002, pp. 63–71.

[5] D.Watson, F. Jahanian, and C. Labovitz, "Experiences with monitoring OSPF on a regional service provider network," in *Proc. 23rd Int. Conf. Distributed Computing Systems (ICDCS'03)*, Washington, DC, 2003,

[6] P. Francois, C. Filsfils, J. Evans, and O. Bonaventure, "Achieving sub-second IGP convergence in large IP networks," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 35, no. 2, pp. 35–44, Jul. 2005.

[7] A. Markopoulou, G. Iannaccone, S. Bhattacharyya, C.-N. Chuah, and C. Diot, "Characterization of failures in an IP backbone network," in *Proc. IEEE INFOCOM*, Mar. 2004, vol. 4, pp. 2307–2317.

[8] S Nelakuditi, S. Lee, Y. Yu, Z.-L. Zhang, and C.-N. Chuah, "Fast local rerouting for handling transient link failures," *IEEE/ACM Trans. Networking*, vol. 15, no. 2, pp. 359–372, Apr. 2007.

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

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

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