A Configuration Analysis over BGP Prefix Filters and Route Leak Effects on Global Routing Network

Ammar K. Al Mhdawi *[1], Mohammed I. Younis[*2]

[*1] *Research Scholar & Senior Network Engineer, USA*
[*2] *Associate Professor & Cisco Instructor, Computer Engineering Department, UOB, Iraq*

Abstract--- *Boarder Gateway Protocol or BGP is considered as one of the biggest protocols in the internet world. BGP has proven to be very secure, scalable and robust. However, with the rapid changes of the internet technologies, there has been some concerns about BGP's efficiency to meet the large needs of the routing system. So in this paper, we conduct an analysis over BGP routing properties such as AS path and route prefix filtering technique, and discuss some of the security concerns in the ISP environment. A case studies of the BGP route leaks and incidents are discussed.*

Keywords: *eBGP, iBGP, Prefix Limit, AS-Path, RR, Confederations.*

I. INTRODUCTION

Internet traffic delivery is based on the distributed operations of routing protocols running among multiple autonomous systems (AS). In this paper, we discuss the view of BGP from two different ISP backbone networks. In addition, this paper discuses how the routing protocols interact with each other and what are the effect of route failure and planned maintenance on the flow of traffic. The AS is a domain that combines a group of networks under a common routing policy [1]. Customer networks such companies and firms employ a known interior gateway protocols (IGP) to exchange routes within network, for example Routing Information Protocol (RIP) and Open Path Shortest First (OSPF). These customers connect to ISP and ISP uses BGP to exchange customer routes. There are two types of BGP: Interior BGP (IBGP), which is configured by the service provider internally to exchange routes within same AS; and External BGP (EBGP), which is used to exchange routes between customer and service provider (SP) [2,3]. EBGP peers are called Neighbours and they require a direct connection to form EBPG neighbours relationship, unlike IBGP, where peers does not have to be connected directly. Current research on BGP is focused on enhancing its features and resolving its related security issues specially when routing tables grow very fast, and issues related to convergence delay, routing stability and performance [4]. The rest of this paper is organised as follows. Section II discusses the interaction among routing protocols. Section III highlights the issues and concerns regarding BGP. Section IV gives examples considering route-filtering techniques, and mentions that the regular expression technique is the preferred one as far as the scalability is concerned. Section V highlights the BGP's route authentication process. Section VI discusses the route leaks and incidents with case studies. Finally, Section VII states the conclusion of this study.

II. ROUTING PROTOCOLS INTERACTION

A large ISP network, typically has multiple BGP routers. For example, in Figure 1 , the orange bubbles refers to different AS's for ISPs which they connect to each other via eBGP, while the blue bubbles are the Customer side which connect via eBGP to ISP as well, but the main ISP routers connect via iBGP within same AS [5,6]. A BGP route has some attributes such as (next-hop, AS-Path, Origin Code, etc) that is delivered with routes advertisement and can by manipulated by network engineers. Route filters can be implemented as well to filter unwanted routers [7]. The attributes make the decision of the route selection criteria as tabulated in Table 1.

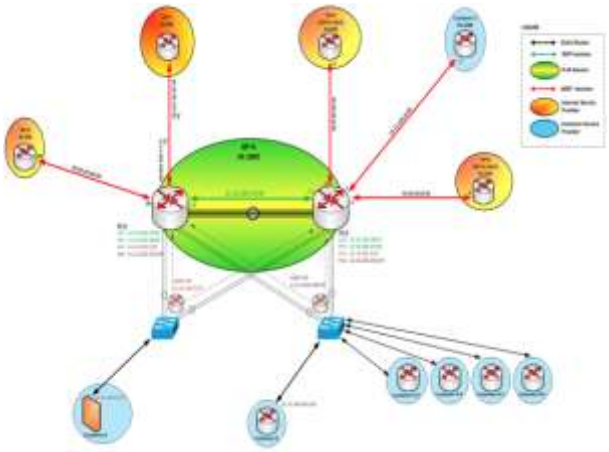


Figure 1: EBGP and IBGP design structure

Table 1: BGP attributes for route selection [11]

Order	Preference	Description
0. Synchronized	TRUE	Use only routes that meet the synchronization requirement
1. Weight	Highest	Administrative override
2. Local Preference	Highest	Used internally to pick path out of AS
3. Self originated	TRUE	Used to prefer paths originated on this router
4. AS-Path	Shortest	Minimize AS-hops
5. Origin	i<?	Prefer stability
6. MED	Lowest	Used external to come in
7. External	EBGP<IBGP	External path preferred over internal path
8. IGP cost	Lowest	Look for more information
9. EBGP Peering	Oldest	Prefer stability
10. RID	Lowest	Choose one with lowest BGP router ID

III.BGP ISSUES AND CONCERNS

1. Routing Table Growth Issue

This issue happens when the routing table grows to the point where some older routers cannot catch up with the high resource requirements. Huge routing table takes long time to do route lookup and that will take long time to stabilize specially when a major route change occurs which may effect the network reliability and reachability and may lead to router crash [8,9].

2. Scalability of iBGP sessions

As we mentioned previously, iBGP session does not require a direct connection between routers, but one of iBGP rules is that any route that is advertised to an iBGP peer, cannot be advertised to the other connected peer, so to overcome this issue, a full mesh connection is required. The full mesh connection requires that each router to maintain a session with each router. When the network grows and number of sessions increase, this could lead to performance issues such as memory and high CPU utilization [10,11]. To over come this issue, route reflectors and confederations are used to reduce the number of sessions that are need to be maintained.

3. Security Concerns

One of the security concerns is the prefix attack in which hackers update BGP routing table with false information and manipulate BGP attributes which will cause serious network outages and misrouted information.

IV. ROUTE FILTERING TECHNIQUES

There are many ways to filter prefixes in BGP, the basic one is Prefix List which is not that much scalable but we are going to discuss it and then go forward with the other techniques of filtering. Prefixes are in two forms [11]:

1- Explicit Permit (permit then deny any)
2- Explicit Deny (deny then permit any)

An example of prefix list is as below:

```
ip prefix-list A1 permit 192.0.0.0/8
le 24
```

The above prefix list will accept a mast of up to 24 bits.

```
ip prefix-list A1 deny 192.0.0.0/8
ge 25
```

The above prefix denies a mask greater than 25. The prefix list can be implemented as we can see in the following configuration [11] :

```
router bgp 67653

no synchronization

neighbour 198.32.228.10 remote-as

65255

neighbour 198.32.228.10 prefix-list

A1 in

neighbour 198.32.228.10 prefix-list

A1 out

neighbour 198.32.228.15 remote-as

65233

neighbour 198.32.228.15 prefix-list

A1 in

neighbour 198.32.228.15 prefix-list

A1 out

no auto-summary

!
```

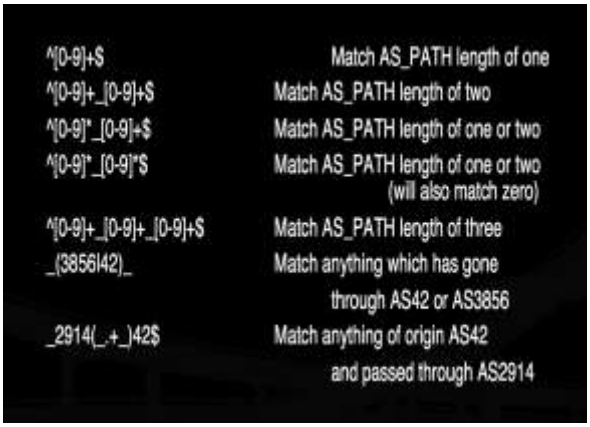
It is clear that the prefix filter is a good way to filter routes but it is not scalable for large network. As new customer and new prefixes added to the network, new

configuration has to be made and implemented as this is not an efficient way to handle this process [6,8].
Another more efficient way of filtering is to use the AS PATH filtering process. This type of filtering is based on the filter list command and the number of AS's that a route goes through as in the following configuration. It uses special characters that are called regular expressions and each ones have a specific meaning as following:

```
router bgp 65577

network 10.10.0.0 mask 255.255.0.0

neighbour 198.168.10.10 remote-as
65233

neighbour 198.168.10.10 filter-list

1 out

neighbour 198.168.10.10 filter-list

200 in

!

ip as-path access-list 10 permit

^63456$

ip as-path access-list 100 permit

^63456$

!
```

The regular expressions that we see here is used to indicate different aspects of the filter list. In Table 2 is a list of different regular expressions that are used widely in BGP environment.

Table 2: Regular Expressions Examples [11]



V. BGP ROUTE AUTHENTICATION

Routes authentication certifies the authenticity of the neighbour and the reliability and integrity of the received routes [9]. Let say we have two routers R1 and R2 and they are connected via eBGP. To perform the authentication, we need to perform the following commands:

On R1:

```
router bgp 400

neighbour 3.3.3.2 remote-as 201

neighbour 3.3.3.2 description Link
to AS-206-Peer

neighbour 3.3.3.2 password cisco123
```

On R2:

```
router bgp 400

neighbour 3.3.3.1 remote-as 206

neighbour 3.3.3.1 description Link
to AS-201-Peer

neighbour 3.3.3.1 password cisco123
```

VI. BGP ROUTE LEAKS AND INCIDENTS

Route leaks are very dangerous and could totally screw up traffic for clients by forcing traffic to between ISP X and ISP Y instead of going through the normal large peering networks. The ISP that leaks traffic could suffer high spikes of saturation. There are

many route leak issues that happened around the world and we are going to discuss one of them by detail. One of the route leaks that happened last year was a route leaks that was initiated by Malaysia Telekom (AS4788), which caused a very significant problem for the global network routing system. Telekom Malaysia has advertised 179,000 prefixes to Level 3 (ISP), and from there, level 3 advertised that back to their customers and peers, now level 3 is responsible as well for this issue for delivering these prefixes to the destinations.

The result of this issue was a big packet loss and slow internet in may parts of the world. Level 3 also suffered sever service degradation between Asia pacific regions. Fig 2 shows packet loss for Level 3 between Hong Kong and London [1].

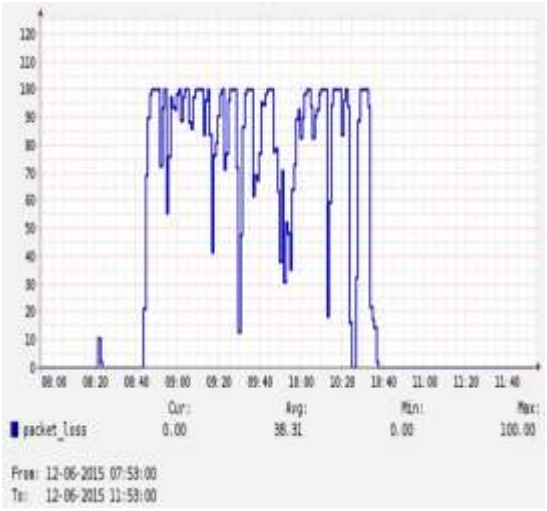


Fig 1: Packet loss Hong Kong to London over Level3 ISP [1]

The round trip time for the same locations has went down significantly as shows in Fig 2 below.

Fig 3: Round Trip Time over Level 3 [1]

To explain this issue for a prefix, one of the affected prefixes is 31.13.67.0/24, which is one of the prefixes that belongs to Facebook. The AS path for this prefix looked like this:

1103 286 3549 4788 (32934 Facebook)

if we examine this route, we found that 4788 is a peer with Facebook which is Malaysia Telekom, which announced it to AS 3549 (Level 3), then to the customers and peers. All traffic was being squeezed through the interconnect between Malaysia Telekom and level 3 and caused a big capacity issue and resulted in packet loss.

The prefixes that were leaked were all Malaysia Telekom customers and all learned peers as well. In a normal situation, Level 3 announces about 534000 prefixes, but during those issues, it advertised another 10000 prefixes. Fig 4 shows the prefix advertisement on Level 3 network.

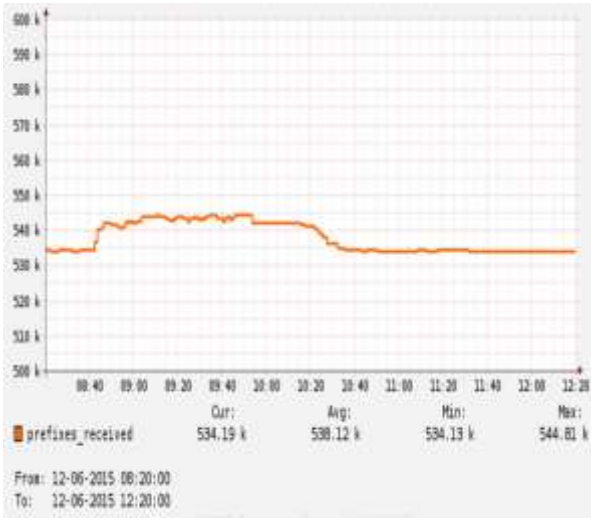


Fig 4: Level 3 prefix count [1]

Since Level 3 was advertising many prefixes than normally, the BGP session was hitting max limits

with its peers. In summary, this issues caused to overwhelm Malaysia Telekom with traffic. Many traffic got dropped and latency levels went up and big internet impact occurred.

VII. CONCLUSION

ISP need to control which data are received and sent over which link, for this reason BGP filters are very critical to prevent any issues that could happen such as route leaks and also it does provide more security levels and maintain privacy for customer prefixes. A very precise configuration must be implemented on the ISP edge and all controls should be set and prefix limit must be defined to prevent any issues that could happen with global routing.

AUTHOR

- **Ammar K. Al Mhdawi** obtained his BSc degree in computer engineering from UOB and MSc Degree in Information Technology and Network Security, AIU, USA. He is Cisco Certified Internetwork Expert CCIE R&S (written), Cisco Certified Network Professional CCNP R&S, and Cisco Certified Network Associate CCNA R&S. He is also a member of the Iraqi Union of Engineers. Ammar Almhdawi's research interest is focused on network design, network security and wireless communications.

- **Mohammed Issam Younis** obtained his BSc in computer engineering from the University of Baghdad in 1997, his MSc degree from the same university in 2001, and his Ph.D. degree from the School of Electrical and Electronics Engineering, USM, Malaysia in 2011. He is currently an associate professor and a Cisco instructor at the Computer Engineering Department, College of Engineering, University of Baghdad. He is also a software-testing expert in the Malaysian Software Engineering Interest Group (MySEIG). His research interests include software engineering, parallel and distributed computing, algorithm design, RFID applications development, embedded systems, networking, and security. Assoc. Prof. Dr. Younis is also a member and Consultant Engineer at the Iraqi Union of Engineers.

REFERENCES

[1] Toonk, Andree. "Massive route leak causes internet shutdown,". *BGP instability*. Bgpmon.com, June 2015

[2] BGP configuration. http://www.cisco.com/c/en/us/td/docs/ios/12_2/ip/configuration/guide/fipr_c/1cfbgp.html

[3] BGP Prefix-Based Outbound Filtering. http://www.cisco.com/c/en/us/td/docs/ios/12_2s/feature/guide/fsbgporf.html

[4] F. Wang, Z. M. Mao, J. W. L. Gao, and R. Bush. A Measurement Study on the Impact of Routing Events on End-to-End Internet Path Performance. In SIGCOMM, 2006.

[5] N. Kushman, S. Kandula, D. Katabi, and B. Maggs. R-BGP: Staying Connected In a Connected World. Technical Report TR-, MIT, 2007

[6] J. Rexford, J. Wang, Z. Xiao, and Y. Zhang, "BGP routing stability of popular destinations," in *Proc. Internet Measurement Workshop*, November 2002.

[7] J. Wu, Z. M. Mao, J. Rexford, and J. Wang, "Finding a needle in a haystack: Pinpointing significant BGP routing changes in an IP network," in *Proc. Networked System Design and Implementation*, May 2005.

[8] L. Gao and F. Wang. The extent of AS Path Inflation by Routing Policies. In Glob. Internet Symposium, 2002.

[9] W. Xu and J. Rexford. Multi-path Interdomain Routing. In SIGCOMM, 2006.

[10] P. Francois, C. Filsfils, J. Evans, and O. Bonaventure. Achieving Sub-Second IGP Convergence in Large IP Networks. CCR, 2005.

[11] Garurab Raj Upadhaya., Peering and Network Group. *Best BGP practises for ISP*. www.pch.net