Interdomain Traffic Engineering Techniques to Overcome Undesirable Connectivity Incidents

Amer Alghadhban, Ashraf Mahmoud, Marwan Abu-Amara, Farag Azzedin, Mohammed Sqalli

Interdomain Traffic Engineering Techniques to Overcome Undesirable Connectivity Incidents

Amer AlGhadhban*, Ashraf Mahmoud, Marwan Abu-Amara, Farag Azzedin*, Mohammed H. Sqalli
*University of Hail, KFUPM
a.alghadhban@uoh.edu.sa, {ashraf, marwan, fazzedin, sqalli}@kfupm.edu.sa

Abstract. The importance of Internet availability is supported by the overwhelming dependence of government services and financial institutions upon said availability. Unfortunately, the Internet is facing different level of undesirable connectivity incidents. So, it is imperative to take serious measures in order to increase Internet connectivity resilience. We consider a scenario where a concerned region is facing an undesirable connectivity incident by its primary Internet Service Provider (ISP) which still advertises reachability to the concerned region. Assuming that connectivity to a secondary ISP is available, software is designed to implement different traffic engineering techniques in order to enhance internet connectivity resilience and send the traffic through the secondary ISP. The work is characterized by the implementation of these traffic engineering techniques in the laboratory through a detailed set of experiments.

1 Introduction

Undesirable Internet connectivity incidents can occur due to many reasons that can be categorized into two main categories: intentional and unintentional. Unintentional reasons include router misconfiguration, hardware and software failures, and security violations of the ISP/BGP operations. On the other hand, intentional reasons may happen with malicious intent or for political reasons [1]. Traffic engineering techniques are used by Autonomous Systems (ASes) in order to optimize the utilization of network resources [2]. In this work software is designed to implement traffic engineering techniques in order to enhance internet connectivity resilience. The work is characterized by the implementation of different traffic engineering techniques in the laboratory through a detailed set of experiments. Performance figures for the different types of background traffic considered and the representative configurations are collected and compared with each other.

1.1 Problem Statement

This study focuses on the network configuration portrayed in Fig. 1 where the concerned region, represented by AS100, is connected to the Internet through the primary ISP and represented by AS300. AS100 is also connected through a secondary ISP, called here the *good ISP* and represented by AS200. In this instance, AS100 faces undesirable connectivity incidents, such as significant bandwidth reduction and/or unacceptable delay by its primary ISP. Nevertheless, the primary ISP's border router continues to exchange BGP messages with the border router of the concerned region (AS100) and advertising its prefixes on the Internet.

1.2 Summary of Contributions

In this work we evaluate and prototype a different set of interdomain traffic engineering techniques that have the capability to control outgoing traffic and attract incoming traffic through a secondary ISP. The evaluation and prototyping is performed in a laboratory setting designed to mimic conventional deployment with support for two distinct topologies referred to by identical and non-identical topologies to symbolize the Internet's connectivity structure. In the identical scenario the *AS-Path* length from AS100 to AS600 over the two ISPs are the same. In the non-identical scenario the *AS-Path* from AS100 to AS600 through the two upstream ISPs are not the same, as shown in Fig. 1. For the sake of accurate and consistent testing procedures, software is created to detect the connectivity incident, deploy the prescribed solution, and to measure the network *convergence time*. When the connectivity incident, such as multiple packets drop, is detected the software forces the concerned region' border router to route the traffic via the good ISP.

2 Proposed Work

In this section, the proposed interdomain traffic engineering techniques are described. The proposed techniques are listed in Table 1. Some of the proposed BGP-based techniques can influence the incoming traffic to go through the *good ISP* while others can control the outgoing traffic.

Overlay Network is a virtual network that works over a real network such as the Internet. The most common type of overlay network is Virtual Private Network (VPN). VPN is usually used to build a secure network over an unsecure network like the Internet. *Overlay Network* methods can be used to overcome internet connectivity issues by establishing an overlay network between the region of concern AS and several cooperative ASes distributed around the world, e.g. IXPs, and route the traffic over a good ISP. Fig. 2 shows the effect of different overlay techniques on FTP and HTTP end-to-end delay. The FTP/HTTP applications are examined in our laboratory and tested under different background loads. Obviously, the end-to-end delay increases proportionally with the increase in the traffic load. The unencrypted overlay techniques show almost the same end-to-end delays when they are compared with no overlay technique.

The BGP methods tested in our labs that can influence incoming traffic, referred to as Attractors, are *AS-Path* Pre-pending, eBGP multihop, and Filtering outgoing advertisement. *AS-Path* Pre-pending [3] allows a router to advertise its prefixes with a longer *AS-Path* through one or more neighboring routers. Hence, this method advertises the prefixes through the primary ISP with a longer *AS-Path* and with a regular *AS-Path* through a *good ISP*. Consequently, the Internet ASes will prefer the shortest *AS-Path* which goes through the *good ISP*. The eBGP *multihop* scheme allows indirectly connected ASes to look as if they are directly connected. Consequently, the *AS-Path* length between the two eBGP *multihop* configured routers appears in the global routing table as one hop. This means that downstream ASes will prefer the path through the eBGP *multihop* routers over all other existing paths that might be physically shorter. Thirdly, filtering of outgoing advertisement method can control and filter the outgoing BGP routing advertisements of the local BGP *speaker*. This means that we can block the local prefixes from being advertised to the primary ISP and have them only advertised to the *good ISP*. Consequently, the local prefixes are not included in the advertisements of the primary ISP to the Internet, and the Internet routers learn about the local side prefixes only through the *good ISP*. The

Outforwarders methods that can control the outgoing traffic are filtering of incoming advertisements, IP default/static, MED, Weight and Local Preference.

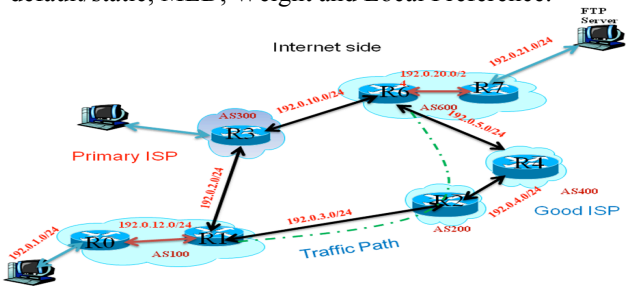

Fig. 1. Non-identical laboratory scenario.

As seen in Table 1, some of the solutions have the ability to forward outgoing traffic via a *good ISP* and other solutions have the ability to attract incoming traffic. To overcome the undesirable connectivity incident we have to combine one solution from the Outforwarder list with another solution from the Attracter list. Then, configure the concerned region's BGP *speaker* with this combination.

2.1 Convergence Time Results

The traffic engineering techniques are examined under three different background traffic loads: 75%, 50% and 25% on the 1.544 Mbps inter-router links used in the laboratory implementation.The obtained *convergence time* of the evaluated solutions is between 0.1 and 0.3 second, as shown in Fig. 2. The *convergence time* exchanged messages are few in number and small in size. Thus, the effect of the background traffic load on the *convergence time* is very small. The combination of *Filter outgoing advertisements* + Weight always gives the fastest *convergence time* even with the different background traffic load. The *Filter outgoing advertisements* solution blocks the concerned region prefixes from being advertised to the Internet through the primary ISP. Also, it does not change or introduce any load on the BGP advertisements, unlike *AS-Path pre-pending* solutions.

3 Conclusions

Government services and financial institution's dependence on Internet availability is sufficient proof of the importance of avoiding connectivity problems. The presented techniques address incidences wherein the primary ISP of the concerned region is showing unacceptable connectivity service. In this work we proposed multiple combinations of the interdomain traffic engineering techniques that can control outgoing traffic and influence incoming traffic. Based on the results, Internet Exchange Points (IXPs) and/or International ISPs can strengthen the Overlay Network and eBGP multihop solutions by agreeing to serve as remote cooperative ASes. The examined overlay techniques showed an acceptable overhead on the evaluated applications.

References

1. Arbor networks: Infrastructure security survey. http://www.arbornetworks.com/sp security report.php.

2. Stefano Secci. et al. Efficient inter-domain traffic engineering with transit-edge hierarchical routing. Computer Networks 57 (2013) 976–989.
3. Y. Rekhter, T. Li, and S. Hares. (2006, Jan.) IETF-A Border Gateway Protocol 4 (BGP-4). www.ietf.org/rfc/rfc4271.txt

Table 1. Classification of the proposed solutions.

	BGP Solution Methods	Incoming	Outgoing
Attracter	*Overly Network*	Yes	No
	AS-Path pre-pending	Yes	Yes
	eBGP *multihop*	Yes	Yes
	Filter outgoing advertisements	Yes	No
Outforwarder	Filter incoming advertisement	No	Yes
	IP static/default route	No	Yes
	MED	No	Yes
	Weight	No	Yes
	Local Preference	No	Yes

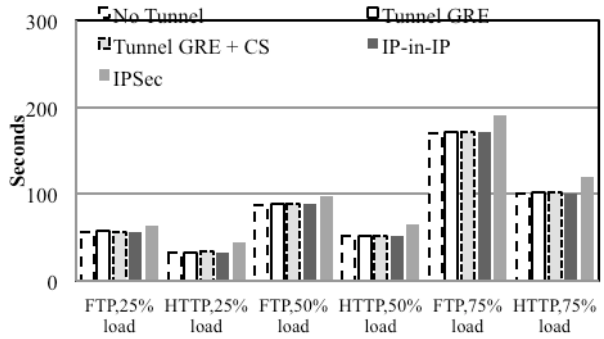

Fig. 2. Shows the end-to-end delay of the examined tunnelling techniques (CS=Checksum)

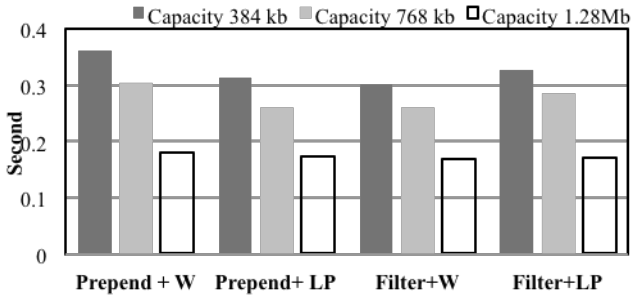

Fig. 3. Convergence time results (LP=Local-Preference W=Weight).