

**Prototyping and Evaluating the BGP-Based
Solutions to Overcome Malicious
IISIP Blocking**

BY

Amer Mohammad Al-Ghadhban

A Thesis Presented to the
DEANSHIP OF GRADUATE STUDIES

KING FAHD UNIVERSITY OF PETROLEUM & MINERALS

DHAHRAN, SAUDI ARABIA

In Partial Fulfillment of the
Requirements for the Degree of

MASTER OF SCIENCE

In

Computer Network

December 2011

KING FAHD UNIVERSITY OF PETROLEUM AND MINERALS

DHAHRAN 31261, SAUDI ARABIA

DEANSHIP OF GRADUATE STUDIES

This thesis, written by **AMER MOHAMMED JARRALLAH AL-GHADHBAN** under the direction of his thesis advisor and approved by his thesis committee, has been presented to and accepted by the Dean of Graduate Studies, in partial fulfillment of the requirements for the degree of **MASTER OF SCIENCE IN COMPUTER NETWORK.**

THESIS COMMITTEE



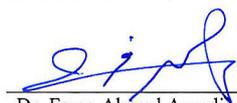
Dr. Ashraf S. Hasan Mahmoud (Chairman)



Dr. Marwan H. Abu-Amara (Co - Chairman)



Department Chairman
Dr. Basem Al Madani



Dr. Farag Ahmed Azzedin (Member)



Dr. Mohammed H. Sqalli (Member)



Dean of Graduate Studies
Dr. Salam Zummo



Dr. Hosam Khaled Rowaihy (Member)

10/1/12

Date

Dedicated to my Parents, Wife, Son and Daughter

ACKNOWLEDGEMENTS

In the name of Allah, the Most Gracious and the Most
Merciful

All praise and glory are due to Almighty Allah (SWT), to Him belongs the sovereignty of the heavens and the earth. I am grateful to Allah for all His favors on me since my birth, these blessings are indeed innumerable, and the greatest of His bounties on me are being a Muslim. Peace and blessings of Allah be upon the noblest of mankind, Muhammad (Peace Be upon Him), his household, his companions and the generality of the true believers to the last day. I would like to thank my beloved parents, beloved grandparents, aunties, uncles, my brothers, cousins and all my family members for their moral support throughout my academic career. I would never have been able to pursue this without their prayers, cooperation, understanding, patience, guidance, and support. I would like to express my profound gratitude and appreciation to my thesis committee chairman Dr. Ashraf S. Hasan Mahmoud for his support, intellectual guidance, suggestions, advice, and readiness to assist during this research. His extensive knowledge, patience, and experience made it possible to shape the thesis. He was always available when I needed him and he answered all my questions, at any time of the day. My deepest appreciation goes to my thesis committee co-chairman Dr. Marwan H. Abu-Amara for his support, guidance,

suggestions, and advice. I am extremely grateful to him for his prompt replies and his encouragement and having trust in me. I would like to extend my deepest appreciation to my thesis committee members Dr. Mohammed Houssaini Sqalli, Dr. Farag Ahmed Azzedin , and Dr. Hossam Rowaihy for their interest, invaluable cooperation and support. I would like to thank Dr. Uthman A. Baroudi for his support in the beginning of my Master program. Their continuous support, advice and encouragement can never be forgotten. I would like to acknowledge the support and facilities provided by King Fahd University of Petroleum and Minerals. This project is funded by King Abdulaziz City for Science and Technology (KACST) under the National Science, Technology, and Innovation Plan (project number 08-INF97-4).

I would like also to acknowledge the KFUPM staff members for their kind support and continuous cooperation. Moreover, I would like to express my deepest thanks to every instructor who contributed in building my knowledge and experience. Thanks are also due to faculty and staff members of the Computer Engineering Department for their cooperation. Finally, I would like to thank everybody who contributed to this achievement in a direct or an indirect way.

Table of Contents

ACKNOWLEDGEMENTS.....	IV
LIST OF TABLES.....	X
LIST OF FIGURES.....	XI
THESIS ABSTRACT.....	XIV
ABSTRACT (ARABIC).....	XV
CHAPTER 1	1
INTRODUCTION.....	1
1.1 Problem Statement	3
1.2 Thesis Objectives	5
1.3 Assumptions.....	5
1.4 Summary of Contributions.....	6
1.5 Thesis Organization	7
CHAPTER 2	8
BACKGROUND AND LITERATURE REVIEW	8
2.1 Border Gateway Protocol (BGP)	9
2.1.1 BGP Attributes [10].....	10
2.1.2 BGP Path Selection Procedure [10]	11
2.2 BGP Security: Weaknesses and Countermeasures	12
2.3 Internet Resilience and Multihoming.....	14
2.4 Router Misconfiguration.....	15

CHAPTER 3	17
PROTOTYPE DESIGN AND IMPLEMENTATION	17
3.1 Testing Laboratory Scenarios	17
3.2 Proposed and Evaluated BGP-Based Solutions	20
3.2.1 Alrefai's BGP-based Solutions.....	20
3.2.2 Our Proposed BGP-Based Solutions.....	23
3.3 Prototype Specifications and Main Features.....	25
3.3.1 Malicious IISP Blocking Configuration.....	27
3.3.2 Internet Application Testing Procedure.....	30
3.3.3 Convergence Time Procedure	31
CHAPTER 4	33
VALIDATION, PERFORMANCE EVALUATION AND RESULTS.....	33
4.1 Validation of BGP-Based Solutions	34
4.1.1 AS-Path Shortening Method.....	34
4.1.2 More Specific Prefix Method	35
4.1.3 BGP community Method.....	37
4.1.4 AS-Path Pre-pending Method.....	38
4.1.5 eBGP Multihop Method	40
4.1.6 Filter Advertisement Method	43
4.1.7 Interface Counter Reset Method.....	45
4.1.8 IP Static/Default Method.....	46
4.1.9 MED Method.....	47
4.1.10 Weight Method.....	48

4.1.11 Local Preference Method	49
4.2 Additional Observation Regarding the Presented Solutions.....	50
4.3 The Evaluated Subset of the Solutions' Combinations.....	53
4.4 Performance Results.....	54
4.4.1 Baseline Testing	56
4.4.2 Performance Figures of BGP-Based Solutions that were Proposed By Alrefai [8]	59
4.4.3 Performance Figures of the Recommended BGP-Based Solutions that Proposed in This Work.....	65
4.4.3.2 Performance Figures for FTP Stream.....	68
4.4.3.3 Performance Figures for HTTP Stream.....	75
4.4.3.4 Performance Figures for VoIP Stream	82
CHAPTER 5	88
CONCLUSION AND FUTURE WORK	88
5.1 Conclusion	88
5.2 Future Work	90
APPENDIX A.....	91
ROUTER CONFIGURATION	91
APPENDIX B.....	109
SOLUTIONS CONFIGURATION COMMANDS	109
Configuring Local Preference Value.....	109
Configuring Weight Value	109
Configuring BGP MED Value	110

Configuring eBGP Multihop Value.....	110
Configuring Interface Counter Reset.....	110
Configuring BGP community.....	111
Configuring More Specific Prefix.....	111
Configuring Filter Incoming Advertisements	112
Configuring Filter Outgoing Advertisements.....	112
Rate Limit Configuration and Burst rate Setting.....	112
APPENDIX C.....	113
JAVA SOFTWARE CODE	113
APPENDIX D.....	117
TRACE ROUTE RESULTS.....	117
AS-Path Shortening Method.....	119
More Specific Method.....	120
BGP community Method.....	121
Interface Counter Reset Method.....	121
IP Static/Default Method.....	122
Filter Advertisements Method.....	123
REFERENCES.....	124
CURRICULUM VITA.....	128

List of Tables

Table 1. The IP addresses of the networks, workstation and sever in the laboratory.....	18
Table 2. The network and applications parameters	20
Table 3. The classification of the BGP methods.	21
Table 4. The BGP-based solutions	22
Table 5. Classification of the proposed solutions.....	23
Table 6. Comparison between BGP methods	50
Table 7. Combinations of the considered BGP-based solutions	53

List of Figures

Figure 1. Malicious IISP blocking the concerned (considered) region traffic while still exchanging BGP messages.	4
Figure 2. Identical laboratory scenario	19
Figure 3. Non-Identical laboratory scenario	19
Figure 4. Malicious IISP ACL configuration commands	28
Figure 5. Ping and trace route results from local to Internet side.	29
Figure 6. AS-Path Shortening explanatory scenario.....	35
Figure 7. More Specific Prefixes explanatory scenario	36
Figure 8. BGP <i>community</i> explanatory scenario.	38
Figure 9 BGP table after implementing AS-Path prepending	39
Figure 10. eBGP multihop between AS100 and AS600.....	41
Figure 11. eBGP configuration sample	42
Figure 12. eBGP multihop between AS100 and AS700.....	42
Figure 13 BGP table after implementing eBGP multihop.....	43
Figure 14 Filtering outgoing advertisements explanatory secanrio.....	45
Figure 15 BGP table after implementing MED	47
Figure 16 BGP table after implementing Weight.....	48
Figure 17 BGP table after implementing Local Preference.....	49
Figure 18. <i>Ping</i> and <i>traceroute</i> results from local to Internet side in our lab over the preferred and alternative paths in identical scenario	55
Figure 19. <i>Ping</i> and <i>traceroute</i> results from local to Internet side in our lab over the preferred and alternative paths in non-identical scenario	57
Figure 20. The baseline throughput of the Internet applications	58
Figure 21. The baseline end-to-end delay of the FTP and HTTP applications	58
Figure 22. The debug results for hard and soft reset.	59

Figure 23. Hard reset convergence time results of the Arefai BGP-based solutions. Note: LP = Local Preference	60
Figure 24. Soft reset convergence time results of the Arefai BGP-based solutions. Note: LP = Local Preference, W = Weight and Ah prefix added to Arefai results.....	61
Figure 25. the percentage increase in end-to-end delay of the examined Internet applications.	63
Figure 26. Percentage of the lost packets during the blocking action	64
Figure 27. Hard reset convergence time results of the BGP-based solutions in identical scenario	66
Figure 28. Hard reset convergence time results of the BGP-based solutions in non-identical scenario.	66
Figure 29. Soft reset convergence time results of the BGP-based solutions in identical scenario.	67
Figure 30. Soft reset convergence time results of the BGP-based solutions in identical scenario	67
Figure 31. End-to-end delay of the FTP applications in identical scenario.....	69
Figure 32. End-to-end delay of the FTP application in non-identical scenario.....	70
Figure 33. Percentage increase of end-to-end delay of the FTP application in identical scenario.	70
Figure 34. Percentage increase in end-to-end delay of the FTP application non-identical.	71
Figure 35. Percentage of traffic drop of the FTP applications in identical scenario	72
Figure 36. Percentage of traffic drop of the FTP applications in non-identical	73
Figure 37. Average throughputs of the FTP applications in identical scenario.....	74
Figure 38. Average throughputs of the FTP Application in non-identical scenario.....	75
Figure 39. End-to-end delay of the HTTP applications in identical scenario.....	76
Figure 40. End-to-end delay of the HTTP applications in non-identical scenario	77
Figure 41. Percentage increase in end-to-end delay of the HTTP applications identical. .	77
Figure 42. Percentage increase in end-to-end delay of the HTTP applications non-identical.....	78
Figure 43. Percentage of traffic drop of the HTTP application in identical scenario.....	79

Figure 44. Percentage of traffic drop of the HTTP application in non-identical.....	80
Figure 45. Average throughputs of the HTTP applications in identical scenario.....	81
Figure 46. Average throughputs of the HTTP application in non-identical Scenario	82
Figure 47. Percentage of traffic drop of the VoIP applications in identical scenario.....	83
Figure 48. Percentage of traffic drop of the VoIP applications in non-identical.....	84
Figure 49. Average throughputs of the VoIP applications in identical scenario	85
Figure 50. Average throughputs of the VoIP applications in non-identical scenario.....	86
Figure A. 1 R0 configuration.....	93
Figure A. 2 R1 configuration.....	95
Figure A. 3 R2 configuration.....	98
Figure A. 4 R3 configuration.....	101
Figure A. 5 R4 configuration.....	104
Figure A. 6 R6 configuration.....	106
Figure A. 7 R7 configuration.....	108
Figure C. 1 <i>Checker</i> software Java code.....	117
Figure D. 1 Trace route over identical scenario.....	118
Figure D. 2 Trace route over non-identical scenario	119
Figure D. 3 Traceroute results for <i>AS-Path shortening</i> method over identical scenario .	119
Figure D. 4 Traceroute results for More Specific method over the non-identical scenario	120
Figure D. 5 Traceroute results for <i>BGP community</i> method over non-identical scenario.	121
Figure D. 6 Traceroute results for interface counter reset	121
Figure D. 7 Traceroute results for IP static/default	122
Figure D. 8 Traceroute results for filter advertisements.....	123

THESIS ABSTRACT

Name: Amer Mohammed Al-Ghadhban
Title: Prototyping and Evaluating BGP-Based Solutions to Circumvent
Malicious IISP Blocking
Major Field: COMPUTER NETWORK
Date of Degree: DECEMBER 2011

The objective of this thesis is to prototype and evaluate the BGP-based solutions that are proposed and analyzed using simulations by Alrefai in [8]. We consider a scenario where a concerned region is intentionally isolated from accessing the Internet by its primary International Internet Service Provider (IISP) which still advertises reachability to the concerned region. Assuming that connectivity to a secondary IISP is available, we prototype and evaluate BGP-based solutions capable of influencing incoming and outgoing traffic to go through the secondary IISP. The prototyping and evaluation of these solutions are performed for two laboratory scenarios: identical and the non-identical scenarios. The work also identifies additional BGP-based methods for controlling incoming and outgoing traffic, and provides a laboratory-based performance evaluation for a selected set of the proposed solutions. For the sake of consistency and repeatability, the experimental work is automated through the use of JAVA scripts to detect the Internet blockage, launching the specific solution, and collecting the required statistics. Laboratory results indicate that *convergence time* for the tested solutions is on the order of 60 seconds and produce minimal effects on traffic delay and application throughput.

ملخص الرسالة

الاسم	عامر محمد جار الله الغضبان
العنوان	نمذجة وتقييم الحلول المبنية على بروتوكول بوابة الحدود لمشكلة حرمان الانترنت المتعمد من قبل مقدمي الخدمة الدوليين
التخصص	شبكات الحاسب
التاريخ	ديسمبر 2011

تهدف هذه الرسالة إلى نمذجة وتقييم الحلول المقدمة من قبل الباحث الرفاعي [6] والمعتمدة على بروتوكول البوابة الحدودية. في حالة وجود منطقة متصلة بالإنترنت وقام مقدم خدمة الانترنت الرئيسي لها بمنعها من الوصول إلى الانترنت. وبافتراض وجود مقدم خدمة انترنت آخر تتصل معه هذه المنطقة قمنا بنمذجة وتقييم الحلول المقدمة من الباحث الرفاعي. وقد امتحنت هذه الحلول في معامل شبكات حقيقة مصممة و مهيئة لتمثيل شبكة الانترنت في العالم الحقيقي. وللحصول على نتائج أدق قمنا ببرمجة أربع برامج لتحسين بيئة تقييم الحلول لتكون بيئة آلية لا تعتمد على العمل البشري. إضافة إلى ذلك اقترحنا ثلاثة وثلاثون حلا جديدا لهذه المشكلة. وتم اختبار مقدرة هذه الحلول على تجاوز العزل بنفس الطريقة التي امتحنت بها الحلول التي قدمها الرفاعي.

CHAPTER 1

INTRODUCTION

The Internet is vastly significant that the majority of traditional media services such as TV, radio, telephones and newspapers have redesigned themselves in order to be compatible with Internet applications. The Internet has provided new human interaction services such as social networking, online shopping, instant messaging and website forums. Also, new government, business, academic and banking services have been offered through suitable web services. As the number of significant applications provided through the Internet increases, so does the dependence on the Internet backbone providing resilient services. Local Internet Service Providers (ISPs) are obliged to enhance the availability and resilience of the services they provide for their clients.

The exchange of information over the Internet travels from a source to a destination through multiple interconnected networks. Some of these networks are small local networks which users are directly connected to and others are large networks that are responsible for interconnecting the smaller ones. Formally speaking, networks are divided into several Autonomous Systems (ASes). An AS is a set of connected computer

networks under the administration of a single entity that is usually an ISP or a larger network called an International Internet Service Provider (IISP). The routing protocol that interconnects different ASes with each other is the Border Gateway Protocol (BGP). BGP is mainly used over network and transport layers and makes its routing decisions based on the number of hops and/or network policies.

Internet connectivity failure, also called isolation, can occur due to many reasons which can be categorized into two main categories: intentional and unintentional reasons. The unintentional reasons include a router misconfigurations, hardware and software failures, and external malicious attacks and security violations on the IISP/BGP operations [1][2]. On the other hand, intentional isolation may happen under malicious intent or political reasons. The IISP has the ability to block incoming and outgoing Internet traffic of one or more ASes. At the same time, the responsible IISP is still exchanging reachability messages with the blocked region and advertising the blocked region's prefixes to the Internet.

The Internet has suffered from many small errors that led to momentous impact and widespread damage [3]. On 25 April 1997, a misconfigured router advertised a routing update claiming it had the best route to all Internet destinations. This mistake disrupted the whole Internet for about 2 hours [4]. In February 2008, a similar mistake made by Pakistan Telecom caused a global denial of service to the YouTube website [3]. On Aug 18, 2009, EFTel and aaNet, two of the main ISPs in New South Wales, suffered from a distributed denial of service attack that caused three weeks of Internet outage for

their customers [5]. Moreover, the root DNS servers faced two attempts to melt them down, the first attempt in 2002 and the second one in 2007 [6].

Internet isolation can be very inconvenient if not disastrous. The harm involved may range from the loss of basic communication between end users to the loss of large amounts of wealth [7]. In many cases isolation is preventable. This study prototypes and evaluates BGP-based solutions that were proposed by Alrefai [8] and proposes several BGP-based techniques for combating intentional Internet isolation. The proposed techniques are developed, prototyped and tested in a laboratory setting and their performance is evaluated in terms of *convergence time* and effect on Internet applications.

1.1 PROBLEM STATEMENT

This study focuses on the network configuration depicted in Figure 1 where the concerned region, denoted by AS100, is connected to the Internet through the primary IISP, defined here as the malicious IISP and denoted by AS300. The concerned region is also connected through a secondary IISP, called here the good IISP and specified by AS200. As indicated by its definition the primary IISP for intentional reasons blocks the incoming and outgoing Internet traffic of the concerned region. Although, the malicious IISP isolates the Internet traffic of the concerned region, the malicious IISP's BGP *speaker* is still exchanging *keepalive* and BGP messages with the concerned region's BGP *speaker* and advertising its prefixes on the Internet. However, without these messages being exchanged, the concerned region's BGP *speaker* will directly route the outgoing

traffic through the good IISP and acquire incoming traffic through it as well. The border router that carries the traffic between different ASes is called a BGP *speaker*.

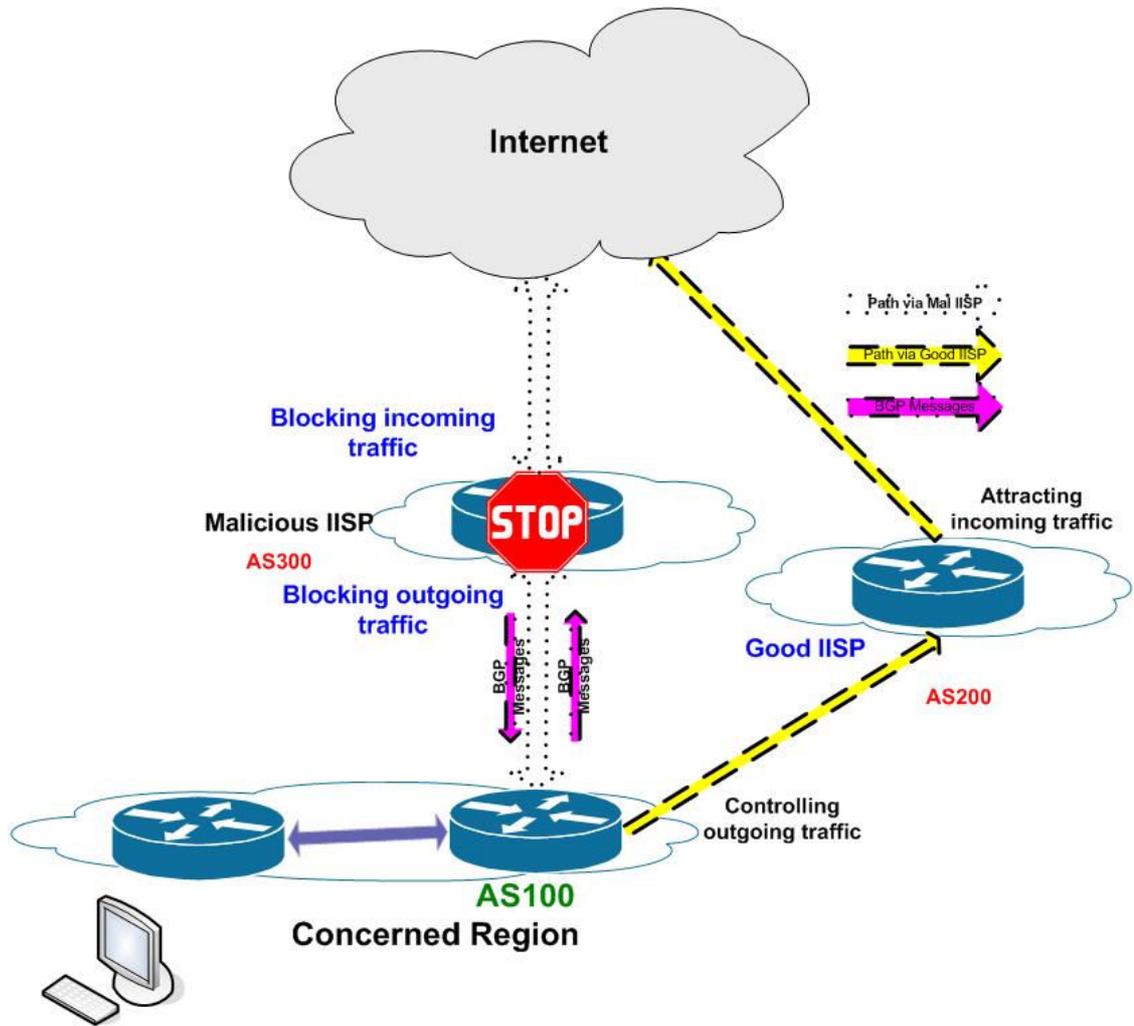


FIGURE 1. MALICIOUS IISP BLOCKING THE CONCERNED (CONSIDERED) REGION TRAFFIC WHILE STILL EXCHANGING BGP MESSAGES.

1.2 THESIS OBJECTIVES

The main objectives of this work are to prototype the previous BGP-based solutions identified by [8] and also to provide enhancements of these solutions whenever possible. The work will characterize the implementation of these solutions in the laboratory through a detailed set of experiments. Performance figures for the different types of traffic considered and the representative configurations will be collected and compared with each other to identify the suitability and scalability of the proposed solutions. Hence, these solutions have to overcome the Internet denial by an IISP with minimum changes in the network and with accepted assumptions and limitations. Furthermore, the testing environment and test cases have to be close to reality in both the configurations and parameters. Also, the testing procedures have to be consistent and repeatable. The evaluated schemes have to be tested in different scenarios and traffic load. In addition, performance figures, such as *convergence time*, throughput and number of lost packets during the blocking are collected for each evaluated scheme.

1.3 ASSUMPTIONS

- Assuming the concerned region has a dual Internet connection one with primary IISP and one with secondary IISP. When blocking is to be enforced, the primary

IISP will continue to advertise reachability to the concerned region while dropping any traffic destined to or originating from this concerned region.

- Focusing on available BGP methods and without changing the BGP standards.

1.4 SUMMARY OF CONTRIBUTIONS

- Evaluating and prototyping the BGP-based solutions that were proposed by Alrefai [8] in a real laboratory.
- Enhancing the BGP-based solutions that were proposed by Alrefai [8] and propose new BGP-based solutions.
- Evaluating and prototyping a new set of BGP-based solutions that are proposed in this work.
- Design automated, consistent and repeatable testing procedures, four Java based programs created to detect the blocking action of malicious IISPs, deploy the prescribed solution and to measure the network *convergence time*.
- The evaluation considered three Internet applications, namely HTTP, FTP, and VOIP applications and accounted for variable background traffic load

1.5 THESIS ORGANIZATION

The remainder of the thesis is put in order as follows. Chapter 2 covers background information about the Border Gateway Protocol (BGP) and literature review about BGP security: weaknesses and countermeasures. Chapter 3 provides an overview of the BGP-based solutions, how testing laboratory scenarios are designed and configured, prototype specifications and evaluation procedures. The solutions description and validation results are discussed in Chapter 4, followed by the solutions discussions and analysis. Finally, the performance evaluation results in terms of end-to-end delay, traffic drop and throughput are provided. The thesis finally concludes in chapter 5, where we point out the overall picture of the proposed and evaluated solutions and the chapter is concluded by a list of suggestions and potential enhancements as future work.

CHAPTER 2

BACKGROUND AND LITERATURE

REVIEW

The Internet is a collection of heterogeneous interconnected ASes. Each AS contains several end-systems (i.e. workstations and servers) and interconnecting systems (i.e. switches and routers). Internet services are provided to Internet users through a local ISP. Typically, the local ISP is classified as a tier-3 ISP in the Internet hierarchy classification. The tier-3 ISPs pay upper ISPs for services and collect fees from their Internet users. Tier-2 ISPs reside between the local ISPs and tier-1 ISPs and they occupy a wide region of the Internet. Unlike the tier-2 ISPs, tier-1 ISPs govern the Internet backbone and they are only connected to other tier-1 or large tier-2 ISPs. Tier-1 ISPs and large tier-2 ISPs are usually called International ISPs (IISP). A serious Internet outage may happen if one of these IISPs experiences a meltdown or is misconfigured. IISPs can also isolate a target region from the Internet if they desire to do so [9].

The only protocol for delivering Internet traffic between the different ASes over the best path is BGP. The following subsections briefly describe the BGP routing protocol and its path selection procedure.

2.1 BORDER GATEWAY PROTOCOL (BGP)

In the literature, network routing protocols are classified into two main classes, which are the Internal Gateway Protocol (IGP) and the External Gateway Protocol (EGP). The IGP protocols are mostly used under one AS. There are several IGP protocols and the two most well known are Routing Information Protocol (RIP) and Open Shortest Path First protocol (OSPF). In contrast, there are only a few routing protocols used to route the traffic among different interconnected ASes. The main routing protocol implemented to interconnect different ASes is the BGP, which is defined in RFC 4271 [10].

The BGP is a path vector routing protocols. The BGP learns about network topology involves identifying the best path to remote indirectly connected sub-networks, and is achieved by receiving and processing the network updates through neighboring routers. However, this class of routing protocols usually does not perform any intelligent path selection procedure as their implemented procedure is mainly based on the hop count which is not considering the link capacity and congestion.

2.1.1 BGP ATTRIBUTES [10]

The following is a list defining and describing important BGP attributes:

- i. *Weight* is a Cisco proprietary attribute that is not advertised to neighboring routers. If the router has more than one route to the same destination in its routing table, the outgoing path associated with the highest *Weight* value will be selected.
- ii. The *local preference* attribute is a general standard value used to prefer an exit point among all available exit points in the local AS. Although, the *Weight* attribute is used inside a router, the *local preference* attribute is disseminated to all routers within the same local AS. The path that is associated with the highest *local preference* value will be selected as the exit point.
- iii. The *multi-exit discriminator (MED)* or *metric attribute* is advertised to external ASes to select the preferred incoming route to the AS which is advertising the *MED*. If there are multiple entry points to the local AS, the entry point that is advertising a lower *MED* will be selected from the external AS as the entry point to the local AS.
- iv. The *origin attribute* denotes how BGP discovered a specific route. The origin attribute can have one of the following values: A) IGP: This value is displayed when the route was inserted into BGP by configuring the router with the *network* configuration command. B) EGP: The route was discovered through the Exterior Border Gateway Protocol (EBGP). C) Incomplete: The origin of the route was unidentified or when a route is redistributed into BGP through the *redistribution* command.

- v. The *AS-Path* which looks like a hop count; each AS number that has been traversed by a route advertisement message is added to an ordered list.
- vi. *eBGP multihop* [11] method allows indirectly connected ASes to appear as if they are directly connected.
- vii. *BGP community* is a cooperation scheme between ASes that allows them to control a BGP path selection procedure of each other.

2.1.2 BGP PATH SELECTION PROCEDURE [10]

On the Internet, packets travel over several routes from a source to a destination. The selection of the best route among the existing routes between the source and destination is the responsibility of the routing protocol. Each routing protocol has a different procedure and criteria for determining route selection. The BGP routing protocol has a unique path selection procedure. The BGP path selection procedure begins by comparing the associated *Weight* value of all existing paths and selects the path with the highest *Weight* value. If the *Weight* values are the same for all existing paths, then the path with the highest Local-Preference value is selected. If they are the same, the path that originated from the BGP running on this router is selected. If they all originated from the same router, the path with the shortest AS-Path length is selected. If they have the same length, the path with the lowest Multi_Exit_Disc (MED) value is selected. If they have the same MED value, the path that goes over an external AS is preferred over the path that goes over an internal AS. If they are the same, the path that goes through the closest IGP neighbor is selected. If they are the same, the path that goes through a link that is learned

before the other existing paths is selected. If they are the same, the path that goes through a next-hop router and has a lowest ID is preferred.

2.2 BGP SECURITY: WEAKNESSES AND COUNTERMEASURES

BGP was designed to provide reliability with minimum overhead. It is not designed with security in mind, which makes it defenseless to imminent routing attacks. In Hu et al. [12] the authors discuss the security weaknesses of BGP which are classified into three main categories. First, BGP does not provide message integrity and message origin authentication mechanisms and it is vulnerable to a replay attack. Second, BGP does not provide a mechanism to verify the legality of the AS-Path or prefix advertisements from the AS. Third, BGP does not verify the validity of BGP attributes included in the BGP advertisements.

BGP attacks have been discussed by Nordstrom and Dovrolis in [13], where they name four main purposes for these attacks as follows: 1. *Blackholing* 2. *Redirection* 3. *Instability* and 4. *Supervision*. *Blackholing* is an attack method of dropping all the traffic passing through the attacking router. Also, the attacker may drop only traffic that belongs to a specific AS. *Redirection* is a method of redirecting all traffic or a specific user's

traffic to another destination or server for content analysis. *Supervision* is similar to the previous method, but the purpose is to modify the traffic content then forward it to the right destination. *Instability* is an attack method initiated to harm the network with destabilizing events such as injecting false updates, link oscillations or announcing successive advertisement then withdrawals.

Several proposed security extensions to BGP are based on cryptographic techniques. The most cited BGP security schemes are Secure BGP (S-BGP) [14] and Secure Origin BGP (soBGP) [3][15]. S-BGP is based on digital signature and public-key cryptography to avoid false routing updates, de-aggregation and update modifications. S-BGP presents three security mechanisms to secure regular BGP. First, it presents a Public-Key Infrastructure (PKI) to provide the routes validity and prefix authority. Second, it presents new transitive attributes to BGP route updates. Finally, it presents IPSec to provide message integrity, confidentiality, authenticity and message replay prevention. Ng in [15] proposes another scheme called Secure Origin BGP (soBGP) which is based on symmetric key cryptography in order to reduce the computational overhead in public-key cryptography. Unlike S-BGP, which is based on PKI, soBGP is based on web of trust. Whereas, path authentication in S-BGP is dynamic, it is static in soBGP, and called path plausibility. Additionally, soBGP adds new security messages between BGP routers and no encryption is required for each update messages. A further difference is that S-BGP is much heavier than soBGP. As a result authenticated data in soBGP is saved, signed, and validated in each router before deployment.

2.3 INTERNET RESILIENCE AND MULTIHOMING

One of our main concerns in this work is to enhance the Internet resilience of the concerned region against malicious IISP blocking. One of the techniques that capable in improving the Internet resilience is multihoming. Multihoming is a method of increasing network reliability by connecting it with multiple external routes. As explained in Liu and Xiao [16], the two main types of Multihoming are BGP Multihoming and NAT Multihoming. In A. Akella et al. [17] they measure the capability of multihoming by enhancing the reliability and the performance of the network. Also, to get accurate measurements they conducted their study on the two well-known types of technologies that usually utilize the multihoming technique. The first type is a data provider (i.e. website) that provides a service for multiple clients. The second type is an enterprise network that receives multiple requests from different customers. The traffic in the data provider is usually directed from the provider to the client (i.e. upstream). In contrast, the traffic in the enterprise network is usually directed from the customers to the enterprise (i.e. downstream). They found that selecting the appropriate set of ISPs has a significant effect on the network performance. In Goldenberg et al. [18] they propose that new *smart routing* algorithms have the ability to improve the performance of multihoming and minimize costs.

The two multihoming techniques improve the Internet connectivity resilience of Internet ASes. The Internet resilience area has been covered in many researches [2][19-22]. In Omer et al. [19] a new method and network model are proposed to measure the resilience of the Internet's infrastructure by identifying the vulnerabilities of global

undersea optical fibers. They evaluate the effect of the possible losses in these cables against the Internet infrastructure and the recovery from it. Kim et al. [20] conducted a study which proved that modifying the network topology improves its resilience. Cohen et al. [21] have shown that the Internet is susceptible to an intentional attack because there exists few ASes, e.g. IISPs, which aggregate a large number of the internet connectivity. They proved mathematically that the removal of one or more of these ASes causes momentous Internet outage.

A more realistic study with practical analysis has been conducted by Dolev et al. [2], they assume the Internet ASes are connected as a directed graph (policy-based). They made their analysis and measurements of the resiliency of the Internet based on that assumption. In addition, they concluded that the Internet is highly sensitive to an intentional attack and could possibly crumble very fast. In contrast, the Internet is resilient to random failure. A major investigation into the sensitivity of the Internet to random faults and attacks were made by Park et al. [22]. They concluded that the Internet is robust and is becoming more robust with time against random failures; and the average internet diameter is stable even though the number of internet users is increasing.

2.4 ROUTER MISCONFIGURATION

Router misconfiguration is one of the Internet isolation causes [23]. A study by Labovitz et al. [24] on Internet routing updates and BGP announcements claims 95% of the updates arise from false origins. They found that one of the main causes of Internet routing false updates are router misconfigurations. Mahajan et al. [25] conducted a comprehensive study on BGP misconfiguration. Their study covered causes, impact and

avoidance of misconfiguration. They obtained their results from analyzing BGP advertisements for 21 days from 23 different vantage points over the Internet backbone. Although, there are several kinds of misconfiguration, they focus only on two main types: Origin misconfiguration and Export misconfiguration. Origin misconfiguration is the unintentional adding of an incorrect route or a route with incorrect information to the global BGP routing table. The causes of Origin misconfiguration are: incorrect filters; advertising the not to be advertised prefixes; incorrect summarization, which causes inaccurate more specific prefixes to be advertised, or prefix hijacking; and originating other ASes prefixes. Export misconfiguration is the unintentional advertising of route advertisements that should not be advertised. An example of this is the stub-AS advertising the incoming routing updates from neighboring AS to another neighboring AS [25]. The causes of Export misconfiguration are incorrect filter and route-map, typo, old configuration and filters, and many others. They found that 75% of daily new route advertisements are caused by BGP misconfiguration. Also, 1% of the prefixes in the global BGP routing table suffer from daily misconfiguration. Moreover, misconfiguration introduces a significant load on Internet routers; it occupies 10% of the overall update load. However, they found that the Internet's connectivity is resilient to BGP misconfiguration.

CHAPTER 3

PROTOTYPE DESIGN AND IMPLEMENTATION

3.1 TESTING LABORATORY SCENARIOS

The prototyping and evaluating of the BGP-based solutions are performed in a real laboratory designed with different scenarios capturing the real Internet's ASes connectivity layout. The AS-Path length from a local AS to a remote AS through two different IISPs is not always identical. Based on this fact, the evaluated solutions are examined in two dissimilar laboratory scenarios. The first scenario, called here identical scenario is shown in Figure 2. In identical scenario the AS-Path length from the local side (AS100) to the Internet side (AS600) over the two IISPs are the same. The second scenario, called non-identical scenario is shown in Figure 3. In non-identical scenario the AS-Path from the local side to the Internet side through the good ISP (AS200) is longer

than the AS-Path to the Internet same side when it goes through the malicious IISP (AS300). In Figure 2 and Figure 3, AS100 represents the concerned region and AS600 represents the Internet side where three servers are installed with different Internet applications: FTP, HTTP and VoIP. Also, the two figures show AS300 as the malicious IISP that is blocking the outgoing and incoming traffic of the AS100. However, AS100 is multihomed to a secondary IISP, i.e. the good IISP, where the proposed BGP-solutions route the outgoing traffic and attract the incoming traffic through it. Table 1 shows the IP addresses of the workstation, server and networks in the testing laboratory. Also, Table 2 shows the network and application parameters.

TABLE 1. THE IP ADDRESSES OF THE NETWORKS, WORKSTATION AND SEVER IN THE LABORATORY

Description	IP address
Local Side Network	192.0.1.0/24
Network between R1 and R2	192.0.2.0/30
Network between R1 and R3	192.0.3.0/30
Network between R3 and R4	192.0.4.0/30
Network between R4 and R6	192.0.5.0/30
Network between R3 and R6	192.0.10.0/30
Network between R0 and R1	192.0.12.0/30
Network between R6 and R7	192.0.20.0/30
Internet Side Network	192.0.21.0/24
Workstation in the Local Side	192.0.1.6/24
FTP Sever	192.0.21.6/24
HTTP Server	192.0.21.5/24
VoIP Server	192.0.21.4/24

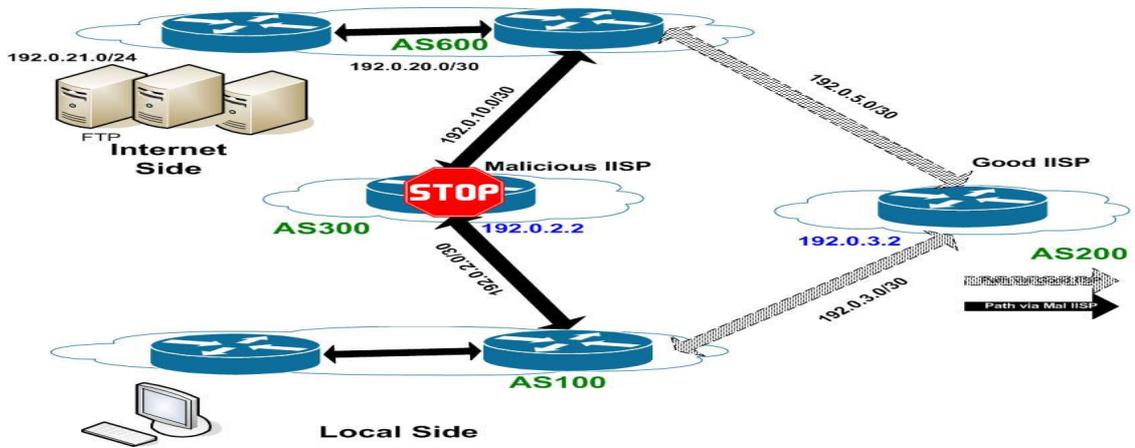


FIGURE 2. IDENTICAL LABORATORY SCENARIO

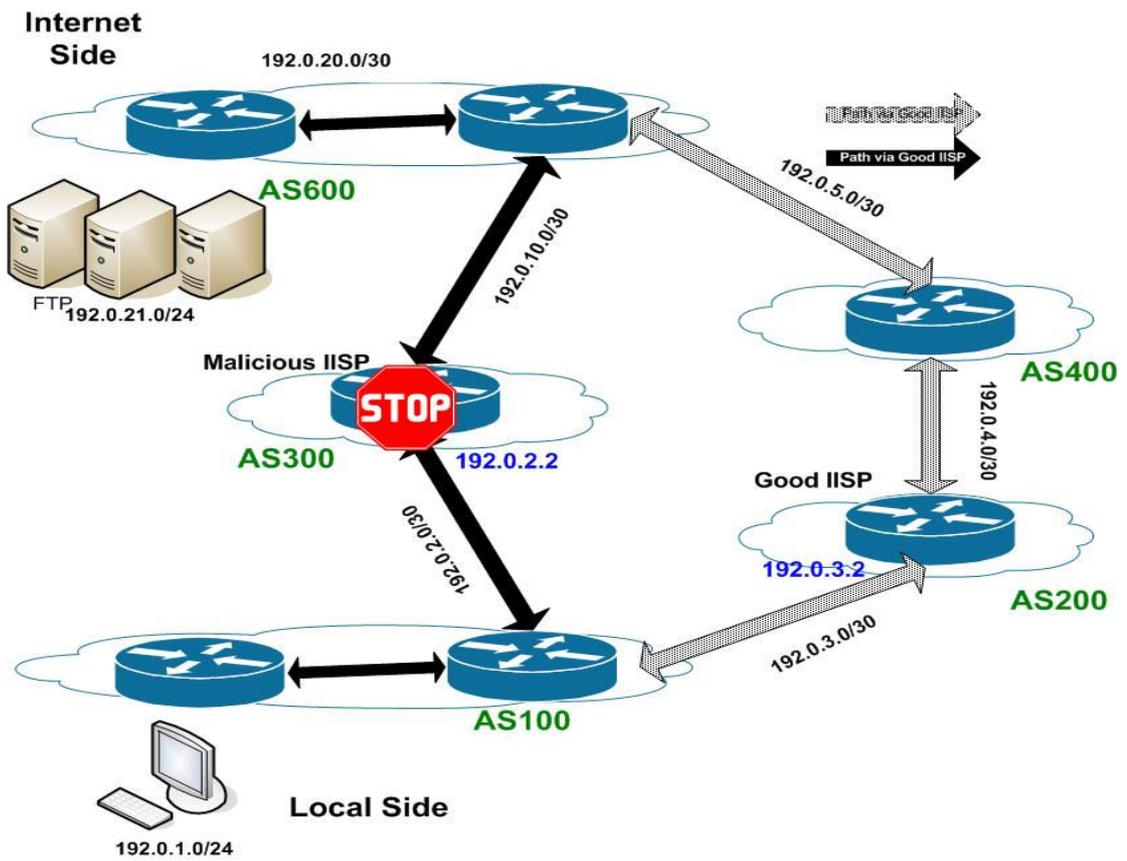


FIGURE 3. NON-IDENTICAL LABORATORY SCENARIO

TABLE 2. THE NETWORK AND APPLICATIONS PARAMETERS

FTP File Size	10MByte
Webpage Size	6MByte
VoIP Call Duration	120 seconds
Routers Link Capacity	1.544 Mbps
Local Side LAN Capacity	100 Mbps
Internet Side LAN Capacity	100 Mbps
FTP Server Software	FileZilla
Web Server Software	IIS 7.5
VoIP Traffic Generator	Iperf [26]
Router Operating System	Cisco IOS 12.4

3.2 PROPOSED AND EVALUATED BGP-BASED SOLUTIONS

In this section the Alrefai and the introduced BGP-based solutions are explained. The BGP routing protocol has a unique path selection procedure as we have explained in the background section. The BGP protocol offers configuration commands capable of controlling the attributes of its path selection procedure, such as AS-Path pre-pending and Local-Preference.

3.2.1 ALREFAI'S BGP-BASED SOLUTIONS

In this section the BGP-based solutions that are proposed by Alrefai [8] are explained. Table 3 shows the classification of the BGP methods on their ability in controlling the outgoing traffic or attracting the incoming one. The methods that can influence incoming traffic are *AS-Path shortening*, *more specific prefixes*, and *BGP community*, defined as

Attractor. Also, the method that can control outgoing traffic is *Local Preference*, defined as *Outforwarder*.

TABLE 3. THE CLASSIFICATION OF THE BGP METHODS.

BGP Function \ Ability	Incoming Attractor	Outgoing Outforwarder
<i>AS-Path shortening</i>	Yes	No
<i>More specific prefixes</i>	Yes	No
<i>BGP community</i>	Yes	No
<i>Local Preference</i>	No	Yes

1. *AS-Path shortening* [27] in this method the good IISP originating the concerned region's prefixes using. As a result, the prefixes appear in the Internet as belonging to the good IISP and the first AS number in the AS-Path associated with these prefixes is the good IISP's AS number (i.e. here it is AS200). Hence, the concerned region's prefixes that are advertised via the good IISP appear in the Internet with a shorter AS-Path than the ones advertised via the malicious IISP. 2. *More specific prefixes*, the routing table algorithm selects the longest prefix match as a network destination to the forwarding traffic. Based on this, attracting the traffic through the good IISP can be achieved by advertising long prefixes. However, the accepted length of the prefix on Internet routers is limited to a fixed length [28]. 3. *BGP community*, the BGP protocol has a *community* attribute which is used in the evaluated solutions to influence the incoming traffic going through the good IISP. This attribute enables any AS to send a *Community* request to its neighbor ASes. When the neighboring AS gets the *Community* request it looks at the

Community value associated with the request then performs an action based on it. The action performed here is assigning a higher *Local Preference* value to the path where the neighbor gets the *Community* request from. This solution requires the ASes between a remote cooperative AS and the concerned region to accept the *Community* advertisements. Table 4 shows part of the *Community* values that are used by Sprint [29], one of the largest ISPs in the world. Any subscriber ISP can influence the BGP path selection procedure of Sprint by associating the appropriate *Community* value with its advertisements to Sprint.

The BGP-based solutions are a combination of one of the *Attractor* methods with the *Outforwarder* methods, such as *Local Preference + BGP community*. Table 5 illustrates the evaluated combinations in this work.

TABLE 4. Sprint Local Preference *BGP community* value

<i>BGP community Value</i>	Resulting Local Pref
1239:70	70
1239:80	80
1239:90	90
1239:100	100
1239:110	110

TABLE 4. THE BGP-BASED SOLUTIONS

	Local Preference
<i>AS-Path shortening</i>	✓
<i>More specific prefixes</i>	✓
<i>BGP community</i>	✓

3.2.2 OUR PROPOSED BGP-BASED SOLUTIONS

In this section, the proposed BGP-based solutions are explained. The proposed solutions are listed in Table 6. Some of the proposed BGP solution methods can influence the incoming traffic to go through the good IISP and others can control the outgoing traffic.

TABLE 5. CLASSIFICATION OF THE PROPOSED SOLUTIONS.

	BGP Solution Methods	Incoming	Outgoing
<i>Attracker</i>	<i>AS-Path pre-pending</i>	Yes	Yes
	<i>eBGP multihop</i>	Yes	Yes
	<i>Filter outgoing advertisement</i>	Yes	No
<i>Outforwarder</i>	<i>Filter incoming advertisement</i>	No	Yes
	<i>IP static/default route</i>	No	Yes
	<i>Interface counter reset</i>	No	Yes
	<i>MED</i>	No	Yes
	<i>Weight</i>	No	Yes

The solutions that can influence incoming traffic are *AS-Path Pre-pending*, *eBGP multihop* and *Filter outgoing advertisement*. In this work these solutions are called *Attrackers*. 1. *AS-Path Pre-pending* [8] 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 malicious IISP with a longer AS-Path and with a regular AS-Path through the good IISP. Consequently, the Internet ASes will prefer the shortest AS-Path

which goes through the good IISP. 2. *eBGP multihop* [10] command allows indirectly connected ASes to look as if they are directly connected. Consequently, the AS-Path's length between the two configured BGP *speakers* is one hop which means the downstream ASes would prefer that path over all other existing paths that are physically short. But, if there is an AS-Path shorter than this one after implementing the *eBGP multihop* command, it is going to be selected by other routers. 3. *Filter outgoing advertisement* method, through this we 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 malicious IISP and have them only advertised to the good IISP. Consequently, the local prefixes are not included in the advertisements of the malicious IISP to the Internet, and the Internet routers only learn about the local side prefixes through the good IISP. However, the malicious IISP can maliciously hijack the local prefixes attracting the incoming traffic and dropping it.

The *Outforwarders* methods that can control the outgoing traffic are *Filter incoming advertisements*, *IP default/static*, *Interface Counter Reset*, *MED* and *Weight*. 1. *Filtering incoming advertisements* method filters/block the BGP advertisements that coming from the malicious IISP to eliminate its influence on the BGP path selection procedure of the concerned region's BGP *speaker*. This method can be implemented by Access Control List (ACL) commands. 2. *IP default/static route* configuration command can force the outgoing Internet traffic to go through the good IISP, even though BGP routing protocol prefers the malicious IISP path. The routing table algorithm prefers the path that has a lower *Administrative Distance* (AD) value. The *static* route has AD value lower than the BGP AD value. 3. *Interface counter reset* works based on the principal that in BGP path selection procedure, if all the paths to a single destination are identical in all the compared

attributes, the BGP will select the one that has been learned earlier. Through *interface counter reset*, solution the counter of the interface that is connected to a malicious IISP is reset resulting in priority being given to the path through the good IISP. 4. *Weight* and 5. *MED*. The BGP provides particular configuration commands to control the *Weight* and the *MED* values. The path that configured with the highest *Weight* value among the existed paths would be preferred by BGP routing protocol. In contrast, the path that configured with highest *MED* value among the existed paths would not be preferred by BGP routing protocol.

As seen in Table 6, some of the solutions have the ability to forward outgoing traffic via a good IISP and other solutions have the ability to attract incoming traffic. To circumvent malicious IISP blocking we have to combine one solution from the *Outforwarder* list with another solution from the *Attractor* list. Then, configure the concerned region's BGP *speaker* with this combination.

3.3 PROTOTYPE SPECIFICATIONS AND MAIN FEATURES

The BGP-based solutions are evaluated in two laboratory scenarios: identical and non-identical, as illustrated in Figure 2 and Figure 3. The laboratory set up contains seven Cisco 2811 routers, four Catalyst 2950 switches, three workstations and three servers. Routers in the laboratory are configured to provide the desired connectivity and also to implement/execute the blocking at specific time instants. Also, the proposed BGP- based solutions are implemented and executed when blocking is detected. The three servers are

set up as they would be on the Internet side and the workstation as it would be on the local side. Also, each server is assigned to a specific Internet application: FTP, HTTP or VoIP. Furthermore, one of these servers and the workstation are equipped with WireShark [30] network analyzer to collect the performance figures (i.e., throughput, end-to-end delay, and number of lost packets) of each test.

Every solution is tested with the same testing procedure. The testing procedure consists of three dissimilar traffic streams (i.e., FTP, HTTP, and VoIP), and each stream is examined with three different link capacities: 80%, 50% and 25%. Additionally, performance figures for the implemented Internet applications are measured and analyzed. Performance figures include *convergence time*, throughput, and end-to-end delay. The examined Internet applications would be affected by the *convergence time*, the time between detects the blocking and recovers from it. A check is made on whether or not the Internet applications face the same effect in term of throughput, and end-to-end delay. The check, also, is made on whether the BGP-based solutions can recover the blocking faster than each other or not. This allows for a comparison of these solutions based on the effect of *convergence time* upon the performance figures.

Four Java network programs are also programmed to automate the testing environment. The first and the main software program, called here *checker*, is capable of checking the Internet connectivity and measuring a network *convergence time*. The *checker* is installed in one of the workstations on the local side (AS100). When it faces a sequence of timeout messages, it records the time. Then, it immediately and remotely login to the local side (AS100) BGP *speaker* and configures it with one of the BGP-based solutions. The second software configures the malicious IISP (AS300) BGP *speaker* with

the ACL commands to block the outgoing and incoming traffic of the local side (AS100). The third and fourth software are designed to erase the previous configurations to conduct new testing attempts. These four programs are designed to automate the experiment steps and allow a consistent procedure in terms of experiment repeatedness.

3.3.1 MALICIOUS IISP BLOCKING CONFIGURATION

When there are multiple paths to the same destination, the BGP routing protocol inherently prefers one of them based on its path selection procedure. The remaining paths are indicated as backups to be used immediately if the preferred path suddenly goes down. In this work the preferred path is always the path that goes through the malicious IISP. The malicious IISP maintains the exchanged BGP messages, such as *keepalive* messages, and advertisements with the concerned region's BGP *speaker*. At the same time, it blocks the rest of the outgoing and incoming data traffic that is sent by or targeted to the concerned region. Maintaining the exchange of BGP messages with the concerned region's BGP *speaker* would prevent it from switching to one of the backup paths (i.e. via the good IISP) and will continue sending the concerned region's traffic via the malicious IISP.

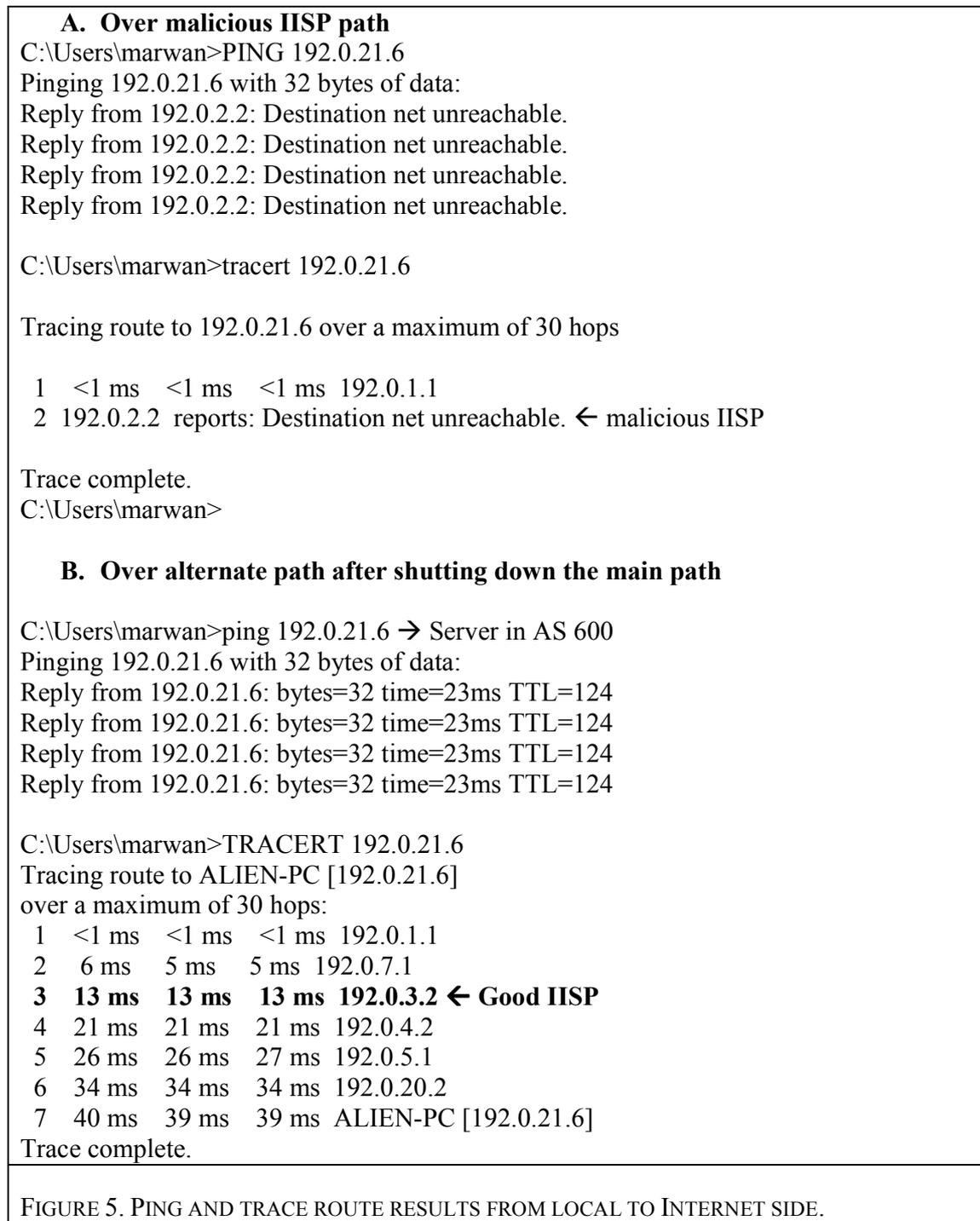
We use ACL to permit the exchange of the BGP messages and advertisements between the malicious IISP and the concerned region BGP *speakers* and to deny the rest of the traffic. Two ACL statements are implemented in the malicious IISP BGP *speaker*, one for blocking the outgoing traffic and another for blocking the incoming traffic. The first one is implemented in the closest interface to the local side, which has 192.0.2.2 as an IP address. The second is implemented in the interface that is closest to the Internet side, which has 192.0.10.1 as an IP address. Figure 4 shows the ACL commands that were applied in the two interfaces of the malicious IISP BGP *speaker*.

```
Interface 192.0.2.2 → block the outgoing traffic
Access-list 101 permit ip any any eq bgp
Access-list 101 deny ip any any
Interface 192.0.10.1 → block the incoming traffic
Access-list 102 deny ip any 192.0.1.0 0.0.0.255
Access-list 102 permit ip any any
```

FIGURE 4. MALICIOUS IISP ACL CONFIGURATION COMMANDS

Figure 5.A shows how the local side BGP *speaker* cannot *ping* to the FTP server after implementing the ACL. Even though the alternative path is available, the local side BGP *speaker* still sends the outgoing traffic via the malicious IISP that is dropping it. Also, in Figure 5.A the *traceroute* result shows the local BGP *speaker* still preferring the path via the malicious IISP (192.0.2.2). After shutting down the main path, the local side can ping

the Internet side and the *tracert* result shows the packets have gone over the good IISP (192.0.3.2) as evident in Figure 7.B.



3.3.2 INTERNET APPLICATION TESTING PROCEDURE

The Internet applications testing procedure is divided into multiple configurations. In each configuration one of the BGP-based solutions is tested with one of the following Internet applications: FTP, HTTP or VoIP under one of the following background traffic load: 80%, 50% or 25%. During testing of the configurations, a network analyzer, Wireshark, is used to collect the required performance figures. Each configuration is tested with the following steps:

1. Configures the link between R6 and R7 with the one of the background traffic load.
2. Run Wireshark and *checker* programs.
3. Run one of the Internet applications' clients, such as FTP client, to communicate with the compatible server.
4. At a specified time instance a program connects to the malicious IISP router and configures it with the blocking configurations.
5. As the *checker* gets sequence of failed replies, it immediately configures the local side BGP *speaker* with one of the BGP solutions, such as *Weight* with *AS-Path pre-pending*.
6. Go to step 2 till all the background loads are visited.
7. Go to step 1 till all the Internet applications are examined.
8. Change the BGP-based solution and go to step 1 until all the BGP-based solutions are evaluated.

3.3.3 CONVERGENCE TIME PROCEDURE

In this part of the testing, the time between detecting the malicious action and recovering from it is measured by the software *checker*. This time includes, the required time for detecting the action, configures the BGP *speaker* with a solution configuration and the required waiting time for getting the echo-replies from the Internet side's server. To be more general, in this work this time is called *convergence time*. Also, this testing procedure is repeated 10 times and the average results are considered.

The *convergence time* testing procedure is as follows:

1. Configures the link between R6 and R7 with the one of the background traffic load.
2. Configures the *checker* with the BGP-based solution.
3. Running the *checker* program.
4. The second software configures the malicious router with the blocking configuration.
5. As the *checker* gets sequence of failed replies, it records the time of blocking, then
6. The *checker* configures the AS100 BGP *speaker* with the BGP solution.
7. The *checker* maintains a sequence of pings to the same application server, and records the time when it gets a successful reply from the server.
8. Run the third and fourth programs to erase the blocking and the solution configurations and clear all the BGP tables.

9. Waiting until the BGP tables of the routers in the laboratory builds again without the effect of the implemented BGP-based solution.
10. Go to step 2, if the number of tries is less than 10.
11. Go to step1 until all the background loads are visited.
12. Go to step1 until all the BGP-based solutions are evaluated.

CHAPTER 4

VALIDATION, PERFORMANCE EVALUATION AND RESULTS

This chapter is divided into three subsections. The first subsection shows the baseline testing. The second subsection illustrates the performance figures of the BGP-based solutions that were proposed by Alrefai [8]. The third subsection illustrates the performance figures of our proposed BGP-based solutions. We have measured the BGP-based solutions with the following background traffic loads: 80%, 50% and 25%. The inter-router links in the laboratory are configured with data rates of 1.544 Mbps. The 80%, 50% and 25% background traffic loads equal to 1.160 Mbps, 758 kbps and 264 kbps, respectively. This means that the links capacities equal to 384 kbps, 786 kbps and 1.28 kbps.

4.1 VALIDATION OF BGP-BASED SOLUTIONS

In the section we validate the capability of the previously discussed methods in controlling outgoing or incoming traffic. The capability of these methods is validated in our testing laboratory: identical and non-identical scenarios. In addition, the methods capability is verified using *traceroute* and the BGP routing table results. After that, subset of the BGP-based solutions will be selected to be evaluated with dissimilar Internet applications and background traffic load. The *traceroute* results of each solution are reported and discussed in Appendix D.

4.1.1 AS-PATH SHORTENING METHOD

This method can influence the BGP path selection procedure of a remote AS. In this method the concerned region prefixes will be originated from the good IISP network. In this way, the AS-Path length will be shortened by one hop. This means that the length of the concerned region's AS-Path that advertised via the malicious IISP will appear in the Internet longer by one hop than the one that advertised via the good IISP. However, if a remote AS is closer to the malicious IISP than the good IISP by more than one hop it will prefer the path through the malicious IISP. This idea is proven after testing this method with the non-identical scenario where the AS-Path length from AS100 to AS600 via the good IISP is longer than the path between the same two ASes via the malicious IISP. Consequently, this method works only in the identical scenario. Figure 6 illustrates a scenario where the good IISP originates the concerned region prefixes and the BGP

speaker of a remote AS (i.e. AS600) sees the AS-Path via the good IISP as being the shortest. The snapshot of *traceroute* result of the validation of this method in our testing laboratory is in Appendix D.

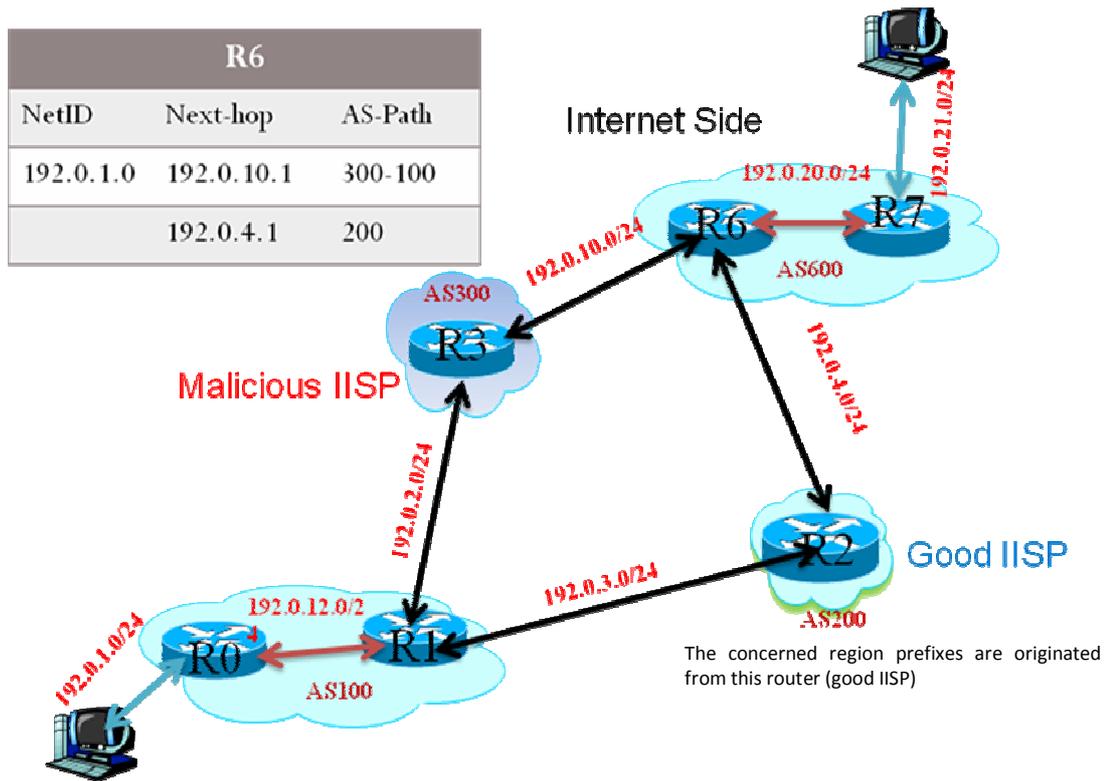


FIGURE 6. AS-PATH SHORTENING EXPLANATORY SCENARIO

4.1.2 MORE SPECIFIC PREFIX METHOD

This method can influence the BGP path selection procedure of a remote AS. The routing table algorithm forwards the traffic over the path associated with the longest prefix match. For example, if we have two paths PATH1 and PATH2 advertising the

same prefix but with different length: PATH1 60.70.80.0/24 and PATH2 60.70.80.0/21. The path associated with the most specific prefix (i.e. PATH1 60.70.80.0/24) will be used to forward the traffic sent to 60.70.80.0 network and PATH2 will be a backup, as shown in Figure 7. Also, the Figure shows an example of the R6 BGP routing table during the validation of this method in our testing laboratory. When the concerned region advertised more specific prefixes via the good IISP, the Internet ASes preferred the path associated with this advertisement which is coming through the good IISP. This method works in both identical and non-identical scenarios.

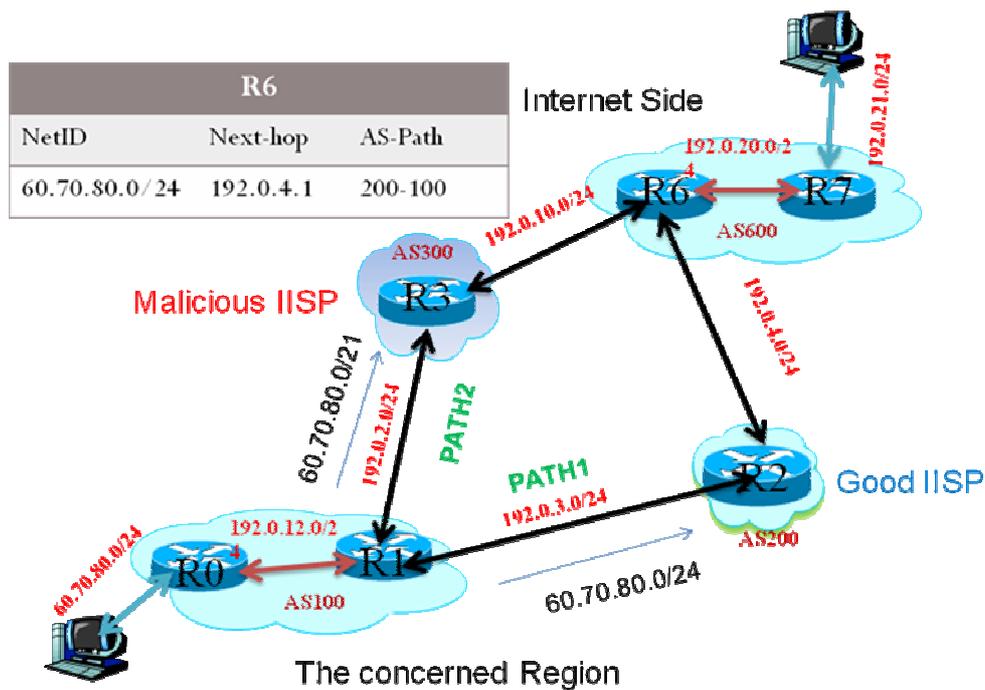


FIGURE 7. MORE SPECIFIC PREFIXES EXPLANATORY SCENARIO

4.1.3 BGP COMMUNITY METHOD

Like the previous two methods, this method can influence the BGP selection procedure of the upstream ASes whenever they implementing the *BGP community*. Usually, upstream ISPs configure its BGP *speaker* with a *community* list that maps between customers' traffic engineering requirements (i.e. Local Preference associated with egress/ingress points) and *community* value. The local AS sends a *community* value within its advertisements to the Internet through a specific upstream IISP, such as the good IISP. While the remote AS receives the *community* request, it performs the traffic engineering function mapped to the *community* value in its *community* list. Moreover, the local AS can send multiple *community* value to perform different traffic engineering functions. Figure 8 illustrates a scenario where the concerned region sends a *community* value within its advertisements to the Internet via the good IISP to attract the incoming traffic through the good IISP. Also, the Figure shows the *community* list where the good IISP and the remote AS are configured with in our testing laboratory. This method succeeded while being tested with identical and non-identical scenario.

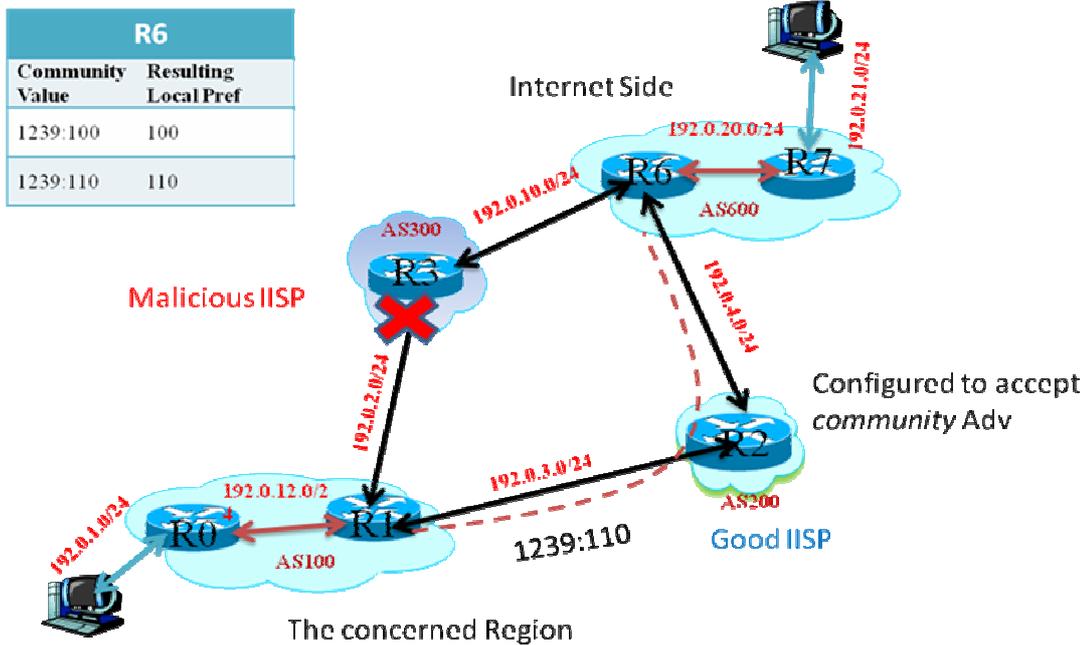


FIGURE 8. BGP *COMMUNITY* EXPLANATORY SCENARIO.

4.1.4 AS-PATH PRE-PENDING METHOD

AS-Path pre-pending method inserts (prepends) extra AS-numbers to the real AS-Path and advertised the resultant AS-Path, defined here as *pre-pended AS-Path*, with the concerned region advertisements to the Internet through the malicious IISP. Thus, the advertised AS-Path through the malicious IISP will appear in the Internet longer than the one that advertised via the good IISP. After validating this method in our testing laboratory (identical and non-identical), we found that the AS-Path pre-pending method can control incoming and outgoing traffic at the same time. Also, it works with identical and non-identical scenario. The method needs some time to converge and the attracting capability is limited by the number of ASes that are added to the real AS-Path. For this reason, the maximum AS-Path length between any two ASes in the Internet must be

identified in order to avoid the possibility of forwarding the incoming traffic via the malicious IISP. Some ASes in the Internet are far away from the good IISP and close to the malicious IISP by number of hops more than the *pre-pended AS-Path* length. The longest *pre-pended AS-Path* in the Internet is 34 ASes and the longest real AS-Path is 11 ASes [31]. In Figure 9 the marked area shows the R6 BGP routing table prefers the AS-Path that goes through the good IISP (192.0.5.2) to the concerned region (192.0.1.1). And the marked area shows all of the AS-Paths that are advertised via the malicious IISP router (192.0.10.2) are pre-pended with 3 extra AS100 values (i.e. 100 100 100).

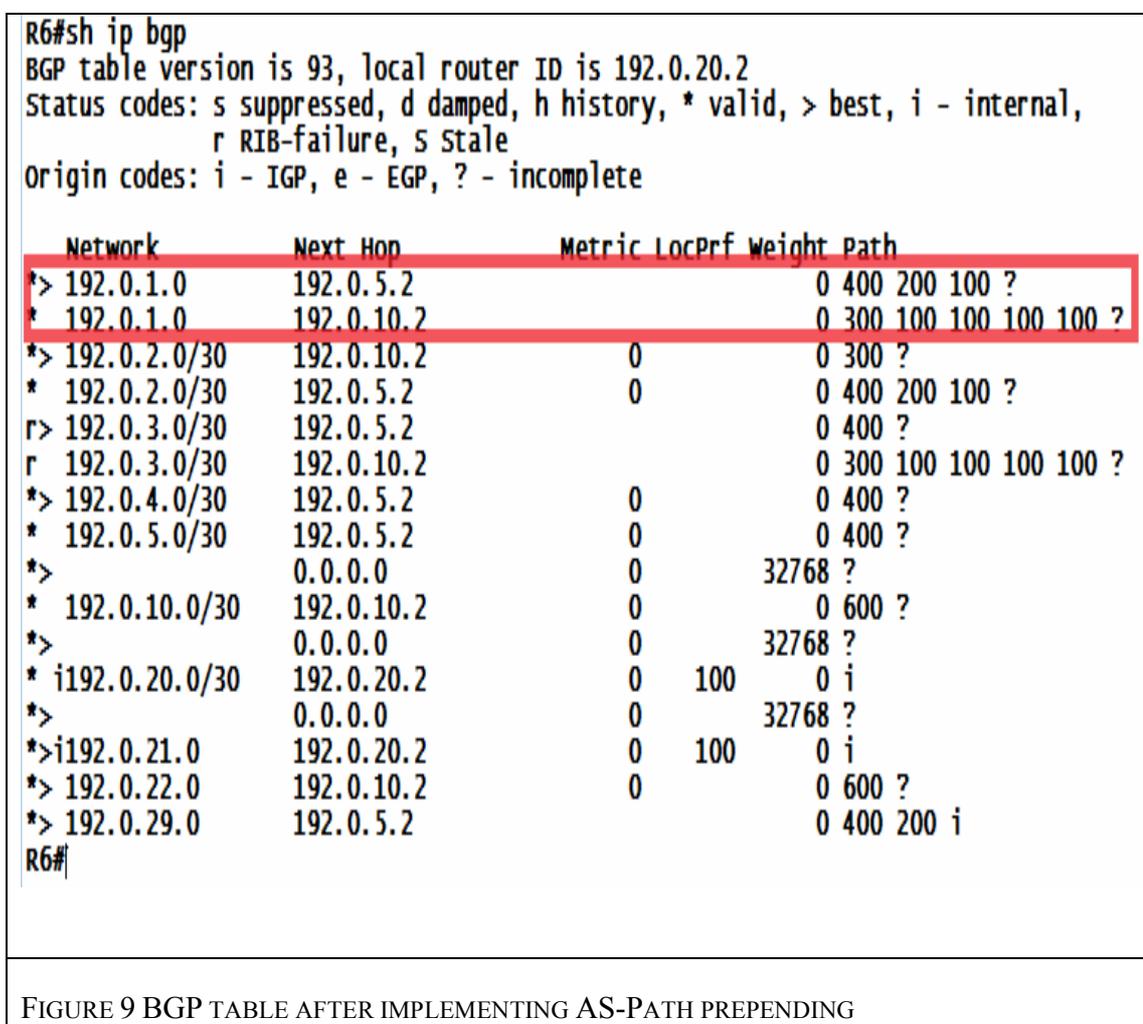


FIGURE 9 BGP TABLE AFTER IMPLEMENTING AS-PATH PREPENDING

4.1.5 EBGP MULTIHOP METHOD

The *eBGP multihop* command allows indirectly connected ASes to appear in the routing table as if they are directly connected. Consequently, the AS-Path's length between the two configured BGP *speakers* is such that the inside and outside BGP routers will prefer their path over all other existing paths that are physically shorter. To fully utilize this method the cooperative AS should reside in a location close to all of the required Internet sources and destinations or the concerned region should cooperate with multiple ASes residing in distinct locations.

This method is similar to the *virtual transit* method that was proposed by [8], but without the overhead and latency of the tunneling protocol. Figure 10 illustrates the implementation of this method in the non-identical laboratory. The AS100 and AS600 are configured with *eBGP multihop* to appear in the routing table as if they are close neighbors. In the *eBGP multihop* configuration, as shown in Figure 11, we should assign to where the traffic between the two *eBGP multihop* ASes has to go. In this configuration step we tell the BGP *speaker* how to reach the new neighbor. For more validation we divided the AS600 into two ASes (AS600 and AS700) and configured AS700 and AS100 with the *eBGP multihop* configuration to make them appear as close neighbors, as illustrated in Figure 12. After this configuration the length of the AS-Path from AS200 to AS700 via AS100 and AS400 are not the same. Yet, the proposed solution, *eBGP multihop*, succeeded with this scenario. The AS100 BGP *speaker* deals with the new neighbor (AS600) as a third IISP and just advertising its prefixes to downstream ASes (AS100 and AS101). The *distribute-list* configuration command allows network engineers to control the network prefixes advertisements. In real Internet BGP

configurations, ISPs use the *distribute-list* configuration command to advertise the prefixes of the downstream ASes. Furthermore, the command allows downstream ISPs to control which prefixes they want to advertise through which upstream ISP. In Figure 13 the marked area shows the AS100 as if it is a direct neighbor to AS600. The marked area, also, shows the interface IP address (192.0.3.1) of the AS100 BGP *speaker* as a physically connected interface with AS600. So, the routing table prefers the path that goes through it (i.e. 192.0.3.1) to the concerned region network.

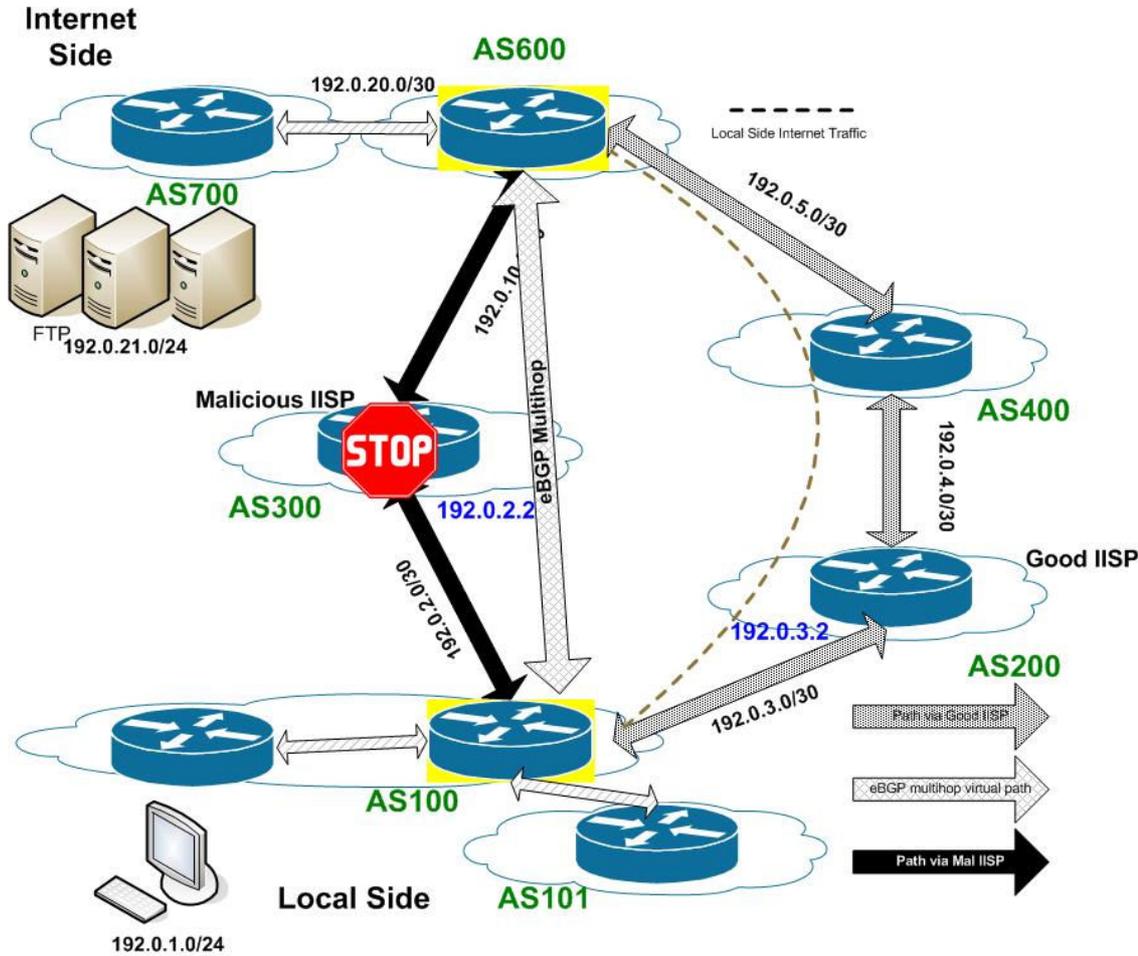


FIGURE 10. eBGP MULTIHOP BETWEEN AS100 AND AS600

```

AS100 BGP Speaker
AS100(config)#router bgp 100
AS100(config-router)#neighbor 192.0.5.2 remote-as 600
AS100(config-router)#neighbor 192.0.5.2 ebgp-multihop
AS100(config)#ip route 192.0.5.0 255.255.255.0 192.0.2.2 ← tell the router how to
reach 192.0.5.0 network

AS600 BGP Speaker
AS600(config)#router bgp 600
AS600(config-router)#neighbor 192.0.3.1 remote-as 100
AS600(config-router)#neighbor 192.0.3.1 ebgp-multihop
AS600(config)#ip route 192.0.3.0 255.255.255.0 192.0.5.1 ← tell the router how to
reach 192.0.3.0 network

```

FIGURE 11. eBGP CONFIGURATION SAMPLE

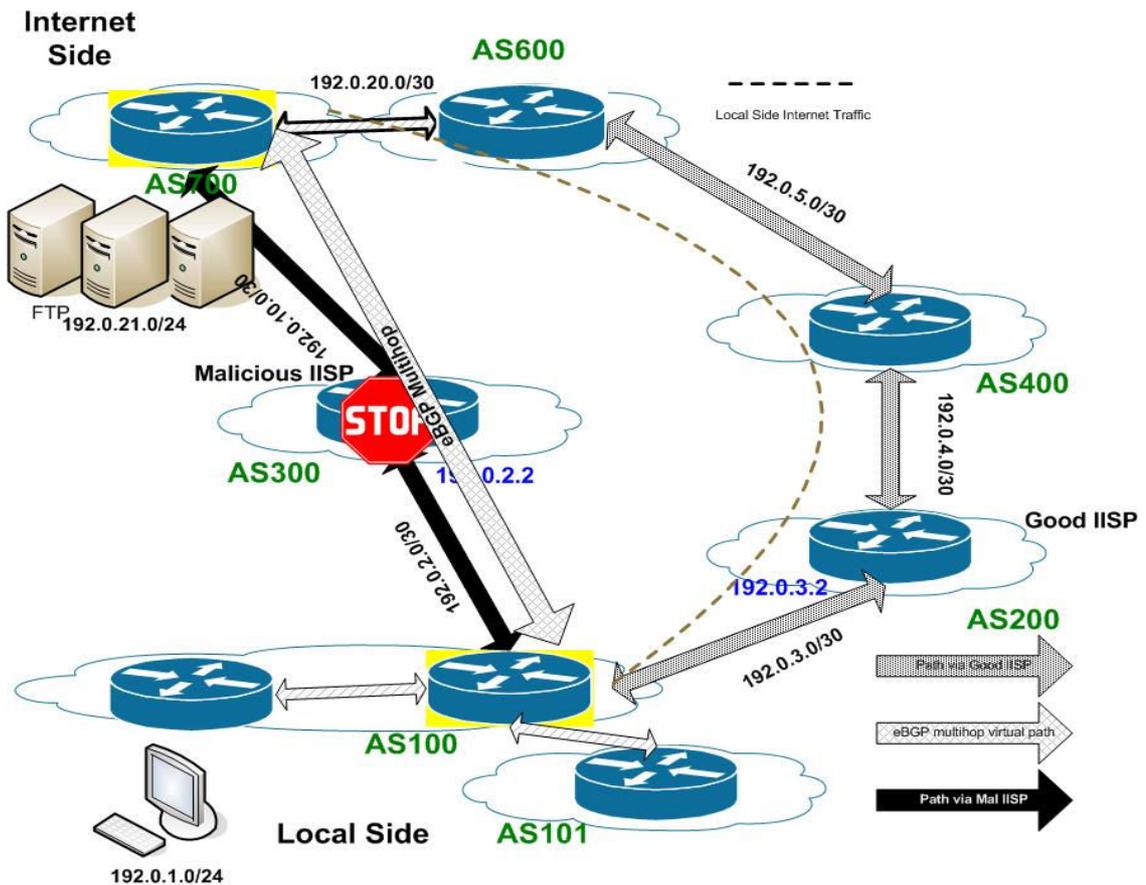


FIGURE 12. eBGP MULTIHOP BETWEEN AS100 AND AS700

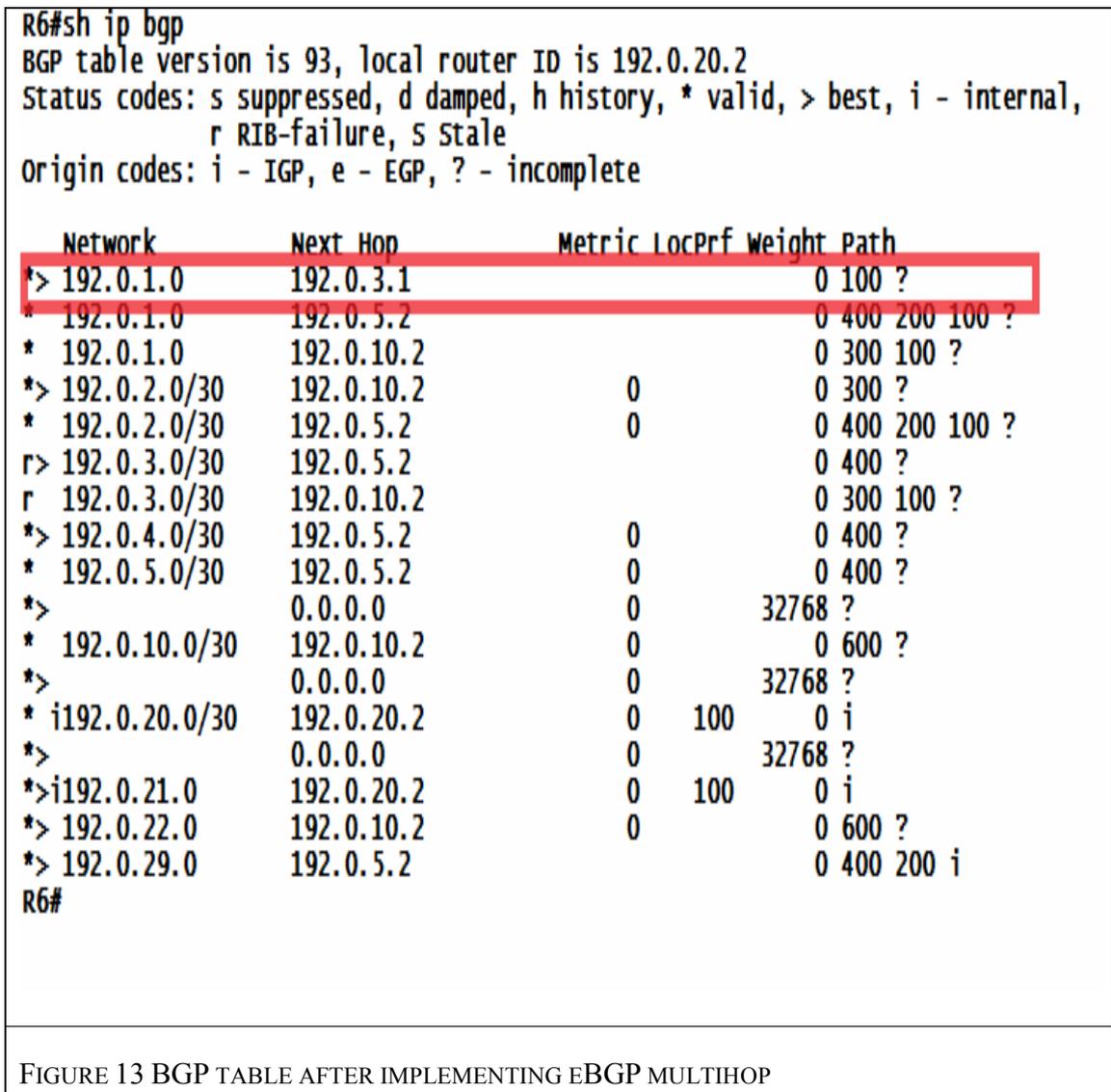


FIGURE 13 BGP TABLE AFTER IMPLEMENTING EBGP MULTIHOP

4.1.6 FILTER ADVERTISEMENT METHOD

Controlling the advertisements from the concerned region router to neighboring (i.e. malicious and good IISP) routers can be achieved through manipulating the *advertisements* and the *advertise-map* BGP configuration commands and ACL commands. These commands enable us to permit or deny specific advertisements to

neighboring routers. After validating this method in our testing laboratory we found that the *filter advertisement* method works in identical and non-identical scenario and requires some time to converge. In the *filter advertisements* method implementation we block the concerned region prefixes from being advertised to the malicious IISP. In this way the concerned region prefixes will not be advertised to the Internet via the malicious IISP. Likewise, instead of advertising the concerned region prefixes, we advertise unused network prefixes, such as 39.110.0.0/16 and 102.60.70.0/24, to mislead the malicious IISP from detecting this method and taking further action. In addition, this method can be used to send the outgoing traffic via the good IISP by blocking the incoming BGP advertisements from the malicious IISP router. Whereas the first implementation can also attract incoming traffic, this implementation can only control outgoing traffic. Figure 14 illustrates a scenario where the AS100 BGP *speaker* instead of advertising the concerned region prefix (60.70.80.0) to the malicious IISP, it advertises the unused prefix (102.80.70.0) to the malicious IISP. The Figure, also, shows an example of the R6 BGP routing table showed during the implementation of this method in our testing laboratory.

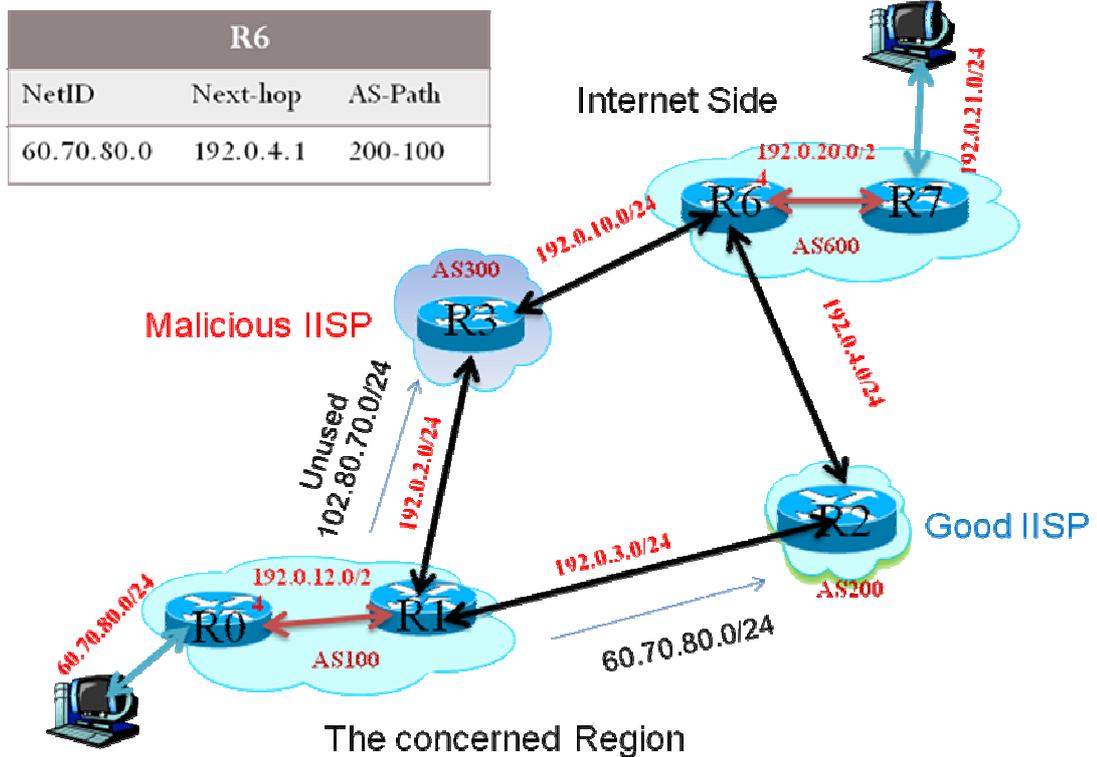


FIGURE 14 FILTERING OUTGOING ADVERTISEMENTS EXPLANATORY SCENARIO.

4.1.7 INTERFACE COUNTER RESET METHOD

When the two paths from source to destination are identical the BGP path selection procedure prefers the path that goes through the oldest interface. The interface counter reset method will reset the counter values of the interface that is connected with the malicious IISP making it the newest. As a result, the interface that is connected with the good IISP will be older and preferred by the BGP path selection procedure. After implementing this method in our testing laboratory, we find that the interface counter reset method is a very simple method and does not require long time in configuration. It

also has an internal effect such that it is not included in BGP messages and advertisements between ASes. Despite these positive characteristics, this method has two major drawbacks. The main drawback of this method involves robustness when the preferred link goes down and up again, it loses its priority as the oldest link. As a result, the non-preferred link gains priority and will be preferred. The second drawback is in that this method only works in the identical scenario. The snapshot of *traceroute* result of the validation of this method in our testing laboratory is in Appendix D.

4.1.8 IP STATIC/DEFAULT METHOD

The IP static method can work with BGP routing protocol at the same time and it has a lower administrative distance (i.e., administrative distance = 1) than the BGP routing protocol (i.e., administrative distance = 170). And, the routing table algorithm prefers the routing protocol that has a lower administrative distance. The main disadvantage of IP static method is that it is not scalable. The network engineer should configure the local BGP *speaker* with all Internet subnets and modifies them whenever they are changed. The IP default method has advantages and disadvantages. The main advantages are that it is easy to configure and it is not included in the BGP messages and advertisements. Also, it can circumvent the isolation in both scenarios: identical and non-identical. In spite of these advantages, the main disadvantage of IP default method is that it can only forward the traffic that is designated to a network that is not included in the BGP routing table. Nevertheless, blocking the incoming advertisements from the malicious router or implementing IP static method could overcome this issue. The snapshot of *traceroute* result of the validation of this method in our testing laboratory is in Appendix D.

4.1.9 MED METHOD

The MED can control outgoing traffic and influence the BGP path selection procedure of the close neighbor AS. In addition, it is not advertised further to subsequent ASes in the path to the destination. Consequently, it does not influence the BGP path selection procedure of the subsequent ASes from source to destination. In addition, as described in background section the BGP path selection procedure prefers the shortest AS-Path over the MED value. However, when all existing AS-Paths for the same destination are identical, like the identical scenario, BGP protocol prefers the path that has the lowest MED value. These characteristics of the MED method were validated in our testing laboratory and we found that the method requires some time to converge and can work only with identical scenario. In Figure 15 the marked area shows the BGP routing table prefers the outgoing path associated with lower MED value = nothing.

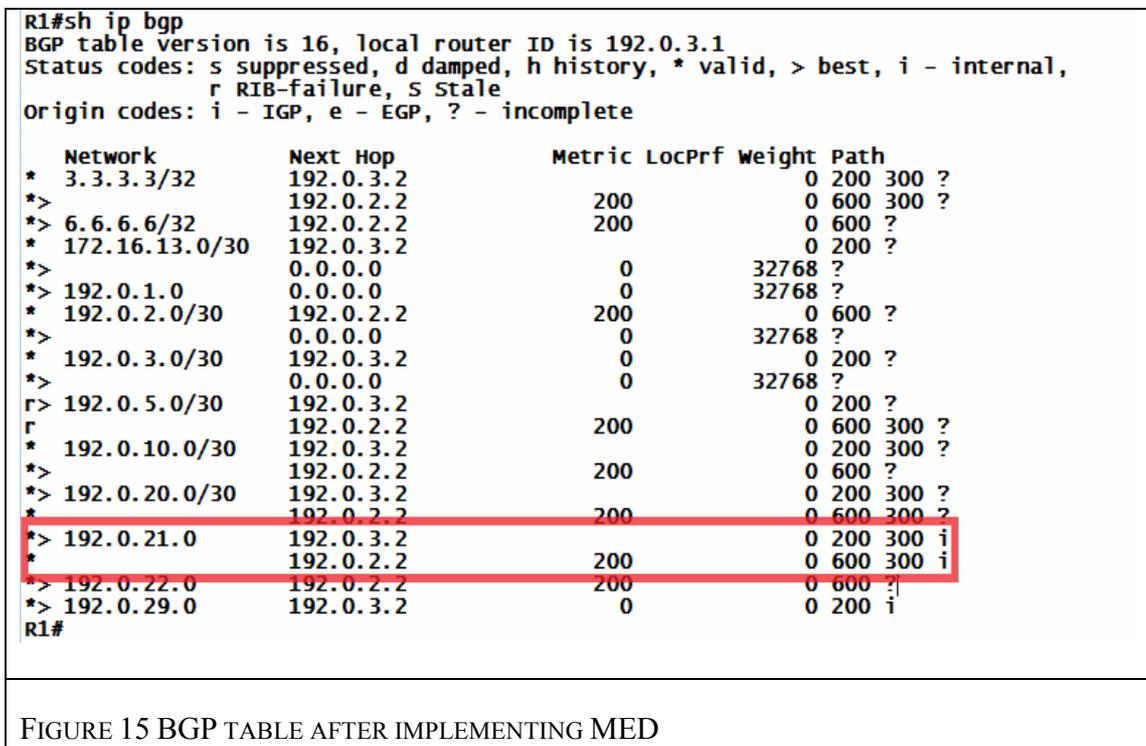


FIGURE 15 BGP TABLE AFTER IMPLEMENTING MED

4.1.10 WEIGHT METHOD

After validating the weight method we found that it could control the outgoing traffic in the identical and non-identical scenarios. It has an internal effect, and it requires time to converge. The marked area in Figure 16 displays the BGP routing table prefers the outgoing path associated with higher *Weight* value = 700 that goes via the good IISP (192.0.3.2). The *Weight* value is neither advertised locally nor externally.

```
R1#sh ip bgp
BGP table version is 15, local router ID is 192.0.3.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network        Next Hop        Metric LocPrf Weight Path
*> 3.3.3.3/32     192.0.3.2             700 200 400 300 ?
*                 192.0.2.2             0 600 300 ?
*> 6.6.6.6/32     192.0.3.2             700 200 400 300 600 ?
*                 192.0.2.2             0 600 ?
* 172.16.13.0/30  192.0.3.2             700 200 400 ?
*>                 0.0.0.0               0 32768 ?
*> 192.0.1.0      0.0.0.0             0 32768 ?
* 192.0.2.0/30    192.0.2.2             0 600 ?
*>                 0.0.0.0               0 32768 ?
* 192.0.3.0/30    192.0.3.2             0 700 200 ?
*>                 0.0.0.0               0 32768 i
*> 192.0.4.0/30    192.0.3.2             0 700 200 ?
*                 192.0.2.2             0 600 300 400 ?
r> 192.0.5.0/30    192.0.3.2             700 200 400 ?
r                 192.0.2.2             0 600 300 ?
*> 192.0.10.0/30   192.0.3.2             700 200 400 300 ?
*                 192.0.2.2             0 600 ?
*> 192.0.20.0/30   192.0.3.2             700 200 400 300 ?
*                 192.0.2.2             0 600 300 ?
*> 192.0.21.0     192.0.3.2             700 200 400 300 i
*                 192.0.2.2             0 600 300 i
*> 192.0.22.0     192.0.3.2             700 200 400 300 600 ?
*                 192.0.2.2             0 600 ?
*> 192.0.29.0     192.0.3.2             0 700 200 i
R1#
```

FIGURE 16 BGP TABLE AFTER IMPLEMENTING WEIGHT

4.1.11 LOCAL PREFERENCE METHOD

After validating the Local Preference method in our testing laboratory we found it can control the outgoing traffic in the identical and non-identical scenarios. It is advertised to the internal BGP routers and it requires time to converge. The marked area in Figure 17 illustrates where the BGP routing table prefers the path associated with higher *Local Preference* value = 700 which goes via the good IISP (192.0.3.2).

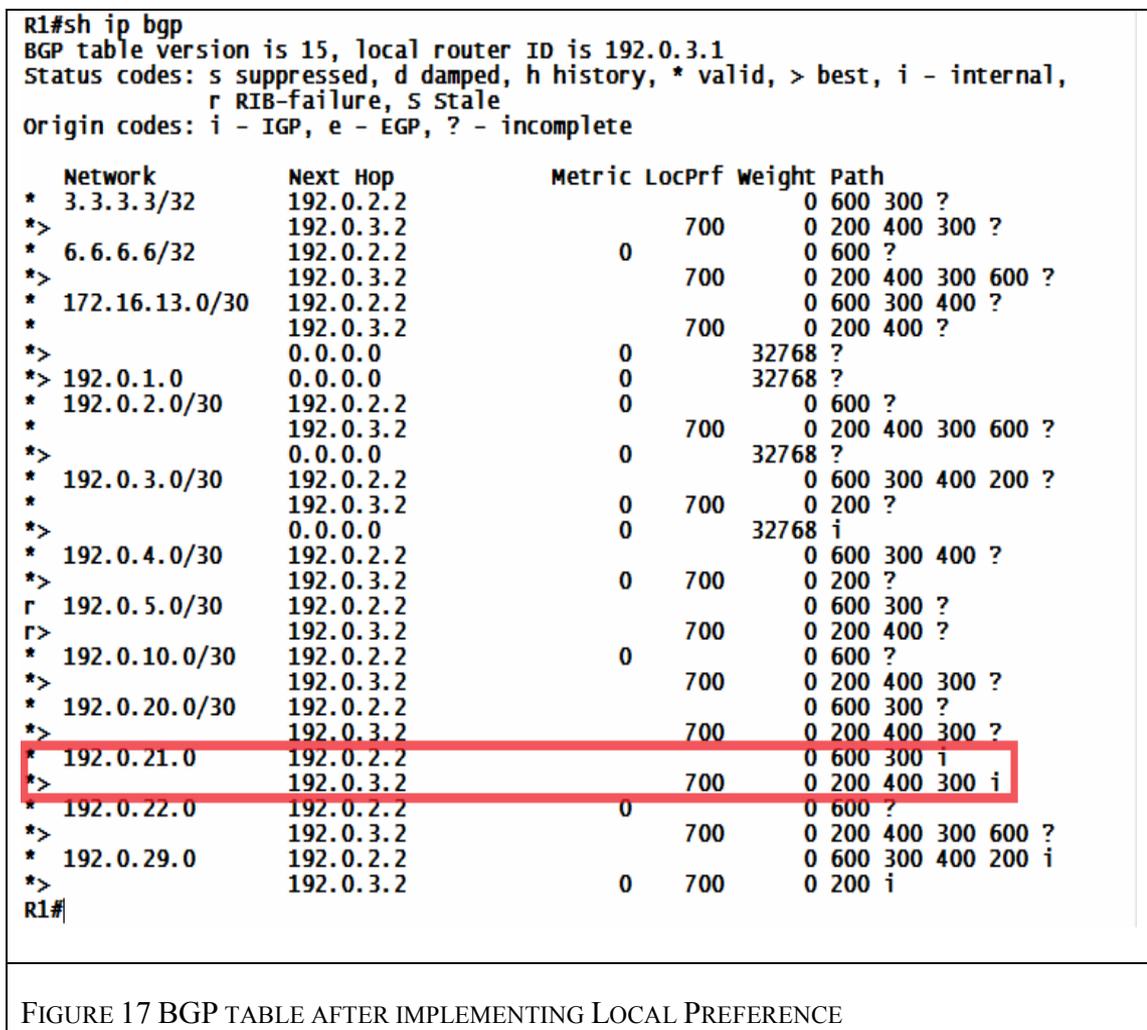


FIGURE 17 BGP TABLE AFTER IMPLEMENTING LOCAL PREFERENCE

TABLE 6. COMPARISON BETWEEN BGP METHODS

	<i>AS-Path shortening</i>	<i>BGP community</i>	<i>More specific prefix</i>	<i>Filter advertisement</i>	<i>AS-Path prepending</i>	<i>eBGP multihop</i>
Setup Overhead	Medium	High	Small	Small	Small	Medium
AS Cooperation	One AS	Several ASes	No	No	No	One AS
Difficulty of Circumvention	Easy	Easy	Easy	Easy	Easy	Difficult
Lab Scenarios	Identical	Both	Both	Both	Both	Both
Scalability	High	High	High	High	High	High

4.2 ADDITIONAL OBSERVATION REGARDING THE PRESENTED SOLUTIONS

In this section, we compare the BGP methods in terms of setup over head, AS cooperation, difficulty of circumvention, laboratory scenarios and scalability, as illustrated in Table 7. The setup overhead is the time and efforts needed to have all the required solution configurations implemented to execute the BGP method. Due to the time and efforts requires to get the BGP *speaker* of the remote AS ready and configured, the *eBGP multihop* method has a medium setup overhead relative to other methods. The *BGP community* method has a medium setup overhead because the required time to implement the *community* configurations on the BGP *speakers* of the cooperative ASes. The remaining methods have a small setup overhead because the complete method

configuration is performed only in the concerned region's BGP *speaker* (i.e., *AS-Path prepending*, *filter advertisement* and *more specific prefix*) or in only two BGP *speakers* (i.e., *AS-Path shortening*).

AS cooperation considers whether the method needs cooperation from one or more ASes in the Internet or not. In *AS-Path shortening* part of the method configurations are implemented in the good IISP's BGP *speaker*. The *BGP community* method needs to be performed in some of the ASes between the concerned region and a destination AS. The *eBGP multihop* method requires cooperation from a particular remote AS. Precisely, it needs to cooperate with multiple ASes in the Internet to prevent, as much as possible, the incoming traffic from going through the malicious IISP.

Difficulty of circumvention includes the quantity of time and efforts required by the malicious IISP to defeat the implemented method. The *AS-Path prepending* and *filter advertisements* methods affect advertisements to the malicious IISP. In contrast, *eBGP multihop*, *BGP community*, *AS-Path shortening* and *more specific prefixes* methods affect advertisements to the good IISP. When a malicious IISP hijacks the concerned region's prefixes the *filter advertisements* method will be defeated. Also, the malicious IISP could overcome *AS-Path prepending* method by blocking the incoming advertisements from the concerned region and hijacks the concerned region's prefixes. Moreover, when a malicious IISP hijacks the concerned region's prefixes and advertises them in a more specific manner than the prefixes that are advertised via the good IISP, the *more specific prefixes* method will be defeated. The *BGP community* method will be defeated when the remote AS or any AS in the path, via the good IISP, from the source to destination is not

performing *BGP community*. Furthermore, the malicious IISP can advertise the concerned region prefixes with the same *community* value advertised through the good IISP. The *eBGP multihop* method is difficult to combat because the concerned region and remote AS are agreed to forward the incoming and outgoing traffic through the good IISP. Also, the remote AS is assumed to be closer to the required destination ASes than the malicious IISP.

The laboratory scenarios means whether the BGP methods succeed while being tested with the testing laboratory scenarios or not. The *AS-Path shortening* method works only with the identical scenario because it shortens the AS-Path only by one hop. The remaining methods succeeded while being tested with identical and non-identical scenarios.

The scalability means the acceptance of expanding the method or implementing it for the entire Internet. All the methods provide high scalability. The prevalence of Internet exchange points (IXP) [32] all over the world supports the position that the most effective and appropriate solution is *eBGP multihop*. The concerned region could make an agreement with multiple IXPs to be the remote peer ASes in the *eBGP multihop* method. However, the methods can attract the incoming traffic through the good IISP, but the methods have some limitations. For example, the ASes that prefer the path that goes through the malicious IISP, those where the malicious IISP is the only service provider for them, those still see the path through the malicious IISP is the shortest, or those ASes that can reach the concerned region only through the malicious IISP.

4.3 THE EVALUATED SUBSET OF THE SOLUTIONS' COMBINATIONS

After validating the capability of the proposed methods in influencing the incoming and outgoing traffic, as discussed in previous subsections. In this work, we select a subset from the possible set of the combinations of our proposed solutions that are posted in Table 6. There are 15 possible combinations from our proposed solutions. The subset of combinations is evaluated with dissimilar Internet applications and background loads. The results of this evaluation are posted and discussed in the performance results subsections. The subset is posted in Table 8 and the corresponding solutions are called herein the considered BGP solutions.

There are several reasons for limiting the number of evaluation to these selected solutions. Some of the solutions are not robustness and scalable (e.g. *IP default/static* and *Interface counter reset*) and some of them require cooperation from remote AS (e.g. *eBGP multihop*). Another reason is that the capability of *MED* and *Filter incoming advertisements* solutions is very similar to *Weight* and *Local Preference* solutions and the latter two attributes are the first two attributes checked by the BGP path selection procedure.

TABLE 7. COMBINATIONS OF THE CONSIDERED BGP-BASED SOLUTIONS

<i>Attractor</i> <i>Outforwarder</i>	AS-Path pre- pending	<i>Filter outgoing</i> <i>advertisements</i>	<i>More specific</i> <i>prefixes</i>
Weight	✓	✓	✓
Local Preference	✓	✓	✓

4.4 PERFORMANCE RESULTS

This section is divided into three subsections. The first subsection shows the baseline testing. The second subsection illustrates the performance figures of the BGP-based solutions that proposed by Alrefai [8]. The third subsection illustrates the performance figures of our considered BGP-based solutions. In BGP routing protocol to execute new changes on the BGP policy and attributes, such as *Weight*, *Local Preference* and prefix advertisements, the BGP sessions must be reset. There two kinds of reset as following: hard reset and soft reset. The hard reset clears all the current BGP sessions to activate the new changes. In contrast, the soft reset activates the new changes without clearing the current BGP sessions.

Over the main path

```
C:\Users\marwan>ping 192.0.21.4 → Server in AS 600
Pinging 192.0.21.4 with 32 bytes of data:
Reply from 192.0.21.4: bytes=32 time=23ms TTL=124
Reply from 192.0.21.4: bytes=32 time=23ms TTL=124
Reply from 192.0.21.4: bytes=32 time=23ms TTL=124
```

```
C:\Users\marwan>TRACERT 192.0.21.6
Tracing route to ALIEN-PC [192.0.21.6]
over a maximum of 30 hops:
  1  <1 ms  <1 ms  <1 ms  192.0.1.1
  2   6 ms   5 ms   5 ms  192.0.12.1
  3  11 ms  11 ms  11 ms  192.0.2.2 ← Malicious HSP
  4  19 ms  19 ms  19 ms  192.0.10.1
  5  31 ms  31 ms  31 ms  192.0.20.2
  6  40 ms  40 ms  40 ms  ALIEN-PC [192.0.21.6]
```

Trace complete.

Over alternate path after shutdown the main one

```
C:\Users\marwan>ping 192.0.21.6 → Server in AS 600
Pinging 192.0.21.6 with 32 bytes of data:
Reply from 192.0.21.6: bytes=32 time=23ms TTL=124
Reply from 192.0.21.6: bytes=32 time=23ms TTL=124
Reply from 192.0.21.6: bytes=32 time=23ms TTL=124
```

```
C:\Users\marwan>TRACERT 192.0.21.6
Tracing route to ALIEN-PC [192.0.21.6]
over a maximum of 30 hops:
  1  <1 ms  <1 ms  <1 ms  192.0.1.1
  2   6 ms   5 ms   5 ms  192.0.12.1
  3  10 ms  10 ms  11 ms  192.0.3.2 ← Good router
  4  19 ms  19 ms  19 ms  192.0.4.2
  5  27 ms  27 ms  27 ms  192.0.20.2
  6  34 ms  34 ms  34 ms  ALIEN-PC [192.0.21.6]
```

Trace complete.

FIGURE 18. *PING* AND *TRACEROUTE* RESULTS FROM LOCAL TO INTERNET SIDE IN OUR LAB OVER THE PREFERRED AND ALTERNATIVE PATHS IN IDENTICAL SCENARIO

4.4.1 BASELINE TESTING

This section shows the baseline results of the Internet applications under different background traffic loads and the basic connectivity and configuration testing of the two laboratory scenarios. Figure 18 shows a ping and *traceroute* results from the local side BGP *speaker* to the FTP server located in the Internet side over the primary path and alternative path in the identical scenario. The primary path passes through the malicious IISP and the alternative path passes through the good IISP. Figure 19 display a ping and *traceroute* results from the local side BGP *speaker* to the FTP server over the primary path and alternative path in the non-identical scenario. Also, Figure 20 illustrates the baseline throughput of the Internet applications under different background traffic load. The y-axis in the figure displays the throughput in bit per second and the x-axis displays the examined Internet applications with different background traffic load. The baseline end-to-end delay of the FTP and HTTP applications under the background traffic load is shown in Figure 21. The y-axis in the figure displays the time in seconds and the x-axis displays the examined Internet applications with different background traffic load (i.e. FTP1.28Mb is FTP stream with 1.28Mbps link capacity). Figure 22 shows the debug results after implementing the *AS-Path prepending + weight* solution in AS100 BGP *speaker*. In both debug results message 1 is the debug output from R1 and message 2 is the debug output from R6. The time required for the BGP table to build up again with hard reset is about 60 seconds and with soft reset is 134 msec.

Over the main path

```
C:\Users\marwan>ping 192.0.21.4 → Server in AS 600
Pinging 192.0.21.4 with 32 bytes of data:
Reply from 192.0.21.4: bytes=32 time=23ms TTL=124
Reply from 192.0.21.4: bytes=32 time=23ms TTL=124
Reply from 192.0.21.4: bytes=32 time=23ms TTL=124
```

```
C:\Users\marwan>TRACERT 192.0.21.6
Tracing route to ALIEN-PC [192.0.21.6]
over a maximum of 30 hops:
 1  <1 ms  <1 ms  <1 ms  192.0.1.1
 2  5 ms  5 ms  5 ms  192.0.2.2 ← Malicious IISP
 3  17 ms  17 ms  17 ms  192.0.10.1
 4  25 ms  25 ms  25 ms  192.0.20.2
 5  33 ms  33 ms  33 ms  ALIEN-PC [192.0.21.6]
```

Trace complete.

Over alternate path after shutdown the main one

```
C:\Users\marwan>ping 192.0.21.6 → Server in AS 600
Pinging 192.0.21.6 with 32 bytes of data:
Reply from 192.0.21.6: bytes=32 time=23ms TTL=124
Reply from 192.0.21.6: bytes=32 time=23ms TTL=124
Reply from 192.0.21.6: bytes=32 time=23ms TTL=124
```

```
C:\Users\marwan>TRACERT 192.0.21.6
Tracing route to ALIEN-PC [192.0.21.6]
over a maximum of 30 hops:
 1  <1 ms  <1 ms  <1 ms  192.0.1.1
 2  6 ms  5 ms  5 ms  192.0.12.1
 3  11 ms  11 ms  11 ms  192.0.3.2 ← Good router
 4  20 ms  20 ms  21 ms  192.0.4.2
 5  27 ms  27 ms  27 ms  192.0.5.1
 6  33 ms  33 ms  34 ms  192.0.20.2
 7  40 ms  39 ms  39 ms  ALIEN-PC [192.0.21.6]
```

Trace complete.

FIGURE 19. *PING* AND *TRACEROUTE* RESULTS FROM LOCAL TO INTERNET SIDE IN OUR LAB OVER THE PREFERRED AND ALTERNATIVE PATHS IN NON-IDENTICAL SCENARIO

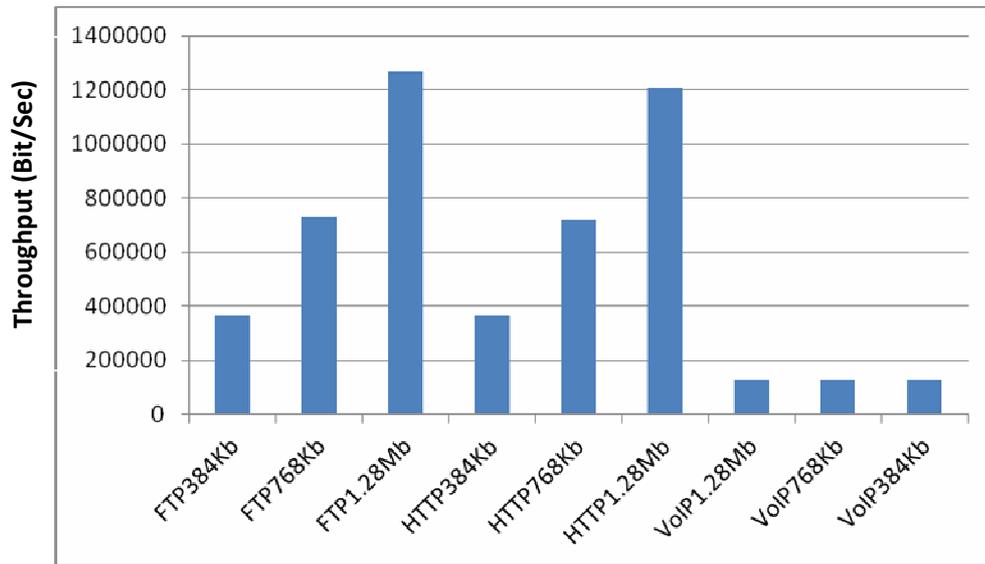


FIGURE 20. THE BASELINE THROUGHPUT OF THE INTERNET APPLICATIONS

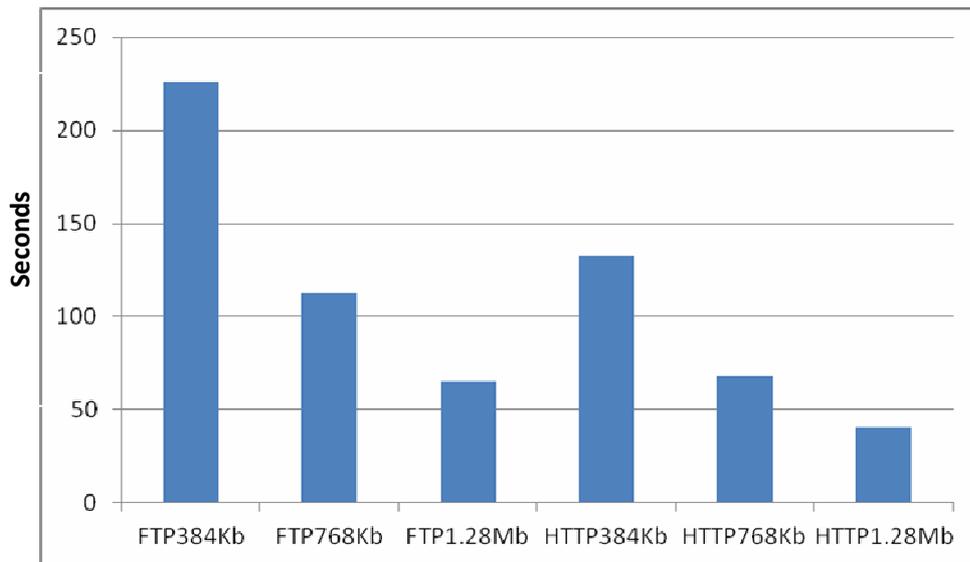
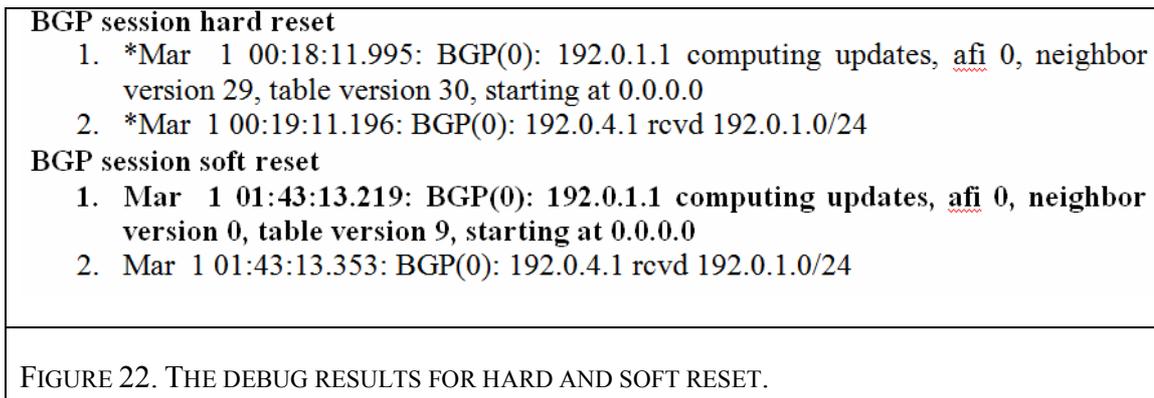


FIGURE 21. THE BASELINE END-TO-END DELAY OF THE FTP AND HTTP APPLICATIONS



4.4.2 PERFORMANCE FIGURES OF BGP-BASED SOLUTIONS THAT WERE PROPOSED BY ALREFAI [8]

We have evaluated the proposed solutions using two different laboratory scenarios, identical and non-identical. We found that the *AS-Path shortening + Local Preference* solutions can work only with the identical scenario. In contrast, the *more specific prefix + Local Preference* and *BGP community + Local Preference* can work in the identical and non-identical scenario. We noticed the HTTP starts slowly in begging of opening the webpage and it is again starts slowly after recovering from the blocking incident.

4.4.2.1 CONVERGENCE TIME RESULTS

The average results of 10 runs of the *convergence time* procedure of each of the BGP-based solutions with different background traffic loads are illustrated in Figure 23 and 24. The y-axis represents the time in seconds and the x-axis represents the evaluated solutions with different background traffic load. Figure 23 displays the hard reset *convergence time* and Figure 24 displays the soft reset *convergence time* compared with the *soft reset*

convergence time results obtained from Alrefai work. The resultant hard reset *convergence time* of the evaluated solutions is between 63 to 64 seconds, and between 0.1 to 0.3 second for soft reset *convergence time*. The obtained *convergence time* of Alrefai work is between 0.3 to 0.6 second. The increase in *convergence time* results of Alrefai is due to the introduced 100 mille second delay while measuring the *convergence time*. The *convergence time* exchanged messages are few in number and small in size. Thus, the affect of the background traffic load on the *convergence time* is very small. The *more specific prefix + Local Preference* solution always gives the fastest *convergence time* even with the different background traffic loads.

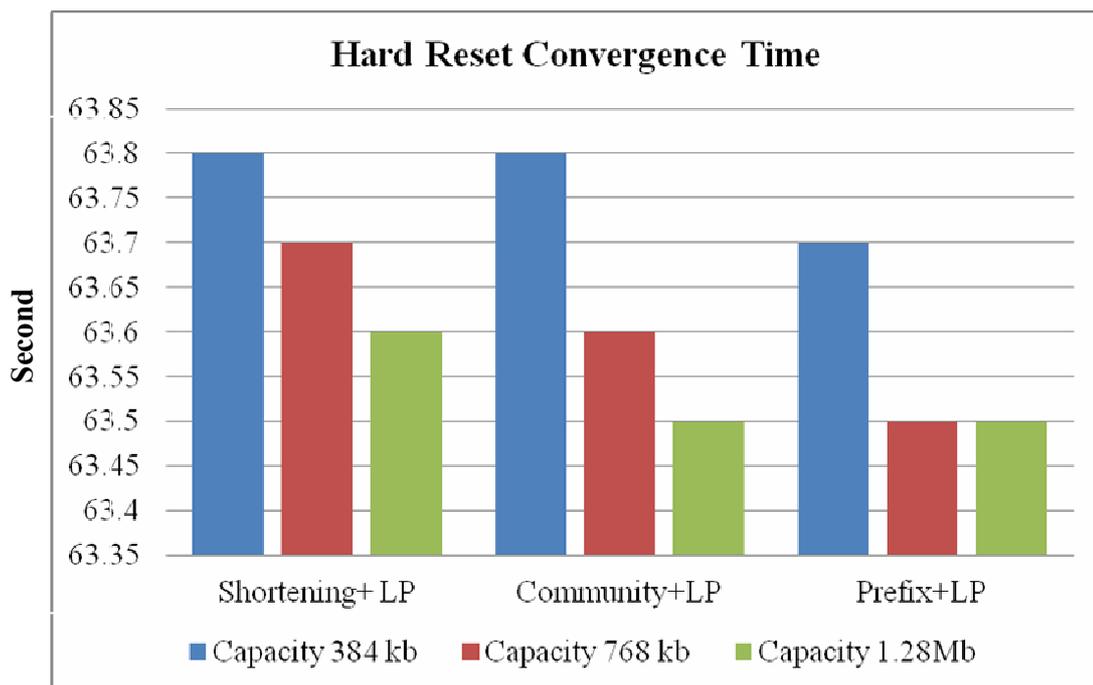


FIGURE 23. HARD RESET CONVERGENCE TIME RESULTS OF THE ALREFAI BGP-BASED SOLUTIONS. NOTE: LP = LOCAL PREFERENCE

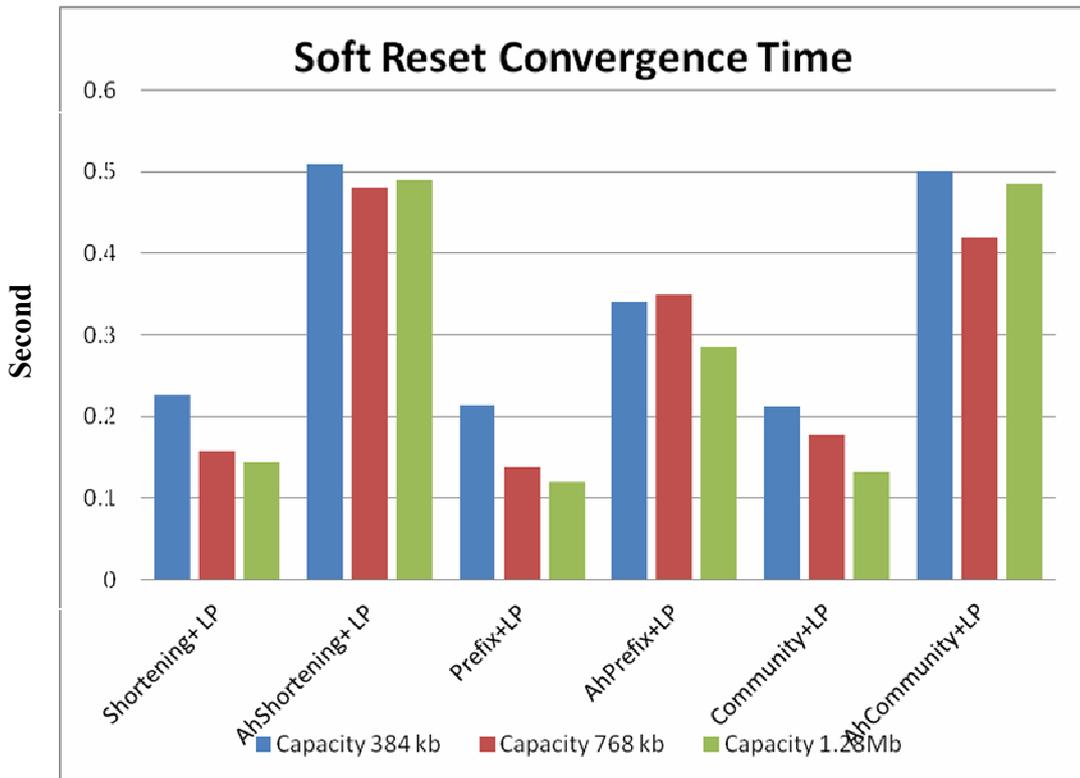


FIGURE 24. SOFT RESET CONVERGENCE TIME RESULTS OF THE ALREFAI BGP-BASED SOLUTIONS. NOTE: LP = LOCAL PREFERENCE, W = WEIGHT AND AH PREFIX ADDED TO ALREFAI RESULTS.

4.4.2.2 THE PERCENTAGE INCREASE IN THE END-TO-END DELAY

The percentage increase in the end-to-end delay of the examined Internet applications is shown in Figure 25. The y-axis in the figure displays the percentage and the x-axis displays the examined Internet applications with different background traffic load. The evaluated solutions are posted on the legend. We examined the FTP end-to-end delay by

downloading a file stored on the FTP server residing in the Internet side from the FTP client installed in the workstation resides in the local side. After downloading 15% of the downloaded file the blocking action is performed, then the solution is activated. The same procedure is performed to examine the HTTP but with 6 MB webpage and the blocking action is performed after downloading 10% of the webpage. This means the hard reset *convergence time* is included in the posted end-to-end delay results in Figure 25. The *more specific prefix + Local Preference* solution provided the lowest end-to-end delay among the evaluated solutions.

4.4.2.3 PERCENTAGE OF TRAFFIC DROP

The percentage of the lost packets for the evaluated BGP solutions is displayed in Figure 26. The y-axis represents the percentage of lost packets in relation to sent packets. By traffic drop, we mean the number of lost packets that were dropped during the blocking incident. The percentage of the lost packets with the HTTP application is double the value of the FTP application. This small percentage proves the sensitivity of the TCP protocol to the carrier. The percentage of the lost packets for the VoIP is in the range of 40% to 41% for all the evaluated solutions and cannot be set in the same graph together with the TCP applications.

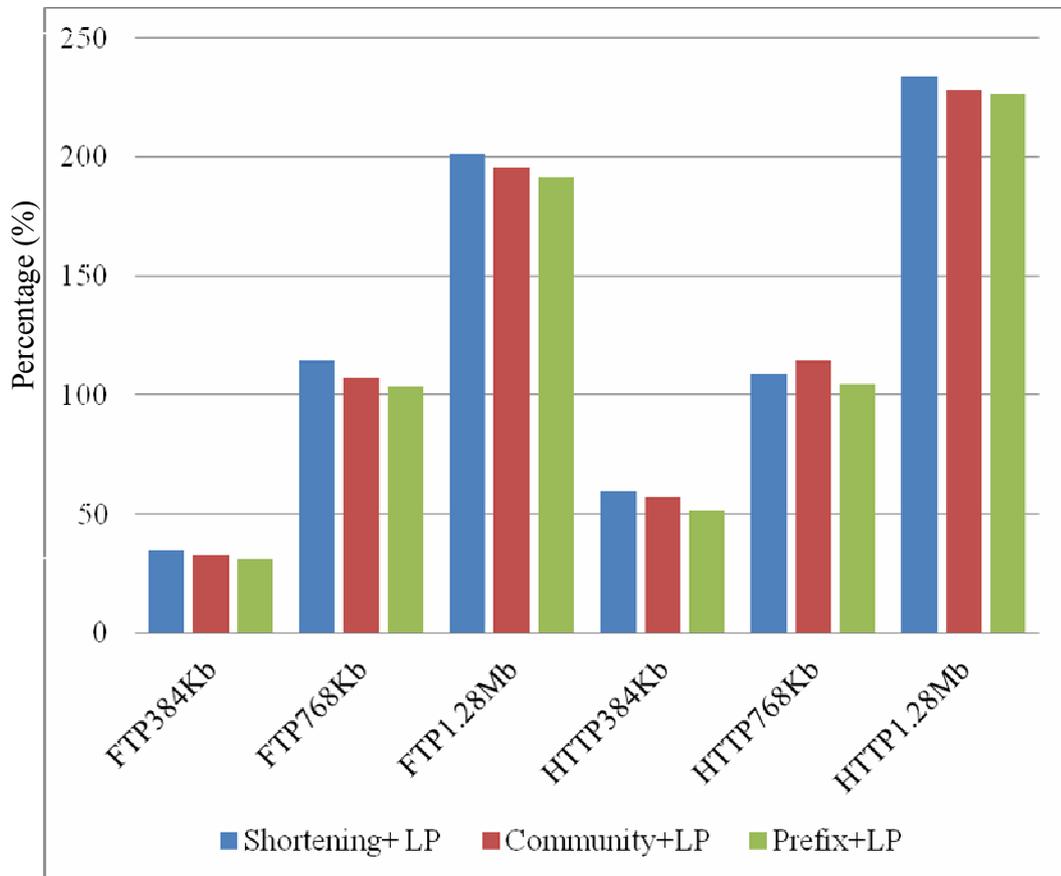


FIGURE 25. THE PERCENTAGE INCREASE IN END-TO-END DELAY OF THE EXAMINED INTERNET APPLICATIONS.

4.4.2.4 SUMMARY

The BGP-based solutions that are proposed by Alrefai [8] were prototyped and evaluated in a real laboratory. The laboratory was configured with the configurations that are usually applied in ISP routers. Furthermore, the solutions were evaluated in two different laboratory scenarios: identical and non-identical. The effects of these solutions were measured by implementing them for different Internet application streams: FTP,

HTTP and VoIP. The evaluating procedures were also conducted with different background traffic loads: 80%, 50% and 25%. The obtained hard reset *convergence time* is in the range of 63 – 64 seconds and soft reset *convergence time* is between 0.1 and 0.3 second for all of the evaluated solutions. The maximum percentage of the end-to-end delay is about 230% found with HTTP1.28Mbps and about 190% with FTP1.28Mbps. The minimum percentage is about 30% found with FTP384kbps and about 55% with HTTP384kbps. All the evaluated solutions succeeded while being tested with identical and non-identical scenarios with the exception of the *AS-Path shortening* solution. This was a result of shortening the AS-Path by only one hop.

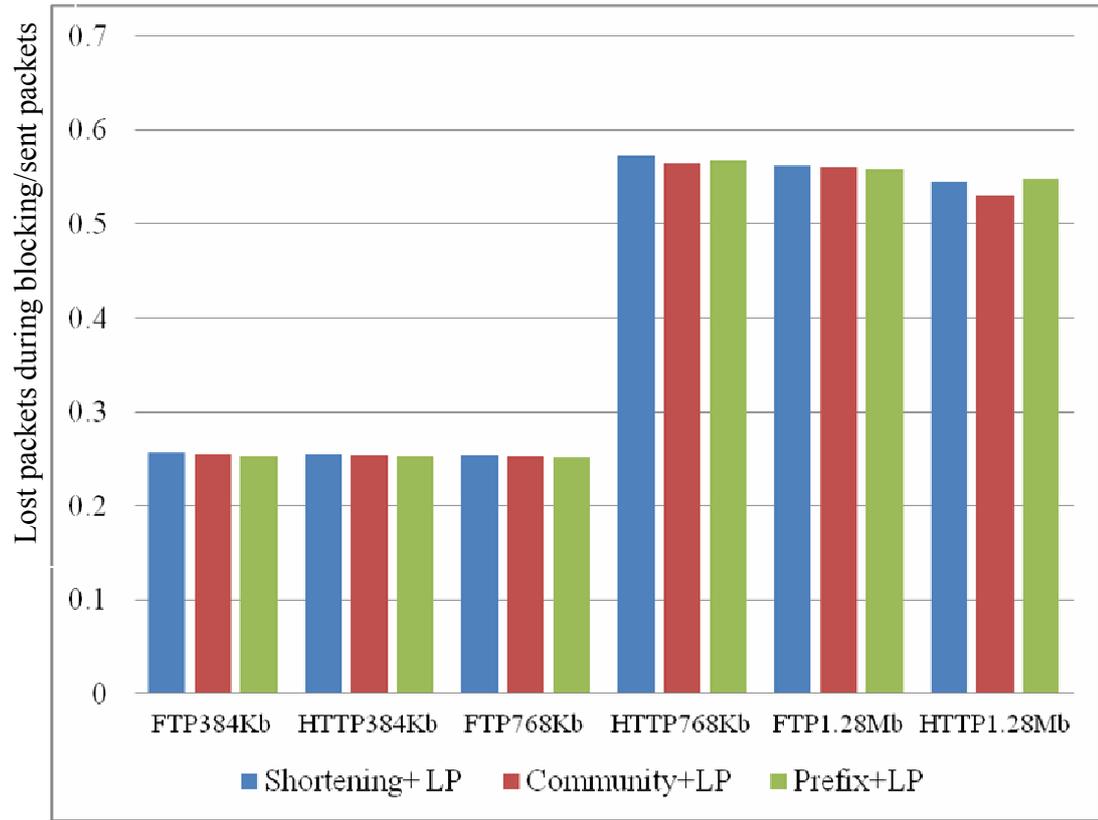


FIGURE 26. PERCENTAGE OF THE LOST PACKETS DURING THE BLOCKING ACTION

4.4.3 PERFORMANCE FIGURES OF THE RECOMMENDED BGP-BASED SOLUTIONS THAT PROPOSED IN THIS WORK

4.4.3.1 CONVERGENCE TIME RESULTS

The average of 10 runs of the *convergence time* procedure of each recommended BGP solutions with different background traffic load are illustrated in Figure 27 and 28. The y-axis represents the time in seconds and the x-axis represents the evaluated solutions with different background traffic load. Figure 27 displays the hard reset *convergence time* and Figure 28 show the soft reset *convergence time*. The result hard reset *convergence time* of the evaluated solutions is between 63 to 64 seconds and the obtained soft reset *convergence time* is between 0.1 and 0.3 second. The *convergence time* exchanged messages are few in number and small in size. Thus, the affect of the background traffic load on the *convergence time* is very small. The combination of *filter outgoing advertisement + weight* always gives the fastest *convergence time* even with the different background traffic load. The *filter outgoing advertisement* solution blocks the concerned region prefixes from being advertised to the Internet through the malicious IISP. Also, it does not change or introduce any load on the BGP advertisements, unlike *AS-Path prepending* and *more specific prefixes* solutions. The same results and capability of the proposed solutions are proved with the non-identical scenario as shown in Figure 29 and 30 for hard reset *convergence time* and soft reset *convergence time*, respectively.

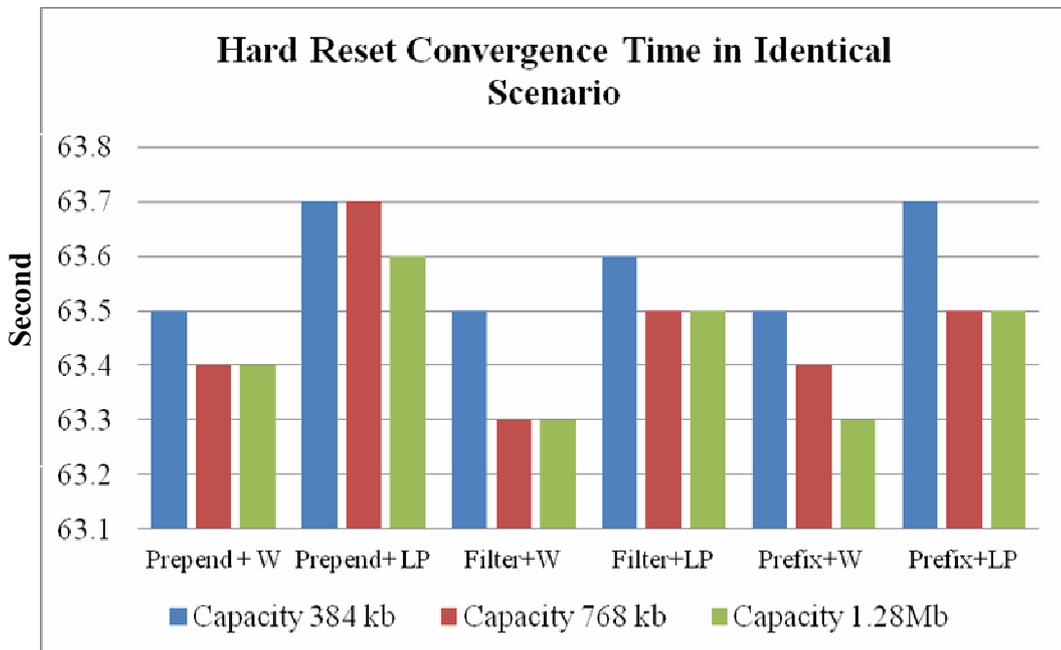


FIGURE 27. HARD RESET CONVERGENCE TIME RESULTS OF THE BGP-BASED SOLUTIONS IN IDENTICAL SCENARIO

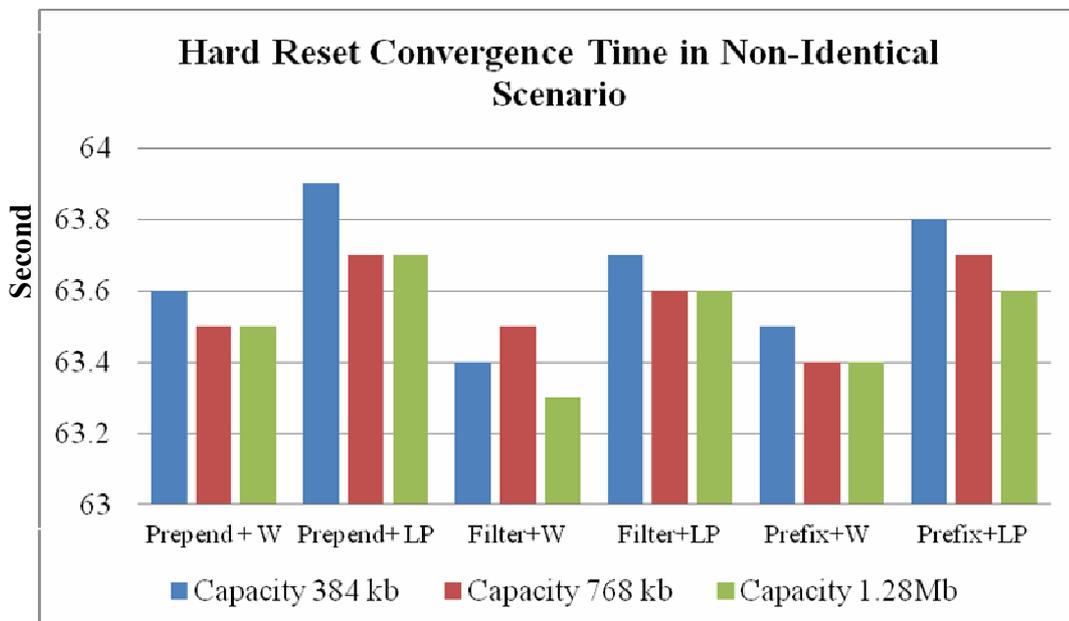


FIGURE 28. HARD RESET CONVERGENCE TIME RESULTS OF THE BGP-BASED SOLUTIONS IN NON-IDENTICAL SCENARIO.

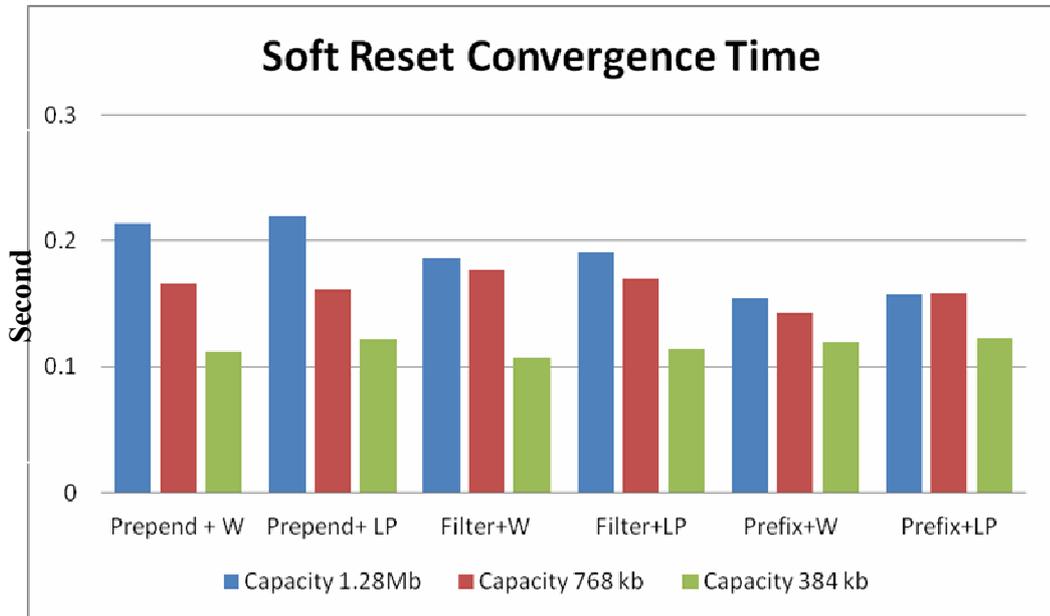


FIGURE 29. SOFT RESET CONVERGENCE TIME RESULTS OF THE BGP-BASED SOLUTIONS IN IDENTICAL SCENARIO.

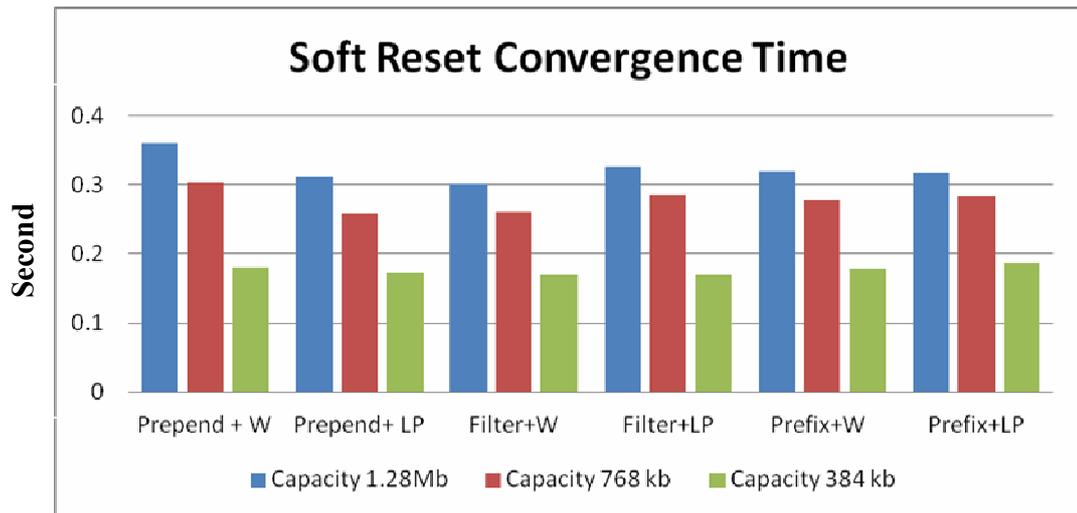


FIGURE 30. SOFT RESET CONVERGENCE TIME RESULTS OF THE BGP-BASED SOLUTIONS IN IDENTICAL SCENARIO

4.4.3.2 PERFORMANCE FIGURES FOR FTP STREAM

END-TO-END DELAY

In this section the end-to-end delay of the FTP application in the identical and non-identical scenario is discussed and the results are shown in Figure 31 and 32, respectively. The y-axis in the figure displays the time in seconds. The evaluated solutions are posted on the legend. We examined the FTP end-to-end delay by downloading a 10 MB file stored on the FTP server residing in the Internet side (AS600) from the FTP client installed in the workstation resides in the local side (AS100). After downloading 15% of the downloaded file the blocking action is performed, then the solution is activated. This means that the hard reset *convergence time* is included in the posted end-to-end delay and the percentage increase results in the two figures. The combination of the *filter outgoing advertisements + Weight* solution provided the lowest end-to-end delay among the evaluated solutions followed by *more specific prefixes + Weight* solution with small difference in time. The end-to-end delay increases proportionally with the increase in the background traffic load. There is a small difference between the end-to-end delay results of the identical and non-identical scenarios. Figure 33 and 34 illustrate the percentage increase in the end-to-end delay of the FTP application in the identical and non-identical scenarios, respectively. The percentage of the end-to-end delay increases inversely with the increase in the background traffic load. Besides, the differences in end-to-end delay

between the evaluated solutions are in the range of 6%. Also, the difference between the end-to-end delay results from the identical and non-identical scenarios is in the range of 6%. Moreover, the differences in the percentage of end-to-end delay between the evaluated solutions are in the range of 18%. And, the difference between the percentage of the end-to-end delay results from the identical and non-identical scenario is in the range of 16%.

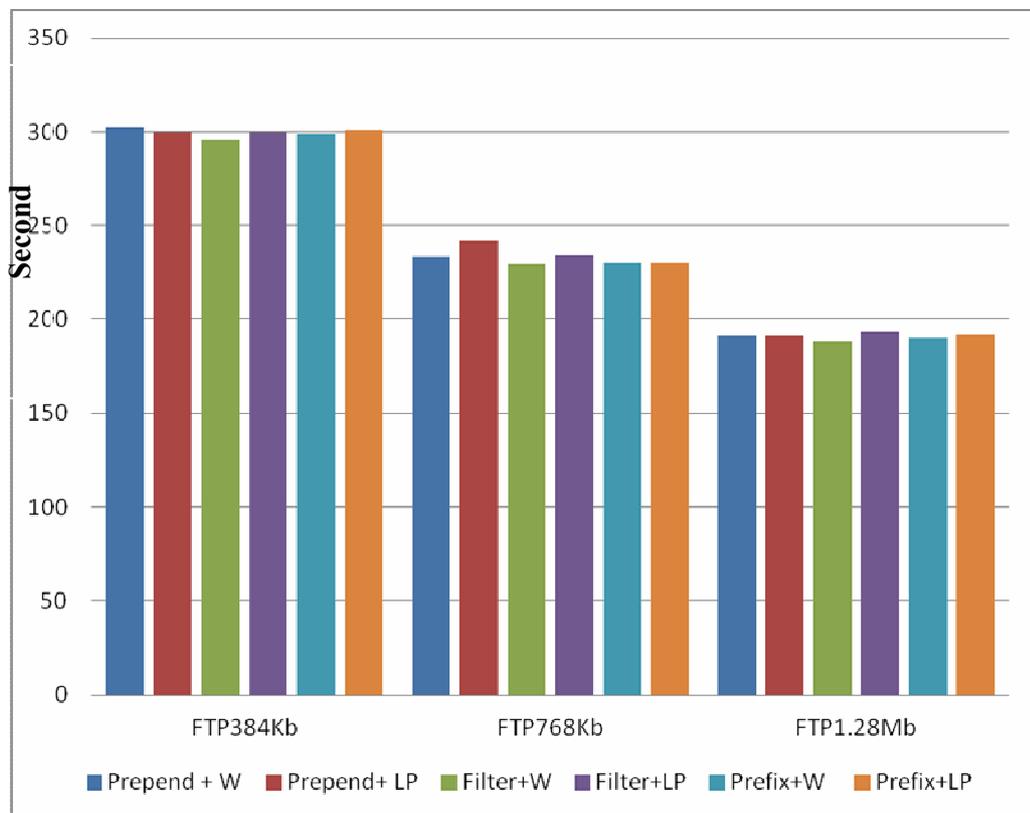


FIGURE 31. END-TO-END DELAY OF THE FTP APPLICATIONS IN IDENTICAL SCENARIO

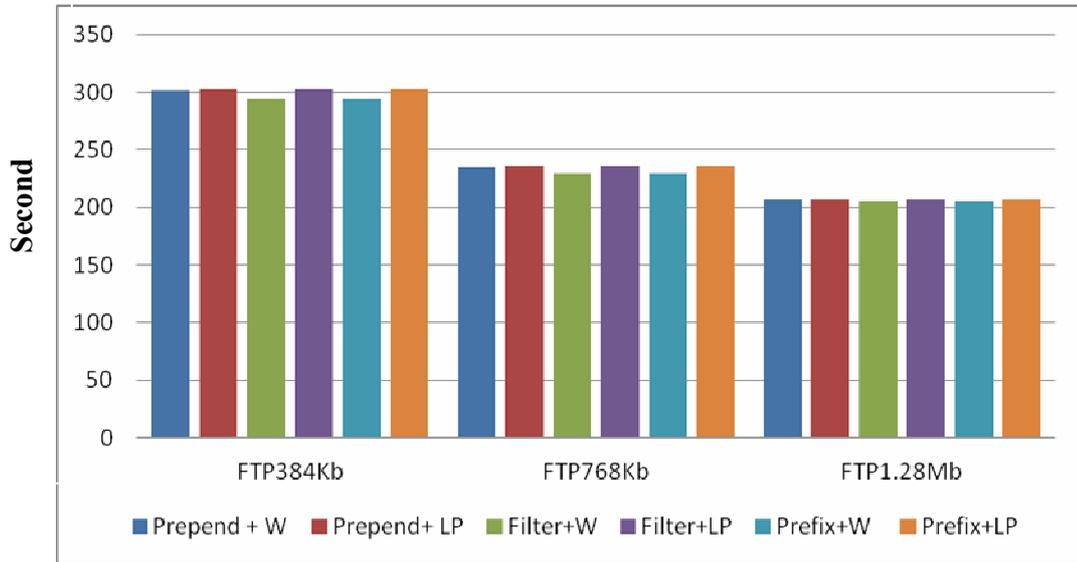


FIGURE 32. END-TO-END DELAY OF THE FTP APPLICATION IN NON-IDENTICAL SCENARIO

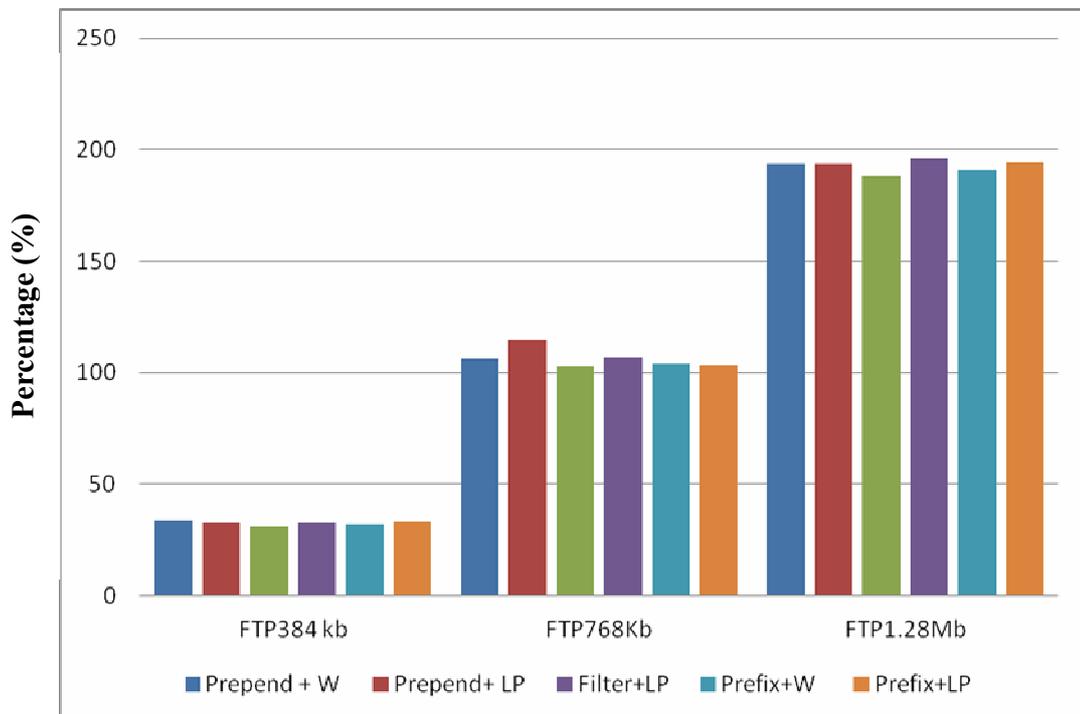


FIGURE 33. PERCENTAGE INCREASE OF END-TO-END DELAY OF THE FTP APPLICATION IN IDENTICAL SCENARIO.

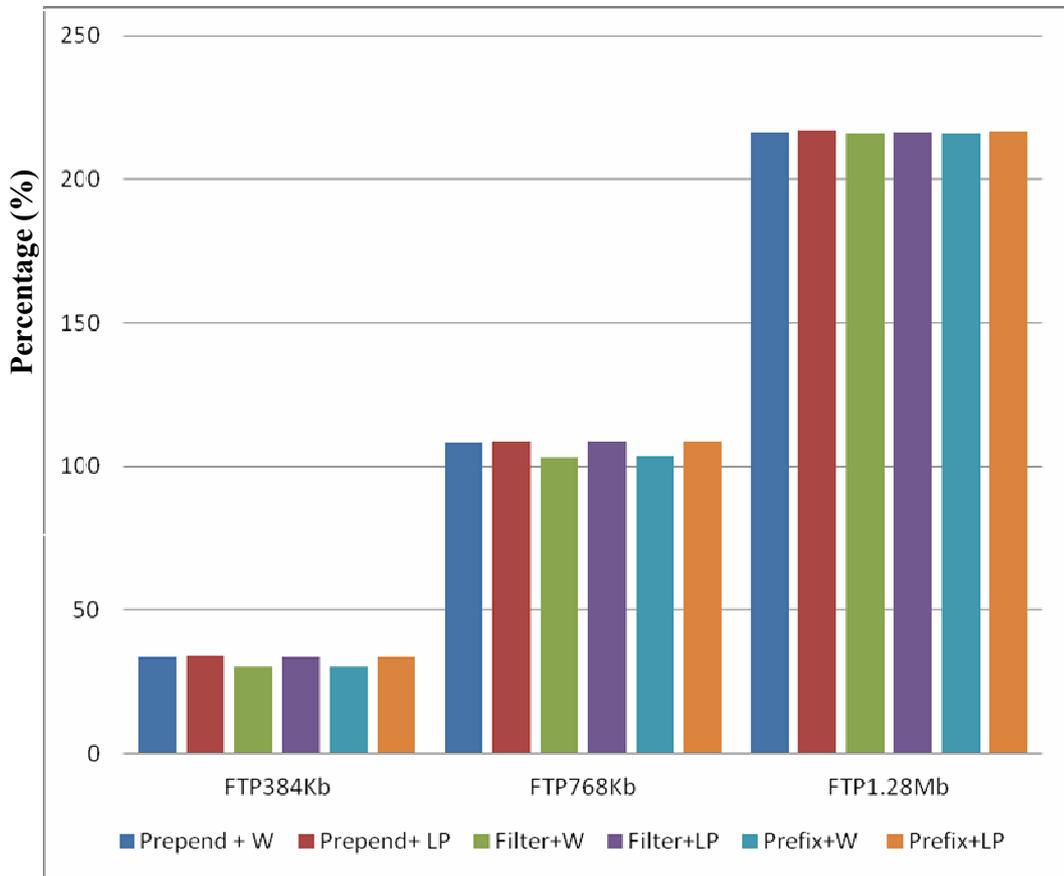


FIGURE 34. PERCENTAGE INCREASE IN END-TO-END DELAY OF THE FTP APPLICATION NON-IDENTICAL.

PERCENTAGE OF TRAFFIC DROP

The percentage of the lost packets for the evaluated BGP solutions in the identical and non-identical scenario is displayed in Figure 35 and Figure 36, respectively. The y-axis represents the percentage of lost packets in relation to sent packets and the x-axis represents the examined FTP application with dissimilar background traffic load. By

traffic drop, we mean the number of lost packets that were dropped during the blocking incident. Obviously, since there was no significant difference in the *convergence time* of the evaluated solutions, there will not be a significant difference on the number of the lost packets. This small percentage proves the sensitivity of the TCP protocol to the carrier. In summary, the differences in the percentage of lost packets between the evaluated solutions are in the range of 8%. Also, the difference between the percentage of the lost packets results in the identical and non-identical scenario is in the range of 15%.

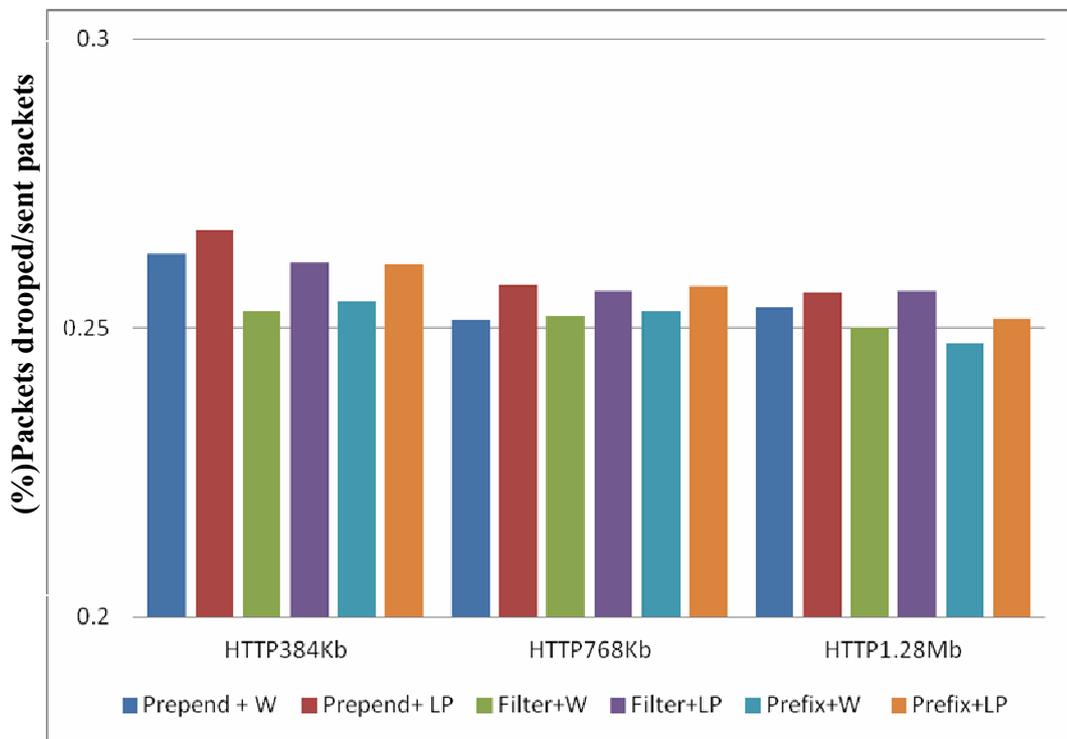


FIGURE 35. PERCENTAGE OF TRAFFIC DROP OF THE FTP APPLICATIONS IN IDENTICAL SCENARIO

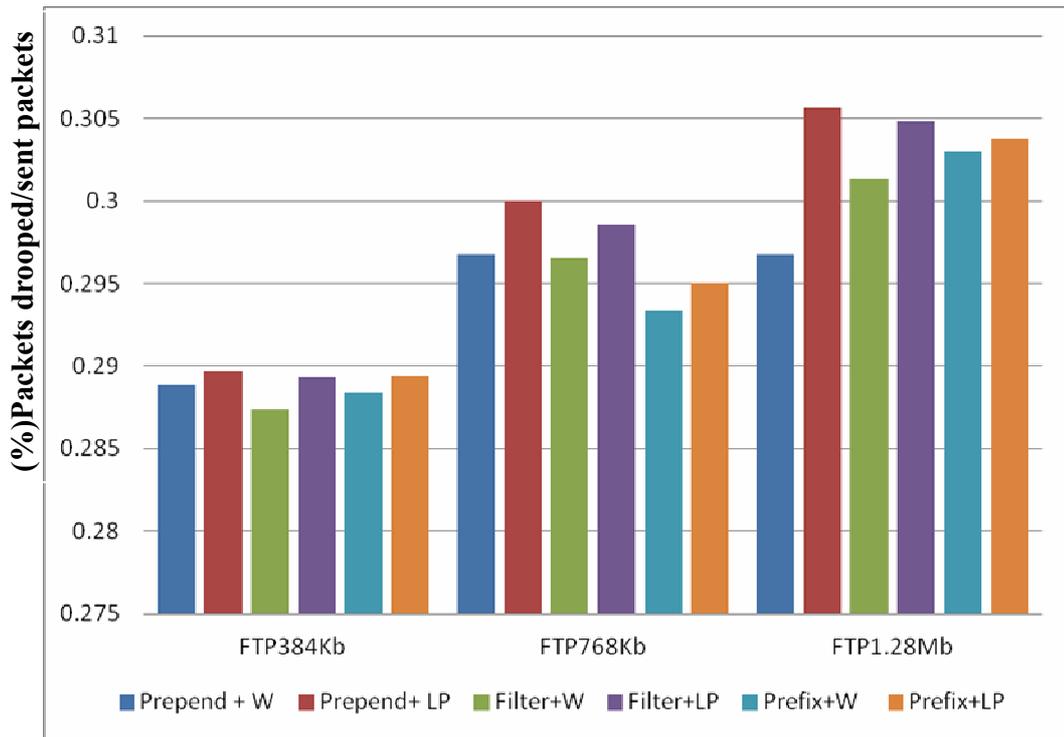


FIGURE 36. PERCENTAGE OF TRAFFIC DROP OF THE FTP APPLICATIONS IN NON-IDENTICAL

AVERAGE THROUGHPUT

The average throughput in bits per second of the examined FTP application with the evaluated solutions is depicted in Figure 37 and 38. The y-axis represents the bits per second values and the x-axis represents the examined FTP application with different background traffic load. The evaluated solutions are displayed on the legend. We examined the FTP average throughput by downloading a 10 MB file stored on the FTP server residing on the Internet side (AS600) from FTP client installed in the workstation residing on the local side (AS100). The posted average throughputs in the two figures are

affected by the hard reset *convergence time*. The TCP applications proved their sensitivity to the link capacity where their throughput increased proportionally with the increase in link capacity. The combination of *filter outgoing advertisements + Weight* solution provided the highest average throughput among the evaluated solutions followed by *more specific prefixes + Weight* solution without much difference in throughput. In summary, the differences in average throughput between the evaluated solutions are in the range of 7%. Also, the difference between the average throughput results in the identical and non-identical scenario is in the range of 9%.

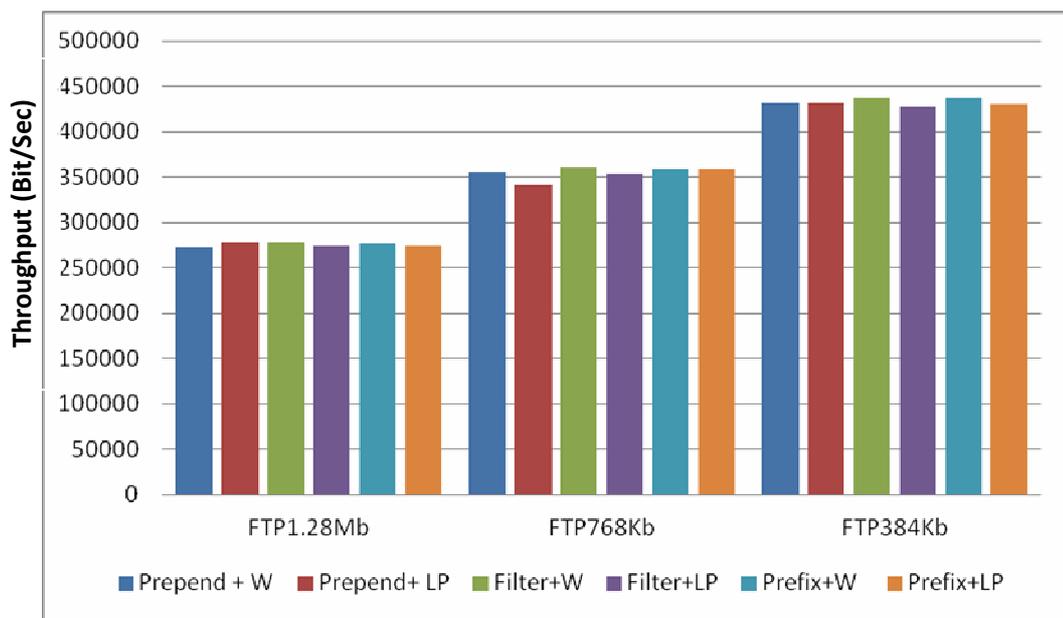


FIGURE 37. AVERAGE THROUGHPUTS OF THE FTP APPLICATIONS IN IDENTICAL SCENARIO

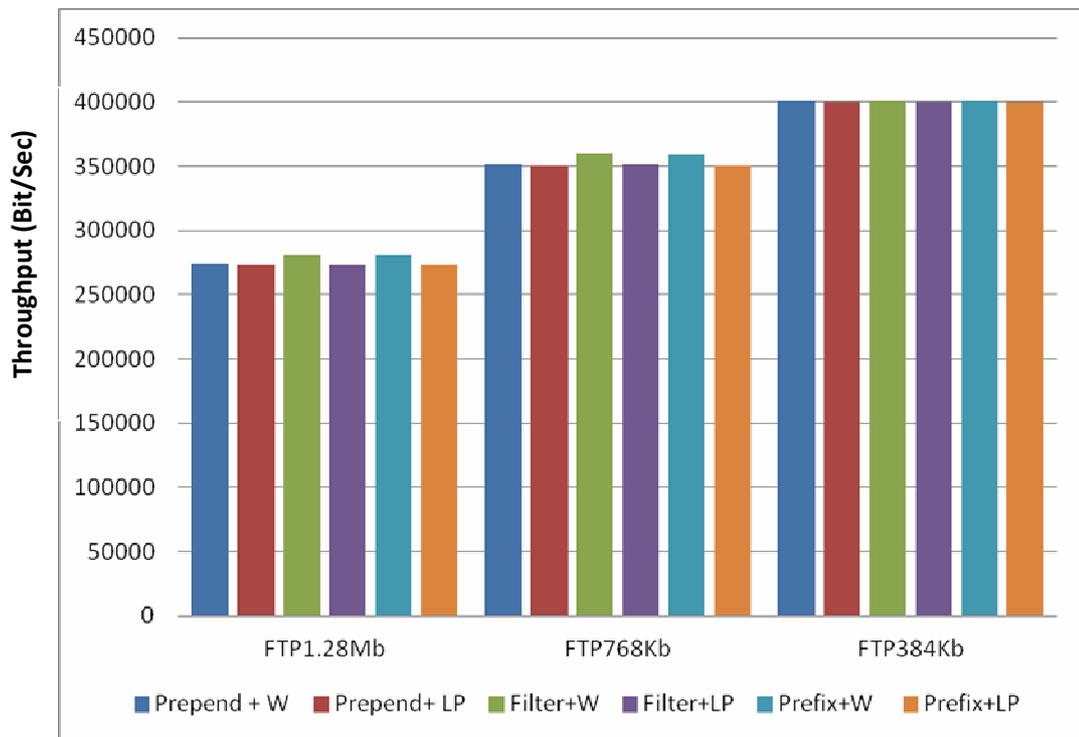


FIGURE 38. AVERAGE THROUGHPUTS OF THE FTP APPLICATION IN NON-IDENTICAL SCENARIO

4.4.3.3 PERFORMANCE FIGURES FOR HTTP STREAM

END-TO-END DELAY

In this section the end-to-end delay of the HTTP application in the identical and non-identical scenarios is investigated and the results are shown in Figure 39 and 40, respectively. The y-axis in the figure displays the time in seconds and the x-axis displays the examined Internet applications with different background traffic load. The evaluated solutions are posted on the legend. The end-to-end delay increases proportionally with the increase in the background traffic load. Figure 41 and 42 illustrate the percentage increase in the end-to-end delay of the examined Internet applications. The end-to-end delay of the

HTTP application increases proportionally with the increase in the background traffic load. The obtained end-to-end delay includes the hard reset *convergence time*. Also, the percentage increase in the end-to-end delay of the HTTP application increases inversely with the background traffic load. In summary, the differences in end-to-end delay between the evaluated solutions are in the range of 5%. Also, the difference between the end-to-end delay results from the identical and non-identical scenarios is in the range of 6%. Moreover, the differences in the percentage of end-to-end delay between the evaluated solutions are in the range of 16%. And, the difference between the percentage of the end-to-end delay results from the identical and non-identical scenarios is in the range of 16%.

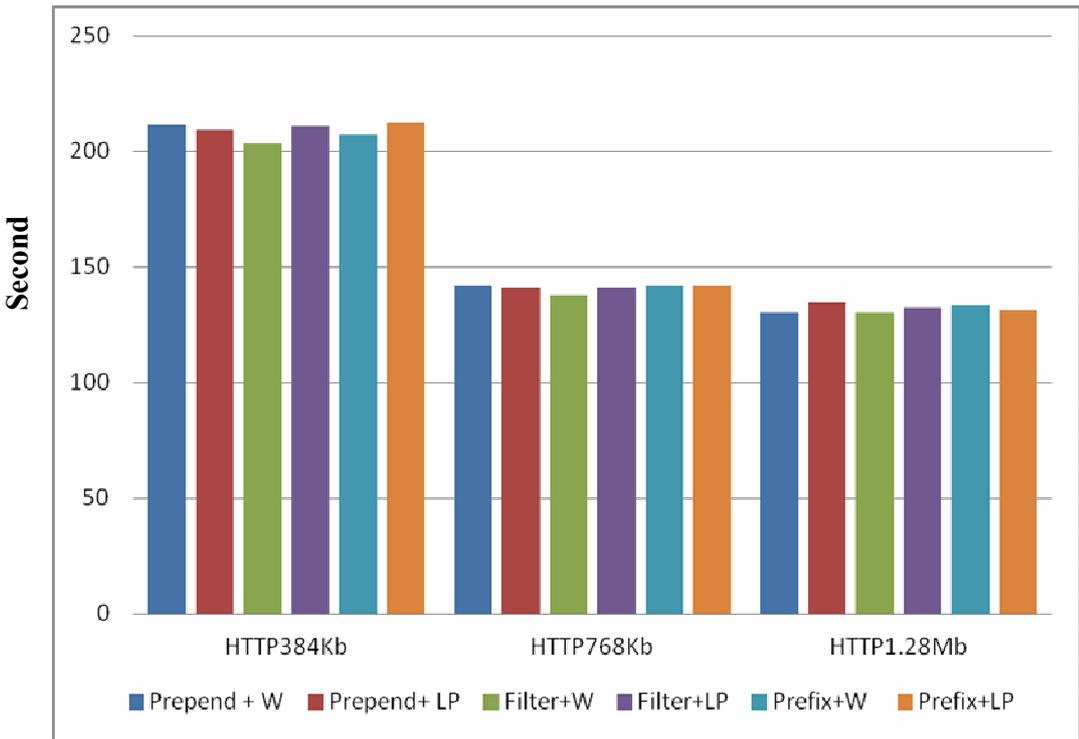


FIGURE 39. END-TO-END DELAY OF THE HTTP APPLICATIONS IN IDENTICAL SCENARIO

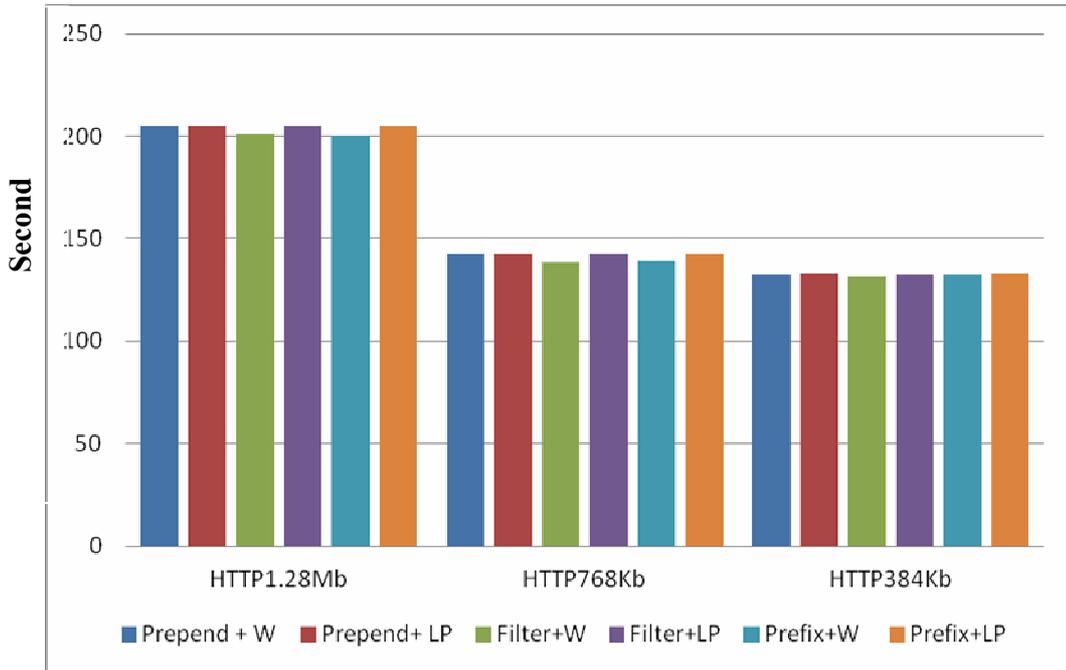


FIGURE 40. END-TO-END DELAY OF THE HTTP APPLICATIONS IN NON-IDENTICAL SCENARIO

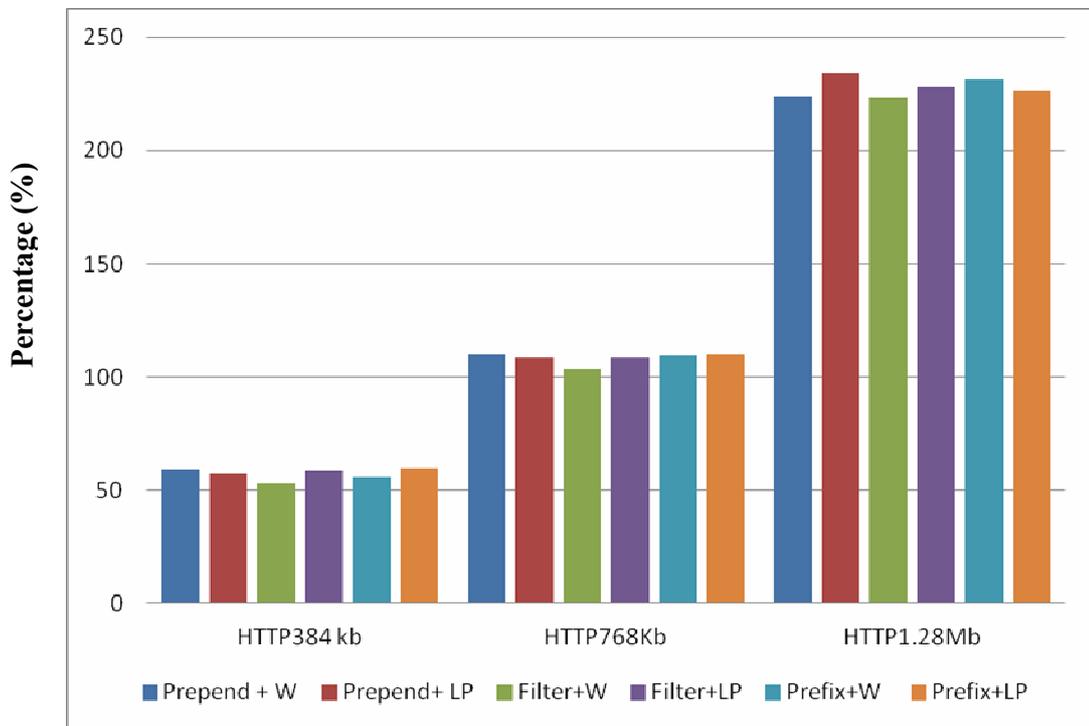


FIGURE 41. PERCENTAGE INCREASE IN END-TO-END DELAY OF THE HTTP APPLICATIONS IDENTICAL.

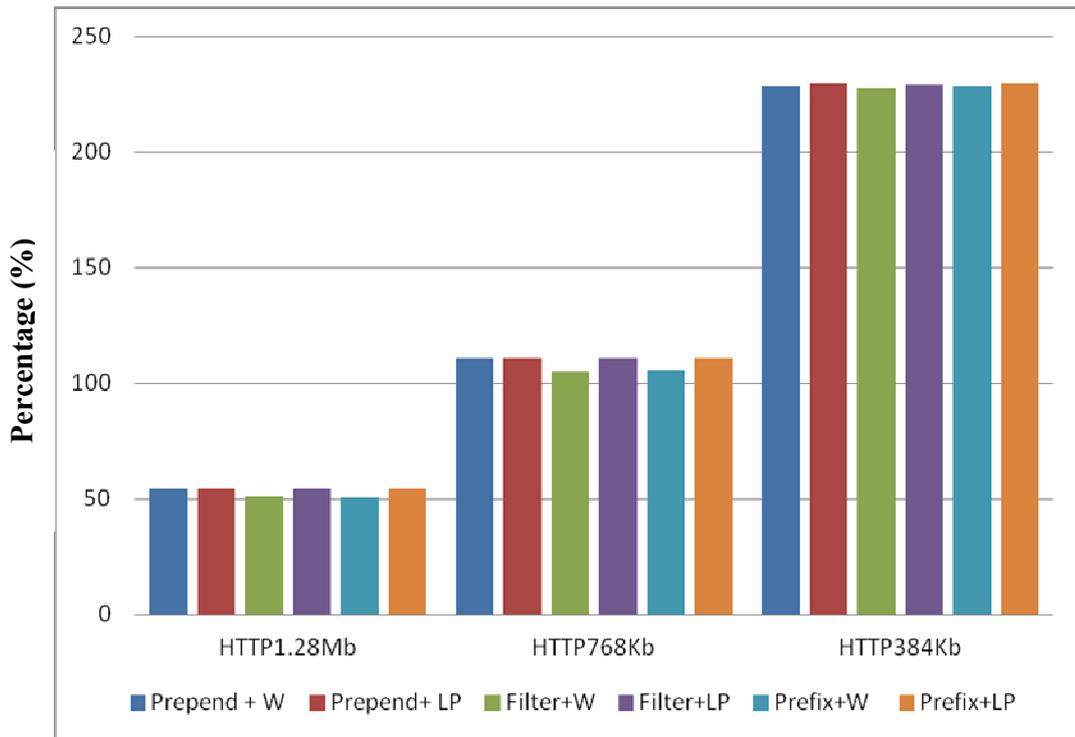


FIGURE 42. PERCENTAGE INCREASE IN END-TO-END DELAY OF THE HTTP APPLICATIONS NON-IDENTICAL.

PERCENTAGE OF TRAFFIC DROP

The percentage of the lost packets for the examined HTTP application in the identical and non-identical scenarios is displayed in Figure 43 and 44, respectively. The y-axis represents the percentage of lost packets in relation to the sent packets and the x-axis represents the examined HTTP application with dissimilar background traffic load. The percentage of the lost packets with the HTTP application is double the value of the FTP application in the previous subsection, which means that the FTP is more sensitive to the carrier than HTTP. In summary, the differences in the percentage of lost packets between

the evaluated solutions during the testing of HTTP stream are in the range of 12%. Also, the difference between the percentage of the lost packets results from the identical and non-identical scenario is in the range of 9%.

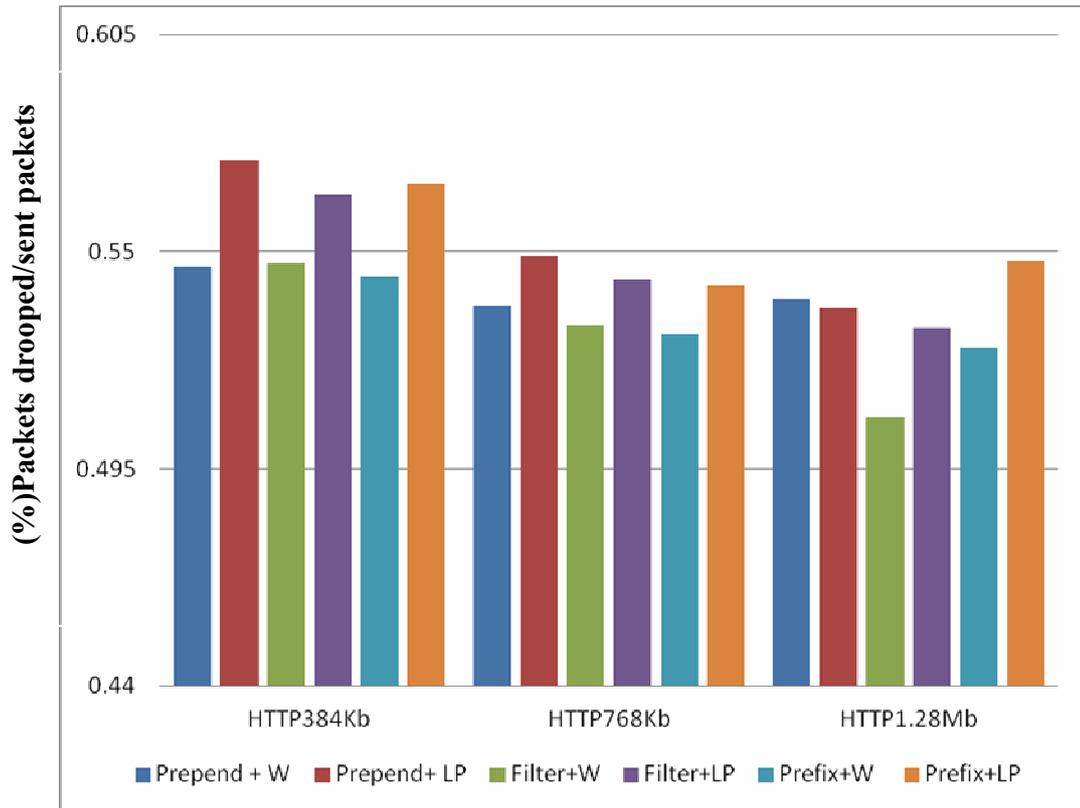


FIGURE 43. PERCENTAGE OF TRAFFIC DROP OF THE HTTP APPLICATION IN IDENTICAL SCENARIO

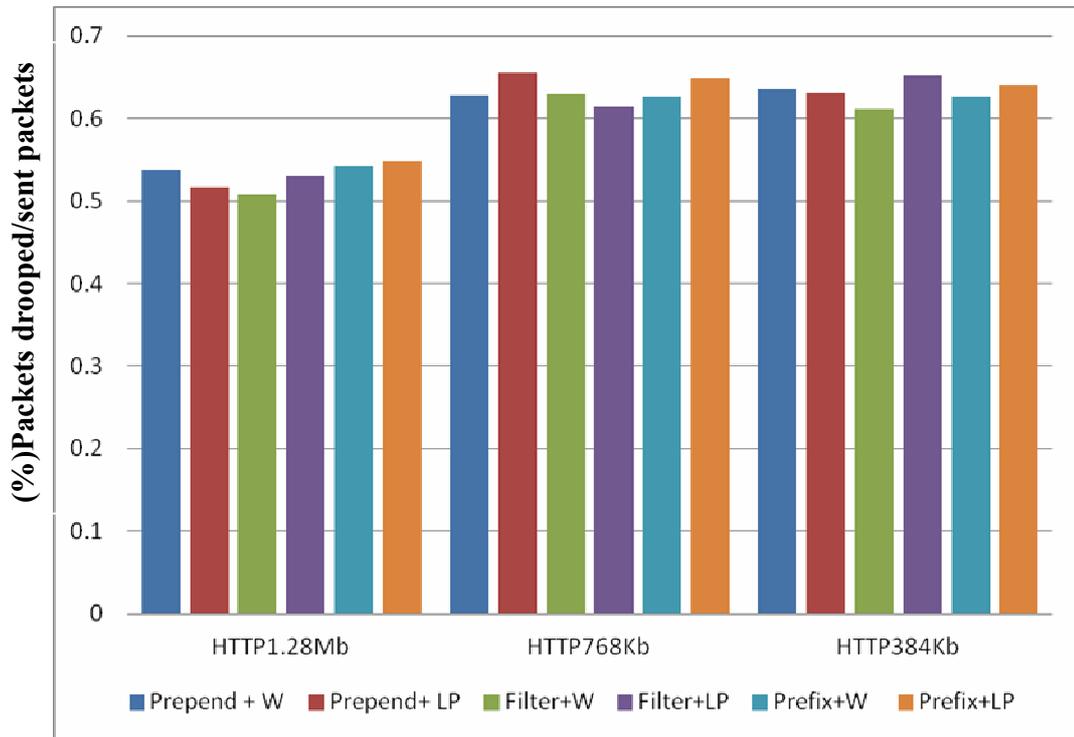


FIGURE 44. PERCENTAGE OF TRAFFIC DROP OF THE HTTP APPLICATION IN NON-IDENTICAL

AVERAGE THROUGHPUT

The average throughput in bits per second of the investigated HTTP application in the identical and non-identical scenario with the evaluated solutions is illustrated in Figure 45 and 46. The y-axis represents the bits per second and the x-axis represents the examined Internet application with different background traffic load. The evaluated solutions are displayed on the legend. We examined the HTTP average throughput by accessing a 6 MB webpage stored on the HTTP server residing on the Internet side from an Internet browser installed in the workstation residing on the local side. The resultant average HTTP throughput is affected by the hard reset *convergence time*. The average throughput

of the evaluated solutions with FTP is higher by 15% than the throughput of these solutions with the HTTP application. In any case, the differences in the average HTTP throughput between the evaluated solutions are in the range of 4%. Also, the difference between the average HTTP throughput results from the identical and non-identical scenarios is in the range of 6%.

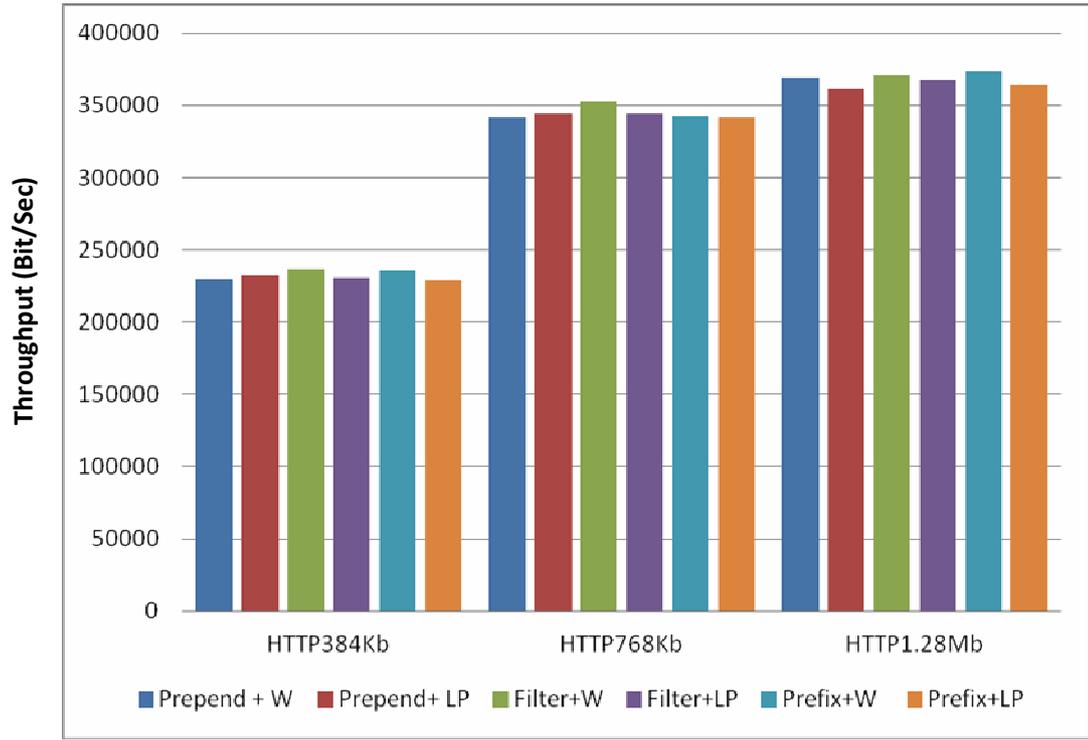


FIGURE 45. AVERAGE THROUGHPUTS OF THE HTTP APPLICATIONS IN IDENTICAL SCENARIO

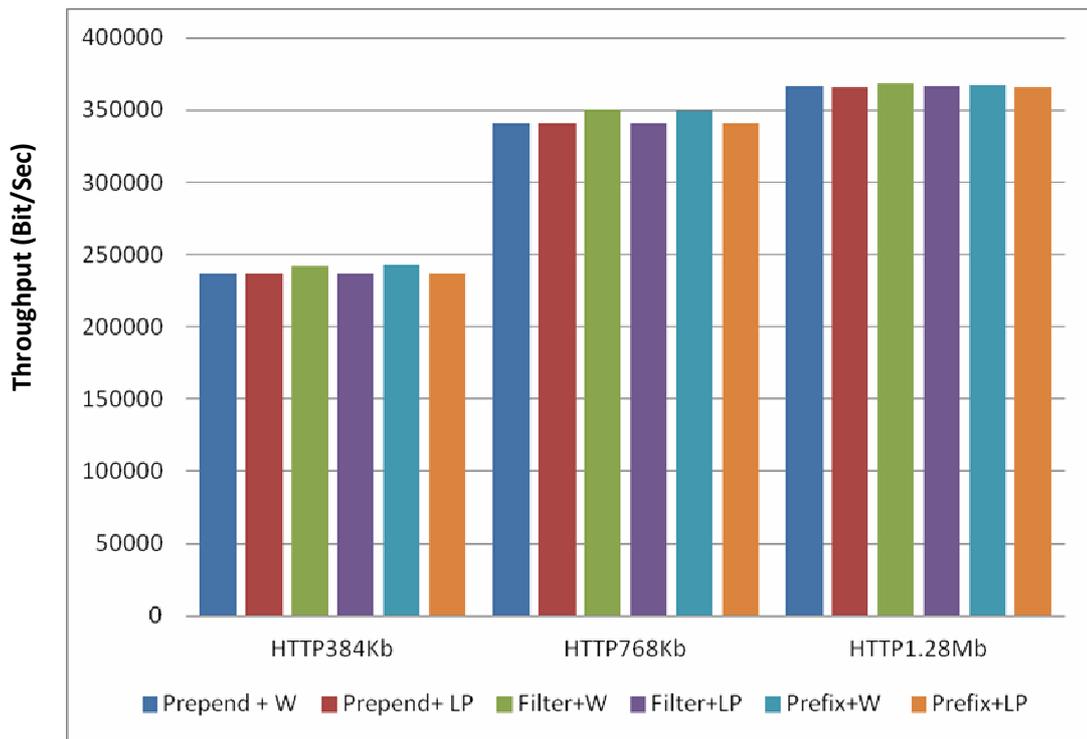


FIGURE 46. AVERAGE THROUGHPUTS OF THE HTTP APPLICATION IN NON-IDENTICAL SCENARIO

4.4.3.4 PERFORMANCE FIGURES FOR VOIP STREAM

PERCENTAGE OF TRAFFIC DROP

The VoIP is a real-time application that works over the UDP protocol. Unlike TCP protocol, the UDP does not have a reliability and congestion control mechanisms. The UDP protocol tries to forward the traffic as fast as possible regardless to the carrier and receiver capacity. The percentage of traffic drop for the examined VoIP application with the evaluated solutions in the identical and non-identical scenarios is displayed in Figure 47 and 48, respectively. The y-axis represents the percentage of traffic drop in relation to the sent packets and the x-axis represents the examined VoIP application with dissimilar

background traffic load. Due to the fact that UDP protocol is insensitive to the carrier, the results show a significant increase in the percentage of the lost packets when compared with previous TCP applications. In summary, the differences in the percentage of lost packets between the evaluated solutions are in the range of 5%. Also, the difference between the percentage of the lost packets results from the identical and non-identical scenarios is in the range of 4%.

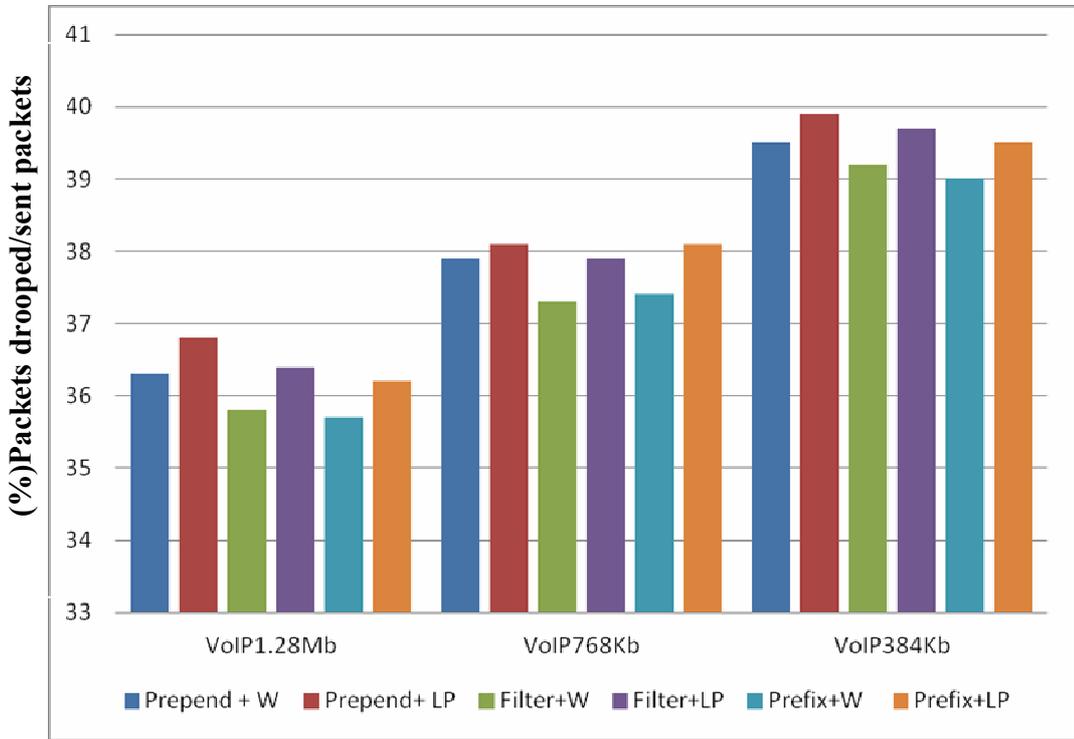


FIGURE 47. PERCENTAGE OF TRAFFIC DROP OF THE VOIP APPLICATIONS IN IDENTICAL SCENARIO

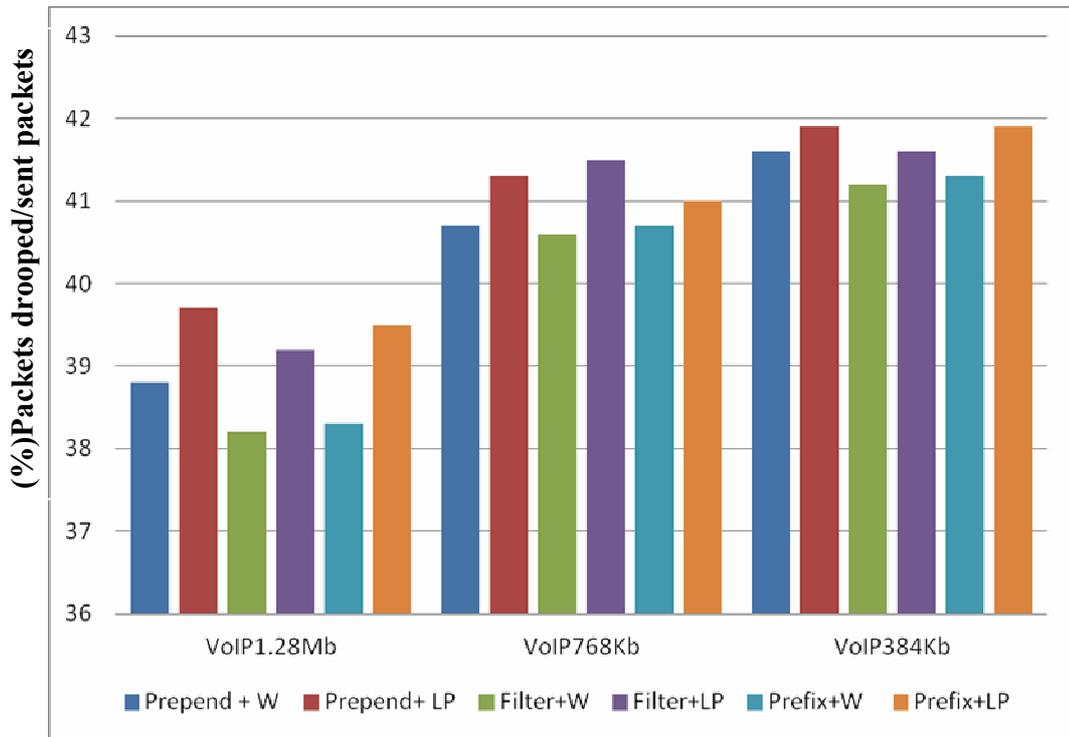


FIGURE 48. PERCENTAGE OF TRAFFIC DROP OF THE VOIP APPLICATIONS IN NON-IDENTICAL

AVERAGE THROUGHPUT

The average throughput in bits per second of the examined VoIP application with the evaluated solutions in the identical and non-identical scenarios is depicted in Figure 49 and 50, respectively. The y-axis represents the bits per second and the x-axis represents the examined Internet application with different background traffic load. The evaluated solutions are displayed on the legend. We examined the VoIP average throughput by performing 120 second UDP traffic from an iperf client installed in a workstation residing on the local side to an iperf server installed in a server residing on the Internet side. During the call, at the instant in time that the blocking action is performed the solution is

activated. This means that the posted average throughput in the two figures is affected by the hard reset *convergence time*. In any case, the differences in the average throughput between the evaluated solutions are in the range of 3%. Also, the difference between the average throughput results from the identical and non-identical scenarios is in the range of 6%.

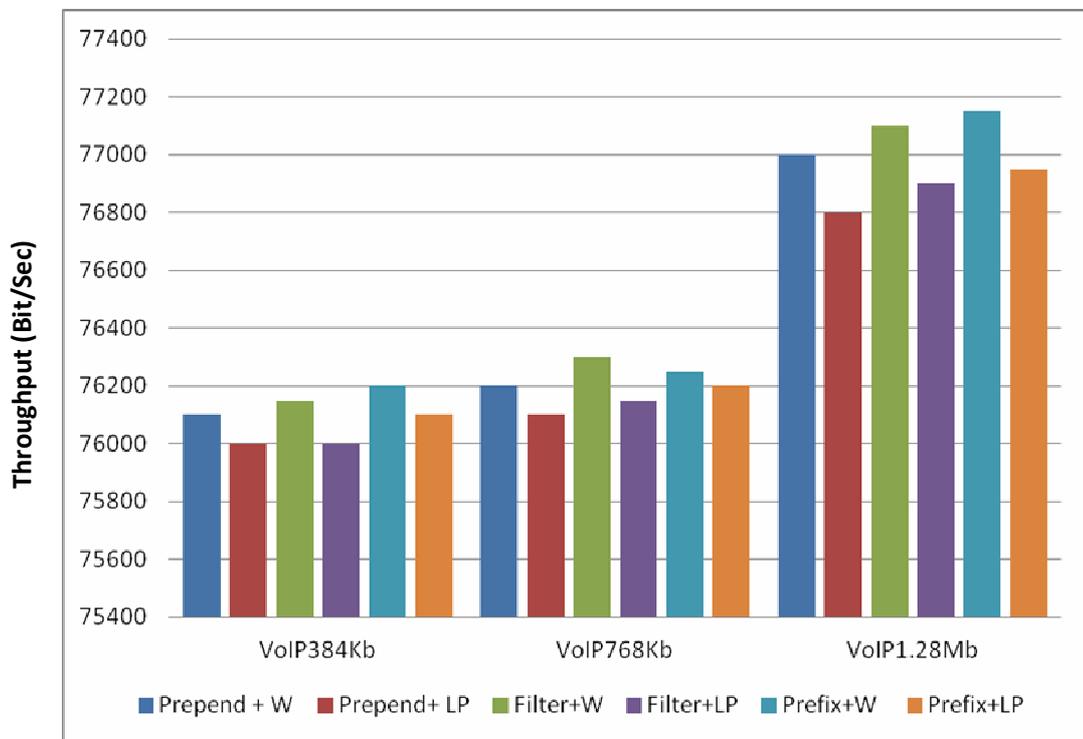


FIGURE 49. AVERAGE THROUGHPUTS OF THE VOIP APPLICATIONS IN IDENTICAL SCENARIO

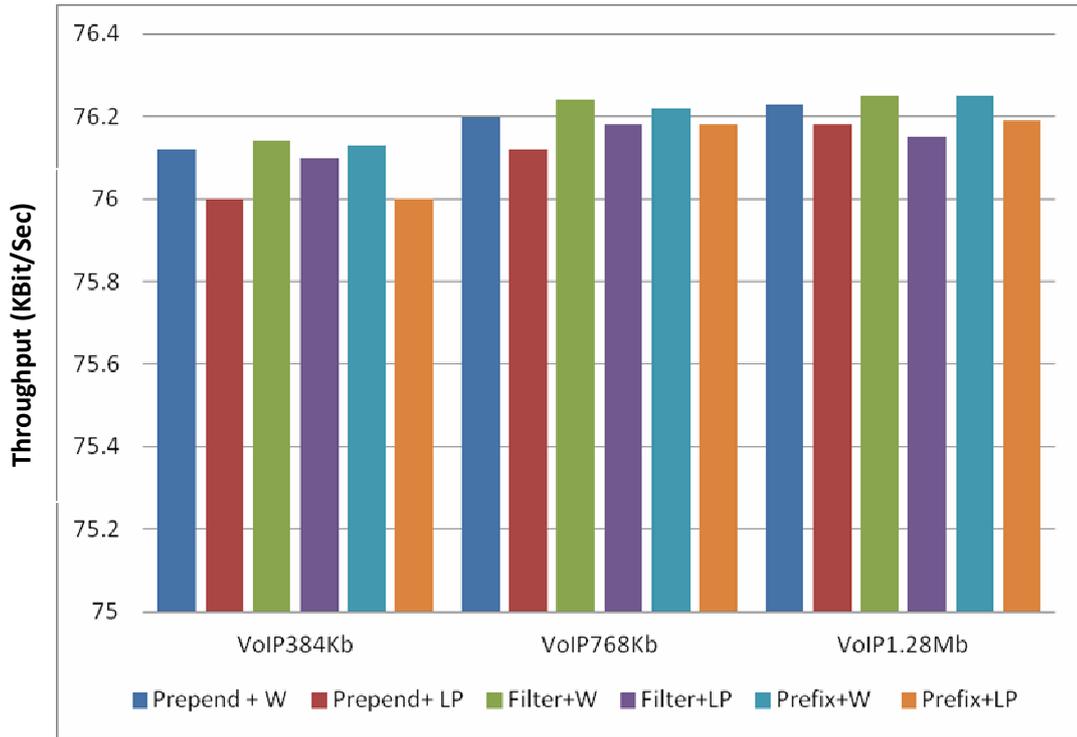


FIGURE 50. AVERAGE THROUGHPUTS OF THE VOIP APPLICATIONS IN NON-IDENTICAL SCENARIO

4.4.3.5 SUMMARY

The BGP-based solutions that are proposed here were prototyped and evaluated in a real laboratory. Moreover, the solutions were evaluated in two different laboratory scenarios: identical and non-identical. The effects of these solutions were measured by implementing them for different Internet application streams: FTP, HTTP and VoIP. The evaluating procedures were also conducted with different background traffic loads: 80%, 50%, and 25%. In both laboratory scenarios, the obtained hard reset *convergence time* is in the range of 63 – 64 seconds for all of the evaluated solutions. In identical scenario and non-identical scenario the resultant soft reset *convergence time* is between 0.1 – 0.3 and

0.1 – 0.4 second, respectively, for all of the evaluated solutions. The maximum percentage of the end-to-end delay is about 230% found with HTTP1.28Mbps and about 190% with FTP1.28Mbps. The minimum percentage of the end-to-end delay is about 30% found with FTP384kbps and about 55% with HTTP384kbps. All the evaluated solutions work fine with identical and non-identical scenario. In the non-identical scenario, the addition of one router in the path between the source and destination has no considerable effect on the performance figures of the investigated Internet applications even under different background traffic load. As well, the differences according to the performance figures between the evaluated solutions are in the range of 3% - 18%. Also, the differences between the performance figures from identical and non-identical scenario are in the range of 4% - 16%.

CHAPTER 5

CONCLUSION AND FUTURE WORK

5.1 CONCLUSION

The importance of Internet availability is supported by the overwhelming dependence of government services and financial institutions upon the said availability. In this work we prototype, evaluate and enhance the BGP-based solutions that are proposed by Alrefai [8]. The solutions address incidences wherein the primary IISP of the concerned region intentionally blocks its incoming and outgoing Internet traffic. Consequently, any traffic that passes through this IISP, defined here as malicious IISP, will be blocked. Under the assumption of the availability of a secondary IISP, called here good IISP, we performed this work.

The outgoing traffic is under the control of the concerned region which makes it easy to control. But the incoming traffic is under the control of remote and intermediate ASes

between the source and destinations. Alrefai [8] proposed three solutions that can control the outgoing traffic and attract the incoming traffic via an available good IISP. The Alrefai solutions include BGP tuning, virtual peering and virtual transit. In this work we have prototyped and evaluated the BGP tuning techniques: *BGP community*, *AS-Path shortening* and *more specific prefix*. The evaluations are performed in two dissimilar laboratory scenarios: identical and non-identical. The *AS-Path shortening* solution can work only with the identical scenario. The performance figures of these solutions are almost the same in both scenarios.

In this work we proposed thirty-three combinations of the BGP-based solutions that can control outgoing traffic and influence the incoming traffic. Some of them can work only with the identical scenario such as the *interface counter reset* and *AS-Path shortening* method. Based on the results of the prototyping and evaluation of the BGP-based solutions, we observe that the *filter outgoing advertisements* and *more specific prefix* methods perform the best. Based on the discussion in section 4.2, the malicious IISP can easily defeat the *filter outgoing advertisements* and *more specific prefix* methods. In contrast, the *eBGP multihop* method is difficult to be defeated by the malicious IISP. The availability of making a service agreement with Internet Exchange Points (IXPs) to be remote cooperative ASes strengthens the *eBGP multihop* based solutions. The *eBGP multihop* method may cooperate with several IXPs attracting almost all of the concerned region traffic via the good IISP. Consequently, it is recommended to use the *eBGP multihop* based solutions for the deployment.

5.2 FUTURE WORK

In this section, we will discuss open research areas related to the Internet denial issue. Some of these areas are:

- A. **Detection Mechanism:** Internet access denial could be caused by malicious or non-malicious action. Also, it could be performed by any AS in the path from a source to a destination. Moreover, a malicious AS can use a technique to hide the blocking action. The detection mechanism needs more attention than only a simple ping based mechanism.
- B. **Prefix Hijacking Prevention:** There are many research efforts and applied solutions for prefix hijacking detection and prevention, yet the Internet continues to face serious prefix hijacking incidents.
- C. **BGP Misconfiguration Detection and Prevention:** Many Internet access/service denial and destabilizing events have occurred due to BGP misconfiguration. BGP misconfiguration detection techniques require more attention and exploiting new techniques, such as using intelligent techniques in detecting the misconfiguration and this may lead to effective solutions and/or prevention.

APPENDIX A

ROUTER CONFIGURATION

```
!  
version 12.4  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname R0  
!  
boot-start-marker  
boot-end-marker  
!  
logging buffered 51200 warnings  
!  
no aaa new-model  
dot11 syslog  
!  
!  
ip cef  
!  
!  
no ip domain lookup  
ip domain name yourdomain.com  
!  
multilink bundle-name authenticated  
!  
!  
crypto pki trustpoint TP-self-signed-2730237386  
enrollment selfsigned  
subject-name cn=IOS-Self-Signed-Certificate-2730237386  
revocation-check none  
rsa-keypair TP-self-signed-2730237386  
!  
!  
username ccseadmin privilege 15 secret 5 $1$SwoA$p08RE7R/qBa9pKZKAQ/v.1  
archive  
log config  
hidekeys  
!  
!  
!  
!
```

```

!
!
!
interface FastEthernet0/0
description $ETH-LAN$$ETH-SW-LAUNCH$$INTF-INFO-FE 0/0$
ip address 192.0.1.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 192.0.12.2 255.255.255.252
duplex auto
speed auto
!
interface Serial0/0/0
no ip address
no keepalive
!
router bgp 100
no synchronization
bgp log-neighbor-changes
redistribute connected
neighbor 192.0.12.1 remote-as 100
no auto-summary
!
ip forward-protocol nd
!
!
ip http server
ip http access-class 23
ip http authentication local
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
!
!
!

!
!
control-plane
!
banner exec _____
% Password expiration warning.

username <myuser> privilege 15 secret 0 <mypassword>

Replace <myuser> and <mypassword> with the username and password you want to
use.

!
line con 0
login local
line aux 0
line vty 0 4
access-class 23 in
privilege level 15
password ($3
login
transport input telnet ssh
line vty 5 15
access-class 23 in
privilege level 15

```

```
login local
transport input telnet ssh
!
scheduler allocate 20000 1000
!
end
```

FIGURE A. 1 R0 CONFIGURATION

```
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime
msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!

logging buffered 51200 warnings
!
no aaa new-model
dot11 syslog
!
!
ip cef
!
!
no ip domain
lookup
ip domain name yourdomain.com
!
multilink bundle-name authenticated
!
!
crypto
pki trustpoint TP-self-signed-2765050578
enrollment selfsigned
subject-name
cn=IOS-Self-Signed-Certificate-2765050578
revocation-check none
rsa-keypair
TP-self-signed-2765050578
!
!
crypto pki certificate chain TP-self-signed-2765050578

!
!
username ccseadmin privilege 15 secret 5 $1$I8g.$ZNAW32fDnwDaaDnFLgFtG/

archive
log config
hidekeys
!
!
!
!
!
```

```

!
interface Tunnel0

!
interface FastEthernet0/0
description $ETH-LAN$ETH-SW-LAUNCH$$INTF-INFO-FE 0/0$
ip address 192.0.12.1 255.255.255.0

duplex auto
speed auto

!
interface FastEthernet0/1

no ip address

shutdown

duplex auto

speed auto

!
interface Serial0/0/0

ip address 192.0.2.1 255.255.255.252

no keepalive

clock rate 256000

!
interface Serial0/2/0

ip address 192.0.3.1 255.255.255.252

no keepalive

clock rate 256000

!
router bgp 100

no synchronization

bgp log-neighbor-changes

redistribute connected

neighbor 192.0.12.2 remote-as 100

neighbor 192.0.2.2 remote-as 300

neighbor 192.0.3.2 remote-as 200

no auto-summary
!
ip
forward-protocol nd
!

```

```

!
ip http server
ip http access-class 23
ip http authentication
local
ip http secure-server
ip http timeout-policy
idle 60 life 86400 requests 10000
!
!
!
!
!
control-plane
!
banner exec _____
% Password expiration warning.
-----
_____
!
line con 0
login local
line aux 0
line vty 0 4
privilege level 15
password (($3
login
transport input telnet ssh
line vty 5 15
access-class 23 in
privilege level 15
login local
transport input telnet ssh
!
scheduler allocate 20000 1000
!
end

```

FIGURE A. 2 R1 CONFIGURATION

```

!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime
msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker

```

```
!  
logging buffered 51200 warnings  
!  
no aaa new-model  
dot11 syslog  
!  
!  
ip cef  
!  
!  
no ip domain lookup  
ip domain name yourdomain.com  
!  
multilink bundle-name authenticated  
!  
!  
crypto pki trustpoint TP-self-signed-3254364069  
enrollment selfsigned  
subject-name  
cn=IOS-Self-Signed-Certificate-3254364069  
revocation-check none  
rsa-keypair TP-self-signed-3254364069  
!  
!  
crypto pki certificate chain TP-self-signed-3254364069  
certificate self-signed  
!  
!  
username ccseadmin privilege 15 secret 5 $1$rUAF$Yp1vIQFatFj3lZnV8MsO00  
archive  
log config  
hidekeys  
!  
!  
!  
!  
!  
!  
!  
!  
interface FastEthernet0/0  
description $ETH-LAN$$ETH-SW-LAUNCH$$INTF-INFO-FE 0/0$
```

```
ip address 192.0.29.1 255.255.255.0

duplex auto
speed auto

!

interface FastEthernet0/1

no ip address

shutdown

duplex auto
speed auto

!

interface Serial0/0/0

ip address 192.0.4.1 255.255.255.252

no keepalive

!

interface Serial0/2/0

ip address 192.0.3.2 255.255.255.252

no keepalive

!

router bgp 200

no synchronization

bgp log-neighbor-changes

redistribute connected

neighbor 192.0.3.1 remote-as 100

neighbor 192.0.4.2 remote-as 300

no auto-summary

!

ip forward-protocol nd

!

!

ip http server

ip http access-class 23

ip http authentication local

ip http secure-server

ip http timeout-policy idle 60 life 86400 requests 10000

!

!
```

```

!
!
!
control-plane

username <myuser> privilege 15 secret 0 <mypassword>

Replace <myuser> and <mypassword> with the username and password you want to
use.

!
line con 0
 login local
line aux 0
line vty 0 4
 privilege level 15
 password ($3
 login
 transport input telnet ssh
line vty 5 15
 access-class 23 in
 privilege level 15
 login local
 transport input telnet ssh
!
 scheduler allocate 20000 1000
!
end

```

FIGURE A. 3 R2 CONFIGURATION

```

!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no
service password-encryption

!

hostname R3

!

boot-start-marker
boot-end-marker

!

logging buffered 51200 warnings

!

no aaa new-model
dot11 syslog

!

!

ip cef

!

```

```

!
no ip domain lookup
ip domain name yourdomain.com
!
multilink bundle-name authenticated
!
!
crypto pki trustpoint TP-self-signed-2000161258
  enrollment selfsigned
  subject-name
  cn=IOS-Self-Signed-Certificate-2000161258
  revocation-check none
  rsakeypair TP-self-signed-2000161258
!
!
!
username ccseadmin privilege 15 secret 5 $1$6CjN$hu6.ZK3PKBWL23NC4GU/E/
archive
log config
hidekeys
!
!
!
!
!
!
!
!
interface Loopback0
ip address 3.3.3.3 255.255.255.255
!
interface FastEthernet0/0
description $ETH-LAN$$ETH-SW-LAUNCH$$INTF-INFO-FE 0/0$
ip address 10.10.10.1 255.255.255.248
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
shutdown

```



```

!
control-plane
!
banner exec -----

username <myuser> privilege 15 secret 0 <mypassword>

Replace <myuser> and <mypassword> with the username and password you want to
use.

-----
!
line con 0
 login local
line aux 0
line vty 0 4
 privilege level 15
 password ($3
 login
 transport input telnet ssh
line vty 5 15
 access-class 23 in
 privilege level 15
 login local
 transport input telnet ssh
!
scheduler allocate 20000 1000
!
end

```

FIGURE A. 4 R3 CONFIGURATION

```

!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no
service password-encryption
!
hostname R4
!
boot-start-marker
boot-end-marker

!

logging buffered 51200 warnings

!

no aaa new-model
dot11 syslog

!

!

ip cef

!

!

ip domain name yourdomain.com

```

```

!
multilink bundle-name authenticated

!
!

crypto pki trustpoint TP-self-signed-2279471600
enrollment selfsigned
subject-name
cn=IOS-Self-Signed-Certificate-2279471600
revocation-check none
rsa-keypair TP-self-signed-2279471600

!
!

!
!

username ccseadmin privilege 15 secret 5 $1$tmxH$w.QG5IjfyPdUf0yZrY/PV/
archive
log config
hidekeys

!
!

!
!

!
!

!
!

interface Tunnel0
ip address 172.16.13.2 255.255.255.252

tunnel source Serial0/0/0
tunnel destination 192.0.3.1

!

interface FastEthernet0/0
description $ETH-LAN$$ETH-SW-LAUNCH$$INTF-INFO-FE 0/0$
ip address 10.10.10.1 255.255.255.248

duplex auto

speed auto

!

interface FastEthernet0/1

no ip address

shutdown

```

```
duplex auto
speed auto
!
interface Serial0/0/0
ip address 192.0.5.2 255.255.255.252
no keepalive
!
interface Serial0/2/0
ip address 192.0.6.1 255.255.255.252
no keepalive
clock rate 2000000
!
router bgp 400
no synchronization
bgp log-neighbor-changes
redistribute connected
neighbor 192.0.5.1 remote-as 300
neighbor 192.0.6.2 remote-as 400
neighbor 192.0.6.2 next-hop-self
default-information originate
no auto-summary
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.0.5.1
!
!
ip http server
ip http access-class 23
ip http authentication local
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
!
!
!
!
```

```

!
control-plane
!
banner exec _____
% Password expiration warning.

-----

username <myuser> privilege 15 secret 0 <mypassword>

Replace <myuser> and <mypassword> with the username and password you want to
use.

-----

!
line con 0
login local

line aux 0

line vty 0 4

privilege level 15
password ($3

login
transport input telnet ssh

line vty 5 15
access-class 23 in
privilege level 15
login local
transport input telnet ssh
!
scheduler allocate 20000 1000
!
end

```

FIGURE A. 5 R4 CONFIGURATION

```

!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R6
!
boot-start-marker
boot-end-marker
!
logging buffered 51200 warnings
!
no aaa new-model
dot11 syslog
!
!
ip cef

```

```

!
!
ip domain name yourdomain.com
!
multilink bundle-name authenticated
!
!
crypto pki trustpoint TP-self-signed-3041265475
  enrollment selfsigned
  subject-name cn=IOS-Self-Signed-Certificate-3041265475
  revocation-check none
  rsakeypair TP-self-signed-3041265475
!
!
!
!
username ccseadmin privilege 15 secret 5 $1$UmDm$MB4.Y4AFm.1twPCKi.kt1
archive
  log config
  hidekeys
!
!
!
!
!
!
!
!
interface Loopback0
  ip address 6.6.6.6 255.255.255.255
!
interface Loopback6
  ip address 192.0.22.1 255.255.255.0
!
interface FastEthernet0/0
  description $ETH-LAN$$ETH-SW-LAUNCH$$INTF-INFO-FE 0/0$
  ip address 10.10.10.1 255.255.255.248
  duplex auto
  speed auto
!
interface FastEthernet0/1
  no ip address
  shutdown
  duplex auto
  speed auto
!
interface Serial0/0/0
  ip address 192.0.10.2 255.255.255.252
  no keepalive
!
interface Serial0/2/0
  ip address 192.0.20.1 255.255.255.252
  no keepalive
  clock rate 128000
!
router bgp 600
  no synchronization
  bgp log-neighbor-changes
  redistribute connected
  neighbor 20.1.1.1 remote-as 100
  neighbor 192.0.10.1 remote-as 300
  neighbor 192.0.20.2 remote-as 600
  neighbor 193.1.1.1 remote-as 100
  no auto-summary
!
ip forward-protocol nd
!
!
ip http server
ip http access-class 23
ip http authentication local

```

```

ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
!
access-list 23 permit 10.10.10.0 0.0.0.7
!
!
!
!
control-plane
!
banner exec _____

username <myuser> privilege 15 secret 0 <mypassword>

Replace <myuser> and <mypassword> with the username and password you want to
use.

!
line con 0
  login local
line aux 0
line vty 0 4
  privilege level 15
  password ($3
  login
  transport input telnet ssh
line vty 5 15
  access-class 23 in
  privilege level 15
  login local
  transport input telnet ssh
!
scheduler allocate 20000 1000
!
end

```

FIGURE A. 6 R6 CONFIGURATION

```

!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R7
!
boot-start-marker
boot-end-marker
!
logging buffered 51200 warnings
!
no aaa new-model
dot11 syslog
!
!
ip cef
!
!
no ip domain lookup
ip domain name yourdomain.com
!
multilink bundle-name authenticated
!
!
crypto pki trustpoint TP-self-signed-2730237386
  enrollment selfsigned

```

```
subject-name cn=IOS-Self-Signed-Certificate-2730237386
revocation-check none
rsa-keypair TP-self-signed-2730237386
!
!
!
!
username ccseadmin privilege 15 secret 5 $1$SwoA$P08RE7R/qBa9pKZKAQ/v.1
archive
log config
hidekeys
!
!
!
!
!
!
!
interface FastEthernet0/0
description $ETH-LAN$$ETH-SW-LAUNCH$$INTF-INFO-FE 0/0$
ip address 192.0.21.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
interface Serial0/0/0
ip address 192.0.20.2 255.255.255.252
no keepalive
!
router bgp 600
no synchronization
bgp log-neighbor-changes
redistribute connected
neighbor 192.0.20.1 remote-as 600
no auto-summary
!
ip forward-protocol nd
!
!
!
ip http server
ip http access-class 23
ip http authentication local
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
!
!
!
!
!
control-plane
!
banner exec _____

username <myuser> privilege 15 secret 0 <mypassword>

Replace <myuser> and <mypassword> with the username and password you want to
use.

!
line con 0
login local
line aux 0
line vty 0 4
access-class 23 in
privilege level 15
```

```
password ($3
login
transport input telnet ssh
line vty 5 15
access-class 23 in
privilege level 15
login local
transport input telnet ssh
!
scheduler allocate 20000 1000
!
end
```

FIGURE A. 7 R7 CONFIGURATION

APPENDIX B

SOLUTIONS CONFIGURATION

COMMANDS

CONFIGURING LOCAL PREFERENCE VALUE

```
R1(config)#route-map LOCALPREF permit 10  
R1(config-route-map)#set local-pref 200  
R1(config-route-map)#exit  
R1(config)#router bgp 100  
R1(config-router)# neighbor 192.0.3.2 route-map LOCALPREF out
```

CONFIGURING WEIGHT VALUE

```
R1(config)#router bgp 100  
R1(config-router)# neighbor 192.0.3.2 weight 700
```

CONFIGURING BGP MED VALUE

```
R1(config)#route-map RMED permit 10
R1(config-route-map)#set med 200
R1(config-route-map)#exit
R1(config)#router bgp 100
R1(config-router)# neighbor 192.0.2.2 route-map RMED out
```

CONFIGURING EBGP MULTI HOP VALUE

Local Side "AS100" eBGP multihop configuration

```
R1(config)#router bgp 100
R1(config-router)# neighbor 192.0.5.2 remote-as 600
R1(config-router)# neighbor 192.0.5.2 ebgp-multihop
R1(config-router)#exit
R1(config)# ip route 192.0.5.0 255.255.255.0 192.0.3.2 ← through the good IISP
```

Remote Side "AS600" eBGP multihop configuration

```
R6(config)#router bgp 600
R6(config-router)# neighbor 192.0.3.1 remote-as 100
R6(config-router)# neighbor 192.0.3.1 ebgp-multihop
R6(config-router)#exit
R6(config)# ip route 192.0.3.0 255.255.255.0 192.0.5.1 ← through the good IISP
```

CONFIGURING INTERFACE COUNTER RESET

```
R1# clear interface s0/0
```

CONFIGURING BGP COMMUNITY

Local Side “AS100” Community Configuration

```
R1(config)#ip bgp-community new-format
R1(config)#route-map CUM permit 10
R1(config-route-map)#set community 100:300
R1(config-route-map)#exit
R1(config)#router bgp 100
R1(config-router)# neighbor 192.0.3.2 send-community
R1(config-router)# neighbor 192.0.3.2 route-map CUM out
```

Community Configuration of the routers in the path

```
R2(config)#ip bgp-community new-format
R2(config)#ip community-list 1 permit 100:300
R2(config)#route-map CUM permit 10
R2(config-route-map)# match community 1
R2(config-route-map)# set local-preference 200
R2(config-route-map)#exit
R2(config)#router bgp 200
R2(config-router)# neighbor 192.0.3.1 route-map CUM in
```

CONFIGURING MORE SPECIFIC PREFIX

Local Side “AS100” Community Configuration R0 is the inside router in AS100 R1 is the border router in AS100

```
R0(config)#router bgp 100
R0(config-router)# neighbor 192.0.12.2 remote-as 100
R0(config-router)# neighbor 192.0.12.2 next-hop-self
R0(config-router)# network 192.0.1.0 mask 255.255.255.0
R0(config-router)# network 192.0.12.0 mask 255.255.255.252
```

```
R1(config)#access-list 10 permit 192.0.1.0 0.0.0.255
R1(config)#access-list 11 permit 192.0.1.0 0.0.0.252
R1(config)#router bgp 100
R1(config-router)# neighbor 192.0.12.1 remote-as 100
R1(config-router)# neighbor 192.0.2.2 distribute-list 10 out
R1(config-router)# neighbor 192.0.3.2 distribute-list 11 out
```

Good IISP Router “R2” configuration

```
R2(config)#access-list 11 permit 192.0.1.0 0.0.0.252
R2(config)#router bgp 100
R2(config-router)# neighbor 192.0.3.1 distribute-list 11 in
```

CONFIGURING FILTER INCOMING ADVERTISEMENTS

```
R1(config)#access-list 101 deny tcp 192.0.2.0 0.0.0.255 any eq bgp
R1(config)#access-list 101 permit ip any any
R1(config)#interface s0/0
R1(config-if)# ip access group 101 in
```

CONFIGURING FILTER OUTGOING ADVERTISEMENTS

```
R1(config)#access-list 102 deny tcp any 192.0.2.0 0.0.0.255 eq bgp
R1(config)#access-list 102 permit ip any any
R1(config)#interface s0/0
R1(config-if)# ip access group 102 out
```

RATE LIMIT CONFIGURATION AND BURST RATE SETTING

Cisco recommends the following procedure to calculate the normal and maximum burst value:

```
router(config-if)# rate-limit input 1544000 289500 579000 conform-action transmit
exceed-action drop
```

normal burst = configured rate * (1 byte)/(8 bits) * 1.5 seconds
maximum burst = 2 * normal burst

1544000
Nr = 289500, Max = 579000



APPENDIX C

JAVA SOFTWARE CODE

```
package AutomatedTelnetClient;

import org.apache.commons.net.telnet.TelnetClient;
import java.io.InputStream;
import java.io.PrintStream;
import java.net.InetAddress;
import java.text.DateFormat;
import java.text.SimpleDateFormat;
import java.util.Date;
public class AutomatedTelnetClient {
private TelnetClient telnet = new TelnetClient();
private InputStream in;
private PrintStream out;
private String prompt = "#";
private static DateFormat dateFormat7 = new SimpleDateFormat("HH:mm:ss");
private static DateFormat dateFormat = new SimpleDateFormat("HH:mm:ss");
//private static Date date = new Date();
//public static String Stampdate = dateFormat.format(date);
public AutomatedTelnetClient(String server, String user, String password) {
try {
// Connect to the specified server
telnet.connect(server, 23);

// Get input and output stream references
in = telnet.getInputStream();
out = new PrintStream(telnet.getOutputStream());
```

```

// Log the user on
//readUntil("login: ");
//write(user);
readUntil("Password: ");
write(password);
// Advance to a prompt
readUntil(prompt);
write("conf t");
readUntil(prompt);
//write("clear ip bgp *");
//readUntil(prompt);
write("inter s0/0/0");
readUntil(prompt);
write("encaps ppp");
readUntil(prompt);
write("ip access-group 1 in");
readUntil(prompt);
//write("ip access-group 171 out");
//readUntil(prompt);
//write("route-map IISP permit 10");
//readUntil(prompt);
//write("set metric 90");
//readUntil(prompt);
//write("set as-path prepend 100 100 100 100 100");
//readUntil(prompt);
//write("route-map PREF permit 10");
//readUntil(prompt);
//write("set local-preference 200");
//readUntil(prompt);
//write("route-map BLOCK permit 10");
//readUntil(prompt);
//write("match ip address 60");
//readUntil(prompt);
//write("route-map GOOD permit 10");
//readUntil(prompt);
//write("match ip address 70");
//readUntil(prompt);
//write("access-list 60 permit 192.0.1.0 0.0.0.255");
//readUntil(prompt);
//write("access-list 70 permit 192.0.3.0 0.0.0.252");
//readUntil(prompt);
write("router bgp 100");
readUntil(prompt);
//write("neighbor 192.0.2.2 advertise-map BLOCK exist-map GOOD");
//readUntil(prompt);
//write("bgp always-compare-med");
//readUntil(prompt);
//write("bgp bestpath med missing-as-worst");
//readUntil(prompt);
//write("neighbor 192.0.3.2 weight 200");
//readUntil(prompt);
//write("neighbor 192.0.3.2 default-originate");
//readUntil(prompt);
write("neighbor 192.0.2.2 route-map IISP out");// for BOTH MED and PrePending
readUntil(prompt);
//write("neighbor 192.0.3.2 route-map PREF IN");// for BOTH MED and PrePending
//readUntil(prompt);
//write("bgp fast-external-fallover");
//readUntil(prompt);
write("exit");
readUntil(prompt);
write("interface s0/0/0");
readUntil(prompt);
write("no encaps ppp");
//readUntil(prompt);
//write("no shut");
//readUntil(prompt);
//readUntil(prompt);
write("exit");
readUntil(prompt);

```

```

write("exit");
//readUntil(prompt);
//write("clear ip bgp *");
//readUntil(prompt);
}
catch (Exception e) {
e.printStackTrace();
}
}

public void su(String password) {
try {
write("admin");
readUntil("password: ");
write(password);
prompt = "admin>";
readUntil(prompt + " ");
//String s = "set";
write("set");
readUntil(prompt + " ");
}
catch (Exception e) {
e.printStackTrace();
}
}

public String readUntil(String pattern) {
try {
char lastChar = pattern.charAt(pattern.length() - 1);
StringBuffer sb = new StringBuffer();
boolean found = false;
char ch = (char) in.read();
while (true) {
System.out.print(ch);
sb.append(ch);
if (ch == lastChar) {
if (sb.toString().endsWith(pattern)) {
return sb.toString();
}
}
}
ch = (char) in.read();
}
catch (Exception e) {
e.printStackTrace();
}
return null;
}

public void write(String value) {
try {
out.println(value);
out.flush();
System.out.println(value);
}
catch (Exception e) {
e.printStackTrace();
}
}

public String sendCommand(String command) {
try {
write(command);
return readUntil(prompt);
}
catch (Exception e) {
e.printStackTrace();
}
return null;
}
}

```

```

public void disconnect() {
try {
telnet.disconnect();
}
catch (Exception e) {
e.printStackTrace();
}
}
}
public static void main(String[] args) {
try {
boolean md = true ; boolean chk = true ;
int i = 0;
while(md) {
//long start = System.currentTimeMillis();
//System.out.println(start);
try {
//Socket socket = new Socket("192.168.1.10", 7);

InetAddress address = InetAddress.getByName("192.0.2.2");
long start = System.currentTimeMillis();
chk = address.isReachable(3000);
long end = System.currentTimeMillis();
System.out.println("time " + (end - start));
System.out.println(chk);
if(chk == false){
i++;}
System.out.println(i);
if(chk== false && i > 2){
Date date = new Date();
String Stampdate = dateFormat7.format(date);
System.out.println("Malicious Action Start at: " + Stampdate);

md = false;}
//socket.close();
} catch (Exception e) {
System.out.println(e);
}
// long end = System.currentTimeMillis();
// System.out.println(end);
}
//
// Start Forcing Our Border Router by telnet //
AutomatedTelnetClient telnet = new AutomatedTelnetClient("192.0.1.1", "admin", "($3");
//System.out.println("program");
//telnet.sendCommand("set");
telnet.sendCommand("\n");
//telnet.sendCommand("dir");

telnet.disconnect();
boolean md2 = false;
boolean chk7 = false ;
while(md2 == false) {

try {
//System.out.println("program");
//Socket socket = new Socket("192.168.1.10", 7);
//long start = System.currentTimeMillis();
InetAddress address = InetAddress.getByName("192.0.21.23");
chk7 = address.isReachable(3000);
//long end = System.currentTimeMillis();
if(chk7 == true){
Date date7 = new Date();
String Stampdate7 = dateFormat7.format(date7);
System.out.println("Good Action Start at: " + Stampdate7);
md2 = true;}
//socket.close();
} catch (Exception e) {
System.out.println(e);
}
}
}

```

```
// System.out.println(md);
//System.out.println("time " + (end - start));
}
System.out.println("\n");
//double s = Stampdate7. - Stampdate;
//System.out.println("TIME: " + s);
}
catch (Exception e) {
e.printStackTrace();
}
}
}
```

FIGURE C. 1 *CHECKER* SOFTWARE JAVA CODE

APPENDIX D

TRACE ROUTE RESULTS

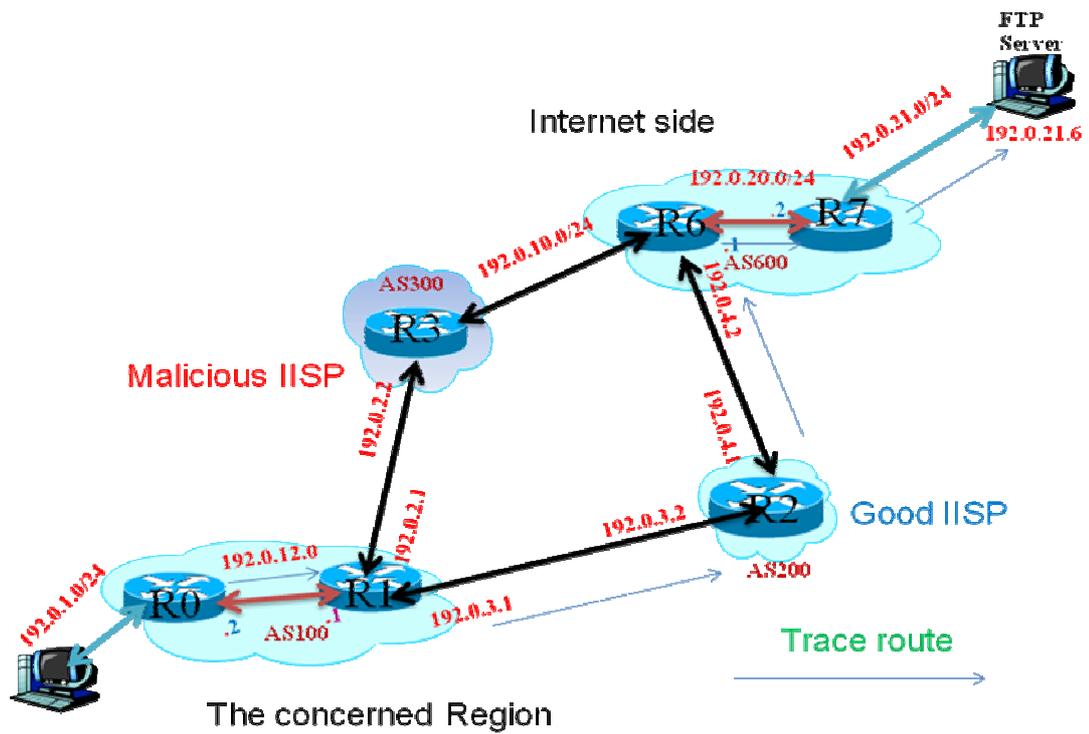


FIGURE D. 1 TRACE ROUTE OVER IDENTICAL SCENARIO

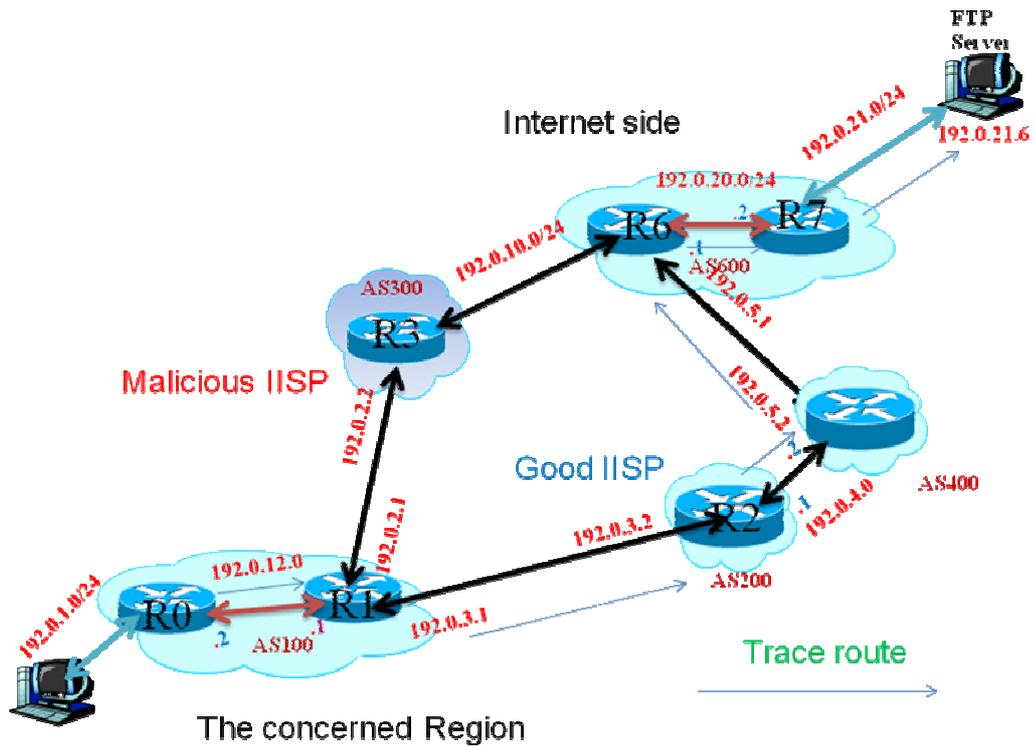


FIGURE D. 2 TRACE ROUTE OVER NON-IDENTICAL SCENARIO

AS-PATH SHORTENING METHOD

```

C:\Users\marwan>TRACERT 192.0.21.6
Tracing route to ALIEN-PC [192.0.21.6]
over a maximum of 30 hops:
 1  <1 ms  <1 ms  <1 ms  192.0.1.1
 2  5 ms   5 ms   5 ms  192.0.7.1
 3  15 ms  15 ms  15 ms  192.0.3.2 ← Good router
 4  27 ms  27 ms  27 ms  192.0.5.1
 5  33 ms  32 ms  32 ms  192.0.20.2
 6  39 ms  39 ms  40 ms  ALIEN-PC [192.0.21.6]

Trace complete.

```

FIGURE D. 3 TRACEROUTE RESULTS FOR *AS-PATH SHORTENING* METHOD OVER IDENTICAL SCENARIO

Figure D.3 shows the *traceroute* result from the FTP server in AS600 to a workstation in AS100 after testing this method in the identical scenario. The results demonstrate that the

tracing packets have gone through the good IISP (192.0.3.2) after implementing this method. Figure D.1 illustrates how the trace route packets traverse over the identical scenario from a workstation resides in AS100 to the server in AS600.

MORE SPECIFIC METHOD

```
C:\Users\marwan>tracert 192.0.1.6
Tracing route to AMER-PC [192.0.1.6]
over a maximum of 30 hops:
  1  <1 ms  <1 ms  <1 ms  192.0.21.1
  2   5 ms   5 ms   5 ms  192.0.20.1
  3  10 ms  11 ms  11 ms  192.0.5.2
  4  21 ms  21 ms  21 ms  192.0.4.1 ← Good router
  5  26 ms  26 ms  26 ms  192.0.3.1
  6  33 ms  33 ms  34 ms  192.0.12.1
  7  40 ms  39 ms  39 ms  ALIEN-PC [192.0.1.6]

Trace complete.
```

FIGURE D. 4 TRACEROUTE RESULTS FOR MORE SPECIFIC METHOD OVER THE NON-IDENTICAL SCENARIO

Figure D.4 shows the *traceroute* results of testing this method in the non-identical scenario. The results demonstrate that the tracing packets have gone through the good IISP (192.0.3.2) after implementing this method. Figure D.2 illustrates how the trace route packets traverse over the non-identical scenario from a workstation resides in AS100 to the server in AS600.

BGP COMMUNITY METHOD

```
C:\Users\marwan>tracert 192.0.1.6
Tracing route to AMER-PC [192.0.1.6]
over a maximum of 30 hops:
  1  <1 ms  <1 ms  <1 ms  192.0.21.1
  2   5 ms   4 ms   4 ms  192.0.20.1
  3  11 ms  11 ms  11 ms  192.0.5.2
  4  19 ms  19 ms  19 ms  192.0.4.1 ← Good router
  5  26 ms  25 ms  25 ms  192.0.3.1
  6  31 ms  31 ms  31 ms  192.0.12.1
  7  39 ms  39 ms  39 ms  ALIEN-PC [192.0.1.6]
Trace complete.
```

FIGURE D. 5 TRACEROUTE RESULTS FOR *BGP COMMUNITY* METHOD OVER NON-IDENTICAL SCENARIO.

Figure D.5 shows the *traceroute* results of testing this method in the non-identical scenario. The results demonstrate that the tracing packets have gone through the good IISP (192.0.3.2) after implementing this method. Figure D.2 illustrates how the trace route packets traverse over the non-identical scenario from a workstation resides in AS100 to the server in AS600.

INTERFACE COUNTER RESET METHOD

```
C:\Users\marwan>TRACERT 192.0.21.6
Tracing route to ALIEN-PC [192.0.21.6]
over a maximum of 30 hops:
  1  <1 ms  <1 ms  <1 ms  192.0.1.1
  2   5 ms   5 ms   5 ms  192.0.7.1
  3  15 ms  15 ms  15 ms  192.0.3.2 ← Good router
  4  27 ms  27 ms  27 ms  192.0.5.1
  5  33 ms  32 ms  32 ms  192.0.20.2
  6  39 ms  39 ms  40 ms  ALIEN-PC [192.0.21.6]
Trace complete.
```

FIGURE D. 6 TRACEROUTE RESULTS FOR INTERFACE COUNTER RESET

Figure D.6 shows the *tracert* result from the FTP server in AS600 to a workstation in AS100 after testing this method in the identical scenario. The results demonstrate that the tracing packets have gone through the good IISP (192.0.3.2) after implementing this method. Figure D.1 illustrates how the trace route packets traverse over the identical scenario from a workstation resides in AS100 to the server in AS600.

IP STATIC/DEFAULT METHOD

```

C:\Users\marwan>TRACERT 192.0.21.6
Tracing route to ALIEN-PC [192.0.21.6]
over a maximum of 30 hops:
  1  <1 ms  <1 ms  <1 ms  192.0.1.1
  2   6 ms   5 ms   5 ms  192.0.7.1
  3  11 ms  11 ms  11 ms  192.0.3.2 ← Good router
  4  20 ms  20 ms  21 ms  192.0.4.2
  5  27 ms  27 ms  27 ms  192.0.5.1
  6  33 ms  33 ms  34 ms  192.0.20.2
  7  40 ms  39 ms  39 ms  ALIEN-PC [192.0.21.6]

Trace complete.

```

FIGURE D. 7 TRACEROUTE RESULTS FOR IP STATIC/DEFAULT

Figure D.7 shows the *tracert* results of testing this method in the non-identical scenario. The results demonstrate that the tracing packets have gone through the good IISP (192.0.3.2) after implementing this method. Figure D.2 illustrates how the trace route packets traverse over the non-identical scenario from a workstation resides in AS100 to the server in AS600.

FILTER ADVERTISEMENTS METHOD

```
C:\Users\marwan>TRACERT 192.0.21.6
Tracing route to ALIEN-PC [192.0.21.6]
over a maximum of 30 hops:
  1  <1 ms  <1 ms  <1 ms  192.0.1.1
  2   6 ms   5 ms   5 ms  192.0.7.1
  3  11 ms  11 ms  11 ms  192.0.3.2 ← Good router
  4  21 ms  21 ms  21 ms  192.0.4.2
  5  27 ms  27 ms  27 ms  192.0.5.1
  6  35 ms  35 ms  34 ms  192.0.20.2
  7  41 ms  40 ms  40 ms  ALIEN-PC [192.0.21.6]

Trace complete.
```

FIGURE D. 8 TRACEROUTE RESULTS FOR FILTER ADVERTISEMENTS

Figure D.8 shows the *traceroute* results of testing this method in the non-identical scenario. The results demonstrate that the tracing packets have gone through the good IISP (192.0.3.2) after implementing this method. Figure D.2 illustrates how the trace route packets traverse over the non-identical scenario from a workstation resides in AS100 to the server in AS600.

REFERENCES

- [1]. P. Boothe, J. Hiebert, and R. Bush, "How prevalent is prefix hijacking on the Internet?," in *Proc. NANOG 36, Feb. 2006*. [Online] <http://www.nanog.org/mtg-0602/boothe.html>
- [2]. Dolev, S. Jamin, O. Mokryn, and Y. Shavitt, "Internet resiliency to attacks and failures under BGP policy routing," *Computer Networks: The International Journal of Computer and Telecommunications Networking* vol. 50, pp. 3183 - 3196 Nov. 2006.
- [3]. K. Butler, T. Farley, P. McDaniel, and J. Rexford. "A survey of BGP security issues and solutions". *Proceedings of the IEEE, vol. 98, pp. 100-122*, January 2010.
- [4]. R. Barrett, S. Haar, and R. Whitestone, "Routing snafu causes Internet outage," *Interactive Week, Apr. 25, 1997*.
- [5]. Security info Watch, "Hackers attack Champaign, Ill.-based Internet Service Provider," *The News-Gazette via NewsEdge Corporation*, <http://www.securityinfowatch.com/ContractWatch/hackers-attack-champaign-ill-based-internet-service-provider>, June 2009.
- [6]. ICANN. DNS attack factsheet. Technical report, ICANN (March 2007) <http://www.icann.org/announcements/factsheet-dns-attack-08mar07.pdf>.

- [7]. Press Release, "Growing Business Dependence on the Internet: New Risks Require CEO Action," *Business Roundtable*, <http://web.docuticker.com/go/docubase/21001>, Sept. 2007.
- [8]. Alrefai, "BGP based Solution for International ISP Blocking," *MS Thesis submitted to Deanship of Graduate Studies, King Fahd University of Petroleum and Minerals*, December 2009.
- [9]. Albaiz, "INTERNET DENIAL BY HIGHER-TIER ISPS: A NAT-BASED SOLUTION," *MS Thesis submitted to Deanship of Graduate Studies, King Fahd University of Petroleum and Minerals*, March 2010.
- [10]. Y. Rekhter, T. Li, and S. Hares. (2006, Jan.) IETF-A Border Gateway Protocol 4 (BGP-4). [Online]. www.ietf.org/rfc/rfc4271.txt
- [11]. "Cisco IOS IP Command Reference, Volume 2 of 4: Routing Protocols, Release 12.3," http://www.cisco.com/en/US/docs/ios/12_3/iproute/command/reference/ip2_nlg.html
- [12]. Y. Hu, A. Perrig, and D. Johnson, "Efficient security mechanisms for routing protocols," in *Proc. ISOC Network and Distributed Systems Security Symp. (NDSS)*, San Diego, CA, pp.57-73, Feb. 2003.
- [13]. O. Nordstrom, C. Dovrolis, "Beware of BGP attacks," in *ACM SIGCOMM CCR*, vol.34, pp.1-8, April 2004.
- [14]. S. Kent, C. Lynn, J. Mikkelsen, and K. Seo, "Secure Border Gateway Protocol (S-BGP) real world performance and deployment issues," in *Proc. ISOC Symp.*

Network and Distributed System Security (NDSS), San Diego, CA, pp.103-116, Feb. 2000.

- [15]. J. Ng, Extensions to BGP to Support Secure Origin BGP (soBGP), Internet Draft, Apr. 2004.
- [16]. X. Liu and L. Xiao, "A Survey of Multihoming Technology in Stub Networks: Current Research and Open Issues," in *IEEE Network Magazine, May/June 2007*.
- [17]. A. Akella, B. Maggs, S. Seshan, A. Shaikh, , and R. Sitaraman, "A Measurement-Based Analysis of Multihoming" In *Proceeding of the ACM SIGCOMM, August 2003*.
- [18]. D. Goldenberg, L. Qiu, H. Xie, Y. R. Yang, and Y. Zhang, "Optimizing Cost and Performance for Multihoming," In *Proc. ACM SIGCOMM, August 2004*.
- [19]. M. Omer, R. Nilchiani, and A. Mostashari, "Measuring the Resilience of the Global Internet Infrastructure System," *Accepted for publication: IEEE International Systems Journal, 2009*, pp. 156-162
- [20]. S. Kim, H. Lee, and Y. W. Lee, "Improving Resiliency of Network Topology with Enhanced Evolving Strategies," in *Proceedings of the Sixth IEEE International Conference on Computer and Information Technology 2006*, p. 149.
- [21]. R. Cohen, K. Erez, D. ben-Avraham, and S. Havlin, "Breakdown of the internet under intentional attack," *Phy Rev Lett*, vol. 86, pp. 3682-3685, Apr. 2001.
- [22]. S.-T. Park, A. Khrabrov, D. M. Pennock, S. Lawrence, C. L. Giles, and L. H. Ungar, "Static and dynamic analysis of the Internet's susceptibility to faults and attacks," in *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies, vol.3, pp. 2144-2154, April 2003*.

- [23]. Marwan H. Abu-Amara, Ashraf Mahmoud, Farag Ahmed Azzedin, and Mohammed Sqalli." Internet Access Denial by International Internet Service Providers: Analysis and Counter Measures". *Research Proposal*, April 2008.
- [24]. C. Labovitz, G. R. Malan, and F. Jahanian, "Origins of Internet routing instability," in Proceedings of INFOCOM 1999, pp. 218-226, 1999.
- [25]. Ratul Mahajan, David Wetherall, and Tom Anderson," Understanding BGP Misconfiguration," In *ACM SIGCOMM 2000*, pp. 3-16, August 2002.
- [26]. "iperf," <http://en.wikipedia.org/wiki/Iperf>
- [27]. R. K. C. Chang and M. Lo, "Inbound traffic engineering for multi-homed ASes using AS path prepending," in *Network Operations and Management Symposium*, vol. 1, 2004, pp. 98-102.
- [28]. Quoitin, "BGP-based Interdomain Traffic Engineering," *Ph.D. Dissertation*, University catholique de Louvain, Louvain-la-Neuve, Belgium, Aug. 2006.
- [29]. "BGP community String for Sprint AS 1239," <http://www.ipbalance.com/routing/bgp/bgp-community-attributes-list/369-bgp-community-string-for-sprint-as-1239.html>
- [30]. "WireShark," <http://www.wireshark.org>
- [31]. "TEAM CYMRU BGP/AS Analysis Report," <http://www.cymru.com/BGP/summary.html>
- [32]. "Internet Exchange Point," http://en.wikipedia.org/wiki/Internet_exchange_point

CURRICULUM VITA

Amer M. Al-Ghadban

PO BOX 3234
Hail, 81000
Saudi Arabia

Mobile: +966 50 515 0487
E-mail: amer7777@hotmail.com

EDUCATION

- **King Fahd University of Petroleum & Minerals (KFUPM) Dhahran, SA**

Degree: Master of Science in Computer Network
Graduation: December 2011
Thesis: Prototyping, Evaluating and Enhancing BGP-Based Solutions to Overcome Malicious IISP Blocking

- **King Fahd University of Petroleum & Minerals (KFUPM) Dhahran, SA**

Degree: B.S degree in Computer Engineering
Graduation: December 2001
Senior Project: Designing and Programming Microcontroller For Signal Analysis

CERTIFICATIONS

- **SANS-GIAC Certified Firewall Analyst (GCFW)**

Skills: Perimeter Protection, Defence-in-Depth, VPN, Firewall, Network Assessment
Grade: 93.3% (Honours)

- **SANS Local Mentor**

- **Certified Ethical Hacking (CEH)**
Grade: 89%
- **Cisco Academy Certificates**

CCNA1, 2, & 3
CCNA Industrial 92.3% Honour
FAST TRACK LAB EXAM >90%
Cisco Academy Wireless LAN Associate
AOC (Academy Orientation Certified from Cisco Academy)
- **Security Certified Network Professional (SCNP)**
Grade: 93% (Honours)
- **Certified EC-Council Membership**

EXPERIENCE

- **Instructor/Trainer**, College of Technology, Hail, KSA
November 2003 - Present

Designing course materials and teaching courses in Routing and Switching, WAN technologies, Introductory Networking and Introductory Network Security.

Providing instruction and training for instructors in Windows Networking and Active Directory, CCNA1 and AOC in addition to supervising the Cisco Local Academy

Advising faculty and staff involved in the institutions E-Learning project.

I was responsible for establishing the new Network and Technical Support Department at our institution. My primary contributions involved ensuring the acquisition of appropriate equipment, creating the organizational structure of the department and monitoring the development and maintenance of institutional labs and networks. I am currently the supervisor responsible for networking.

I have been the recipient of the Dean's Award for Excellence on three occasions.
- **Network Engineer**, Ministry of Interior, National Information Centre, Riyadh, KSA
March 2002 - November 2003

Configuring and maintaining Cisco routers and switches. Also, testing a VPN site, OSPF, static route, and Huawei routers to work regularly with the Cisco routers in environments such as OSPF, VPN and Access List.

Configuring routers to work with CiscoWorks to: launch reports; schedule tasks, archiving, and configuration updates; and monitor and troubleshoot the network.

Designing and working with Microsoft VPN network, Microsoft ISA Firewall as well as configuring a small IPSec network between Cisco Routers.

Planning and conducting presentations for staff members about DHCP service in Cisco routers and ACL.

Participating in training and courses involving network security and administration such as SANS GCFW, SANS GCSE, eTrust IDS, eTrust Audit, eTrust Antivirus, eTrust PCM, Cisco BSCI and Cisco BCMSN.

In addition to my primary duties, I served as an on-call volunteer for trouble-shooting end user and network problems. I also made contributions to special projects involving firewalls and upgrading the institute's active directory.

EXPERIENCE

- **Assistant Network Engineer** (Trainee), Saudi Telecom Company, Hail, KSA
June-July 2001

This was an eight-week cooperative training experience during which I was trained and made responsible for maintaining computer workstations and designing the LAN. I also provided network, software and hardware support services.

SELECTED RESEARCH, PROJECTS & AWARDS

- Prototyping and Evaluating Tunnel-Based Solutions to Circumvent Malicious ISP Blocking, prepared for IEEE.
- Sensors Location Privacy During Mission Assignment, currently being prepared for IEEE.
- Comprehensive Survey on Internet Resilience and Available Solutions to Overcome Higher-tier ISP Internet Access Isolation, IEEE Journal paper in process

- Malicious IIS Blocking, funded by King Abdulaziz City of Science and Technology under the National Science, Technology, and Innovation Plan (project number 08-INF97-4).
- Survey in Proposed Approaches for Migrating PSTN network to NGN
- Study Attackers Skills By Deploying Honeynet in Two Different Real Environment
- Probabilistic-Based approach for Key Management in Ad Hoc Wireless Network

**SELECTED RESEARCH,
PROJECTS & AWARDS**

- Monte-Carlo simulation and SIR statistics for Mobile and Cellular Systems
- Honors Award from Ministry of Higher Education for contribution in SSC 2010.
- Honors Award from STC for Next Generation Network Migrating Project 2009.