A Comparative Study of IGP and EGP Routing Protocols, Performance Evaluation along Load Balancing and Redundancy across Different AS

Amrah Baba Ali, Mujahid Tabassum, *Member, IAENG,* Kuruvilla Mathew, *Member, IAENG*

***Abstract*—Routing is a vital part of a communication network that enables data transmission over a local and wide area networks. Each routing protocol has different features, performance, architecture, and algorithms to achieve the data communication and reliability. The data is moved around different network topologies and handled by different protocols within and outside different Autonomous Systems (AS). A reliable, secure and scalable communication platform relies on a correct combination of protocols. In this paper, we have performed a comparative analysis of Interior Gateway Routing Protocols (IGRP) and an Exterior Gateway Routing Protocol (EGP) performance evaluation. This is to find out the best protocol combination for any complex scenario to achieve fast and reliable communication. Hot Standby Routing Protocol (HSRP) and Gateway Load Balancing Protocol (GLBP) are also simulated to analyse the load balancing and redundancy parameter for Border Gateway Protocol (BGP).**

***Index Terms* — BGP, IGRP, EGP, HSRP, GLBP, GNS3, WireShark and Routing Protocols.**

I. INTRODUCTION

IN today's era, communication technologies growing rapidly to accommodate the increasing demand of high speed applications and networks. Therefore, technological inventors are expected to design and develop efficient solutions and applications to support the end user high speed network requirements. The Network is a combination of multiple connected hosts over cables or via wireless media to exchange information or data. The Open Systems Interconnection (OSI) reference model was created, to determine the compatibility of various connected devices for communication [1]. The routing protocols are implemented in the Network layer of the model, providing the set of rules for devices to route data packets towards the destination. Two kinds of routing protocols are used for internal and external network communication, namely, Interior Gateway Protocols (IGP) and Exterior Gateway Protocols (EGP). IGPs are used for routing within an AS and EGPs are used for routing between different AS.

Among the IGPs, Open Shortest Path First (OSPF) and Enhanced Interior Gateway Routing Protocol (EIGRP) are considered prominent protocols for real-time applications within a single AS. Intermediate System to Intermediate System (IS-IS) is mostly used in large scalable networks, and, therefore, is more popular in use within Internet Service Provider's (ISP) networks. Border Gateway Protocol (BGP) is the Exterior Gateway Routing Protocol, which allows different Autonomous Systems (AS) to intercommunicate. An Autonomous System is a group of networks under the same administrative control.

Since each protocol has a unique set of features, it's very important to choose an ideal combination of protocols for a reliable, fast and secure network communication. The right choice in the selection of routing protocols depends on the network parameters and requirements. Related works [2] has shown EIGRP to be a better choice when dealing with real time applications within the network like instant-messaging and video-conferencing; whereas OSPF and IS-IS are better suited for scalable and service provider networks. In the following [3] paper combination of multiple protocols was suggested to achieve a fast, convergence and secure communication platform. EGP was used to interconnect different autonomous systems in treelike topologies [4]. Later on, Border Gateway Protocol (BGP) was introduced as a successor to EGP, which allows fully decentralized management of the network. Unlike the IGPs, BGP is a path vector protocol; it selects the best path through the Internet by choosing the route that has to traverse the fewest number of AS.

In this research paper, we have used three scenarios running on the different combination of multiple routing protocols. The simulation is implemented on the "GNS3" network simulation software and Wireshark is used to observe the data transmission traffic and capture the packets. The results provide a guideline for the selection of the best combination of protocols for any given scenario under specific parameters. Hot Standby Routing Protocol (HSRP) and Gateway Load Balancing Protocol (GLBP) are also simulated to analyse the load balancing and redundancy for Border Gateway Protocol (BGP).

II. RELATED WORKS

Over the past two decades, a lot of research has been published on the comparative performances of IGPs. BGP is advisable when multi-homing to multiple ISP's or when

Manuscript received Jan 06, 2016; revised Jan 19, 2016. This paper was supported in part by the Swinburne University of Technology, Sarawak Campus.

B. A. Ali is with the Swinburne University of Technology, Sarawak Campus, Jalan Simpang Tiga, 93350, Kuching, Malaysia (e-mail: 4230078@students.swinburne.edu.my).

M. Tabassum is with the Swinburne University of Technology, Sarawak Campus, Jalan Simpang Tiga, 93350, Kuching, Malaysia (phone: +60 82 260902, e-mail: mtabassum@swinburne.edu.my).

K. Mathew is with the Swinburne University of Technology, Sarawak Campus, Jalan Simpang Tiga, 93350, Kuching, Malaysia (e-mail: kuruvilla.mathew.k@ieee.org).

trying to communicate with an alternate AS [5]. [6] Concluded that OSPF has the best detection mechanism but is practically more suitable for limited networks because of the higher possibility for packets to drop from different areas while EIGRP is better suited for scalable networks. [3] Suggests that EIGRP is more suitable for topologies with few routers while IS-IS is ideal for complex topologies because of its higher scalability feature. [7] Studied their implementation with varying sizes of topologies and suggested that EIGRP is better suited for networks with the critical delivery that cannot tolerate errors while OSPF is more suitable for networks with bandwidth constraints. [8] Suggested that implementation of multiple IGPS within a single topology, so as to be able to use the best of all the protocols for higher throughput and lower bandwidth utilization, would be a more effective approach to gain higher throughput while minimizing bandwidth utilization.

Another project [9] discussed the possibility of persistent route oscillations in BGP for varying complexities of topologies. Their research showed that the cause of this oscillation was not necessarily confined to the policy configuration of one AS alone, but more likely occurs due to the policies of several different AS. They also highlighted that these anomalies can actually occur even without misconfigurations, which makes them difficult to detect and correct. [10] Studied forwarding loops caused by BGP misconfigurations. His work agreed with the findings of [9] that forwarding loops in iBGP networks are inherently difficult to detect. He proposed a polynomial-time algorithm for clustering AS's and showed that the AS are configured using his method results in a forwarding-loop free network. [11] Presented a study of Internet economics and how it can naturally guarantee route stability. [12] Proved that the routing system will converge to a stable path when service providers can set rankings and filters autonomously.

In the current paper, we have simulated multiple protocols within single topology and used parameters suggested in the [8].

A. Routing Protocols Overview

The Interior Gateway Routing Protocols have two broad classifications, Distance-Vector and Link State. The Distance-Vector Protocols use the Bellman-Ford algorithm, which calculates the shortest path from a single node by considering the negative edge weights. Data is forwarded using the best paths selected from the routing tables. They are further classified into RIP (version 1 - version 2) and EIGRP. Link-State Routing Protocols calculates the best path from source to destination using the Dijkstra algorithm, then present this information to all neighbouring routers. They are further classified into OSPF and IS-IS [1]. They also have the added advantage of being able to segment a network into multiple administrative clusters, known as areas. BGP is the Exterior Gateway Protocol, and unlike the others; is a path-vector protocol.

1) Routing Information Protocol (RIP) (version 1-2)

RIP is among the earliest introduced routing protocols. V1 works by sending out a copy of its routing table to neighbours every 30 seconds and triggered updates whenever the metric of a route change. V2 was introduced as an upgrade to V1, with classless and VLSM support.

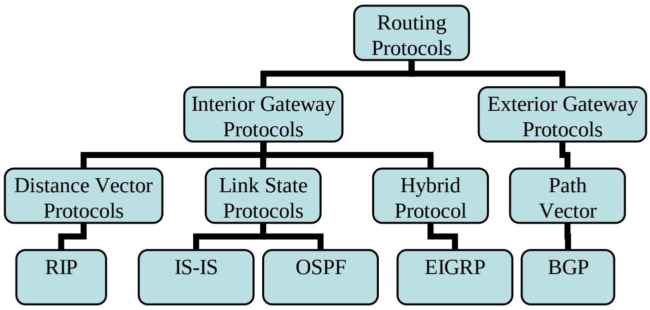

Fig. 1. Classification of the Protocols

2) Enhanced Interior Gateway Routing Protocol (EIGRP)

EIGRP is a hybrid of the Link-State and the Distance-Vector routing protocol. EIGRP uses Diffusion Update Algorithm (DUAL) for routing optimization and fast convergence. It was introduced as an upgrade to IGRP. EIGRP only sends out updates only when changes occur, reducing the traffic between routers. Its hop count is also larger, at 224, making it compatible with larger networks [1].

3) Open Shortest Path First (OSPF)

OSPF was introduced as an improvement to RIP, with faster convergence and more configurable parameters. It sends out hello packets, link state requests, updates and database descriptions, and applies the Dijkstra's algorithm to determine the shortest path to the destination. Updates are limited to when there is a change, though the Link State Advertisement (LSA) table is refreshed every 30 minutes. OSPF implements hierarchical routing, by bounding different networks into several areas. OSPF does not scale well as more routers are added because more memory will be used and routing loops can occur [13].

4) Intermediate System to Intermediate System (IS-IS)

IS-IS is mostly used by ISPs because it's a great protocol for large internetworks due to its simplicity, stability, and better support for MPLS. This protocol is similar to OSPF, for it also uses areas to break down the routing domain into smaller. It also establishes adjacencies using the Hello protocol and exchanges link state information using LSPs [7 - 1]. Within an AS, IS-IS routing only takes place at level 1 and level 2.

Level 1 – occurs within the IS-IS area. All devices in this level have a single area address, where routing is done using a locally significant address portion, choosing the lowest-cost path.

Level 2 – learns the location of Level 1 routing areas and builds an inter-area routing tables. All ISs on this level use the destination area address to route traffic using the lowest-cost path.

5) Border Gateway Protocol (BGP)

BGP is a path vector protocol, built to work between multiple AS. It maintains path information that gets updated dynamically with incremental updates, unlike the IGPs which periodically flood the whole network with the known topology information. BGP maintains a separate routing table based on the shortest AS path and other attributes, as opposed to IGP metrics like distance, or cost [14]. BGP uses

ISBN: 978-988-14047-6-3
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

multiple neighbours, known as peers. These are further classified into - iBGP peers, which route within the same AS, and eBGP peers, which route between separate AS. In iBGP, there is no restriction that states that neighbours have to be directly connected. However, an iBGP peer will not advertise the prefix learned from one to another iBGP peer to avoid routing loops within the same AS.

TABLE 1
SUMMARISED COMPARISON OF THE ROUTING PROTOCOLS

	RIPv2	EIGRP	OSPF	IS-IS	BGP
Int/Ex	Int	Int	Int	Int	Ex
Type	DV	Hyb	LinkS	LinkS	PV
Def Metric	Hop C	BW/ Delay	Cost	Cost	Mul attri
Adm D	120	90 int 170 ext	110	115	200 intn 20 ext
Hop CL	15	224 (100 def)	None	None	EBGP: 1 IBGP: None
Conv	Slow	Very fast	Fast	Fast	Averag e
Upd	Full T	O Chg	O Chg	O Chg	O Chg

B. *Problems of BGP and their solutions*

Transient failures in backbone networks can cause a catastrophic loss to millions of internet end users. Research to analyse and combat the growth dynamics mostly show that during the BGP convergence, triggered by a withdrawal or link failure, BGP faces temporary dis-connectivity, even in the event the policy compliant path from the source to the destination still exists [15]. To combat this, HSRP and GLBP were introduced as gateway failovers.

1) *Problems of BGP and their solutions*

HSRP is a Cisco proprietary protocol used to establish a fault-tolerant default gateway. The protocol provides a gateway failover for the network connected to the router. This protocol can be used for redundancy and load-sharing.

2) *Gateway Load-Balancing Protocol (GLBP)*

GLBP allows load-balancing of traffic from a network segment without the different host IP configurations required to achieve the same results with HSRP. Load balancing does not actually depend on the traffic load incoming and outgoing but is based on the number of hosts connecting to the gateway router.

III. Experiment Setup

In this research, we have created three network models to test the suggestion by [8], and analysed the load balancing and redundancy performance of BGP. The simulated scenarios were designed to be as realistic as possible. All the models were designed to connect with a single internet service provider (ISP), implemented in the form of a router. The hosts were used to test connectivity from end to end, and how long it takes to recalculate the routes in case of link failure. The scenarios were later modified and then interconnected to create 3 different ASs for monitoring BGP operations. For a more realistic evaluation of multi-homing and load-balancing, traffic generation was also introduced. The simulation was done on the simulation software "GNS3", with packet capture and network analyser tool "Wireshark".

A. *Scenario 1(RIP v2 and EIGRP)*

The first scenario (Fig. 2) was created to accommodate a simple topology, with 4 routers - 1 simulated an ISP and 3 switches connected to 3 routers and a host from each network connected to each router to test the connectivity and monitor traffic from each end of the topology.

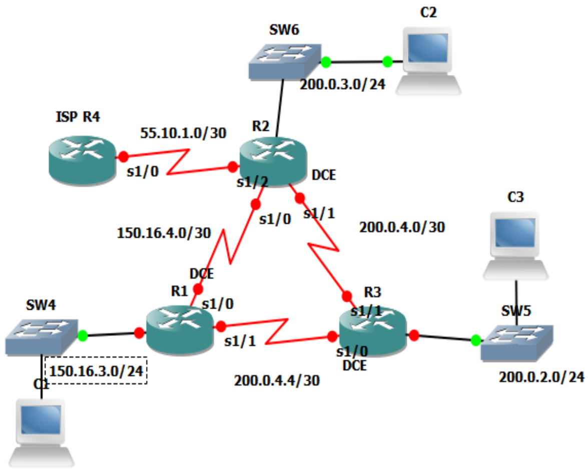

Fig. 2. Scenario 1

B. *Scenario 2(EIGRP and OSPF)*

The second scenario (Fig. 3) is similar to the first. 2 more routers are introduced in another cluster, each connected to the same ISP. The first cluster serves as a backbone area for OSPF, which is implemented independently and evaluated, with EIGRP configured on the other cluster. The ISP is connected via the default route to both clusters.

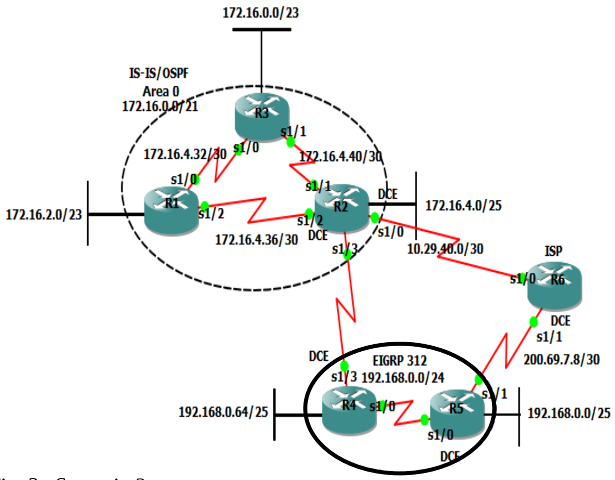

Fig. 3. Scenario 2

C. *Scenario 3(OSPF and ISIS)*

The third scenario (Fig. 4) is more complex as compared to earlier scenarios, with 8 routers including one service provider. The connection is in the form of a tree-topology, where 1 router is connected to the ISP, and the other two routers have separate branches that will ultimately serve as the stub areas. Only two protocols are implemented in this scenario, IS-IS and OSPF, because these two are more similar than the other routing protocols, and are tailor-made to communicate within and between large regions with segmented areas.

ISBN: 978-988-14047-6-3
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

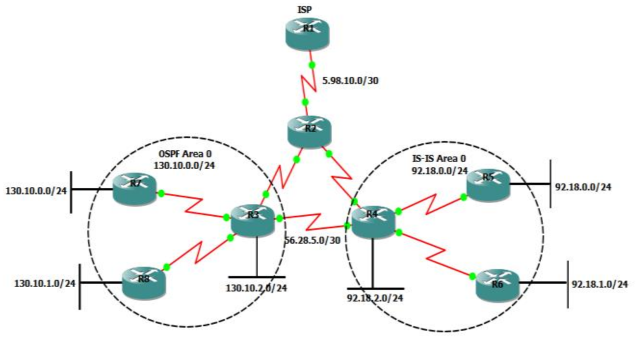

Fig. 4. Scenario 3

D. *Scenario 4 (BGP)*

There was one major variation done to each scenario before interconnecting them (Fig. 5). Since each scenario is connected to another with two different links, there is no direct need of a service provider link. To evaluate the better option, HSRP and GLBP were implemented at different times, before generating traffic using “Chargen”, a feature built-in to TCP. It is disabled by default for security purposes, as it can be used to launch DoS attacks by spoofing an IP address [13]. The server sends a continuous stream of TCP packets once the connection is made, up to 5mb of data per minute, which is just enough to evaluate the effectiveness of redundancy and load-balancing protocols. The amount of generated traffic is not much in these cases, because only the workstation is connected, resulting in about 500kb of data, depending on how long the session runs.

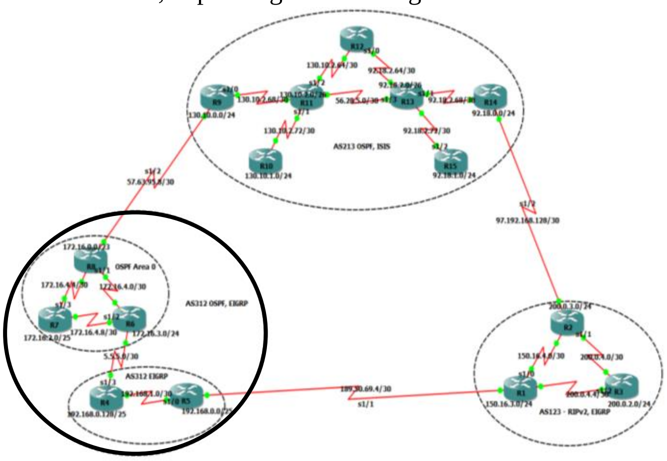

Fig. 5. Connected Scenarios for BGP

IV. Results And Discussions

A. *Scenario 1- RIP vs EIGRP*

The scenario was first run on RIPv2, then EIGRP. The timestamps of each frame and the total number of frames were recorded. After the analysis, the serial links between R4 and R5, R5 and R6 were configured with RIPv2 and EIGRP respectively. The link between R1 and R2 was removed to check the effectiveness of the redundant link between R4 and R6. To allow the protocols to communicate with each other, the redistribution command was used. Each simulation was recorded for a period of 300 seconds. For further testing, after the result analysis, multiple hosts were added to each connected network to study the convergence time under a higher traffic load.

TABLE 2
SUMMARY OF SCENARIO 1 RESULTS

RIP	
Total No of frames	92
Total captured bytes	(156+116)*11 = 2992
EIGRP	
Total No of frames	218
Total captured bytes	(109*64) = 6976 bytes where 109 = number of EIGRP frames
After Redistribution	
Total No of frames	1110
Total captured bytes	(44+56)*100 = 10000 bytes where 100 = number of frames captured after convergence

Table 2 and Fig. 6 show the results of the first scenario. We see a better communication grid when RIP and EIGRP work together after redistribution of both than when only one protocol is running on all the routers. This may be due to the hybrid feature in EIGRP working with the routing-by-rumor feature of RIP. RIP is observed to have much lower traffic as compared to EIGRP even after multiple hosts were added.

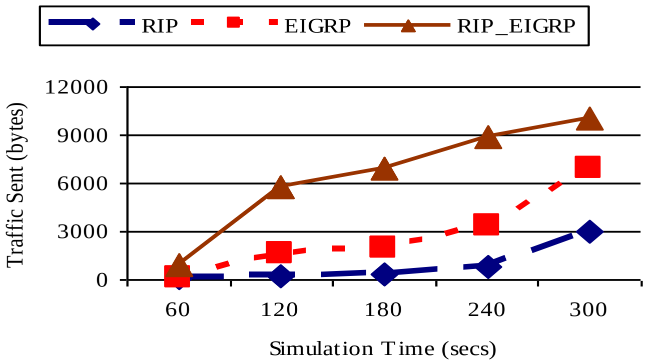

Fig. 6. Summary of Scenario 1 results

B. *Scenario 2 – EIGRP vs OSPF*

This scenario used a different approach because of the segmentation into separate areas and the protocols running simultaneously. Both areas connect to the same ISP and are also set to redistribute and intercommunicate. Results of connectivity within both areas were separately monitored before the intercommunication link was configured.

TABLE 3
SUMMARY OF SCENARIO 2 RESULTS

EIGRP	
Total No of frames	216
Total captured bytes	216*64 = 13824
Total observation time	315S
OSPF	
Total No of frames	142
Total captured bytes	84*142 = 11928
Total observation time	320s
After Redistribution	
Total No of frames	225
Total captured bytes	148*64 = 9472
Total observation time	320s

Table 3 and Fig. 7 shows that even when multiple hosts are added to the topology to advocate heavy traffic, the sizes of the frames remain relatively the same, and the simulation and observation time also remain similar.

ISBN: 978-988-14047-6-3
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

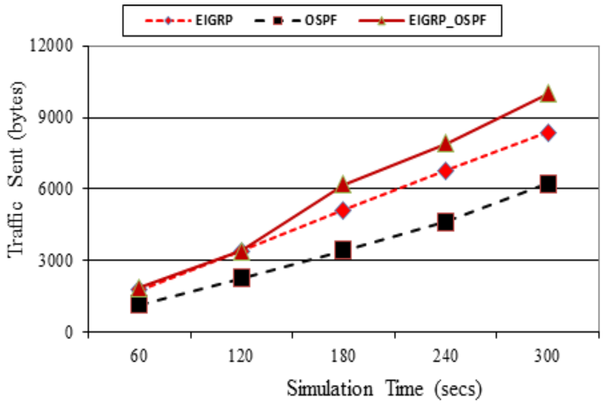

Fig. 7. Scenario 2 results

C. Scenario 3 – OSPF vs ISIS

In this scenario, we had adopted the same approach as scenario 2, because the branches are specifically assigned to a particular protocol. Each area was configured and monitored separately before the intercommunication grid was configured and monitored. On successful connectivity, traffic generated by both protocols on each router was recorded.

TABLE 4
SUMMARY OF SCENARIO 3 RESULTS

OSPF	
Total No of frames	142
Total captured bytes	72*84 = 6048
Total observation time	317s
IS – IS	
Total No of frames	75
Total captured bytes	75*74 = 5550
Total observation time	318s
After Redistribution	
Total No of frames	74
Total captured bytes	74*85 = 6290
Total observation time	318s

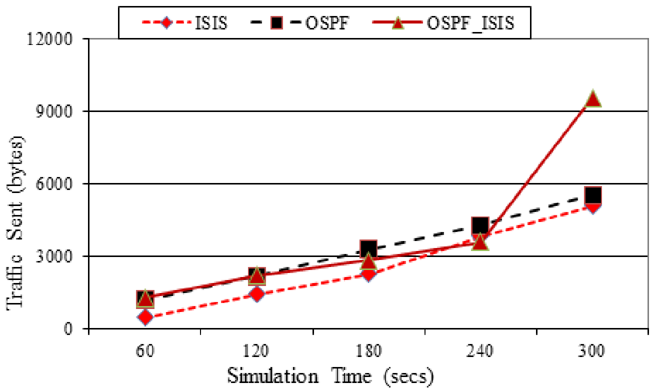

Fig. 8. Scenario 3 results

Table 4 and Fig. 8 show scenario 3 results. We can observe that OSPF communicates better, which was unexpected, as ISIS is theoretically and practically known to be a fast convergence protocol. The result also shows, in a case when both protocols were running together, after convergence the communication become better which is because of exchanging their routing table information. The decline and exponential increase in the performance of the intercommunicating protocols could be an attribute to the recalculation of routes because of the increased number of LSP's with the new information coming from the routing tables of both protocols.

D. Scenario 4 – HSRP and GLBP Evaluation

HSRP was configured on an alternate topology with the same parameters to analyse the comparative studies. GLBP was configured as the final step of the simulation, to distribute the traffic loads accordingly while giving priority to the most complex scenarios with a higher number of hosts. We produced as much traffic as possible and all links were individually monitored for 10 minutes. We can observe from table 5 that the complexity of the AS links did not matter because the generated traffic remained approximately the same. These routing protocols do not offer load balancing. Therefore, protocols like HSRP and GLBP is needed for redundancy and load balancing.

TABLE 5
ANALYSIS OF HSRP (LINK VS TRAFFIC GENERATED)

R1 to R5 (AS 123 to AS 312)
7098 frames (total) Bgp 30 frames, size 63 bytes TCP window updates, 69 frames, size 44 bytes TCP chargen, 6999 frames, size 118 bytes Total = (30*63)+(69*44)+(6999*118)=0.833mb
R8 to R9 (AS 312 to AS 213)
7101 frames (total) Bgp 37 frames, size 63 bytes TCP window updates, 70 frames, size 44 bytes TCP chargen, 6994 frames, size 118 bytes Total = (37*63)+(70*44)+(6994*118)=0.830mb
R14 to R2 (AS 213 to AS 123)
7099 frames (total) Bgp 29 frames, size 63 bytes TCP window updates, 71 frames, size 44 bytes TCP chargen, 6999 frames, size 118 bytes Total = (29*63)+(71*44)+(6999*118)=0.8308mb

TABLE 6
ANALYSIS OF GLBP (LINK VS TRAFFIC GENERATED)

R1 to R5 (AS 123 to AS 312)
11089 frames (total) Bgp 32 frames, size 63 bytes TCP window updates, 81 frames, size 44 bytes TCP chargen, 10976 frames, size 118 bytes Total = (32*63)+(81*44)+(10976*118)=1.300mb
R8 to R9 (AS 312 to AS 213)
12671 frames (total) Bgp 67 frames, size 63 bytes TCP window updates, 193 frames, size 44 bytes TCP chargen, 10952 frames, size 118 bytes Total = (67*63)+(193*44)+(12411*118)=1.4772mb
R14 to R2 (AS 213 to AS 123)
10010 frames (total) Bgp 27 frames, size 63 bytes TCP window updates, 51 frames, size 44 bytes TCP chargen, 10932 frames, size 118 bytes Total = (27*63)+(51*44)+(9932*118)=1.176mb

We can conclude from the table 5 that HSRP does not offer load balance service, because even with increasing and decreasing levels of complexity of the links, the generated traffic remained the same. By observing the result of table 6, we can conclude that after configuring the GLBP the specific link was able to handle the generated traffic. In a complex AS, more traffic will be generated to accommodate its complexity. Unlike HSRP, GLBP is seen to redirect traffic accordingly to cater to the dynamic complexity of the link to the AS.

Testing the redundancy effectiveness of both protocols produced expected results. Since iBGP has fully meshed, causing a link failure on one end triggered a BGP update to the iBGP peer to inform it that the first router was down, leaving connectivity seamless.

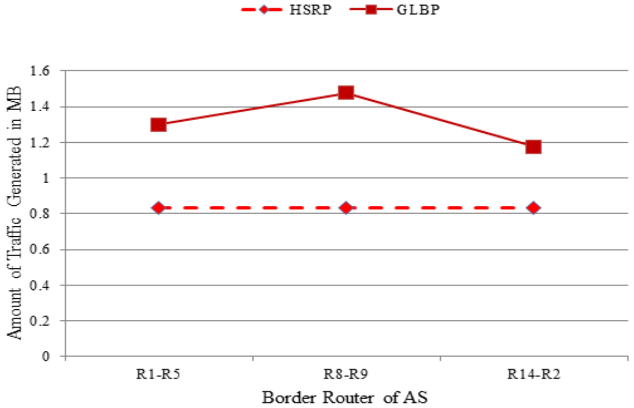

Fig. 9. Summarized results of HSRP and GLBP for BGP

This was expected because both HSRP and GLBP are redundancy protocols. However, the traffic generation and balancing experiments produced different results. We can observe in Fig. 8, that HSRP does nothing to the incoming or outgoing traffic load of an AS. Only when a link failure occurred, HSRP diverted the traffic through another route to provide seamless connectivity. GLBP also performs the same functionality as HSRP, and more, by providing an appropriate gateway which load balances traffic to accommodate the bandwidth variations of the different ASs. This demonstrates that GLBP is more effective over HSRP for any complex scenario.

V. Conclusion

Based on the simulation results and recorded values, it can be concluded that EIGRP and OSPF are the best combination of protocols for a given network with about 1000 hosts. However, a combinations EIGRP and RIPv2 would be better suited for a smaller network because of the absence of segmented areas. IS-IS has been known as the best protocol for ISP's and really large enterprises because of its scalability, fast convergence and added the advantage of not needing IP connectivity to be able to communicate with neighbours. The results also show that it communicates well with OSPF, due to their similarities. Therefore, the combination of the two protocols would be better than configuring only 1 of them for any given scenario with complex parameters.

As a key component in enabling Internet routing worldwide, the BGP routing table is an important aspect that needs to be very carefully monitored. Although GLBP is not actually a new protocol, it is not very popular because of its operational cost and traffic allocations. Although HSRP has been the most popular choice because of its ease of use, it does not efficiently utilise all available links. As a result, more resources are wasted. GLBP provides a solution to this wastage of resources by utilising all available links, which ideally eliminates the need for HSRP. This means, a single load balancing router can handle and utilise multiple virtual redundant links, thereby saving resources and reducing the addition of new links to the Internet routing tables.

Future extension of this work can include a simulation of the network with the number of devices and a much larger traffic volume. A comparison of the simulation with an actual test implementation of the same is also in the plan.

Acknowledgment

We would like to thank Mr. Jefferey Sim from Swinburne Sarawak ITS department for his valuable technical input to this project.

References

[1] Leahy, Eric (2011). "EIGRP - Packets & Neighborships" Retrieved 18-11-2013, from http://ericleahy.com/index.php/eigrp-packets-neighborships/
[2] McGrath, D., et al. (n.d.). Netsim: A distributed Network Simulation to Support Cyber Exercises, Institute for Security Technology Studies, Dartmouth College.
[3] Waqas, A. (2009). An Empirical Study to Observe Route Recoverability Performance of Routing Protocols in Real-Time Communication
[4] Stretch, Jeremy (n.d.) "BGP" Retrieved 13-05-2014, from https://www.dnlab.se/pdf/BGP.pdf
[5] Kurose, J. F. and K. W. Ross (2010). Computer Networking: A Top-Down Approach. Boston, Pearson Education Inc.
[6] Mirzahossein, K., et al. (2013). "Analysis of RIP, OSPF, and EIGRP Routing Protocols using OPNET." Simon Fraser University, School of Engineering Science.
[7] Sendra, S., et al. (2010). "Study and Performance of Interior Gateway IP Routing Protocols." Network Protocols and Algorithms 2(4).
[8] S., Farhangi, et al. (2012). "Performance Comparison of Mixed Protocols Based on EIGRP, IS-IS and OSPF for Real-time Applications." Middle Eastern Journal of Scientific Research 12(11).
[9] K. Varadhan, R. Govindan, D. Estrin, Persistent Route Oscillations in Inter-Domain Routing, Computer Networks, 1999.
[10] H. Gobjuka, "Forwarding-loop-free configuration for iBGP networks," in Proceedings of IEEE International Conference on Networks (ICON), September 2003.
[11] L. Gao, T. G. Griffin, and J. Rexford, Inherently Safe Backup Routing with BGP. In proceedings of IEEE INFOCOM 2001. IEEE Computer Society, IEEE Press, April 2001.
[12] Labovitz, C., Ahuja. A., Bose, A., Jahanian, F., Delayed Internet Routing Convergence. SIGCOMM Comput. Commn. Rev., 30:175-187, August 2000
[13] No name (n.d.) "IS-IS Routing Protocol" Retrieved 19-11-2013, from http://www.interlab.ait.ac.th/tein2/Presentations/Basic%20Routing/IS-IS%20-%20Routing%20Protocol.pdf
[14] Balchunas, A. (2013). Cisco CCNP Routing Study Guide, www.routeralley.com.
[15] Stretch, Jeremy (n.d.) "BGP" Available at: https://www.dnlab.se/pdf/BGP.pdf.
[16] Wikipedia. 2014. Border Gateway Protocol. Available at: http://en.wikipedia.org/wiki/Border_Gateway_Protocol [Accessed: 27 Mar 2014]
[17] Wojciechowski, M. Border gateway protocol modelling and simulation. Master's thesis, University of Warsaw and Vrije University of Amsterdam, July 2008.
[18] Amrah Baba-Ali, Mujahid Tabassum and Kuruvilla Mathew, 'Performance Analysis of Interior Gateway Routing Protocols across different AS', The Fourth International Conference on Computer Science & Computational Mathematics (ICCSCM 2015), 7th - 8th May 2015, Langkawi, Malaysia.
[19] Conlan, P. J. (2009). Cisco Network Professional's Advanced Internetworking Guide. Canada, Wiley Publishing, Inc.
[20] Differencebetween.com, (2014). Difference Between EBGP and IBGP. Available at: http://www.differencebetween.com/difference-between-ebgp-and-vs-ibgp/ [Accessed 5 Apr. 2014].
[21] IP Balance (2009) "How DIS is elected in ISIS protocol" Retrieved 11-11-2013, from http://www.ipbalance.com/routing/isis/121-how-dis-is-elected-on-isis-protocol-.html.