A Study of Path Protection in Self-Healing Routing*

Qi Li, Mingwei Xu, Lingtao Pan, and Yong Cui

Department of Computer Science, Tsinghua University, Beijing 100084, China
Tsinghua National Laboratory for Information Science and Technology, Beijing 100084, China
{liqi,xmw,plt,cy}@csnet1.cs.tsinghua.edu.cn

Abstract. Recent routing failure accidents show that routing systems are not so stable as we estimated because most of accidents caused packet delivery failure in Internet. In order to resolve this problem, many fast reroute solutions are proposed to guarantee reroute path provision after network failures without high packet loss. However, most of these solutions are not deployed in practice, and some key issues still need further consideration, such as the route loop issue and the deployment cost issue. In this paper, we present state machine models to analyze how path protection works in self-healing routing solutions and identify the drawbacks in traditional path protection approaches. We identify several requirements of path protection approaches, and present principles of our path protection approach to protect Internet routing based on our analysis result. Furthermore, we conduct a detailed study to measure our proposed path protection approach in production networks and the study shows that availability and stability of routing systems is improved in real production networks.

1 Introduction

Internet Routing is a critical element as Internet infrastructure and plays a key role in packet delivery in Internet. However, we know that they are not so robust to defend against network failures/attacks. For instance, Cisco routers caused major outage in Japan in 2007 and Earthquake in Taiwan caused global network accidents in 2006. The main failure causes, such as route/link damage, buggy software update and router configuration errors, may be the origins of these Internet accidents. Some study shows that most of these Internet instability accidents are resulted from short term failures [5]. However, current routing systems fails to adapt these network accidents. For example, to defend against short term failures, RIP requires hundreds of seconds, OSPF requires tens of seconds and BGP requires several minutes or longer. Obviously, these protocols are not stable and available enough for packet delivery requirements when network failures happen in Internet.

Several researches are conducted to investigate Internet routing convergence and fast reroute issues to address the routing problem caused by network failures. Fast routing convergence is a classical problem well addressed in literature [1,3]. Although these approaches are carried out to fast routing convergence, they are not deployed in real

* This work is supported by the Natural Science Foundation of China (No. 90604024),the Key Project of Chinese Ministry of Education (No. 106012), NCET and HI-Tech Research and Development Program of China (863) (2007AA01Z2A2).

A. Das et al. (Eds.): NETWORKING 2008, LNCS 4982, pp. 554–561, 2008.

production networks because of their complexity to adopt, design fault or something else. Moreover, these work can not ensure low packet loss and guarantee successful packet delivery to destination after network failures. Another line of self-healing routing work is to implement some fast reroute approaches which are active activities in IETF [7,2]. However, these proposed fast reroute schemes share some big drawbacks, such as hard deployment and management, and not good enough performance.

In this paper, we analyze the problem of Internet routing and identify the effect and efficiency of path protection in protecting network failures including short term and long term failures. As we analyzed, traditional path protection approaches proposed in IETF are not stable enough, we propose an improved path protection solution. In our solution, the L2TP technology is used to provide path protection which overcomes the shortcomings in traditional approaches. As we mentioned above, short term failures are the main cause of Internet instability, our solution can directly recover from these failures. Besides, our path protection approach can mitigate performance impact posed by the routing convergence process if long term network failures happen. Therefore, our path protection solution well resolve the Internet availability and stability problem.

The paper is organized as follows. Section 2 introduces Internet Routing Failures and describe several solution to address path protection issues in routing. State machine models are proposed to analyze self-healing routing process after network failure in Section 3. We identify several requirements of path protection in self-healing routing and propose our path protection solution to defend against network failure in Section 4. Section 5 presents the conclusion of this paper.

2 Internet Routing Failures and Path Protection

Several studies have analyzed that routing instability and impact of routing failures in Internet. Those studies found three important results [5]. First, routing protocols can efficiently handle common events of link failures. Second, a small number of links are responsible for a large fraction of the failures in Internet. This is the common but troublesome problem of flapping links. Third, link failures are usually short-term events except some big network accidents, such as the Taiwan earthquake, and they caused major events of routing failures.

We need to consider two properties when measuring Internet routing, availability and stability. Availability refers to the ability of routing system to work for normal packet delivery no matter network failures happen. Stability refers to routing dynamic of routing system no matter network failures happen. However, current routing systems perform poorly in these two aspects. Actually, routing divergence also happens because of configuration errors and other factors besides the large routing convergence delay problems. Although some improved routing schemes can improve routing convergence, they can not guarantee fast routing convergence and eliminate the routing divergence problem. So, these cause poor availability of routing systems and flapping routes cause poor stability of routing systems. In order to address routing slow convergence or divergence problems after network failures, many path protection solutions are proposed. We describe these approaches and identify the drawbacks of these approaches.

SONET rings can significantly reduce the recovery time by switching around the failure, but they are expensive. Fast reroute (FRR) schemes are proposed to resolve this problem, in which alternate paths are set up between routers detecting failures and some intermediate routers in the paths to the destinations. In an MPLS Traffic Engineering (MPLS-TE) network, FRR pre-calculates shortest paths around individual nodes and links so that if a failure occurs, traffic can be quickly switched to the reroute path. In these approaches, route paths are promised to be built in 50 ms. FRR does not take into consideration any best-path parameters, and its reroute paths are intended only as short-term detours around a failure. O(nk) repair paths should be set up in the network for link repair and O(nk^2) repair paths for node repair. Moreover, MPLS-TE requires an MPLS infrastructure. It is feasible to implement a path protection mechanism natively in an IP infrastructure without using MPLS-TE.

Shand *et al* carry out an Internet draft of IETF for a number of years now called IP Fast Reroute Framework that proposes an FRR solution without MPLS-TE [2,7]. For operators who use MPLS only for the FRR functionality, this solution could be promising for simplifying their networks. Also, they propose several Internet drafts to implement FRR, such as FRR with IP tunnel and FRR using via address. However, it is hard to build pre-computed paths for these solution and guarantee the pre-defined paths are best paths because complete topological information are heavily relied, besides the drawbacks in the MPLS-TE approach analyzed above. In addition, route loops may happen during routing convergence in these approaches.

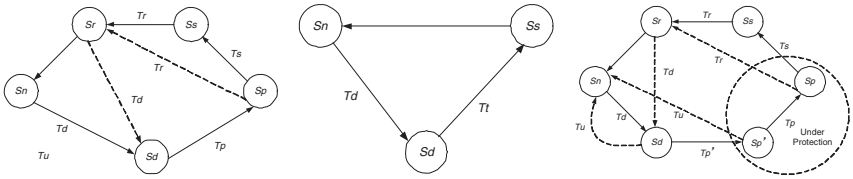
In summary, these solutions are not scale enough and may cause route loops and Internet instability even if they improve routing availability. In addition, these approaches may negatively affect traffic flows or the performance of the routing because they may not use best routing paths.

3 Self-Healing Routing

As we discussed above, most of network change events are single network failures. For simplicity, we only analyze network state using the single failure model in this section. As a standard routing convergence process illustrated in Figure 1(a), there are five states, S_n denotes a normal state of network, Sd denotes that the adjacent nodes detect the network failure, Sp denotes that the adjacent nodes finish route re-computation and propagate the update messages, Ss denotes that all the nodes finish route re-computation and the whole network stays in sub-normal status [1] and Sr denotes that network failure recovers. After a network failure event, network status will get to the state Ss via the state Sd and Sp, so Td + Tp + Ts is the routing convergence time. During the routing convergence process, packets sent through the failure node/link may be lost during Td, and our-of-order packets may appear during Tp and Ts. Moreover, during Tp and Ts, some packets may still be lost because of transient route loops. Most of fast routing convergence work is to reduce Td and optimize Tp and Ts [2]. However, these approaches can not completely resolve route divergence problem and avoid packet loss.

[1] This status is introduced to illustrate that the network convergence after network failures.

[2] Most of work do not not simple reduce Tp and Ts and it may cause route flap and route loops.



(a) Original Machine (b) Machine with FRR (c) Machine with Protection

Fig. 1. State Machine of Self-Healing Routing

In order to address these issues, fast reroute approaches are proposed. In these approaches, tunnels are used to provide fast rereoute (FRR) in which Bidirectional Forwarding Detection (BFD) mechanism is used to realize fast failure detection. Once network failure is detected, the pre-configured tunnel is activated to guarantee that packets detour the failure path and are forwarded to destination. The network state machine with FRR is showed in Figure 1(b). We see that the state machine with FRR is quite simple. The rerouting time is Td and Tt (Tt denotes the tunnel activation time). Since Tt is largely less than Tp and Ts, packet loss can be avoided (or greatly reduced) after network failures. However, some new problems rise. For instance, it is hard to avoid route loop and guarantee rerouting paths are the best available paths. So packet delivery performance may not be good enough, and these works fail to consider these problems. Furthermore, if a short term failure event happens, the tunnel will be activated to deliver the packets, and will stay in a sub-normal state and never go back to the normal state if no operators' involvement.

In this section, we present a path protection approach to resolve problems discussed above. The improved state machine with path protection is illustrated in Figure 1(c). We add a state Sp' where a tunnel is activated to hold time for short term protocol failure. During this process, low packet loss and packet delivery is guaranteed. After holding the failure in Sp', the adjacent nodes start to begin routing convergence process.Otherwise, the network directly come back to the normal state if it recovers from the short term failure. So, Sp' is only a temporal state and guarantees packet delivery to destination under the failure. That is, tunnels will be disactivated no matter whether failure link/node recovers. From this view of the point, path protection is only part of Self-Healing routing solution, because routing convergence is still necessary if the network failure is a long term event. In this way, holding network failures can effectively improve routing stability [6], and protection paths can guarantee routing availability once failure happens.

4 Path Protection in Self-Healing Routing

In this section, we study path protection to react to network failures in self-healing routing. Before that, we need to identify some key requirements of a path protection solution, and the principles of our path protection solution follow.

4.1 Requirements of Path Protection

Several approaches are proposed to protect Internet routing including intra-domain routing and inter-domain routing. However, few approaches are implemented and deployed in real Internet. Many reasons caused this situation, such as wrong (or not good enough) working motivation and design fault. In this section, we identify some key requirements of path protection should be met when designing or deploying path protection solutions based on our study of path protection approaches and the analysis of self-healing routing in Section 2and 3.

- *Simplicity.* Most of fast rerouting approaches and fast routing convergence schemes are not deployed in Internet because these scheme are too complex and put much complexity in core network. For a complex solution, there is less possibility to be deployed. The MPLS-TE approach contains this drawback.
- *Easy Deployment and Management.* The proposed self-healing routing solution should be easily deployed and managed. For instance, not all networks support MPLS, and MPLS-related solution is not feasible because this solution needs the MPLS infrastructure in Internet. In addition, since all the backup rerouting path are pre-computed, it hard for traditional FRR to react to failures using best routing paths dynamically.
- *Efficiency.* This point desires that proposed solutions should be deployed with good efficiency. From the view of efficiency, there is no need to pre-configure tunnels for every node/link. For instance, if non-backbone network resource can be used to protect these networks who are always unstable, a better Internet routing stability is achieved and performance of whole Internet will improve much.
- *Incremental Deployment Support.* It is an important factor when considering and designing a novel routing protocol, because we all can not ensure that we can deploy it once. As we discussed in the above requirements, we can protect 10% of network where network failure always happens to improve routing systems at first.
- *Business model Support.* The designed solution should consider the business model of path protection application in production networks. In order to protect unstable network and backbone network areas, contrasts between different ISPs should be signed to guarantee routing availability in these areas. Path protection solutions should not require protection contrasts for every links. Otherwise, ISPs may not consider this solution because it may release their routing privacy.
- *Low Cost.* The path protection solution should provide routes without many computation processes or additional computation power needed on routers, and provide packet delivery performance guarantee with low packet loss. In addition, the solution should covers protection under both short term or long term network failures.

4.2 Principles of Our Solution

In this section, we briefly describe the key elements of our path protection approach in self-healing routing based on some simple examples. We consider the two ISPs shown Figure 2 and focus on path protection in self-healing routing for the view of stub networks.

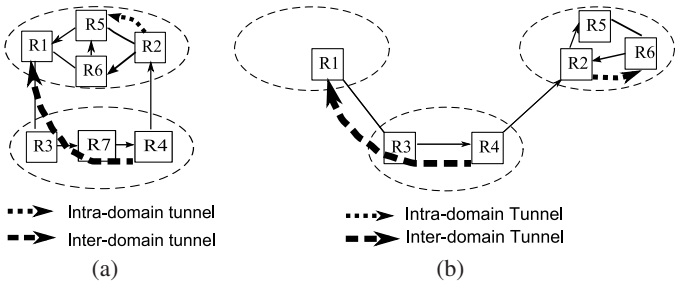


Fig. 2. Reference Network

As Figure 2 shown, two types of stub networks are multi-homed when they are attached to provider network(s). Our path protection approach works in both these two scenarios if the provider ISP has a path differentiated to the original path of stub network to destinations. To quickly react to a failure of directed link R2→R4 in Figure 2(a) and 2(b), router R4 must be able to quickly detect the failure, activate the pre-configured inter-domain tunnel and send following packets to router R1 in the provider network. At last, R1 take the responsibility to forward these packets to destinations. Similarly, in the intra-domain case, if the link R2→R6 in Figure 2(a) fails, router R2 need to activate the tunnel between router R2 and router R5, and router R5 help R2 forward packets from router R2 to destinations. In this section, we need to identify three key elements to implement path protection, fast failure detection, tunnel technique for path protection and tunnel disactivation.

- **Fast Failure Detection.** The failures of routing links are detected by using a trigger from Bidirectional Forwarding Detection (BFD) mechanism [4]. BFD runs on top of any data protocol being forwarded between two systems, and supports adaptive detection times to balance fast detection and network stability.
- **Path Protection Technique.** As explained earlier, the self-healing solution is required to allow routers to provide path protection for packets immediately if the adjacent router/link fails. For this, although two different types of routing protocol need be considered, intra-domain routing and inter-domain routing tunnel in Figure 2, there is no need for us to provide path protection techniques for different routing instances. In this paper, we choose a label-based tunnel protocol, Layer 2 Tunneling Protocol (L2TP) [8], as the protection technique in self-healing routing.
- **Tunnel Disactivation.** Since paths provided in the path protection scheme may be not best paths, path protection is only a short term solution to defend against routing failure events, and not substitution to routing convergence if long term failures happen. So, tunnels should be disactivated if the short term failure recovers or route converges again after a long term failure. In this situation, tunnel inactivation mechanism is essential to guarantee Internet availability and stability.

5 Methodology and Evaluation

In this section, we study performance of path protection in production networks and measure the basic mechanism provided in our path protection approach. In order to

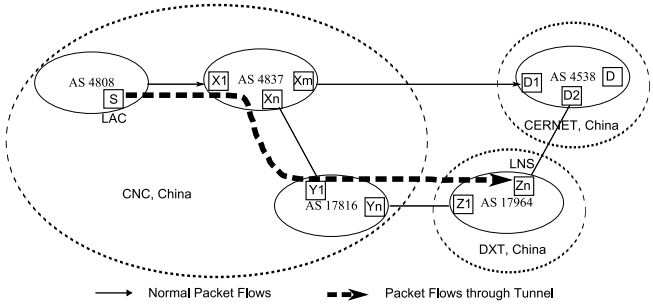
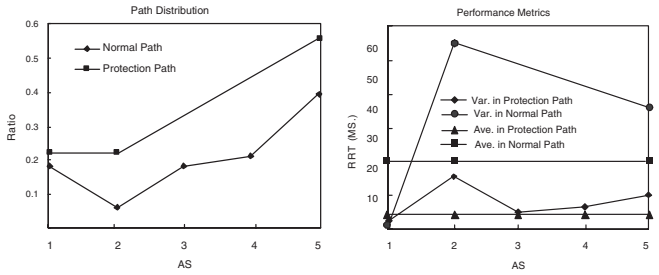


Fig. 3. BGP Peer Relationship

study performance of the path protection approach in self-healing routing, we deploy the path protection scheme in real production networks of Chinese ISPs. Since we can not change much in routing architecture in real production network in case of Internet stability, for simplicity, we deploy an experimental tunnel which covers Intra-domain routing Inter-domain routing paths to study performance of path protection and measure the performance of path granularity protection, such as routing availability and stability.

As Figure 3 illustrated, we deployed hosts at three different ASes which belong to three different ISPs. Effectively, this allowed us to build a L2TP tunnel between two different ISPs(ASes), and forward the traffic to the third ISP(AS). These ISPs and ASes at each ISP are shown in Figure 3. The idea behind the experiments was to choose a third ISP/AS to protect routing paths and measure the routing performance under path protection. Figure 3 shows one host with the AS in CNC China acting as a session initiator and another one with AS in CERNET acting as a session receiver, which form a data-plane path called the normal path. Assumed that the link Xm→D1 fails, the L2TP tunnel between AS 4808 and AS 17964 is activated to protect the assumed failure link, which is called the protection path.

The measurement methodology described above was used to study path distribution in ASes and packet forwarding performance. Figure 4(a) shows that the distribution ratio in protection path is less than 20% and path protection successfully diversifies



(a) Path Diversity (b) Performance Metric

Fig. 4. Performance Comparison

the routes which are maintained by intra-domain routing systems in ASes. Path protection can effectively guarantee availability of routing system after network failures if we suitably choose protection strategies under contracts with ISPs. For instance, the non-backbone networks are involved to protect the backbone networks in this experiment. Figure 4(b) shows that average RTT in AS 4837 is about 16ms and average RTT in the whole protection path is about 8ms, which are smaller than that in the normal routing paths because busy paths are detoured in this experiment. As can be seen, our deployed solution can effectively eliminate path re-computation and improve local routing stability if network failure events happen.

6 Conclusion and Future Work

Internet routing is a critical element in important Internet infrastructure. We have shown that current routing systems are not so stable and unable to work well under network failures. In this paper, we propose a state machine model to analyze impacts of path protection in routing, which shows that traditional path protection approaches fail to protect routing effectively. We propose a L2TP approach for path protection, which efficiently defends against network accidents no matter short term or long term failures. Moreover, we deployed our solution in real production networks to measure performance of our path protection approach. The result shows that the proposed solution provides strong protection for routing and well improves Internet stability and availability.

References

1. Afek, Y., Bremler-Barr, A., Schwarz, S.: Bgp-rcn: Improving bgp convergence through root cause notification. IEEE Journal On Selected Areas In Communications 22(10), 1933–1948 (2004)
2. Atlas, A., Zinin, A., Torvi, R., Choudhury, G., Martin, C., Imhoff, B., Fedyk, D.: Basic specification for ip fast-reroute: Loop-free alternates, Internet draft, draft-ietf-rtgwg-ipfrrspec- base-10.txt (November 2007)
3. Nguyen, N., Chen, J., Massey, D., Pei, D., Azuma, M., Zhang, L.: Bgp-rcn: Improving bgp convergence through root cause notification. Computer Network 48(2), 175–194 (2005)
4. Katz, D., Ward, D.: Bidirectional forwarding detection, March 2007. Internet draft, draft-ietf-bfd-base- 06.txt (2007)
5. Markopoulou, A., Iannaccone, G., Bhattacharyya, S., Chuah, C., Diot, C.: Characterization of failures in an ip backbone. In: Proceeding of the IEEE INFOCOM, pp. 2307–2317 (2004)
6. Nelakuditi, S., Lee, S., Yu, Y., Zhang, Z., Chuah, C.: Fast local rerouting for handling transient link failures. IEEE/ACM Transactions on Networking 15(2), 359–372 (2007)
7. Shand, M., Bryant, S.: Ip fast reroute framework, June 2007. Internet draft, draft-ietf-rtgwg-ipfrrframework- 07.txt (2007)
8. Townsley, W., Valencia, A., Rubens, A., Pall, G., Zorn, G., Palter, B.: Layer two tunneling protocol L2TP. RFC2661 (August 1999)