Fine Tuning Approach for Quality of Service in Border Gateway Protocol

Akash Saini[#1], Gunjan Gandhi[*2]

[#] Department of Electronics and Communication, Lovely University
[1]Project.1198@gmail.com

[*] Department of Electronics and Communication, Lovely University
[2]gunjan.16779@gmail.com

***Abstract*— As the Internet becomes the critical information infrastructure for both personal and business applications, fast and reliable routing protocols need to be designed to maintain the performance of those applications in the presence of failures. BGP (Border Gateway Protocol) as a kind of mature routing protocols has been widely applied in all kinds of large scale network. With regard to routing protocol, the important problem is the convergence time, which is an important index to evaluate the availability and robustness of network. Today's inter-domain routing protocol, BGP, is known to be slow in reacting and recovering from network failures. Many works and techniques have been focused on the reliability of inter domain routing. However, those approaches require modifying the BGP, which makes them impractical in the Internet. In this research, we will propose a simple and practical approach for redistribution of the routes among BGP route updates which will strengthen the reliability without any modification on BGP. This research will particularly focus on providing a redistribution approach which will reduce the overall converge time of the Border Gateway Protocol.**

***Keywords*— Aspect oriented programming, Unified modeling language, Sequence diagram, Agro UML, Aspect j, Activity diagram.**

I. INTRODUCTION

Due to huge usage of internet and growing business, bandwidth required prove to be difficult resource to fulfill with normal structure of networks. Moreover to provide a good level of quality service is also a big concern. One big solution comes in form of inter domain device management in which we can use various types of networks and structures according to requirements. Technology like multi-homing is becoming essential for large and small enterprise to fulfill the requirements of clients and daily routines usage of technology. In order to enhance the reliability of the Internet, more and more ASes use multi-homing technology to provide redundant connection. When one of the connections fails or is in maintenance, the AS can still connect to the Internet via other connections. Multi-homing configuration can be achieved through multiple connections to different upstream providers or the same ISP. Multi-homing to a single provider is referred to as multi-ataching. In simple words, the idea of using multiple access links (so called multi-homing) is commonly used to improve the aggregate bandwidth and the overall service availability, which has been employed by large enterprises and data centers as a mechanism to extract good performance and enhance the network reliability from their service providers for a while. Below is the example of multi-homing support [6].

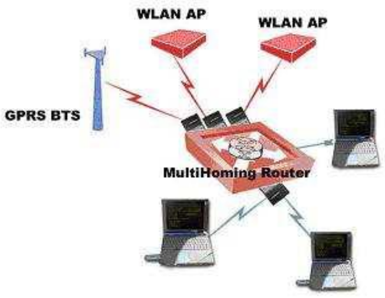

Fig. 1 Structure of Aspect Oriented programming

Now when we are seeking different supports for different networks and to fulfill both reliability and quality of service then we needs these types of networks but as network grows we need different protocols which can fine tune and maintain the integrity, reliability and quality of the growing network. Border Gateway protocol is one of the only protocols that can do so.

II. BORDER GATEWAY PROTOCOL

Border Gateway Protocol is the widely used exterior gateway protocol which is used to connect different autonomous system. Further in this paper we will discuss the various parameters of Border gateway protocol.

A. Route Redistribution

It is preferable to employ a single routing protocol in an internetwork environment, for simplicity and ease of management. Unfortunately, this is not always possible, making multi-protocol environments common.

Route Redistribution allows routes from one routing protocol to be advertised into another routing protocol. The routing protocol receiving these redistributed routes usually marks the routes as external. External routes are usually less preferred than locally-originated routes.

At least one redistribution point needs to exist between the two routing domains. This device will actually run both routing protocols. Thus, to perform redistribution in the following example, Router B would require at least one interface in both the EIGRP and the OSPF routing domains:

It is possible to redistribute from one routing protocol to the same routing protocol, such as between two separate OSPF domains (distinguished by unique process ID's). Static routes and connected interfaces can be redistributed into a routing protocol as well.

Routes will only be redistributed if they exist in the routing table. Routes that are simply in a topology database (for example, an EIGRP Feasible Successor), will never be redistributed.

Routing metrics are a key consideration when performing route redistribution. With the exception of IGRP and EIGRP, each routing protocol utilizes a unique (and thus incompatible) metric. Routes redistributed from the injecting protocol must be manually (or globally) stamped with a metric that is understood by the receiving protocol.

B. AS Level Internet

Internet is divided into a large number of distinct regions of administrative control, commonly called Autonomous Systems (AS). An AS, also known as routing domain, typically consists of a network service provider or a large organizational unit, such as a college campus or a corporate network. An AS is collection of networks under a single technical administration that means that sharing the same routing protocol and routing policy. Autonomous System are identified by AS numbers. AS numbers are 16 bit, unsigned integer ranging from 1 to 65535. A range of private AS numbers (64512-65535) has been reserved for customers that needed an AS number to run BGP in their private network.

In turn, each AS interconnects a number of sub-networks, such as remote corporate ones or customer networks. An AS has a single set and clearly defined routing policies and connects to one or more remote ASes at neutral private or public exchange points.

The routers in Internet are responsible for receiving and forwarding packets through this interconnected maze of sub-networks and ASes. Each router makes routing decisions based on its knowledge of the topology, the conditions on the network, and complex routing policies specified by network administrators within their domain. In order to make such dynamic decisions, routers exchange path and topology information using special purpose routing protocols.

C. Intra-domain Routing Protocols

An intra-domain (or interior) routing protocol, is used to pass information between routers within an AS.

Internally within an AS, service provider and customer network, universities and corporations usually use an Interior Gateway Protocol (IGP) such as Routing Information Protocol (RIP), Enhanced Interior Gateway Protocol (EIGRP) or Open Shortest Path First for exchange the routing information within their network. Usually interior protocols build their own reliability on top of a datagram service.

D. Inter-Domain Routing Protocol

An intra-domain (or interior) routing protocol, is used to pass information between routers Within an AS. Any communication between the Interior Gateway Protocols and the Internet or between service providers will be accomplished through BGP.

Border Gateway Protocol (BGP) is an inter-autonomous system (AS) routing protocol used to exchange the routing information between the Internet and Internet service providers. BGP is very robust and scalable routing protocol.

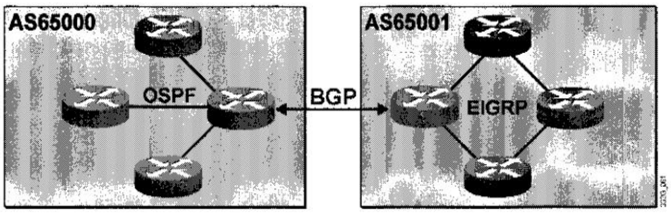

Fig. 2 Example of Inter-domain Routing

Our focus is towards exterior routing protocols, more specifically Border Gateway Protocol (BGP) which is the most common, rather de facto inter-domain (exterior) routing protocol used by ASes in Internet. BGP uses TCP as its underlying transport layer protocol to exchange routing information about how to reach the destination prefixes. Routers exchange information of a route when there is a change in old information, such as an old route disappearing or a new route becoming available. The BGP update message includes list of ASes with reachability information, along with other attributes such as next-hop IP address. This enables BGP to hide the topological details and routing inside each network domain. The routers that communicate each other using BGP protocol across a network domain are called BGP speakers. Routing information is propagated according to complex policies configured in BGP speakers by administrator.

BGP speakers within a domain synchronize using intra-domain routing protocols. Synchronization means routers exchange reachability information in such a way that all speakers have consistent information. Consequently, the BGP information collected from any border router should reflect the routing behavior of the AS depending upon local router policies, and local hardware or software failures.

E. BGP as a Routing Protocol

As stated earlier, BGP is an exterior routing protocol. The position of BGP amongst the other routing protocols can be understood by considering Figure 2.1. The AS65101, AS65202, AS65404, AS65303 represent independent ASes having routers R1, R2 and R3, R4 and R6, R7 and R9 respectively as BGP routers, having inter-connectivity as shown in Figure 2 As we can see that a single AS has more than one BGP speaking routers, but typically they reflect identical behavior based on how they are configured by administration.

The routers belonging to same AS interact with each other using interior routing protocols. Since they belong to same administration domain, they help the AS to maintain a stable behavior for the rest of Internet. This allows us to abstract the whole AS by a single node, based on consistent similar routing role of different routers within an AS.

After a policy change or a network failure affects the availability of a path to a set of destinations, the routers topologically closest to the failure will detect the fault, withdraw the route and make a new local decision on the preferred alternative route, if any, to the set of destinations. For instance in Figure 1, in case of link failure between R1 and R2, R2 will withdraw the route information in which the path includes R1. These routers thus propagate the new topological information to each router within the AS. The network's border routers will in turn propagate the updated information to each external peer router, pending local policy decisions. Routing policies on an AS's border routers may result in different update information being transmitted to each external peer.

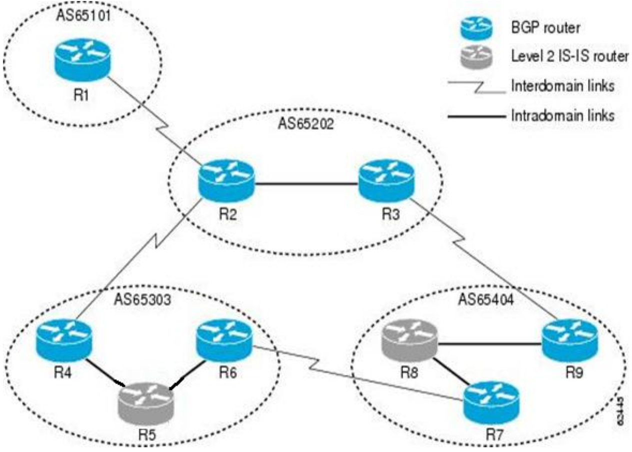

Fig. 3 BGP protocol illustration

III. Proposed Work

A. Problem Definition

Due to huge transmission of data through different channels and different technical devices, reliability became an important part of routing. Inter-domain routing is the complex part when it comes to quality assurance in routing process. Different autonomous systems need to use Border gateway protocol for best inter-domain routing. Different Autonomous systems fail to take advantage of the redundant connections and usually face the disconnectivity and fading issues. Huge bandwidth and better management are the requirement for solving this sort of issues. Many techniques have been proposed for solving these issues but due to growing needs, better inter-domain routing solutions are required for providing fault tolerance and quality assurance.

B. Objectives

To analyze and developing a better routing strategy for resilient inter-domain routing with Border Gateway Protocol.

C. Experimentation

Our focus will be on developing a better solution to this problem as to solve inter-domain routing issues in OPNET simulator. We will do our implementation in Five Phases

1st Phase: This phase will contain the study of already existing techniques.

2nd Phase: In this phase, we will simulate the internal behavior protocols like RIP, EIGRP and OSPF for checking the basic area redistribution process with parameters like Length of route, Maximum possible cost, Maximum route time, Route Time, Load per link, Number of hops, average load and variation in load.

3rd Phase: In this phase, we will implement the dynamic routing filtering, redistribution routing techniques and dynamic routing techniques in Border Gateway protocol for different autonomous systems. This work will be fitted with different scenarios of the BGP simulation with route updates, traffic behavior, updates behavior and behavior under attacks. Comparison will be there to reflect the changes under different conditions

4th Phase: We will implement our proposed strategy dynamically and also compare it with already existing techniques

5th Phase: We will finally propose the solution for congestion control, route failure and cost cutting under Border Gateway protocol by implementing the redistribution approach.

Our focus will be on developing a better solution to this problem as to solve inter-domain routing issues. In this problem we will study works and techniques have been focused on the reliability of inter domain routing. However, those approaches based on the factor of huge bandwidth and resources. In case of delay caused by any factor (DOS attack, Routing Flood attacks etc) in BGP redistributed networks will act as huge bottle neck. In our work we will find the behavior of routing under delay and will propose solutions to normal flow of routing in Redistributed BGP routing. This research will carry out the idea of modifying the updates for BGP routing, refining of routing process based on filtering of routes, Decreasing of failures by checking the regular status of the routes on device itself. This research will significant minimize packet loss during an inter-domain link failure, and also preserve BGP instability.

Our experimentation contains the Border Gateway protocol Scenario configuration with different Autonomous systems. Figure 4 shows the basic layout of network.

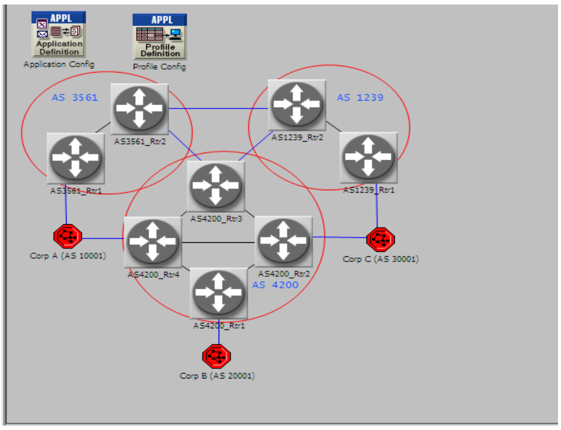

Fig. 4 BGP configuration in Opnet

Below Figure 5 Suggests the number of hops through which data travelled during BGP routing process.

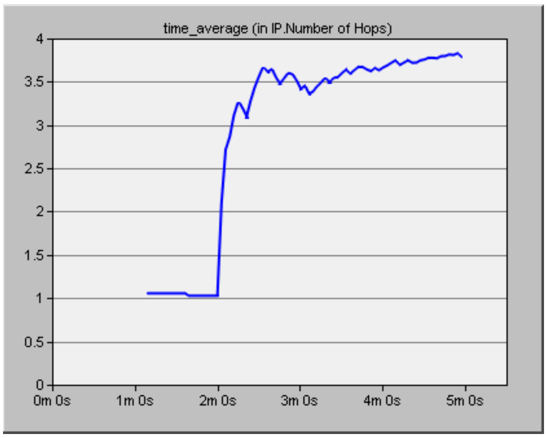

Fig. 5 BGP with IP number of Hops

Below Figure 6 shows the convergence of Border Gateway protocol with sending and receiving of data from one AS to another.

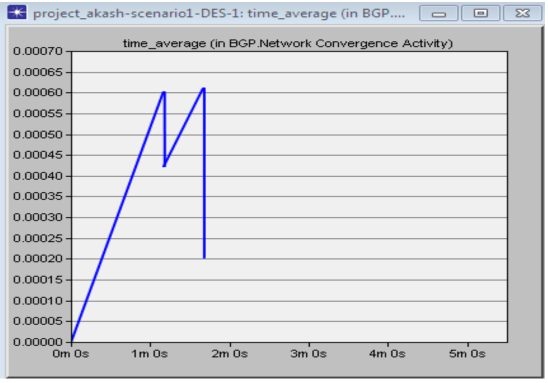

Fig. 6 BGP convergence with time

IV. Conclusions

Our experimentation is in process for finding the better routing process and quality in BGP process. We haver done some initial experimentation on BGP updates and configurations and we are working on the further experimentation in BGP roiuting.

.

References

[1] [1] Zhan-Zhen Wei, Feng Wang," Achieving Resilient Routing through Redistributing Routing Protocols", Communications (ICC), IEEE International Conference, pp 1-5, 2011.

[2] Kevin Butler, Patrick McDaniel," A Survey of BGP Security Issues and Solutions", Proceedings of the IEEE, Volume- 98, No- 1, January 2010.

[3] R. Perlman, Interconnections," Bridges, Routers, Switches, and Internetworking Protocols", 2nd ed. Reading, MA: Addison Wesley, 1999.

[4] C. Ellison and B. Schneier," BTen risks of PKI: What you're not being told about public key infrastructure", Comput. Security J., vol. 16, no. 1, 2000.

[5] M. Lepinski and S. Kent," An Infrastructure to Support Secure Internet Routing", Internet Draft draft-ietf-sidr-arch-08.txt, Jul. 2009.

[6] Thomas C. Bressoud, Rajeev Rastogi," Optimal Configuration for BGP Route Selection", INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies, vol. 2, pp 916- 926, 2003.

[7] Bin Wang," The Research of BGP Convergence Time", Information Technology and Artificial Intelligence Conference (ITAIC), 6th IEEE Joint International Conference, vol- 2, pp 354-357, 2011.

[8] Jong Han Park, Ricardo Oliveira, Shane Amante," BGP Route Reflection Revisited" , IEEE Communications Magazine, Vol- 50, Issue- 7, pp 70-75, July 2012.

[9] Xiaozhe Zhang, Xicheng Lu, Jinshu Su, Baosheng Wang," SDBGP: A Scalable Distributed BGP Routing Protocol Implementation", High Performance Switching and Routing (HPSR), IEEE 12th International Conference, pp 191-196, 2011.

[10] Jaeyoung Choi, Jong Han Park, Pei-chun Cheng, Dorian Kim," Understanding BGP Next-hop Diversity", Computer Communications Workshops (INFOCOM WKSHPS), IEEE Conference, vol- 1, pp 846-851, 2011.