Achieving Fast BGP Reroute with Traffic Engineering Using Multiple Routing Planes

Yu Guo[1], Ning Wang[1], Kin-Hon Ho[1], Michael Howarth[1], and George Pavlou[2]

[1] Centre for Communication Systems Research, University of Surrey,
United Kingdom, GU2 7XH
{Y.Guo,N.Wang,K.Ho,M.Howarth}@surrey.ac.uk
[2] Networks and Services Research Lab, University College London (UCL),
United Kingdom, WC1E 7JB
G.Pavlou@ee.ucl.ac.uk

Abstract. In today's BGP routing architecture, traffic delivery is in general based on single path selection paradigms. The lack of path diversity hinders the support for resilience, traffic engineering and QoS provisioning across the Internet. Some recently proposed multi-plane extensions to BGP offer a promising mechanism to enable diverse inter-domain routes towards destination prefixes. Based on these enhanced BGP protocols, we propose in this paper a novel technique to enable controlled fast egress router switching for handling network failures. In order to minimize the disruptions to real-time services caused by the failures, backup egress routers can be immediately activated through locally remarking affected traffic towards alternative routing planes without waiting for IGP routing re-convergence. According to our evaluation results, the proposed multi-plane based egress router selection algorithm is able to provide both high path diversity and balanced load distribution across inter-domain links with a small number of planes.

1 Introduction

The current Internet topology offers high path richness between domains [21], mainly due to the increasing use of multi-homing. However, the standard BGP protocol only allows single path selection, which does not take full advantage of this inter-domain path richness. Although the rationale behind this is to achieve high scalability in BGP routing, the lack of diverse paths significantly hinders support for Quality of Services (QoS) and resilience against network failures, both of which are vital for real-time multimedia services. On the other hand, Internet Traffic Engineering (TE) [1] is often used for optimizing network resources (e.g. load balancing) and sometimes also for supporting end-to-end QoS with high assurance guarantees. Without path diversity enabled by the inter-domain routing paradigms, the effectiveness of this TE could be significantly limited. This problem is especially significant for inter-domain peering links which often become the bottleneck of the end-to-end path in the Internet due to their scarce bandwidth resources [2].

It has been observed that handling intra-domain network failures is a daily occurrence in today's Internet [22]. As far as real-time multimedia services are concerned,

N. Akar, M. Pioro, and C. Skianis (Eds.): IPOM 2008, LNCS 5275, pp. 41–52, 2008.

network failures may lead to significant disruptions to end users. First of all, in order to minimize or even eliminate perceived service disruption by end users due to QoS degradation, the overall loss-of-connectivity duration should be no more than 50 milliseconds [3]. Given the relatively slow re-convergence behavior of the current IGP/BGP protocols, it is not possible to achieve this goal without introducing additional complications. Secondly, another important issue to be considered for QoS assurance is how to avoid network congestion in both the normal state and the post-failure state. To tackle the first challenge, Fast Reroute (FRR) techniques can be applied for rapidly diverting affected traffic from failed network components to repairing paths. It should be noted that most of the existing FRR techniques only deal with intra-domain routing [4, 5, 6], while very few consider the simple scenario of inter-domain link failures [3]. One important observation is that inter-domain routing can be also disrupted by intra-domain link failures, typically due to the Hot Potato Routing effect [7]. For instance, the breakdown of an intra-domain link may lead to a change of egress points for the affected transit traffic. In general, FRR techniques, which have only the single aim of minimizing the duration of loss-of-connectivity, do not tackle such routing disruption. Instead, inter-domain traffic engineering mechanisms [2, 8, 9] are responsible for routing optimization in both normal and post-failure states. In the literature, FRR and TE are two separate research topics being investigated independently, while a holistic solution for eliminating service disruptions is still yet to be obtained.

Recently, the concept of network virtualization has been developed, with the basic idea being to partition network resources for different service/engineering requirements, not only including the physical bandwidth, but also "soft" resources such as routing/forwarding tables. Related multi-plane techniques have been proposed both for intra- and inter-domain routing, such as Multi-topology OSPF/IS-IS [10, 11], QoS-enhanced BGP [12] and BGP path splicing [13, 14]. As far as inter-domain routing is concerned, the main idea is to provision coexisting diverse BGP routes towards each destination prefix. In the literature, proposals have typically been made to use these multi-plane routing mechanisms for *one* of the following purposes: service differentiation [12], traffic engineering [15] and fast failure recovery [4, 16]. In this paper, we consider how existing multi-plane techniques can be used as the underlying routing platform for achieving both FRR and bandwidth resource optimization, both of which are vital for supporting QoS assurance. More specifically, we consider how to enable *controlled* fast egress router switching for handling intra-domain link failures through multi-plane aware BGP protocols. The main idea is that additional egress routers can be pre-provisioned in backup routing planes, so that the affected transit traffic can be immediately switched to backup egress points without waiting for IGP re-convergence. A fundamental issue to be considered in the management plane is how the primary and backup egress points for each destination prefix are selected in multiple planes in order to maximize intra-domain path diversity for high failure coverage. Based on this multi-plane routing platform, existing egress point selection algorithms based on conventional BGP routing are extended for achieving improved load balancing across inter-domain links.

2 Multi-plane BGP Fast Reroute Overview

In our proposed scheme, multi-plane routing is used to enable fast reroute for customer traffic when intra-domain links fail without waiting for IGP re-convergence. In addition, we also investigate intelligent egress router selection is also addressed for achieving improved load balancing on inter-domain links. We first consider the scenario where conventional BGP is used as the underlying routing protocol without any fast reroute support. Once an intra-domain link fails, the IGP routing protocol needs to re-converge before the updated routing table is populated. In addition, the new IGP path may force BGP to switch egress points for some affected traffic due to the hot potato routing effect, as some ingress points may find that other border routers become closer (in terms of IGP distance) than the original primary egress points after the intra-domain link fails. Such egress point switching might not be always anticipated by the network administrator, and as a result post-failure network congestion may happen due to uncontrolled traffic shifting across inter-domain links.

In our proposed scheme, if multiple border routers have received BGP advertisements towards a specific destination prefix, instead of only installing one single route a dedicated egress point can be enforced within each BGP routing plane. In the normal state, only the egress router in the *primary* routing plane is used for delivering traffic. Once an intra-domain link fails, its head node, which is also called repairing router, immediately switches to use alternative egress point(s) installed in other routing planes by changing the tag (also known as remarking) of the IP packets, which indicates which plane should be used for carrying the affected traffic. Take the BGP path splicing [13, 14] as an example, $log_2(k)$ bits are used in the splicing header for indicating the active routing plane out of k planes. This value can be remarked at the repairing routers for achieving path switching. As far as BGP FRR is concerned, a basic requirement is that *the failed link should not be included in the shortest IGP path from the repairing router to the backup egress point*. In order to enable fast recovery, careful egress point selection needs to be performed in order to achieve maximum intra-domain path diversity across multiple routing planes. To be compliant with the current BGP route enforcement, the rule of Single Egress Selection (SES) [2] is followed within each specific plane, which means that all the customer traffic assigned to that plane to a certain prefix should exit through one single egress router. This is effectively enforced by assigning the highest BGP *local preference* value to the selected egress point in each plane. Let's take the simple network shown in Fig. 1 as an example where individual routers have full-mesh i-BGP sessions. Assume ingress routers i_1 and i_2 have transit traffic to be delivered towards a specific remote prefix P, which can be reached via border routers j_1, j_2 and j_3. As Fig. 1(a) shows, the IGP link weights of all intra-domain links are assumed to be 1 except the one between i_1 and c which is 3. If the network operator decides to use three BGP routing planes, then each of these three border routers can be selected as the primary egress point for prefix P in one of these planes. As shown in the Fig. 1(b), if egress router j_1 is selected in the first plane, customer traffic injected from individual ingress routers will follow the solid paths towards the destination prefix. Similarly, the paths with dot and dash links represent respectively the shortest IGP paths from ingress routers to the selected egress points j_2 and j_3 towards prefix P in the second and third planes.

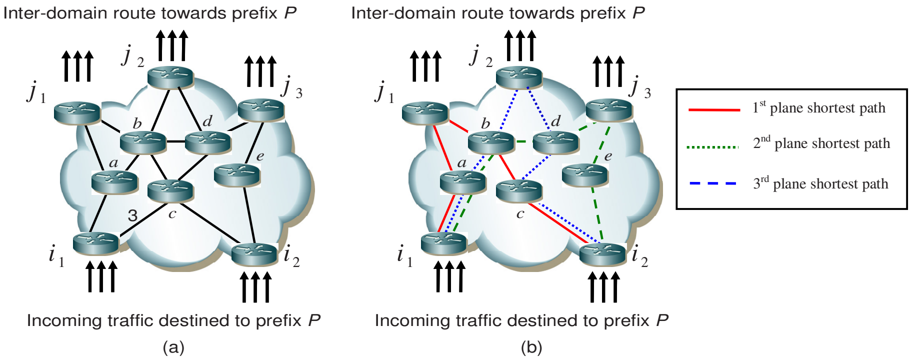
Inter-domain route towards prefix P
j1
j2
j3
a
b
c
d
e
3
i1
i2
Incoming traffic destined to prefix P
(a)
Inter-domain route towards prefix P
j1
j2
j3
a
b
c
d
e
i1
i2
Incoming traffic destined to prefix P
(b)
1st plane shortest path
2nd plane shortest path
3rd plane shortest path

Fig. 1. IGP paths in different routing planes

The first plane is used as the default one for traffic delivery in the normal state, which means j_1 is the actual primary egress router for carrying customer traffic to destination prefix P in the absence of link failures. In this case the actual shortest IGP paths from individual ingress routers to j_1 are $i_1 \rightarrow a \rightarrow j_1$ and $i_2 \rightarrow c \rightarrow b \rightarrow j_1$ respectively. If the head router c of link $c \rightarrow b$ has detected the failure of the link, it immediately remarks the traffic toward prefix P to switch the customer traffic from the default plane to an alternative plane where the failed link is not involved in the corresponding IGP paths. For example, the affected traffic can be remarked to use the second plane where j_2 is selected as the primary egress for P after the failure has been detected. In this case the backup IGP path $c \rightarrow d \rightarrow j_2$ is activated to deliver the affected traffic out of the local domain without waiting for the underlying IGP to re-converge. A more general case is to activate more than one backup plane so that the affected traffic can be delivered out of the local domain via multiple alternative egress points. The proportion of the shifted traffic across these backup planes can be determined according to the current available bandwidth associated with these alternative egress routers.

A key issue to be considered in the management plane is how to optimize the egress router selection in individual planes in order to maximize protection coverage against intra-domain link failures. It can be easily inferred that if an intra-domain link is involved in the IGP paths in all planes for a specific destination prefix, the affected traffic cannot avoid using it no matter which plane is used (e.g. link $i1 \rightarrow a$ in Fig. 1(b)). To avoid this situation, the egress point selection should aim to obtain high path diversity inside the local network across individual planes. As a result there is a high chance of having alternative feasible egress points that do not involve the failed intra-domain link. As far as traffic engineering is concerned, we consider how transit traffic can be balanced across individual inter-domain links based on multi-plane BGP routing. In the literature, optimized egress point selection for inter-domain TE based on conventional BGP routing has been widely investigated. In this paper we address the issue of achieving both BGP fast reroute and inter-domain traffic engineering in order to provide a holistic solution for resilience against link failures. More specifically, an optimization problem is formulated and solved with a heuristic for maximizing link failure protection as well as load balancing across multiple inter-domain links. Finally it should be noted that, we only propose in this paper a generic optimization problem in the management plane rather than going into details on how the idea is actually implemented using any specific routing mechanism. On the other hand, although we use multi-plane BGP protocols where packets can be tagged to indicate the active planes for traffic delivery, other advanced BGP protocols are also applicable, e.g. the MIRO scheme [17]. In this case packets need to be encapsulated in order to be tunnelled to alternative egress points, rather than changing the tag of the packets to be rerouted. Finally, it can be easily inferred that the proposed scheme can be also used for inter-domain link failures, as any primary egress router can also remark the affected traffic to use backup ones in other routing planes when it detects the failure of the directly attached inter-domain link.

3 Egress Router Selection for Path Diversity and Load Balancing

3.1 Network Modeling and Problem Formulation

As previously mentioned, the problem we are considering is to perform intelligent egress point selection across multiple planes for achieving (1) maximum intra-domain path diversity in order to maximize the chance for controlled fast BGP reroute in case of intra-domain link failures, and (2) load balancing on inter-domain links in the normal state. As far as network modeling is concerned, each Autonomous System (AS) has a set of edge routers which can be further classified into an ingress router set I and an egress router set J, through which transit traffic is injected into and delivered out from this domain respectively. In addition an AS may contain some core routers that are not directly connected to customers or other ASes. In BGP routing, egress routers receive reachability advertisements for remote destination prefixes through e-BGP sessions from neighboring domains. Let K denote the set of prefix advertisements received across all edge routers. For each prefix k ($k\in K$), let $Out(k)$ denote the set of egress routers at which an advertisement for prefix k has been received. On the other hand, the overall customer flows entering the domain through individual ingress routers with destination prefix k need to be estimated *a priori* before being assigned to individual egress routers. We use $t(i,k)$ to denote the aggregate traffic demand with destination prefix k ($k\in K$) that is injected into the domain through ingress router i ($i\in I$).

Regarding multi-plane extensions to BGP, we consider M logical planes to be pre-provisioned by the local AS so that a dedicated egress router can be selected for each destination prefix k within each plan $m\in M$. To enforce egress router selection for customer traffic, specific local preference (Local-Pref) values can be configured independently within each plane m. It is also worth mentioning that the intra-domain routing protocol running within the local domain is standard IGP which is not multi-plane aware. In this case the IGP distance between each ingress/egress pair is the same across all routing planes.

Considering our purpose to maximize path diversity, a fundamental issue is how to "represent" path diversity appropriately. Recall from the example shown in Fig. 1, it is important to avoid the situation that for one ingress router, no matter which egress router is to be used for carrying the incoming traffic in individual plane, the traffic cannot avoid traversing a certain link (for instance, link $i1 \rightarrow a$ in Fig. 1, which is fully shared by the IGP paths from *i* across all three planes). This would mean that all the possible IGP paths from that ingress router have to go through this critical link, which we call it *fully-shared link*. It can be easily inferred that if a fully-shared link fails, there are no alternative IGP paths in any plane for the affected traffic to perform fast reroute, and most probably IGP needs to re-converge before the traffic delivery service is restored. In this case, egress router selection with minimum number of fully-shared links is desirable. Towards this end, we design a variable $Q^{l}_{(i,k)}$ to indicate whether the intra-domain link *l* is the fully-shared link with regard to each aggregate customer flow injected from ingress router *i* and destined to prefix *k*. More specifically

$$Q^{l}_{(i,k)} = \begin{cases} 1 & if \ \sum_{m \in M} Y^{l,m}_{(i,k)} = M \\ 0 & otherwise \end{cases}$$

where

$$Y^{l,m}_{(i,k)} = \begin{cases} 1 & if\ l\ constitutes\ the\ IGP\ path\ in\ plane\ m\ for\ the\ injected\ traffic \\ & from\ ingress\ i\ and\ destined\ to\ prefix\ k \\ 0 & otherwise \end{cases}$$

We also define another binary variable $X^{j,m}_{k}$ to indicate the actual egress point selection for prefix *k* in each plane *m*. As previously mentioned, Single Egress point Selection (SES) is adopted in our scheme, which means one single egress is selected for each prefix across *all* ingress routers within each plane. That is

$$X^{j,m}_{k} = \begin{cases} 1 & if\ \ j \text{ is selected for prefix } k \text{ as the egress router in plane } m \\ 0 & otherwise \end{cases}$$

In summary, the overall objective is to determine the value of a set of $X^{j,m}_{k}$ for each considered prefix *k* in each routing plane *m* in order to:

$$\text{Minimize} \sum_{i \in I} \sum_{k \in K} \sum_{l \in E} Q^{l}_{(i,k)}$$

subject to the following constraints:

$$\text{if } X^{j,m}_{k} = 1 \text{, then } j \in Out(k) \qquad \forall j \in J,\ m \in M,\ k \in K \tag{1}$$

$$X^{j,m}_{k} \in \{0,1\}, Y^{l,m}_{(i,k)} \in \{0,1\} \qquad \forall j \in J,\ m \in M,\ k \in K \tag{2}$$

$$\sum_{m \in M} \sum_{i \in I} \sum_{k \in K} X^{j,m}_{k} \times t(i,k) \le C^{j}_{inter} \qquad \forall j \in J \tag{3}$$

Constraint (1) means the selected egress router *j* must be able to reach the destination prefix *k*. Constraint (2) makes sure that both variables *X* and *Y* are binary. Constraint (3) indicates the inter-domain link capacity constraint, meaning that all the customer traffic going through the selected egress router *j* should not exceed its inter-domain link capacity (C^j_{inter}).

3.2 Proposed Heuristic Algorithm

We proposed a simple heuristic algorithm to solve the problem. First of all, we adopt single plane traffic assignment in the normal state, that is, customer traffic is always assigned to the single egress router selected for the default plane. Other backup planes are only used when they are needed for fast BGP reroute in case of link failures. Entries for these additional egress routers selected for other planes are maintained in the router memory.

Step 1. Sort all the destination prefixes in the descending order according to their overall customer traffic demand, which is represented as $\sum_{i \in I} t(i,k)$. This strategy aims to put higher priority in the egress point assignment for the prefixes with higher traffic volume. Following that all the egress routers that satisfy the reachability constraint $j \in Out(k)$ are taken into consideration which ensures that by selecting egress router *j*, each destination prefix *k* can be reached. Any other egress routers that cannot satisfy this constraint are not considered any further.

Step 2. This step can be viewed as a pre-selection phase regarding bandwidth availability on candidate egress routers. In each plane, the problem is based on the Single egress selection problem, so all the customer traffic assigned to that plane to the same prefix from different ingresses should exit through a single selected egress router. Before the selection algorithm proceeds, the feasibility in terms of bandwidth constraint is checked. More specifically, any candidate egress router that does not have sufficient bandwidth resources to accommodate the traffic demand associated with the current destination prefix is excluded.

Step 3. For the first (default) plane, the egress router with the currently lowest bandwidth utilization is selected. This utilization is represented as the ratio of bandwidth used up by previously assigned traffic to the capacity of the inter-domain link. If there are equally lowest utilized links, one is selected randomly. Once the egress router in the default plane is selected for the prefix, we map the overall traffic demand onto the corresponding inter-domain link and update its bandwidth utilization.

Step 4. Now we consider the backup egress point selection in other planes. A key problem is how to perform the selection that can achieve the highest path diversity as we defined. For each backup plane, we consider the IGP paths the customer traffic will follow if we choose a certain egress router, and compare them with the paths already fixed in the previous step. We first count and sum up the total number of shared links between the two trees (the egress routers being considered as the root, and individual ingress routers as leaves). This summation value is inverse proportional to the degree of path diversity as we explained in Section 3.1. So the egress router associated with the smallest summation value can provide the highest path diversity. If there are several egress routers with equal path diversity, the selection will tie-break on the minimum bandwidth utilization of the inter-domain link associated with the egress router. If there are still equal candidates, one will be selected randomly. We then consider the next plane and follow the above selection process until all the planes have been considered. Until now, the selection process for one prefix is completed and the customer traffic for this prefix will all be assigned to the egress router selected for the default plane.

Step 5. We then consider the next prefix in the sorted order and repeat the procedure from steps 2 to 4. The heuristic finishes when all the prefixes have been considered.

4 Performance Evaluation

4.1 Experiment Setup

In order to evaluate the performance of our proposed algorithm, we used the topologies of two operational networks, namely the Abilene network [18] and the GÉANT network [19]. The Abilene network contains 11 Point-of-Presence (PoP) nodes and 28 unidirectional links. The GÉANT network contains 23 PoP nodes and 74 unidirectional links. In our experiments we use the actual IGP link weights configured in both operational networks. According to [20], only a small fraction of IP address prefixes are responsible for a large fraction of the Internet traffic. Based on this, we consider 100 popular routing prefixes in our experiments. As these routing prefixes are usually popular destinations, we assume that each egress router can reach all of them. For simplicity we assume that all inter-domain links have the same bandwidth capacity for both network topologies, and the traffic demand associated with each destination prefix is randomly generated. To produce more accurate results, each of the data points is an average of 10 independent trials.

4.2 Experiment Results

We first examine the overall path diversity performance by comparing the percentage of links that are fully shared by all M planes over the total number of links used by these planes (M is the number of planes used in the network). We assume 4 and 9 egress routers associated with the Abilene and the GÉANT network respectively. It should be noted that the total number of egress routers can be used as the upper bound for the number of routing planes to be used, as any additional routing plane will not help to increase path diversity any further. Consequently we only consider up to 4 routing planes in the Abilene network and 9 routing planes in the GÉANT network. What we are interested in is the proportion of those links that are fully shared or nearly fully shared by all routing planes as far as each ingress-prefix pair (i, k) is concerned. The reason for this is as follows. In order to maximize the chance of BGP fast reroute in case of intra-domain link failures, minimum number of fully shared links is desired. In addition, for those links that are not fully shared but are nearly fully shared by all routing planes, although it is still possible to perform fast reroute, as the number of feasible alternative egress routers is low, chances might be that these egress routers could suffer from congestion as the head node of the failed link has no alternative but to switch to them after the failure. Instead, if each head node has ample alternative egress routers in backup planes, it is able to perform intelligent egress

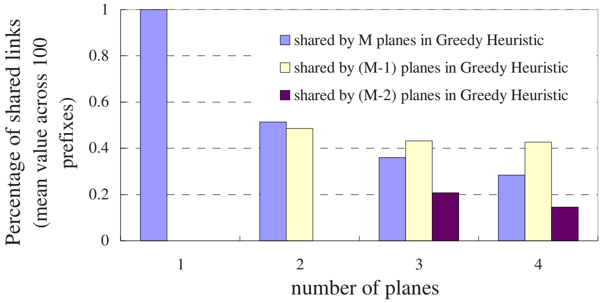

Fig. 2. Percentage of links shared by *M*, *(M-1)* and *(M-2)* planes separately in the Abilene network

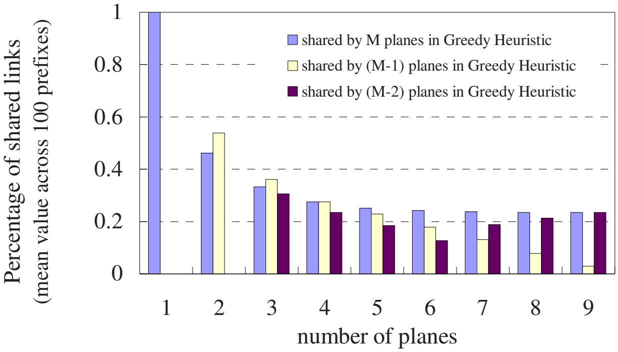

Fig. 3. Percentage of links shared by *M*, *(M-1)* and *(M-2)* planes separately in the GÉANT network

router switching in order to avoid post-failure congestion at backup egress routers. This feature will be investigated in our future work. Figures 2 and 3 present the percentage of links shared by *M, (M-1)* and *(M-2)* planes in the Abilene and GÉANT topologies respectively.

Both figures show that by increasing the total number of planes used in the network, the percentage of links shared by all *M* planes decrease. This can be explained as follows. When the number of planes increases, the total number of diverse paths that can be used to deliver customer traffic also increases; this can be reflected by the dramatic decreased number of shared links across individual topologies. For instance, if only one single topology is used (i.e. the conventional BGP routing), there is only one single intra-domain path from each of the ingress routers towards the selected egress point and apparently fast BGP reroute cannot happen in case of intra-domain link failures. If two routing topologies are used (M=2), the overall proportion of fully shared link drops significantly down to 52% and 46% in the Abilene and GÉANT networks respectively. As far as BGP fast reroute is concerned, let us assume one particular link fails in the current IGP path in the default plane from an ingress router to an egress router. If we use only one single plane, the traffic delivery will be disrupted because the traffic is unable to use the path until IGP re-converges. While by using two planes, there is 54% chance in GÉANT to successfully fast reroute the affected traffic by remarking it to backup planes which are already in place. If we continue to increase the number planes to 4 planes in Abilene and up to 9 planes in GÉANT, there is some further improvement but not significant.

Another important feature is load balancing across inter-domain links. In addition to the Greedy Heuristic we have proposed, we also implemented a Random Heuristic where no consideration is taken for any load-balancing purpose. More specifically, in Step 3 and Step 4 in the original Greedy Heuristic (shown in section 3.2), we ignore the procedure of choosing the egress router with the lowest bandwidth utilization, and instead we perform a purely random selection procedure. Figures 4 and 5 illustrate the maximum bandwidth utilization of each inter-domain link after network configuration using the Greedy Heuristic and Random Heuristic separately.

Figures 4 and 5 show nearly 30% improvement in the maximum bandwidth utilization from the Greedy Heuristic in comparison to the Random Heuristic. This is because the Greedy Heuristic takes bandwidth utilization into consideration in the path selection process, while Random Heuristic does not have such concern. Therefore in the Greedy Heuristic the bandwidth utilization of the egress links among the egress routers are better more than in the Random Heuristic. It can be also noticed

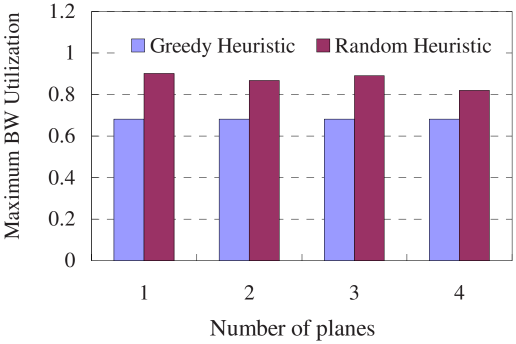

Fig. 4. Bandwidth utilization of each egress in the Abilene network

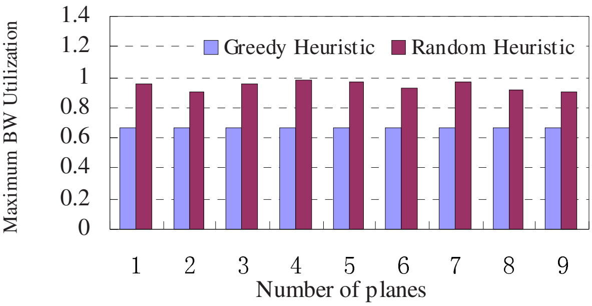

Fig. 5. Bandwidth utilization of each egress in the GÉANT network

that the maximum bandwidth utilization does not decrease with the increase in the number of routing planes. This is because we adopt the strategy that only one default plane is used for traffic delivery in the normal state with additional planes only activated in case of intra-domain link failures for fast reroute purposes. Of course further load balancing can be achieved *in the normal state* by optimally splitting the traffic across multiple active routing planes, therefore they can follow different IGP paths and use more than one egress router to be delivered out of the local domain. We will continue our investigation with this feature in our future research work.

5 Summary

Multi-plane aware routing protocols have been designed for providing diverse paths in traffic delivery. Based on the existing techniques, we have proposed a simple but efficient paradigm that enables multiple egress router selection for fast BGP reroute purposes in case of intra-domain link failures. More specifically, dedicated backup routing planes are provisioned a priori so that the repairing router is able to immediately remark the affected customer traffic to use additional egress points to be delivered out of the local domain without waiting for IGP to re-converge. In order to enable maximum chance for fast reroute, we developed a heuristic algorithm that aims to obtain maximum intra-domain path diversity across individual planes with the consideration of load balancing across egress routers. Our experiment results based on existing operational networks show that our proposed algorithm is able to produce significant diverse IGP paths with improved traffic engineering performance in comparison to random selection based solutions.

Our future work will focus on the improvement of the intra-domain path diversity, and we envisage that by intelligently manipulating IGP link weights will help improving such performance even without necessarily introducing multi-plane IGPs. In addition we will also investigate the scenario of using co-existing routing planes in the normal state (instead of using always one as described in this paper) in order to achieve adaptive load balancing against unpredicted traffic dynamics.

References

1. Awduche, D., et al.: Overview and Principles Of Internet Traffic Engineering, Request for Comments 3272, Network Working Group (May 2002)
2. Bressoud, T.C., et al.: Optimal Configuration for BGP Route Selection. In: IEEE INFOCOM (2003)
3. Bonaventure, O.: Achieving Sub-50 Milliseconds Recovery upon BGP Peering Link Failures. IEEE/ACM Transactions on Networking 15(5) (October 2007)
4. Kvalbein, A., et al.: Fast IP Network Recovery using Multiple Routing Configurations. In: Proc. IEEE INFOCOM 2006 (2006)
5. Shand, M., et al.: IP Fast Reroute with Notvia Addresses, IETF Internet draft, work in progress (February 2008)
6. Atlas, A.: Basic Specification for IP Fast-Reroute: Loop-free Alternates., IETF Internet draft, work in progress (2008)

7. Teixeira, R., et al.: Network Sensitivity to Hot-Potato Disruptions. In: Proc. ACM SIGCOMM, pp. 231–244 (2004)
8. Quoitin, B., et al.: Interdomain traffic engineering with BGP. IEEE Communications Magazine 41(5), 122–128 (2003)
9. Amin, M., et al.: Making Outbound Route Selection Robust to Egress Point Failure. In: Proc. IFIP Networking (May 2006)
10. Psenak, P., et al.: Multi-Topology (MT) Routing in OSPF, RFC 4915 (June 2007)
11. Przygienda, T., et al.: M-ISIS: Multi Topology (MT) Routing in IS-IS. RFC 5120 (February 2008)
12. Grffin, D., et al.: Inter-domain Routing through Quality of Service Class Planes. IEEE Communications 45(2), 88–95 (2007)
13. Feamster, N., et al.: Path Splicing with Network Slicing. In: Proc. ACM SIGCOMM HotNets (2007)
14. Motiwala, M., et al.: Path Splicing. In: Proc. ACM SIGCOMM (2008)
15. Wang, J., et al.: Edge Based Traffic Engineering for OSPF Networks. Computer Networks 48(4), 605–625 (2005)
16. Menth, M., et al.: Network Resilience through Multi-Topology Routing. In: Proc. IEEE DRCN 2005 (2005)
17. Xu, W., et al.: MIRO: Multi-path Inter-domain Routing. In: Proc. ACM SIGCOMM (2006)
18. The Abilene Network, `http://www.stanford.edu/services/internet2/abilene.html`
19. The GÉANT Network, `http://www.geant.net`
20. Feamster, N., et al.: Guidelines for inter-domain traffic engineering. ACM SIGCOMM Computer Communications Review (fall 2003)
21. Han, J., et al.: An Experimental Study of Internet Path Diversity. IEEE Transactions on Dependable and Secure Computing 3(4) (October 2006)
22. Iannaccone, G., et al.: Analysis of Link Failures in a Large IP Backbone. In: Proc. ACM Internet Measurement Workshop (IMW) (2002)