International Journal of Computer Science Trends and Technology (IJCST) – Volume 3 Issue 4, Jul-Aug 2015

RESEARCH ARTICLE OPEN ACCESS

Performance and Security Analysis of Border Gateway Protocol

Parvesh Kaushal [1], Mr. Amarvir Singh [2]
Department of Computer Science
Punjabi University
Patiala
Punjab – India

ABSTRACT
Border Gateway Protocol is the protocol of the Internet. All the Internet Service Providers in the world use BGP to connect with other ISPs. As the Internet traffic is growing with the time, BGP routing table is also growing. This paper explains the BGP and its performance analysis. It also describes the various faster-convergence methods for BGP like Fallover and External Failover. Both IPv4 and IPv6 based BGP is analyzed in the paper. Apart from this, security analysis is done in this paper on how IPSec secures the WAN traffic or BGP based traffic. Also Neighbor Authentication methods and TTL Security mechanism has been described in the paper. This paper provides best practices that can be used while implementing Border Gateway Protocol.
Keywords:- TTL, WAN, BGP

I. INTRODUCTION

On October 29, 1969, when ARPANET project was first started with interconnection of two nodes i.e. Leonard Kleinrock's Network Measurement Center at the UCLA's School of Engineering and Applied Science and Douglas Engelbart's NLS system at SRI International in Menlo Park, California, who would have thought that this invention will change the way we see this world. Internet got commercialized in the early 1990s and with ecommerce companies like ebay, Amazon, Alibaba, Indiamart etc, ecommerce industry rised at a rapid pace. With the time, Social Networking Sites, Instant Messaging, VoIP Calling, Emails etc features took Internet to a totally new level. Internet users were increasing day by day, so at that time we needed a protocol which can be easily scalable to handle large service provider networks and can work well with internet scalability issues.

Border Gateway Protocol was proposed in IETF RFC 1105 [1], June 1989 by K. Lougheed of Cisco Systems Inc., and Y. Rekhter of T.J. Watson Research Center, IBM Corp.. This RFC describes a specific approach for the exchange of network reachability information between Autonomous Systems.

Border Gateway Protocol was built on experience gained with Exterior Gateway Protocol, and its usage in NSFNET Backbone. EGP was not scalable for fast paced internet. Currently BGP version 4 is in use which became standard on March 1995, with RFC 1771[5], which got obsoleted by RFC 4271 [6] in January 2006.

BGP is the only inter-autonomous system routing protocol, so it is the protocol that makes internet work. Border Gateway protocol enables internet service providers(ISPs) to establish routing among each other and maintain the global reachability. BGP uses an algorithm which cannot be classified as a pure "Distance Vector", or pure "Link State". It is a path vector routing protocol as it defines a route as a collection of a number of AS that is passes through from source AS to destination AS. This list of ASes are called AS_PATH and is used to avoid eBGP routing loop. The performance of Global Routing System is very important for all the entities operating the autonomous systems, which makes up the internet. BGP enables the traffic flow from one point to another connected to the internet. Figure showing BGP peering for Internet or we can say that the below figure by itransformers displays how all the ISPs are connected with each other via BGP.

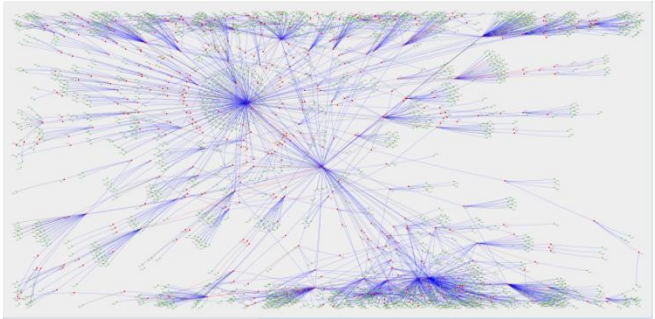

Figure 1.1 - BGP peering between different ASes for Internet.[26]

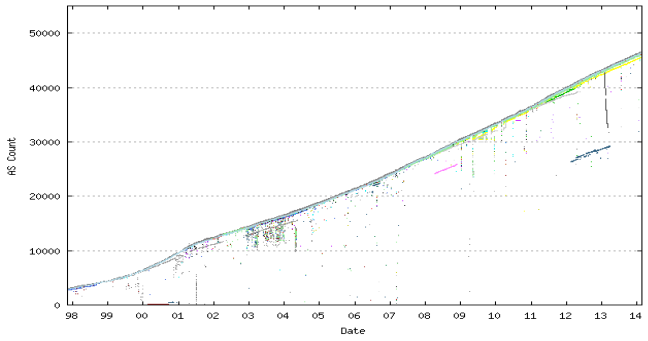

Figure 1.2 - Rise in ASes seen in BGP Routing Table from 1998 to 2014 [23]

II. BORDER GATEWAY PROTOCOL

Border Gateway Protocol is the only exterior Gateway Protocol in the world at present. It is also known as Internet's Protocol. It comes in both IPv4 and IPv6 versions. Currently BGPv4 is used in IPv4. Following are the characteristics of Border Gateway Protocol :

Characteristics of Border Gateway Protocol -

- BGP is the only exterior gateway protocol(EGP) used in routing between different Autonomous Systems.
- BGP is a path vector routing protocol which is suited for strategic routing policies.
- eBGP is used for neighborship between different autonomous systems. For example BSNL uses AS 9829 and Bharti Airtel uses AS 9498. Neighborship and route sharing between these two ISPs is done via eBGP.
- iBGP is used between internal neighbors i.e. bgp neighborship between routers which are part of the same autonomous system.
- For best path selection towards destination, BGP uses several attributes. Most of the attributes are open standard, while some are proprietary.
- BGP uses TCP port 179 to establish connections between neighbors.
- Incremental Updates
- Classless Inter Domain Routing(CIDR)

BGP Terminology -

- **Autonomous System** - set of routers under a single technical administration. IGP is used inside an Autonomous system for routing purposes, while BGP is used to share routing information between different autonomous system.
- **Peers(neighbors)** - Two routers running BGP, exchanging route information are called peers or neighbors.
- **External BGP(eBGP)** - Two routers belonging to different ASes running BGP to share routing information.
- **Internal BGP(iBGP)** - Two routers belonging to same AS running BGP to share routing information.
- **Path Attributes** - Metrics used to BGP to select the best path to reach destination.

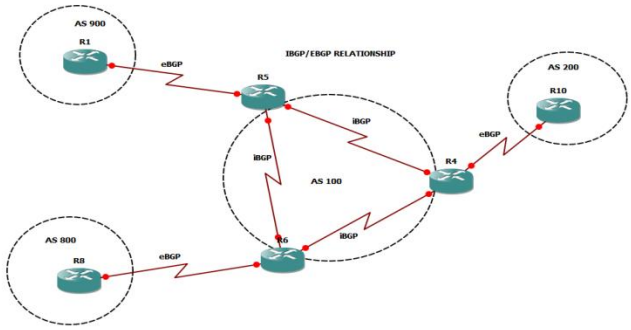

Figure 2.1 - IBGP/EBGP Relationship

Statement of the problem - Some stats from International Telecommunications Union shows that Internet users out of total population in the world has increased from 16 percent in 2005 to 40 percent in 2014.

As the internet still growing with demands increasing with newer services and heavy loaded applications and services like VoIP and Video Traffic. BGP needs to be more better with performance and security. BGP is a slow protocol as it is made with having focus on Internet. But with the high speed networks today, bgp updates to its neighbors are still not as fast as needed in today's financial and stock related customers environment where every second is important. It takes around 5 to 15 minutes to update the full routing table. Also the peer authentication mechanism in BGP is also quite straightforward and needs to be much better for security purpose.

IPv4 BGP routing table has over 500,000 routes installed with over 40,000 Autonomous System. Internet Routing

Table has its routes increased from 180,000 routes to over 500,000 since last BGPv4 was standardized. Network speeds have changed a lot, 40Gbps and 100Gbps are used in ISPs and Data Centers, and with these great bandwidths, bgp needs to have some enhancements related to performance. Also it needs to be much more secure as if not properly implemented it can be easily be vulnerable to denial-of-service(DoS) attacks and route hijacking.

III. BRIEF LITERATURE SURVEY

K. Lougheed of Cisco Systems and Y. Rekhter of T.J. Watson Research Center, IBM Corp. [1] proposed in "IETF Request For Comments 1105" in June, 1989 outlines a specific approach for the exchange of network reachability information between Autonomous Systems. At the time of its writing, the Border Gateway Protocol implementation exists only for Cisco Routers and NSFNET Nodal Switching Systems. It was the first version of BGP. In this version, Message size varies from 8 to 1024 bytes.

K. Lougheed and Y. Rekhter[2] proposed "RFC 1163 and RFC 1164" on June 1990.**[3]** RFC 1164 was proposed by J. Honig, of Cornell Univ. Theory Center, D. Katz and J. Yu, of Merit/NSFNET, M. Mathis, Pittsburgh Supercomputing Center, and Y. Rekhter.It was known as BGP version 2. This version removed the concept of "up", "down", and "horizontal" relations between autonomous systems that were present in Version 1.BGP-2 introduced the concept of path attributes. In addition, BGP-2 clarified parts of the protocol that were "under-specified". Message size varies from 19 to 4096 bytes.

K. Lougheed and Y. Rekhter.[4]proposed BGP version 3 in "IETF Request For Comments 1267" on October 1991. This version lifts some of the restrictions on the use of NEXT_HOP path attribute, and added the BGP Identifier field to the BGP OPEN message. It also clarifies the distribution process of BGP routes between the BGP Routers within an autonomous system. Message size varies from 19 to 4096 bytes.

Y. Rekhter, T. Li, S. Hares [5] proposed BGP version 4 in "Request For Comment 1771" on March 1995. It is the current version of BGP. It was obsoleted by **[6]** RFC 4271 in January 2006. It redefines the previously class-based network layer reachability(NLRI) portion of the updates to specify prefixes of arbitrary length in order to represent multiple classful networks in a single entry. AS_PATH attribute is also modified so that sets of autonomous systems, and individual ASs may be described. In addition, the INTER-AS METRIC attribute is redefined as the MULTI-EXIT DISCRIMINATOR(MED). The LOCAL-PREFERENCE and AGGREGATOR attributes are also added in BGP version 4. Message size still varies from 19 to 4096 bytes. BGP-4 also provides a set of mechanisms for supporting Classless Inter-domain Routing(CIDR).

V. Gill, J. Heasley, D. Meyer, P. Savola, Ed., C. Pignataro[9] proposed in RFC 5082, the Generalized TTL Security Mechanism(GTSM), which is designed to protect a router's IP-based control plane from CPU-utilization based attacks.

A. Heffernan of Cisco System[10]proposed in "Request for comments: 2385" a TCP extension to enhance security for Border Gateway Protocol. It defines a new TCP option for carrying an MD5 digest in a TCP segment. This digest acts like a signature for that segment, incorporating information known only to the connection end points.

Heng Yin ; Coll. of William & Mary, Williamsburg ; Bo Sheng ; Haining Wang ; Jianping Pan et. al. [12] proposed in their paper "Securing BGP through keychain based signatures" the use of keychain based signatures while doing authentication between bgp peers.

Stephen Kent, Charles Lynn, and Karen Seo el. al.[13] proposed in their paper "Secure Border Gateway Protocol" a secure, scalable, deployable architecture (S-BGP) for an authorization and authentication system that addresses most of the security problems associated with BGP. The paper discusses the vulnerabilities and security requirements associated with BGP, describes the S-BGP countermeasures, and explains how they address these vulnerabilities and requirements.

Kevin Butler, Tony R. Farley, Patrick McDaniel, and Jennifer Rexford el. al.[14] proposed in their paper "A survey of BGP security issues and solutions" describing a major limitation of BGP is its failure to adequately address security. Outages in the past and various security analysis clearly indicate the vulnerabilities in Internet Routing. This paper considers current vulnerabilities in BGP routing and surveys both research and standardization efforts relating to BGP security.

Geoff Huston, Swinburne Univ. of Technol., Melbourne, VIC, Australia, Rossi, M. , Armitage G.et. al. [15] proposed in their paper "Securing BGP Literature Survey "examines the Internet's routing architecture and the design of BGP in particular, and surveys the work to date on securing BGP.

Ricardo Oliveira and Lixia Zhang of University of California, Los Angeles, Mohit Lad of Nokia [16] proposed in their paper "Understanding the Challenges in Securing Internet Routing" describes the challenges for securing Internet Routing(BGP) that includes DDoS attacks, protection of BGP configurations and various other vulnerabilities.

S. Kent and K. Seo, BBN Technologies [25] proposed in "Request for comments: 4301" describes the Security Architecture for IPsec – compliant systems. It describes how to provide a set of security for traffic at the IP layer. Comparative analysis of BGPv4 and BGPv6 on the basis of security

IV. OBJECTIVES

a) Comparative analysis of BGPv4 and BGPv6 on the basis of performance
b) Comparative analysis of BGPv4 and BGPv6 on the basis of security
c) Comparing key-chain based signature authentication mechanism with BGP TCP MD5 Signature mechanism

V. METHODOLOGY

The steps followed for methodology are given below:

1) The First step is to study various BGP Standards documentation by IETF and various vendors.

2) BGP is implemented in GNS3 for performance and security analysis with IPv4 and IPv6.

3) Performance is evaluated by creating graphs in PRTG Monitoring tool using SNMP.

4) Graphs are created in PRTG and a performance comparison will be made.

5) Security is evaluated by comparing VoIP traffic with and without IPsec and other BGP security techniques are evaluated.

VI. RESULTS AND DISCUSSIONS

6.1) Performance Analysis of BGP routing protocol with IPv4 and IPv6

BGP routing table is huge and with IPv6, the capacity can only become larger than before. Performance of BGP decides performance of Internet as BGP is the routing protocol of Internet. Tons of links get up and down and with that convergence is one of the big things with BGP, convergence time means how much time it takes to BGP protocol to shift the traffic from primary to secondary or backup link in case of primary link failure. BGP is created as slow protocol with a intention that tons of links getting up and down can create a havoc in the router's processing those having the internet routing table. What I have done is that I have compared BGP's default convergence time with both IPv4 and IPv6 and then used some of its faster convergence features with IPv4 and IPv6 to compare both versions of BGP that is with IPv4 and IPv6 along with faster convergence.

Topology that I used for my testing work is :

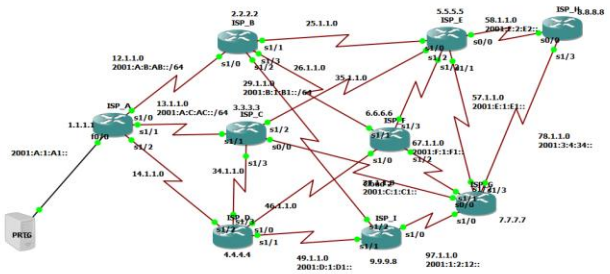

Figure 6.1 - BGP topology used in GNS3

In the above topology, 9 different ISPs are connected together and sharing their routes using eBGP. A PRTG Monitoring tool is connected with them monitoring all the links, their availability, their convergence time, CPU resources used. PRTG monitoring tool is acting as a source IP and destination IP is 8.8.8.8 on ISP_H. PRTG is connected with ISP_A and to reach destination 8.8.8.8, it has three major paths from ISP_A :

1. **PRTG - ISP_A - ISP_B - ISP_E - ISP_H - 8.8.8.8**
2. **PRTG - ISP_A - ISP_C - ISP_E - ISP_H - 8.8.8.8**
3. **PRTG - ISP_A - ISP_D - ISP_F - ISP_E - ISP_H - 8.8.8.8**

As we are using BGP with default parameters, PRTG selects the path via ISP_B, as it involves the lowest router-id and if all the parameters are matched with more than 1 links towards destination. BGP selects the one with the lowest router-id. In my case, Link 1 is selected as the best path to reach destination 8.8.8.8. When the best path goes down, the traffic from PRTG shifts to the other path and the convergence it takes is shown below in the graph taken with PRTG monitoring tool :

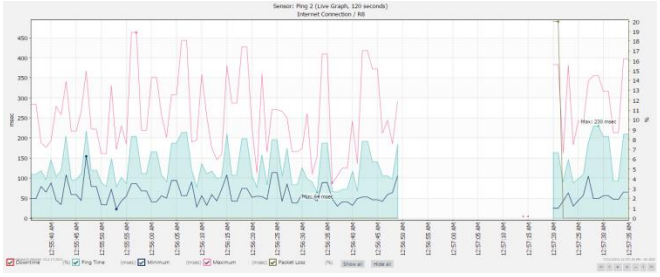

Figure 6.2 - Default BGP convergence time

Above is the convergence time shown in case of primary link failure and traffic shift from Primary Path towards Backup Path is around 30 seconds. BGP is a slow protocol with its default parameters and if faster convergence or faster recovery is needed, we need to implement faster convergence features of BGP protocol. We have used two faster convergence methods of BGP which can detect the failure of BGP neighbor in a fast manner and shifts the traffic to other link quickly. We have BGP Fast extern Failover and neighbor fallover method as a faster convergence technique. BGP Fast-external-fallover technique terminates external BGP sessions of any directly adjacent peer if the link used to reach the peer goes down; without waiting for the hold-down timer to expire. BGP neighbor fail-over method monitors RIB(Routing Information Base) and if route to peer is not present in routing table it will immediately deactivate peer session without waiting for hold down timer. Results that we achieve after implementing Faster BGP convergence is shown below :

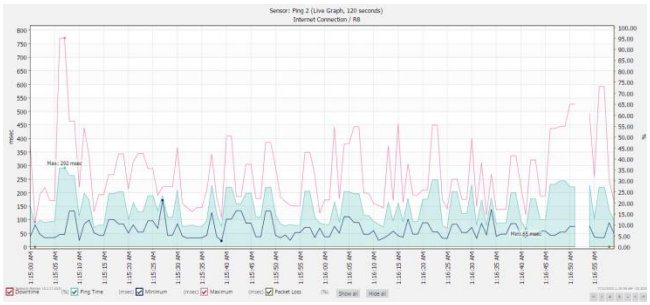

Figure 6.3 - BGP convergence time with Faster Convergence Methods applied.

As you can see in the graph taken from PRTG clearly shows that Convergence time is reduced from 30 seconds to just around 3-4 seconds, which is much faster than the default BGP parameters. Table below shows the difference between the two graphs - the one with the default parameters and the other one with Faster convergence configured :

Protocol	Minimum Time	Maximum Time	Convergence Time
BGP	4msec	230msec	30-31seconds
BGP with Faster	5msec	292msec	3-4seconds

Convergence			

Table 6.1 - Comparison Table showing BGP with default parameters and with Faster Convergence Method

Also as Next-Generation Networks is on a rise, networks across the world are shifting to IPv6 and so is Internet. I have also used BGP with IPv6 and does a comparison just like with BGPv4. Same topology is used for BGPv6 and PRTG here monitors the traffic between him and ISP_H, all the ISPs in the topology are having a dual stack topology as they run both IPv4 and IPv6 at the same time. We are monitoring 8888::8 address and there are three major paths from ISP_A to reach the destination address 8888::8 -

1. PRTG - ISP_A - ISP_B - ISP_E - ISP_H - 8888::8
2. PRTG - ISP_A - ISP_C - ISP_E - ISP_H - 8888::8
3. PRTG - ISP_A - ISP_D - ISP_F - ISP_E - ISP_H - 8888::8

Path 1 towards 8888::8 is selected as the best path as by default it has the lowest router-id and we are using default parameters and with default parameters if nothing is matched then in the end, the best path is selected on the basis of Lowest Router-ID. Below snapshot taken from ISP_A shows that Path 1 is selected as the best path :

```
ISP_A#sh bgp ipv6 unicast 8888::8/128
BGP routing table entry for 8888::8/128, version 74
Paths: (3 available, best #1, table Global-IPv6-Table)
  Advertised to update-groups:
     1
  2 5 8
    2001:A:B:AB::B (FE80::C202:1CFF:FEC0:0) from 2001:A:B:AB::B (2.2.2.8)
      Origin IGP, localpref 100, valid, external, best
  4 3 5 8
    2001:A:D:AD::D (FE80::C204:1DFF:FE74:0) from 2001:A:D:AD::D (4.4.4.8)
      Origin IGP, localpref 100, valid, external
  3 5 8
    2001:A:C:AC::C (FE80::C203:20FF:FEFC:0) from 2001:A:C:AC::C (3.3.3.8)
      Origin IGP, localpref 100, valid, external
ISP_A#
```

Figure 6.4 - Path 1 shown as the best path in ISP_A router

As I am doing performance analysis and convergence is checked from source to destination in case of the primary link goes down. Resulted graph in case of primary link failure and traffic shift time taken by it is shown in the following graph :

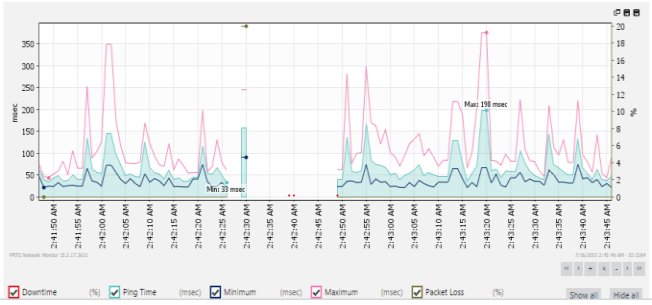

Figure 6.5 - Convergence Time in BGPv6 in PRTG with default BGP parameters

As shown above, convergence time taken by BGP in case of IPv6 routing with default parameters is around 20 seconds, and this is lower than that of BGPv4. But as with BGPv4, BGPv6 is also a slow protocol and if faster convergence or fast failover is needed then we can implement Faster Convergence methods. I have used BGP Fast extern failover and neighbor fallover which makes BGP converges faster in case of the primary link goes down and traffic needed to be shifted from primary to backup link. Below is the graph taken in PRTG showing the convergence time from Primary to backup path :

Figure 6.6 - BGPv6 Convergence Time with Fast Convergence Techniques applied

As shown above BGPv6 with Fast Convergence has around 3 seconds of convergence time in case of primary link failure and traffic shift from primary to backup link. Comparison table between BGPv6 default convergence and Faster Convergence is shown below :

Protocol	Minimum Time	Maximum Time	Convergence Time
BGPv6	3msec	98msec	0-21seconds

BGPv6 with Faster Convergence	27msec	77msec	seconds

Table 6.2 - Comparison Table showing BGPv6 with default parameters and with Faster Convergence Method
A comparison table of both BGPv4 and BGPv6 is shown below :

Protocol	Minimum Time	Maximum Time	Convergence Time
BGP	64msec	230msec	0-31seconds
BGP with Faster Convergence	65msec	292msec	-4seconds
BGPv6	83msec	298msec	0-21seconds
BGPv6 with Faster Convergence	27msec	77msec	seconds

Table 6.3 - BGPv4 and v6 comparison Table

6.2) Security Analysis of BGP protocol

a) IPSec

BGP is the protocol of the internet and to make it secure, we can use various security mechanisms, sending IP traffic over public network without using any security mechanism can never be a good idea. So to make our traffic secure we can use **IPSec**. IPSec is security protocol suite that gives Data Integrity, Encryption and Authentication features and make data much more secure.

We have used the same topology that we have used for performance analysis for BGP security analysis and created a IPSec VPN from one ISP to other ISP, we have used IPSec between ISP_A and ISP_H in our topology and used Cisco Configuration Professional for configuration to build a graph for traffic between ISP_A and ISP_H.

After issuing ping command on ISP_A, I issued the **debug crypto engine packet** command on ISP_H to check incoming traffic created with the ping command on ISP_A to see if the incoming traffic from ISP_A is coming in encrypted form or not. Result is shown on the next figure

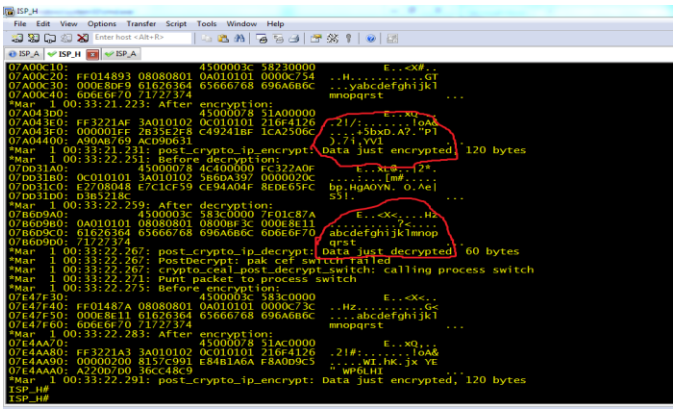

Figure 6.7 - Output of debug crypto engine command showing encrypted and decrypted traffic on ISP_H

To get into more detail, I have also used Wireshark Packet analyzer to sniff data that is going over Service Provider Network. Below is the capture taken from Wireshark :

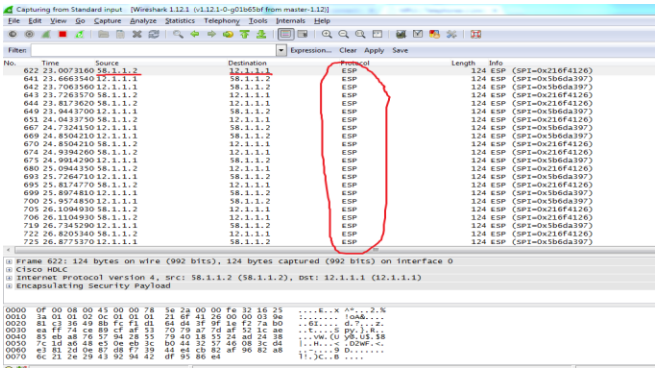

Figure 6.8 - Wireshark capture showing traffic from 10.1.1.1 to 8.8.8.1 using ESP using Tunnel Source and Destination.

Above capture from Wireshark shows that Source and Destination IP addresses are hidden because we are using Tunnel Mode in IPSec. With Tunnel Mode, original IP address gets hidden and Tunnel's Source and Destination IP addresses are used which is an add-on to the network security. For more details, I have also extracted a packet using Wireshark going from 10.1.1.1 towards 8.8.8.1

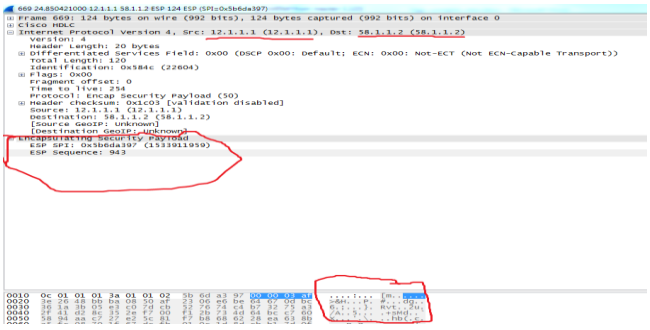

Figure 6.9 - Specific ESP packet captured in Wireshark

Above Figure shows that traffic generated from ISP_A to ISP_H is encrypted when traffic is sent between 10.1.1.1 and 8.8.8.1. ESP shows encrypted data under the payload section.

Below is the comparison done between VoIP based traffic between two IP Phones which is going via WAN link. A call when initiated between two IP Phones at distant locations, produces RTP(Real-Time Transport Protocol) based traffic. Below is the Wireshark capture of the RTP traffic on the WAN link between two Edge routers.

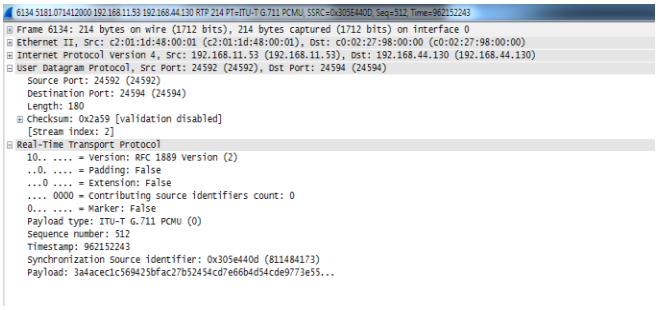

Figure 6.11 - RTP Capture in detail in Wireshark

When two persons have some conversation going on between them via IP Phones, RTP packets are generated. If no security is used, then these RTP packets can be decoded to wave tones, which can give us the ongoing voice between the people in human understandable form. Below are the screenshots that shows how the RTP traffic can be decoded in Wireshark easily :

First we select the RTP stream as shown in the following figure :

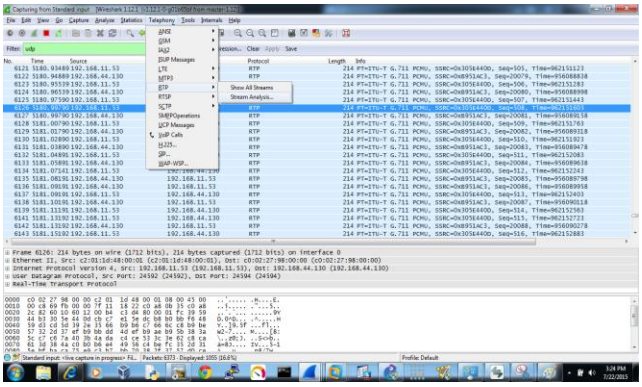

Figure 6.12 – Selecting RTP for stream analysis

Then after selecting any RTP packet, we can click on stream analysis, and the following figure will be shown :

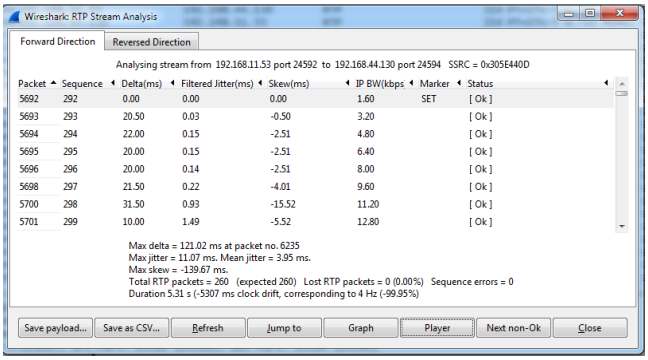

Figure 6.13 – RTP stream analysis in Wireshark

Here we will select player and the output in the following figure will be displayed :

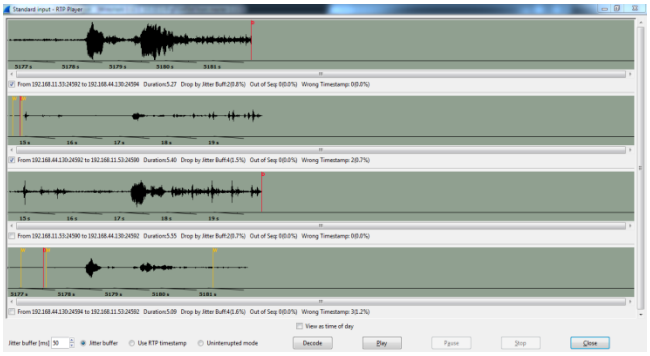

Figure 6.14 – Decoding of RTP into wave form

Here we can select the stream and click on play, and with that we are able to listen the conversation and decoding has just been performed.

Now with IPSec used, let's see what will happen when we try to decode. IPSec will use tunnel mode and the everything is encapsulated in ESP packets between the WAN link. Following is the Voice packet captured after IPSec is configured :

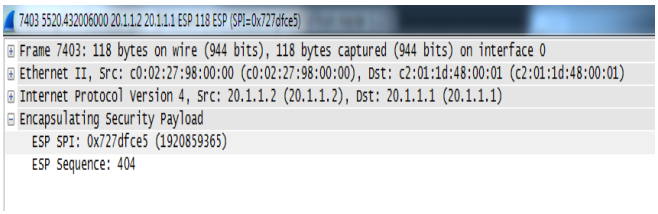

Figure 6.15 – Voice Packet after IPsec implementation between WAN.

When we try to decode ESP to RTP, then it did not convert the ESP to RTP, then I first tries it to convert it to UDP as RTP uses UDP, it can be converted into RTP. After converting into UDP, following figure is the resulted :

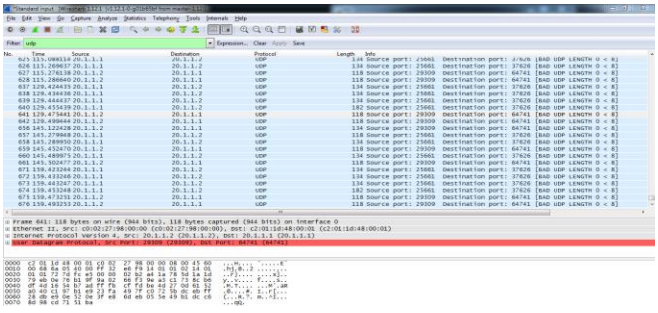

Figure 6.16 – ESP packets converted into UDP

And at last when I tried to decode UDP to packet capture shows that UDP packet is malformed and cannot be used.

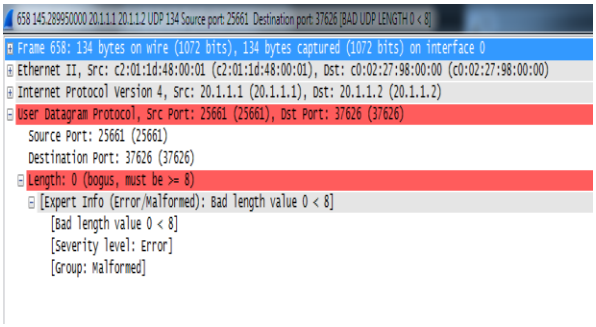

Figure 6.17 – UDP malformed packet after being decoded from ESP

This proves that IPSec provides the best possible security for data on BGP WAN links.

b) TTL Security Mechanism

We can also secure our BGP using **TTL security mechanism**, which can be used to protect BGP from Denial of Service(DOS) Attack. The BGP Time-to-Live Security Check is designed to protect the BGP processes to CPU utilization and Route manipulation attacks.

By default external BGP session has a TTL value set to 1 in its header. This setting acts pretty useful as it prevents establishment of ebgp session beyond single hop. But an attacker can be located up to 255 hops away and still send spoof packets to BGP speaking router successfully. Attacker can send large number of TCP SYN packets to overwhelm the BGP process which cannot be prevented using BGP TCP MD5 Signature based Authentication Mechanism as it can actually cause the router CPU to expend resources while it attempts to compute MD5 hashes with large number of attack packets. So another mechanism that can be useful in this type of conditions is TTL security mechanism check.

When a BGP TTL security check is enabled on a BGP router, the initial TTL value starts from 255 rather than 1 and a minimum TTL value is enforced to all the eBGP peers . As the IP Header TTL value is decremented by each router along its path towards the final destination, the diameter is then limited only to the directly

connected peers. Hence it helps preventing the DOS attacks on BGP routers.

Below screenshot is taken from Router's terminal, which shows that by default outgoing ttl value is 1, but when we apply TTL-Security then it changes to 255

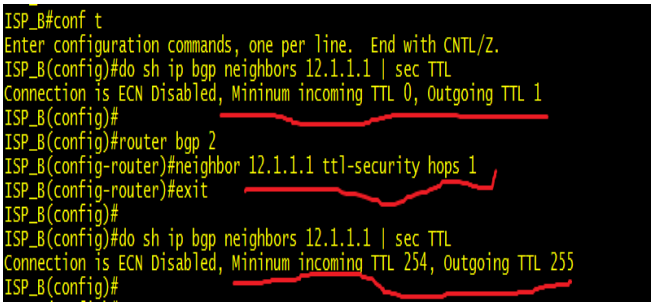

Figure 6.18 - BGP TTL Security Mechanism

c) Key-Chain Mechanism

BGP also can be secured by using Password authentication. BGP uses TCP MD5 Signature based mechanism. BGP uses single password and it is in the TCP segment. If the Password do not match then the TCP session is not created, which is needed in order to start sending BGP data packets. A wireshark capture of BGP password within the TCP segement is shown below :

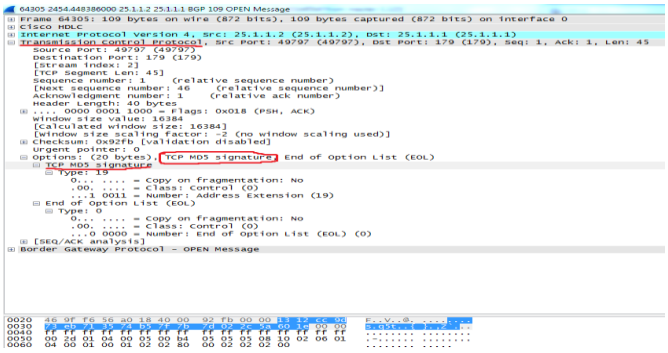

Figure 6.19 - BGP TCP MD5 Signature captured in Wireshark

Another alternative of password authentication is **key-chain mechanism** which is used in Enhanced Interior Gateway Routing Protocol(EIGRP), the best thing about Key-chain mechanism is that we can create multiple number of keys which can be used in a way that one key is used for some amount of time and second key is used after time of first key is expired, and then third key is used after time of second key is expired automatically. It can be synced in all the routers as time is synced in Internet routers or in enterprise network devices using Network Time Protocol(NTP). Captures of Key-chain based mechanism in EIGRP taken in Wireshark is shown below :

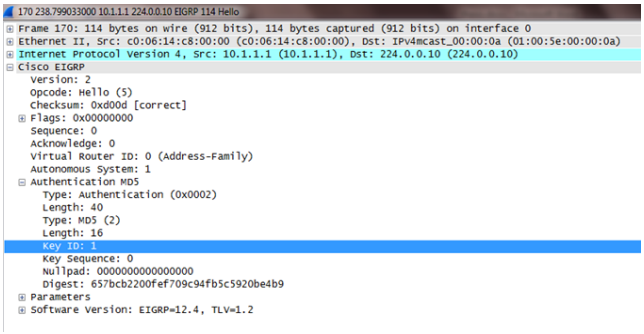

Figure 6.20 - Keychain Mechanism with Key-Id 1 in Use

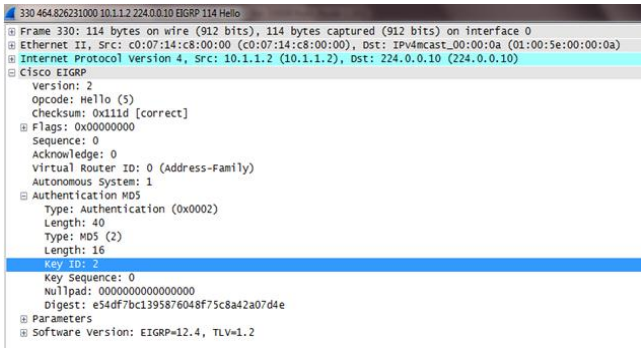

Figure 6.21 - Keychain Mechanism with Key-ID 2 in Use

VII. CONCLUSION

BGP is a slow protocol, but it made as slow for the behavior of Internet as there are hundreds of thousands routes present in the routing table, so flapping of routes can produce large number of updates which can be harmful if protocol is fast. But there are some cases where protocol needs to be fast converged, performance analysis results shows that BGP can be made fast with Faster convergence features like fall over and BGP

Extern Failover methods. Security can be achieved with the IPSec, if we want to have all the data going over BGP links to be secure. Neighbor Authentication methods are necessary in the BGP as BGP traffic is always critical . TTL security can be used in the BGP to secure the network from denial-of-service attacks. BGPv4 and BGPv6 performance is almost same. In Security perspective, BGPv6 can achieve same level of security as with BGPv4.

ACKNOWLEDGEMENT

This paper has been made possible through the constant encouragement and help from my parents and guide. I would like to thank Assistant Prof. Mr. Amarvir Singh , for his generous guidance, help and useful suggestions.

REFERENCES

[1] **K. Lougheed, Y. Rekhter**, "A Border Gateway Protocol ", Request for Comments: 1105, Internet Engineering Task Force, June 1989.

[2] **K. Lougheed and Y. Rekhter**,"BGP Version 2", Request for Comments: 1163, Internet Engineering Task Force, June 1990

[3] **J. Honig, D. Katz, M. Mathis, Y. Rekhter**,"Application of the Border Gateway Protocol in the Internet", Request for Comments: 1164, Internet Engineering Task Force, June 1990

[4] **Y. Rekhter and K. Lougheed**, "A Border Gateway Protocol 3 (BGP-3)", Request for Comments: 1267, Internet Engineering Task Force, October 1991.

[5] **Y. Rekhter and T. Li**, "A Border Gateway Protocol 4 (BGP-4)", Request for Comments: 1771, Internet Engineering Task Force, March 1995.

[6] **Y. Rekhter and T. Li**, "A Border Gateway Protocol 4 (BGP-4)," Request for Comments: 4271, Internet Engineering Task Force, January 2006.

[7] **D. Meyer and K. Patel**, "BGP Protocol Analysis",Request for Comments: 4274, Internet Engineering Task Force, January 2006.

[8] **D. McPherson and K. Patel**,"Experience with BGP-4 Protocol ", Request for Comments: 4277, Internet Engineering Task Force, January 2006.

[9] Understanding BGP Convergence - **http://blog.ine.com/2010/11/22/understanding-bgp-convergence/**

[10] Protecting Border Gateway Protocol - **http://www.cisco.com/web/about/security/intelligence/protecting_bgp.html**

[11] **V. Gill, J. Heasley, D. Meyer, P. Savola, Ed., C. Pignataro**," The Generalized TTL Security Mechanism (GTSM)", Request for Comments: 5082, Internet Engineering Task Force, October 2007.

[12] **A. Heffernan**,"Protection of BGP Sessions via the TCP MD5 Signature Option", Request for Comments: 2385, Internet Engineering Task Force, august 1998.

[13] **R. Bonica, B. Weis, S. Viswanathan, A. Lange, O. Wheeler**," Authentication for TCP-based Routing and Management Protocols draft-bonica-tcp-auth-04", Internet draft, Internet Engineering Task Force, February 2006.

[14] **Heng Yin, Bo Sheng, Haining Wang and Jianping Pan**,"Securing BGP with keychain based signatures", IEEE,2007,International Workshop on Quality of Service, pp. 154-163

[15] **Stephen Kent, Charles Lynn, and Karen Seo,"Secure Border Gateway Protocol**", IEEE Journal on Selected areas in Communications,Vol – 18,Issue: 4,April 2000,pp.582 - 592

[16] **Kevin Butler, Toni R. Farley, Patrick McDanie and Jennifer Rexford**," A survey of

BGP security issues and solutions",Proceedings of the IEEE, Vol: 98, Issue: 1, January 2010, pp. 100 - 122

[17] **Geoff Huston, Mattia Rossi, Grenville Armitage**,"Securing BGP Literature Survey", Communications surveys and tutorials, IEEE, Vol: 13, Issue: 2, May 2010, pp. 199 - 222

[18] **Ricardo Oliveira, Lixia Zhang and Mohit Lad**,"Understanding the Challenges in Securing Internet Routing" ,SAINT '09. Ninth Annual International Symposium on Application and the Internet, pp. 144 - 148

[19] Internet Assigned Numbers Authority(IANA) BGP Parameters - **http://www.iana.org/assignments/bgp-parameters/bgp-parameters.xhtml**

[20] Analyzing the Internet's BGP Routing Table by Geoff Huston, Telstra Telecommunications, Australia - **http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_4-1/bgp_routing_table.html**

[21] **Rick Kuhn KotikalapudiSriram Doug Montgomery**,"Border Gateway Protocol Security", National Institute of Standards and Technology, U.S. Department of Commerce, July 2007

[22] BGP Case Studies by Cisco Systems Inc. - **http://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/26634-bgp-toc.html**

[23] **http://bgp.potaroo.net**

[24] **KotikalapudiSriram, Doug Montgomery, Oliver Borchert, Okhee Kim and D. Richard Kuhn**," Study of BGP Peering Session Attacks and Their Impacts on Routing Performance", IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS: Special issue on High-Speed Network Security, VOL. 24, NO. 10, OCTOBER 2006

[25] **S. Kent , K. Seo**, "Security Architecture for the internet protocol" Request for Comments: 4301, Internet Engineering Task Force, December 2005.

[26] http://www.itransformers.net/logo/bg_peering.png

[27] http://www.inetdaemon.com/tutorials/internet/ip/routing/dv_vs_ls.shtm