

Performance Analysis on a BGP Network using Wireshark Analyzer

*MaryAnne Binarao Taquiqui, PhD
College of Computer Studies, AMA International University – Bahrain, Kingdom of Bahrain

Abstract
Border Gateway Protocol (BGP) is a standardized exterior gateway protocol designed to exchange routing and reachability information among autonomous systems (AS) on the Internet. The protocol is often classified as a path vector protocol but is sometimes also classed as a distance-vector routing protocol.
This study focused on the performance analysis of BGP when implemented in a network. The configuration of BGP was done using Graphical Network Simulator (GNS3). To test the performance of BGP in a network, Wireshark was used for this purpose. The Wireshark is a network packet analyzer where it can capture live packet data from a network interface and display packet with every detailed protocol information.
Performance details of the packet in terms of several parameters are used in this study namely: length of packet, total packets captured, packets captured between first and last packet, average packet per second, average packet size in bytes, number of bytes , and average bytes per second.
Based on the results, all routers have the same packet length and packets captured. However, the packets captured between the first and last, the average packet/sec, Avg. packet size (bytes), Bytes, and Avg. bytes/sec differ in all the routers.
Keywords: BGP, Autonomous system, packet, GNS3, Wireshark

Introduction

Border Gateway Routing Protocol (BGP) is a routing protocol that literally makes the Internet work as it is used to route traffic across the internet. BGP is considered to be one of the most relevant protocols especially in large organizations connecting to two or more Internet Service Providers (ISPs) as well as ISPs connecting to other network providers.
To implement a BGP in a network allows creation of loop-free inter-domain routing between Autonomous System (AS). An AS identifies network under a single technical administration and is required when running a BGP.

The focus of BGP is scalability and stability and as a result, it behaves differently than most routing protocols which is why, it is most often used between ISPs and between enterprises and their service providers. This study focused on the performance analysis of BGP when implemented in a network. The configuration of BGP was done using Graphical Network Simulator (GNS3). To test the performance of BGP in a network, Wireshark was used for this purpose. The Wireshark is a network packet analyzer where it can capture live packet data from a network interface and display packet with every detailed protocol information. The output was obtained by examining the results taken from the console of the packet analyzer as the detailed information was displayed by the Wireshark. This enabled the researcher to examine the captured packets for analysis.

As to the methodologies used, Part I made use of a descriptive method to discuss the characteristics of the protocol used. In Part II, network implementation was done using the GNS3. Experimentation method was used in the analysis part using the Wireshark Packet Analyzer.

Related Literature

Border Gateway Protocol (BGP) is an interdomain routing protocol using path vector routing. The Internet is divided into hierarchical domains called autonomous systems. For example, a large corporation that manages its own network and has full control over it is an autonomous system. A local ISP that provides services to local customers is an autonomous system. We can divide autonomous systems into three categories: stub, multihomed, and transit. A stub AS has is either a source or a sink. A good example of a stub AS is a small corporation or a small local ISP. A multihomed AS has more than one connection to other ASs, but it is still only a source or sink for data traffic. It can receive data traffic from more than one AS. It can send data traffic to more than one AS, but there is no transient traffic. It does not allow data coming from one AS and going to another AS to pass through. A good example of a multihomed AS is a large corporation that is connected to more than one regional or national AS that does not allow transient traffic. A transit AS is a multihomed AS that also allows transient traffic. Good examples of transit ASs are national and international ISPs [1].

In the article by Lammle, T., Odon, S., Wallace, K. (2001) mechanisms of functioning of the dynamic routing protocol BGP are examined in details. Guides for configuring Cisco routers and Quagga package on basis of Gentoo Linux are given. A stand in which coherence between networks is realized due to routes promoted via BGP was assembled. On this stand a reconnection to a reserve channel on failure of the primary line has been tested. BGP is the basic protocol on the Internet, and due to it ISPs in the whole world are available. The study further mentioned that: Border Gateway Protocol (BGP, RFC-1265-1268,1467,1655,1771,1772) was developed by companies IBM and CISCO. A pair of BGP neighbors establishes a connection via TCP, port 179. Neighbors that belong to different autonomous systems should be available for each other directly; for neighbors from the same AS there is no such restriction because the internal routing protocol provides all necessary routes between nodes of the autonomous system. BGP routers exchange messages on changing routes. The maximal length of such a message is 4096 octets, the minimal is 19 octets. Each message has a header of a fixed size. The volume of an information field depends on the message type [2].

The study conducted by Hanif (2010) focused on the analysis of the dependence of BGP performance upon a given topology. It attempted to understand the response of BGP if Internet faces unavoidable substantial growth and if the current topology changes in characteristics other than its magnitude More precisely, the research is an attempt to comprehend the influence of topology dynamics, in terms of its scale and Internet's operational topological characteristics, upon BGP performance.

The researcher used a BGP simulator that implemented BGP protocol with certain level of abstraction. In the study, the abstraction enables the simulator to model at the order of magnitude of current Internet and higher, letting up to 60,000 AS's to interact with each other and maintain sessions of BGP. In the simulator, each AS is implemented as single entity similar to a vertex of a graph. The researchers' purpose was to find out different trends of behavior BGP exhibits, if it is run with different kinds of topologies and varying parameters. The study wanted to understand the way BGP expresses its strong and weak points that appear due to certain kind of underlying topology. It is important to note that he analyzed BGP behavior with respect to its convergence delay and signal duration across a topology. In simple terms, convergence delay is the amount of time in which a network information change is propagated over Internet. Signal duration also has a similar definition. It is not the researchers' intention to measure the amount of churn (number of BGP update messages) faced by the routers across Internet. Nor did he intend to analyze variation in routing table sizes as the years pass [3].

The project of Szekeres (2011) shed some more light into the behavior of multi-path routing mechanisms and how they affect BGP. The research studies on the inferred topologies from CAIDA show that the Internet is very well connected, with more and more ASs choosing to have multiple providers. This aspect is very favorable as it will provide many disjoint paths that can be explored. However, BGP was not designed to propagate multiple paths, and therefore, it doesn't take advantage to the fullest of the current Internet topology. His experiment showed that introducing the multi-path methods in the current Internet will not have a great impact on BGP's stability, i.e. the convergence time. It will delay the convergence time with less than 30 seconds. Another aspect worth noting is that the convergence time increased very slowly from year 2004 to 2010. This means that the size of the topology doesn't have a great impact on the convergence time [4].

Methodology

This study made use of three (3) approaches, namely: Part I used a descriptive approach to discuss the characteristics of the protocol used which is the Border Gateway Protocol. In Part II, network implementation approach was done using the Graphical Network Simulator 3 (GNS3). Experimentation approach was used in the analysis part using the Wireshark Packet Analyzer.

This research is concerned on the actual data generated from a given network topology and a routing protocol. The data were analyzed and certain parameters were used such as: length of packet, total packets captured, packets captured between 1st and last packet, average packet per second, average packet size in bytes, number of bytes , and average bytes per second.

Findings

Network Implementation

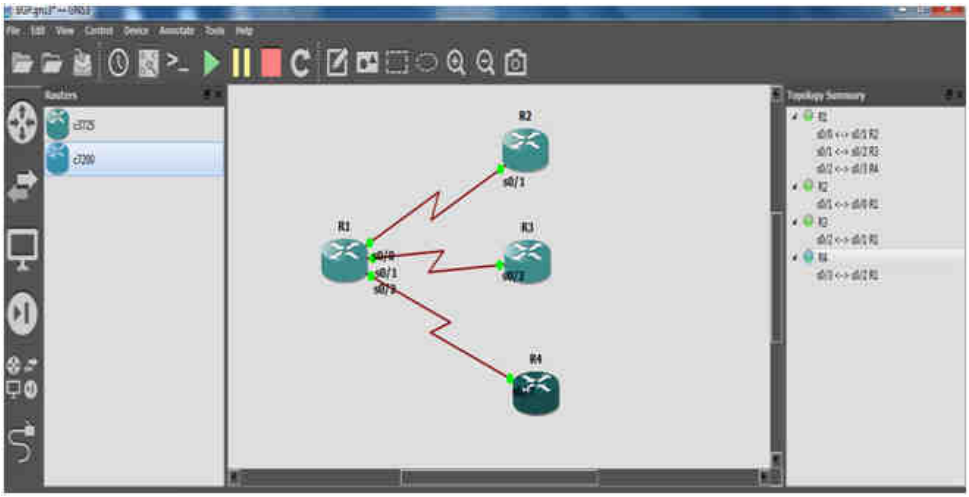

Fig.1. Network Topology

Figure 1 shows the network topology where BGP was implemented in each of the routers. Details for the IP addresses are as follows.

TABLE 1. IP ADDRESSES USED

Network Address of the WAN link (R1-R2)			192.168.1.0/24
Network Address of the WAN link (R1-R3)			172.16.0.0/16
Network Address of the WAN link (R1-R4)			10.0.0.0/8
Device Label	*Interface*	*IP Address*	*Subnet Mask*
R1 (AS100)	s0/0	192.168.1.1	255.255.255.0
	s0/1	172.16.0.1	255.255.0.0
	s0/2	10.0.0.1	255.0.0.0
R2(AS200)	s0/1	192.168.1.2	255.255.255.0
R3(AS300)	s0/2	172.16.0.2	255.255.0.0
R4(AS400)	s0/3	10.0.0.2	255.0.0.0

The assignment of Network addresses was such to show all the network classes, Class A, B and C. The default subnet mask was used for the purpose of discussion; however, a subnetting mechanism can also be used as per the user's requirement. . As such, a prefix length of /30 or 255.255.255.252 subnet mask can be used to eliminate the number of wasted addresses.

Parameters Used

The following are the parameters used in the performance Analysis: *Length.* An integer value indicating the total length of the message; *Packets captured.* In this study, there are 100 captured packets; *Between 1st and last packet.* The time between the first packet and last packet which were captured; *Packets/sec.* The time it takes a packet to move and is measured in seconds; *Packet size.* It is the size of the packet; *Bytes.* It is a unit of digital information which is eight digits long; *Bytes/sec.* It is the number of bytes per second.

Results of the performance analysis

To analyze the first packet, a hello packet was sent between R1 as the source to all the destinations R2, R3 and R4. The conversations that took place between the source and destination showed that:

TABLE 2: IPv4:1 CONVERSATIONS (R1-R2)

IPv4:1 Conversations	*Details*
Address A (Source)	192.168.1.1
Address B (Destination)	192.168.1.2
Packets	18
Bytes	1020
Packets A to B	6
Bytes A to B	378
Packets B to A	12
Bytes B to A	642
Rel Start	12.7617
Duration	300.3332
bps (A to B)	10.07
bps (B to A)	17.10

TABLE 3. TCP CONVERSATIONS (R1-R2)

TCP Conversations	*Details*
Address A (Source)	192.168.1.1
Port A	45798
Address B (Destination)	192.168.1.2
Port B	179
Packets	18
Bytes	1020
Packets A to B	6
Bytes A to B	378
Packets B to A	12
Bytes B to A	642
Rel Start	12.7617
Duration	300.3332
bps (A to B)	10.07
bps (B to A)	17.10

TABLE 4. IPv4:1 CONVERSATIONS (R1-R3)

IPv4:1 Conversations	*Details*
Address A (Source)	172.16.0.1
Address B (Destination)	172.16.0.2
Packets	20
Bytes	1070
Packets A to B	10
Bytes A to B	535
Packets B to A	10
Bytes B to A	535
Rel Start	45.4756
Duration	240.2807
bps (A to B)	17.81
bps (B to A)	17.81

TABLE 5. TCP CONVERSATIONS (R1-R3)

TCP Conversations	*Details*
Address A (Source)	172.16.0.1
Port A	49270
Address B (Destination)	172.16.0.2
Port B	179
Packets	20
Bytes	1070
Packets A to B	10
Bytes A to B	535
Packets B to A	10
Bytes B to A	535
Rel Start	45.4756
Duration	240.2807
bps (A to B)	17.81
bps (B to A)	17.81

TABLE 6. IPv4:1 CONVERSATIONS (R1-R4)

IPv4:1 Conversations	**Details**
Address A (Source)	10.0.0.1
Address B (Destination)	10.0.0.2
Packets	18
Bytes	1020
Packets A to B	6
Bytes A to B	378
Packets B to A	12
Bytes B to A	642
Rel Start	40.5353
Duration	300.2562
bps (A to B)	10.07
bps (B to A)	17.11

TABLE 7. TCP CONVERSATIONS (R1-R4)

TCP Conversations	**Details**
Address A (Source)	10.0.0.1
Port A	13996
Address B (Destination)	10.0.0.2
Port B	179
Packets	18
Bytes	1020
Packets A to B	6
Bytes A to B	378
Packets B to A	12
Bytes B to A	642
Rel Start	40.5353
Duration	300.2562
bps (A to B)	10.07
bps (B to A)	17.11

In all the tables, most of the parameters for both IPv4 and TCP are the same except the ports in the TCP conversation. In a TCP conversation, TCP port 49270 uses the Transmission Control Protocol. TCP is one of the main

protocols in TCP/IP networks. TCP is a connection-oriented protocol, it requires handshaking to set up end-to-end communications. Only when a connection is set up user's data can be sent bi-directionally over the connection. TCP guarantees delivery of data packets on port 49270 in the same order in which they were sent [7].

BGP uses different source and destination ports other than 179 depending on who originates the session. BGP is essentially a "standard TCP based protocol, which means that it is client and server based. When a TCP client attempts to establish a connection to a TCP server it first sends a TCP SYN packet to the server with the destination port as the well known port. This first SYN essentially is a request to open a session. If the server permits the session it will respond with a TCP SYN ACK saying that it acknowledges the request to open the session, and that it also wants to open the session. In this SYN ACK response the server uses the well known port as the source port, and a randomly negotiated destination port. The last step of the three way handshake is the client responding to the server with a TCP ACK, which acknowledges the server's response and completes the connection establishment [8].

Summary of Captured Packets

TABLE 8. TCP COVERSATIONS (R1-R4)

Parameters	R1- R2	R1-R3	R1-R4
Length	9992 bytes	9392 bytes	9992 bytes
Packets captured	100	100	100
Between 1st and last packet (sec)	340.200	341.120	340.791
Avg. packets/sec	0.294	0.293	0.293
Avg. packet size (bytes)	66	60	66
Bytes	6576	5980	6576
Avg. bytes/sec	19.330	17.531	19.296

Table 8 shows the summary of data in all the routes, R1 being the source and R2, R3 and R4 being the destination. Based on the data, it can be seen that the length and packets captured have the same values. On the other hand, the other parameters show a difference in values. This implies that, even if the length of the packet and the number of captured packets are the same, the other parameters will differ. Figure 2 shows the captured packets in graphical form.

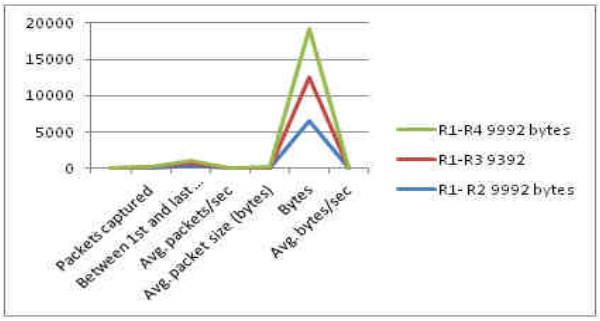

Fig.2. Captured Packets

Conclusion

To fully understand the behavior of a specific protocol, it is important to know its features and characteristics. These will lay the foundation on the network implementation. The performance of a network can be examined and analyzed based on specific pre-determined parameters. These are essential in creating and operating a reliable and available networks and services.

Bibliography

[1] Forouzan, B. (2007). "Border Gateway Protocol (BGP)". Data Communications and Networking. Fourth Edition. McGraw Hill.ISBN-13 978-0-07-296775-3. Chapter 22.4

[2] Lammle, T., Odon, S., Wallace, K. (2001). “Configuring and Testing Border Gateway Protocol (BGP) on Basis of Cisco Hardware and Linux Gentoo with Quagga Package (Zebra)”. CCNP: Routing. Study Guide. SYBEX Inc.
[3] Hanif, S. “Impact of Topology on BGP Convergence”. Parallel and Distributed Computer Systems. Vrije University Amsterdam, 2010.
[4] Szekeres, A. “Multi-path inter-domain routing: The impact on BGP’s scalability, stability and resilience to link failures”. University “Politehnica” of Bucharest Faculty of Automatic Control and Computers Vrije University of Amsterdam, 2011
[5] Kozierok, M. ”BGP Detailed Messaging, Operation and Message Formats”. The TCP/IP Guide. (http://www.TCPIPGuide.com). Version 3.0, 2005
[6] Kacprzynski, T.(2012). “BGP Decision Process”. Kemot-net.com. http://kemot-net.com/blog/bgp-decision-process
[7] Admin (2016). “TCP/UDP Port Finder”. Adminsub.net. http://www.adminsub.net/tcp-udp-port-finder/49270
[8] Dath (2014). “Significance of TCP Port 179 in BGP”. Cisco Support Community. https://supportforums.cisco.com/discussion/12228296/significance-tcp-port-179-bgp

***MaryAnne B. Taquiqui**, Assistant Professor and currently the Associate Dean of the College of Computer Studies (ABET-CAC Accredited), AMA International University, Kingdom of Bahrain. She holds a Bachelor’s Degree in Computer Engineering, Masters in Information Technology and PhD in Educational Management specializing in Administration and Supervision. She has taught at the School of Engineering and Technology, St. Paul University Philippines (ISO 9001) for 6 years before moving to Bahrain. She has taught a wide-range of courses in Computing and Information Technology. She is a Cisco-Certified Instructor and currently the Cisco Legal Main Contact and Curriculum Lead at AMAIUB.
She has authored researches on the field of Net-Centric Computing, Software Development, Mobile Programming and Institutional Programme Design and Development and has advised several Graduate and Undergraduate theses in the same fields including Human-Computer Interaction. She was the mentor of the 2015 Microsoft Imagine Cup, Team Easy Com *Bahrain Winner* - Citizenship Category which qualified the team to the PAN-ARAB Finals.