Enhancing Border Gateway Routing Protocol with Software Defined Networking

Vidhu Baggan, Surya Narayan Panda

***Abstract*: The interminable Internet Connectivity is imperative for the present style of living and the swelling size of network traffic has kindled challenges for establishing a no jitter network. The twists of Routing Protocols and underlying mechanisms were undercover and need to be explored enough. In this paper, we explored various dimensions of Border Gateway Routing Protocol (BGP), a de-facto Routing Protocol for inter-autonomous systems. Numerous Anomalies may emerge through BGP which should be tended to through Software Defined Networking (SDN). In this paper, a simulation through SDN- Ryu controller in Mininet for BGP has been done and it has been observed that the assimilation of SDN with BGP improve the efficiency of networks.**

***Index Terms*: Border Gateway Protocol (BGP), Network Path Restoration (NPR), Software Defined Network (SDN), Multi-protocol Label Switching (MPLS), Controller –POX and Ryu.**

I. INTRODUCTION

The development of new uses of computer networks has improved our lives with solace. Nonetheless, with the ascent of continuous applications on the Internet, for example, Skype, e-banking, and so on, organize traffic has expanded quickly. This immense system traffic prompts organize clog or connection disappointment. Amid this condition of blockage or connection disappointment in the system, packet loss and irregularities may occur. This system state is outstanding to affect the activity of video conferencing and web trade inadequately. The issues, for example, versatility, security, and system speed can seriously block the execution of the present network devices due to regularly expanding system traffic [1]. So as to stand up to the system traffic, a conceivable arrangement is to re-engineer the system framework, as the current network devices may not be synchronized with the consistently changing requests of system-traffic [2]. Rather than chipping away at system framework, which in itself is certifiably not a versatile arrangement, in any case, the routing protocol component has many degrees for development. The BGP is the protocol which holds responsibility for the Internet. It has come a long way and still needs updating. The required updates may differ from network to network. This led to the need for customization of BGP. Software Defined Networking (SDN) provides a platform for addressing this challenge of BGP. The Ryu controller in SDN has built-in libraries for BGP.

Revised Manuscript Received on June 05, 2019

Vidhu Baggan, Associate Professor Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India

Surya Narayan Panda, Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India

Various dimensions of BGP can be programmed as per the requirement of the network. Moreover, on the way to reduce the Network Path Restoration (NPR) in between autonomous systems, the emerging technologies like Software Defined networking alongside routing protocol assume a huge job [3]. Consequently, this shouldn't be looked in an independent way, yet it would be more productive if deployed as a pair i.e Border Gateway Protocol (BGP) and Software Defined Networking (SDN) in a consecutive manner. Border Gateway Protocol (version 4) is the de facto protocol for connecting Autonomous systems. It is a path vector routing protocol and follows metrics as shown in Table 1 for the selection of the best path towards the destination [4].

Table 1: BGP Path Selection Priority

Priority	Policy Attribute
1	Highest LOCAL-PREF value
	Lowest AS-Path
3	Lowest origin type
4	Lowest MED value
5	EBGP Learned over IBGP Learned
6	Lowest IBGP Cost
7	Lowest Router ID

Many anomalies may arise in BGP due to incorrect routing policy, growing network traffic, inbuilt features, etc. These anomalies attract many researchers to address the issues of BGP. Software Defined Networking (SDN) is engineering that expects to make networks coordinated and adaptable. The objective of SDN is to improve organize control by empowering endeavours and Internet Service providers to react rapidly to changing business necessities. It enables the network devices to work in a decoupled way as the devices would work in a thin client manner and would operate as defined by the SDN controller.

II. BACKGROUND

The endless web availability is basic for the present style of living and the swelling size of system traffic has encouraged difficulties for setting up a no jitter arrange. The job of routing protocol is crucial while planning the network path restoration mechanism [5].

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

The way toward sending network traffic starting with one system then onto the next by a router is known as routing. The routing is of following types:

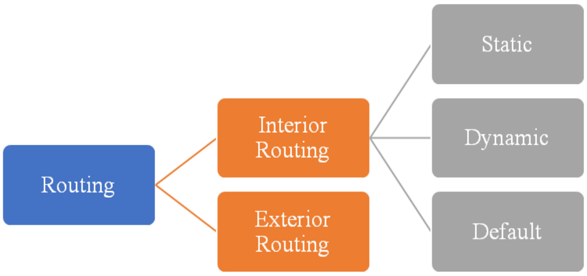


Fig 1. Types of Routing

To deploy these routing types, idiosyncratic protocols are there. For example, to actualize dynamic routing, three specific protocol types for different situations are shown through Fig. 2.

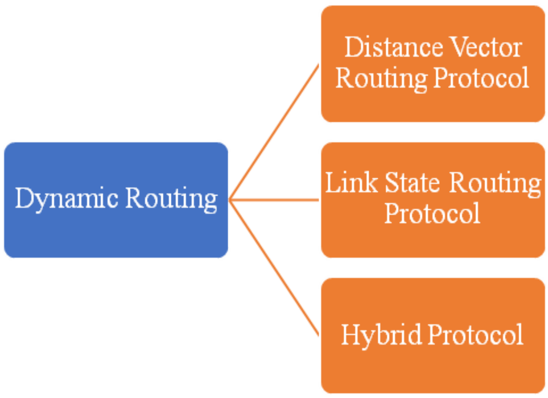


Fig 2. Types of Dynamic Routing Protocols [6]

At the highest dimension, the Internet makes out of thousands of Autonomous System (ASes). The Border Gateway Protocol (BGP) is the standard convention for sharing between the inter-autonomous system [5]. A BGP router can be either interior or exterior.

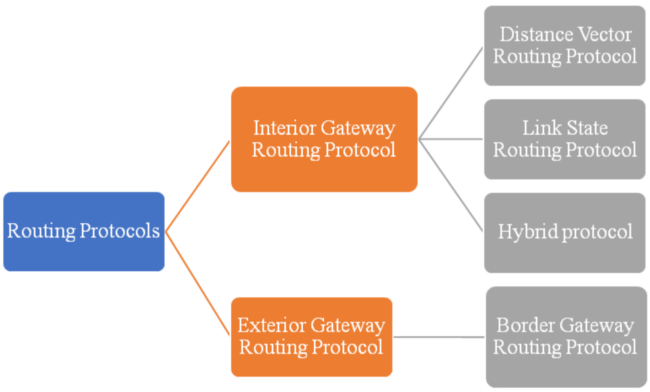


Fig 3. Types of Routing Protocols [7]

In the real scenarios, an AS comprises of different BGP routers, as appeared in Fig. 4. The BGP speaking routers exchange updates with each other to attain stability. These BGP speakers if peer themselves with other BGP speakers in the same AS then they are known as following IBGP and if they peer with BGP speakers that are present in other AS then they are known to follow EBGP. In the least complex case, each router has an IBGP session with each exterior router, shaping a "full mesh" arrangement. This "full mesh" design neglects to scale as the measure of the AS increments [8] [9].

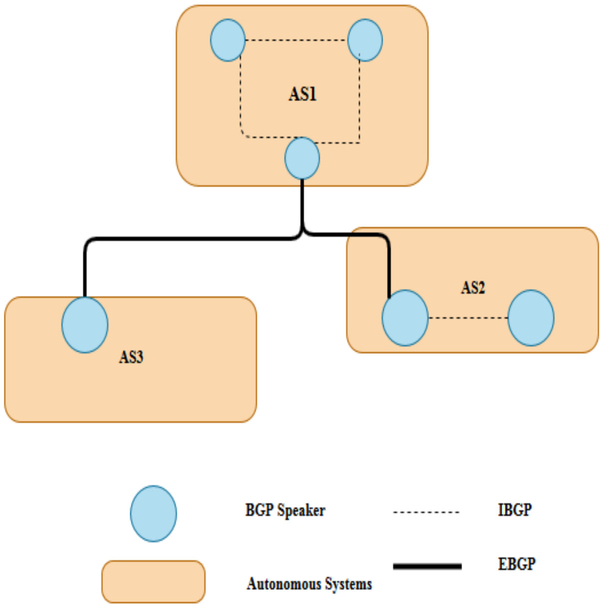


Fig. 4: Inter-Autonomous Systems Connected through BGP routers[4]

The Border Gateway Protocol (BGP) is the default inter-autonomous system routing protocol. Clients interface with (Internet Service Provider) ISP and ISPs use BGP as a steering convention to impart starting with one ISP then onto the next ISP. It is a path– vector routing protocol and possesses the property of an anti-loop mechanism. The BGP speakers trade routing updates with one another dependent on the directing or routing policy. When a BGP speaker sends updates to its BGP Peer, the sender has to wait for Minimum Route Advertisement Interval (MRAI) seconds for sending another advertisement concerning same destination networks.The network path directing approach may comprise of local preferences, number of ASes and multi-exit discriminator [10].

The BGP routing protocol has many extensions for development. The difficulties in BGP like higher intermingling delay because of system instability must be tended to by a component that can improve the speed of an Internet Protocol (IP) network [11].

The domain of issues in BGP has multiple dimensions which include convergence delay, multihoming scalability, routing policy mismatch, multipath routing scheme, security and scalability, lack in performance at QoS parameters and multiple announcements [12].

Regardless of the way that the capacities of BGP (coordinating methodologies), making them perfect for Network Path Restoration (NPR) in any case, the issue of customization of protocols speaks to a test for the future enthusiasm of the Internet. Recently, the Software Defined Networking (SDN) has pulled in uncommon interests to manage the network designing with respect to the customization of routing protocols [13]. The SDN gives imaginative organizations to the creating enthusiasm of the Internet [14]. To the best of our understanding, there are ponders that only consider the impact of BGP and SDN

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

on speed and adaptability in gigantic framework traffic. Regardless, the joining of these two promising progressions may amazingly improve speed, security, and adaptability. In this paper, the system topology maintained with BGP as a packet sending instrument and SDN as a controlling show. The SDN gives the phase to realize BGP and hereafter vouch for the blend of BGP and SDN to achieve NPR, with the irrelevant deferment and least packet loss [15]. The domain of issues in BGP has multiple dimensions which include convergence delay, multi homing scalability, routing policy mismatch, multipath routing scheme, security and scalability, lack in performance at QoS parameters and multiple announcements [12].

III. ISSUES AND CHALLENGES: BGP

Multiple Announcements: Growing Size of Routing Table

BGP is a case of a Bellman-Ford distance vector directing calculation. This calculation permits a gathering of associated BGP speakers to each to become familiar with the general topology of the interfacing system. The essential methodology of this calculation is extremely straightforward: each BGP speaker educates all its different neighbors concerning what it has realized whether the newly learned data changes the nearby perspective on the system [11].
This characteristic leads to the growing size of the routing table which gives birth to long delays in searching route entry from the routing table of a BGP speaker.

Ghost Entries

There is no inherent update timer in BGP, the router may not have latest updates entries which may lead to 'ghost entries' as those destination prefixes are never reachable [11].

Routing Policy mismatch

BGP speakers share their data in compliance with their routing policies which may disagree while the selection of best route [16].

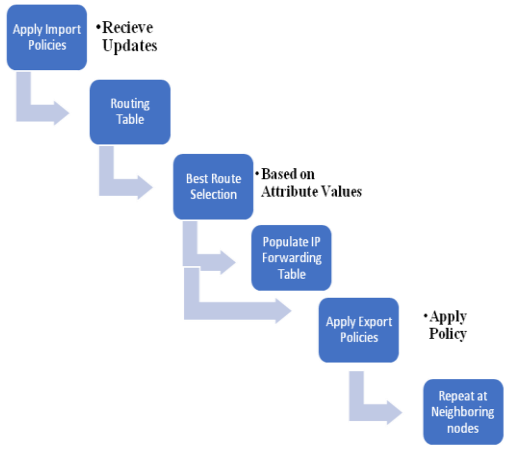


Fig. 5: BGP Route Selection Dynamics [16]

Further, since its inception in 1989, BGP has evolved with new challenges and possibilities. One of the challenges is the fact that BGP is the only exterior protocol connecting inter-autonomous systems. Since each inter-autonomous system is controlled by many operators which need the mutual agreement for multipath transmissions. This possibility of collaboration is strenuous as well as opening the opportunities [17].

MRAI: Reduces updates while adding delay

When a BGP speaker sends updates to its BGP Peer, the sender has to wait for Minimum Route Advertisement Interval (MRAI) seconds for sending another advertisement concerning same destination networks [18]. The MRAI may ultimately reduce the number of updates at the cost of added delay.

BGP hijacking

BGP hijacking is when attackers maliciously redirect Internet traffic. Attackers accomplish this by falsely announcing ownership of IP address groups, called IP prefixes, not actually owning, controlling, or routing to them. A BGP hijack is like changing all the signs on an expressway and rerouting automobile traffic to incorrect exits [19].

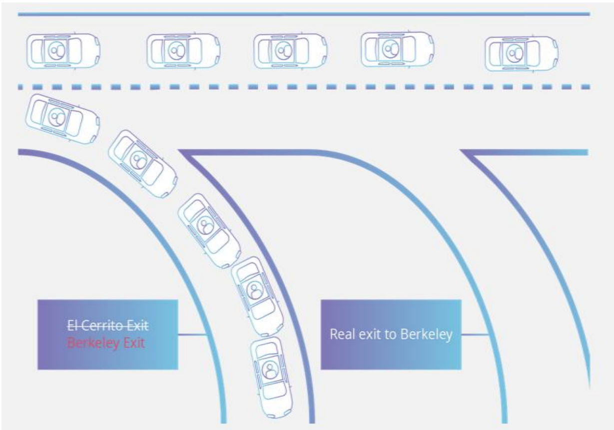


Fig. 6: Rerouting Traffic to incorrect exit (Source: https://www.cloudflare.com/learning/security/glossary/bgp-hijacking/)

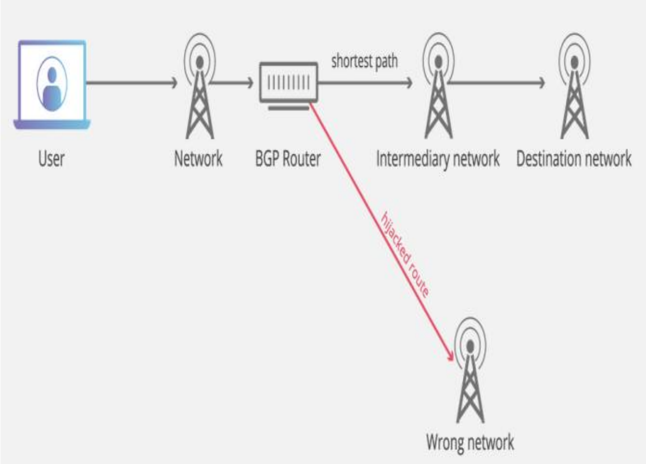


Fig. 7: Black hole Routing [19] (Source:
https://www.cloudflare.com/learning/security/glossary/bgp-hijacking/)

Security: Black Hole Routing

As a consequence of Prefix hijacking, the malicious, as well as legitimate traffic, will be routed to a null route or node is known as Black Hole Routing. If a protocol uses UDP which is connectionless, the sender will not get the reply or notification regarding the lost or dropped packet. However, BGP uses TCP which is connection-oriented and require a 3-way handshake for the connection establishment will receive the notifications for lost or dropped packet [19].

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

IV. SOFTWARE DEFINED NETWORK

The Software Defined Networks can be portrayed through the perspective of interchange perspectives. It is a thought, which can be practiced through controllers, conventions, and interfaces [13]. The idea of SDN has been acquired from the component where individuals utilized distributed computing framework to decouple the working framework from gadgets [19]. Fig. 6 is giving a perspective on Cloud Infrastructure, where gadgets are constrained by an incorporated switch and the switch on the other edge is associated with the gathering of gadgets to accomplish Network versatility, accessibility and vigor can be accomplished [20].

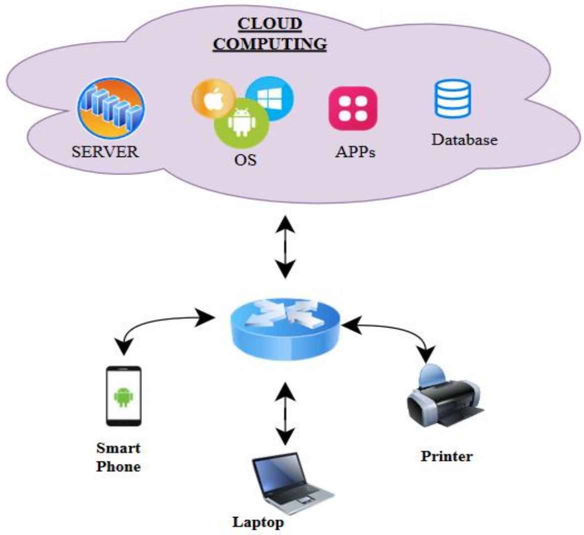


Fig. 8: Cloud Infrastructure [20]

The rising development of SDN gives a brought together controller to arrange organize gadgets which are routers and switches. Because of the nearness of one controller, different gadgets would completely rely on this for any system update [21]. In standard/customary frameworks the systems administration gadgets are the complete heap of Forwarding plane (Hardware Components) and Control plane (Operating System). The job of SDN is to de-couple the sending and control plane [22]. Fig. 7 presents the examination of Traditional and SDN frameworks.

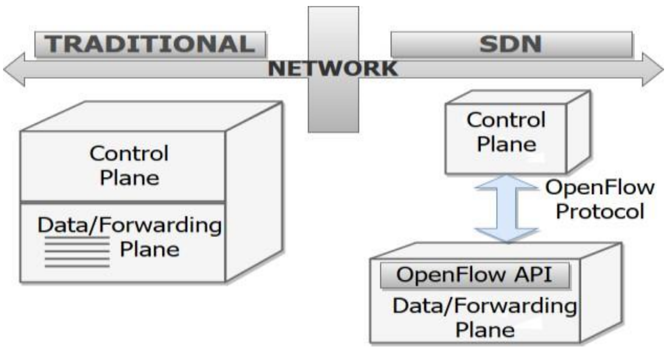


Fig. 9: Traditional Network vs SDN Networks [22]

In SDN the insightful and decoupled control plane offers an unbelievable dimension of adaptability to make the framework direct effective and therefore makes room to progress new protocols and applications [22]. Fig. 10 introduces the decoupled view for the design of SDN.

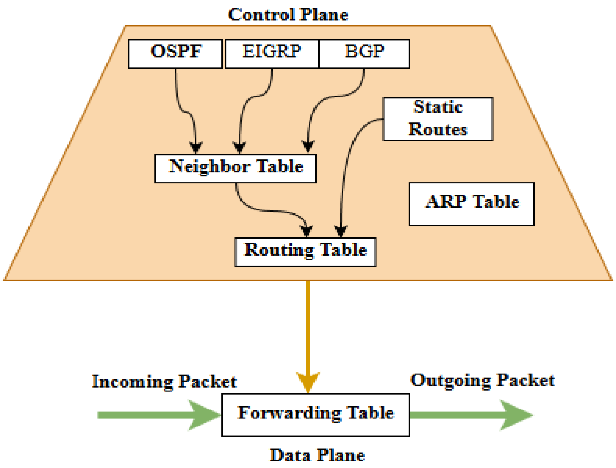


Fig. 10: SDN-decoupled architecture [22]

As indicated by the Open Networking Foundation (ONF), the unconventionality of the present applications must be tended to by the characteristics of SDN, for instance, dynamic, financially savvy and reasonable [23]. SDN configuration is made out of three layers:

(i) Infrastructural Layer
(ii) Control Layer
(iii) Application Layer

The Infrastructural layer describes the sending or data plane. The Control Layer is portrayed by different controllers like NOX, POX, Ryu, etc and the Application layer is depicted by applications like firewall, load balancer, etc. Distinctive contraptions like POX, Ryu and ODL are accessible to make the Control Plane. These gadgets, give a stage to the framework masters and researchers to structure the systems [24]. Fig. 11 traces the SDN Controller features.

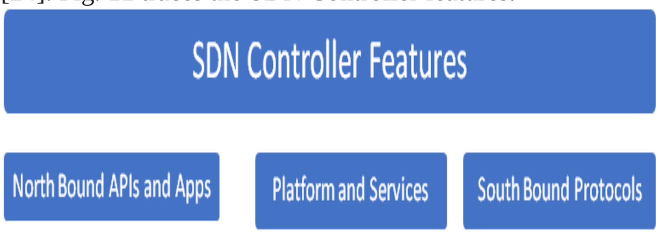


Fig. 11: SDN Controller Features [24]

As the goal of this examination is to address network path restoration with minimal delay, SDN also offers a component of the fault tolerance [25]. The protocol, which connects the control plane and the forwarding/data plane is Open Flow (Version1.5.1). It enables the association of multiple controllers to a switch so that if there ought to emerge an event of failure of one controller, the other controller would be available [14]. Fig. 12 uncovers the SDN as A Fault-Tolerant engineering.

Besides, because of the nearness of brought together controller, the postponement caused in rebuilding amid Network Failure identification and area is less when contrasted with regular systems [26]. Fig. 13 presents SDN with the viewpoint of Centralized Controller.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

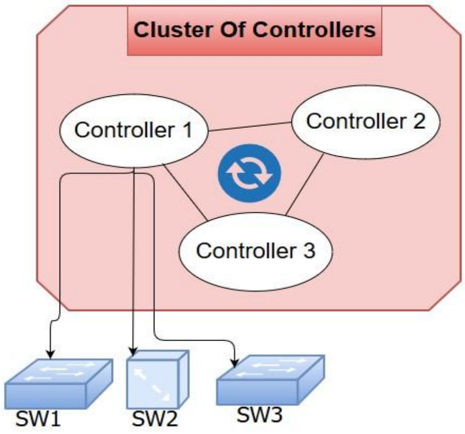


Fig. 12: SDN as Fault-Tolerant architecture [12]

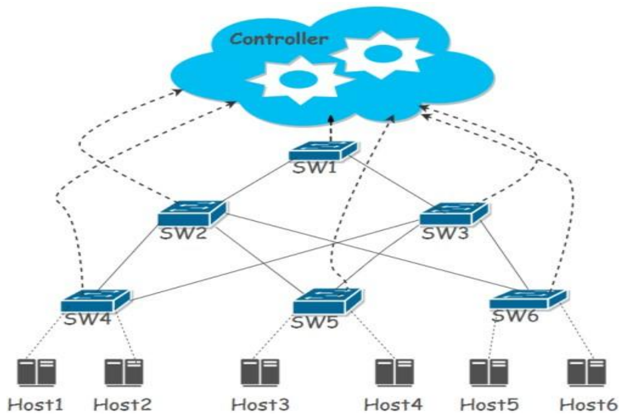


Fig. 13: SDN-Centralized Controller [26]

An investigation proposed a methodology that is used for synchronizing time and from now on system refreshes. The continuous system way updates can make brief anomalies, for example, traffic loops, congestion etc. and these updates must be performed in an approach to constrain these peculiarities. The system portrayed here is 'TIME4' which requires the clock synchronization among switches and controller. The model delineated here improves network performance, security approach amid system topology refresh. Moreover, SDN must be surveyed, as far as Traffic Engineering. For achieving this, the domains in flow management, Load balancing, Fault Tolerance and Consistency while Topology update must be thought about [23].

V. ISSUES CHALLENGES: SDN

This section discusses the features, advantages, disadvantages, Issues, and Challenges of above-discussed mechanisms:-

A. SDN-Speed and Security

The advantages of SDN are versatility, better transmission capacity usage, capacity to customize routing protocols and applications, reduced network congestion, and flexibility. SDN itself does not give encryption, but rather it is a virtual private system and, in that capacity, is divided off from the public Internet. In this manner, SDN is viewed as a protected transport mode. However, It is vulnerable to the DDOS attacks, which might impact networks [27].

B. SDN-Cost

On the positive side, SDN allows utilizing multiple, high bandwidth and inexpensive internet connections. However, the cost of SDN switches and controllers are higher than traditional switches. In addition to SDN switches and controllers, network bandwidth also plays a role while analyzing the cost of an SDN network. This equation for the cost can be expressed as: Cost = $\alpha (S) + \beta (C) + \gamma (B)$

S = cost of SDN switches

C = cost of controller

B = Bandwith usage charges

α, β, γ signifies the heterogeneity of the factors for cost.

Appended to the above, SDN also profess for streamlined staff utilization.

C. SDN-Performance

On the other edge, SDN uses the public internet and public internet is more vulnerable to packet loss, latency, and Jitter and hence no performance guarantees. Hence SDN vouches for better performance in terms of scalability, availability along with resource utilization but no guarantees for QoS.

D. BGP/SDN-Convergence Speed

Furthermore, the research explored that the BGP possess many advantages along with certain problems like routing table growth, instability, slower convergence, and security. These problems can also be solved by appending the network architecture with SDN. Due to the presence of centralized controller in SDN, the state propagation process can be accelerated and due to global overview present at the controller, the decision for the alternate path will be based upon the current updates.

Table 2. Comparing Traditional/Existing and Software Defined Networks [29]

Metrics	Existing Network	SDN
Network Perspective	Hardware Dominated	Software Dominated
Configuration Control	Hardware Vendor	User
Technology Openness	Closed Structure	Open Structure
Interlock Compatibility	Independent Protocol	Standardized Protocol
Managerial efficiency	Low-efficiency/ high cost operation	High-efficiency / Logical Operation
New Technological Adoption	Acc to the vendor needs	Acc to users' needs
Market Fairness	Monopoly	Fair Competition

SDN –Quick Diagnosis

The time for problem identification and orchestration of resources to resolve the issue is minimal in the case of SDN [28].

A. SDN/Existing Network-Comparison

The advantage of SDN is that an enterprise network traffic architect can sit at a central point and easily apply policies across all WAN devices. Table 2 summarizes the comparison between traditional and Software Defined Networking.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

SDN Controllers Comparison

Furthermore, the SDN is equipped with various controllers. Table 4 shows a comparison of the three controllers on 'Mininet' a network emulator for SDN, controllers available in SDN and it also depicts that the Network Performance with 'Iperf' tool. It depicts that we can implement BGP only through RYU Controller [18].

Table 3: Comparison Summary of SDN Controllers

	NOX	POX	Ryu
Language	C++	Python	Python
Performance	Fast	Slow	Slow
OpenFlow	1.0/1.3	1.0	1.0 - 1.4
BGP Library	No	No	Yes
MPLS Library	No	Yes	Yes

VI. EXPERIMENT TESTBED

The topology is shown in Fig. 14, depicts four hosts with their respective IP addresses and MAC addresses and all hosts are connected to an OpenFlow Virtual Switch(Version 2.0.2). The controllers are installed on dedicated Ubuntu 14.04.2 LTS VMs running on a 8GB RAM Intel(R) Core(TM) i7-7500 CPU @ 2.70GHZ. The Switch is further deployed first with POX (version 0.2.4) and then with Ryu (version 4.10) controller. Both POX and Ryu are a python-based controller that operates at port 6633 [30].

The topology implemented through POX and Ryu controller deployed on 'Mininet' a network emulator for SDN, and recorded the network performance with 'Iperf' tool, as shown in Table 5. The results of the implementation are shown in Table 6.

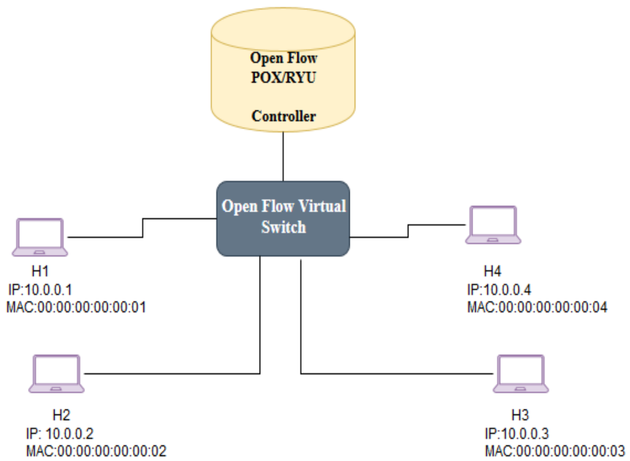


Fig. 14: Single Switch 4 hosts topology

Table 4. Table used for experimentation

Tools Used
Mininet _A Network Emulator for SDN
Iperf-Network Performance measurement tool

Table 5: Network Performance of POX and Ryu

Parameters	POX	Ryu
Round Trip Time	3.0129(ms)	0.036(ms)
Throughput	5.01Gbit/sec	5.81 Gbit/sec
Web Server Latency	4.6(ms)	3.5 (ms)
BGP Library	No	Yes
MPLS Library	Yes	Yes

From the above study, it has been cleared that for designing and developing an Enhanced Network Path Restoration Mechanism, the Ryu controller possesses the potential of libraries of BGP and MPLS, appended with less RTT and Web Server Latency value. The Ryu controller allows an easy way to run Open Flow/SDN experiments on testbeds as well as in real topologies [24] [31].

The discussion above mentioned vouched for an integrated approach of BGP and SDN. Fig. 15 depicts the proposed architecture to be implemented for achieving results of enhancing QoS in BGP.

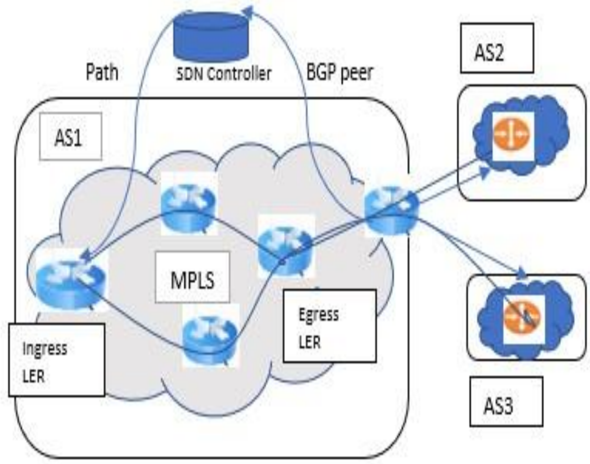


Fig. 15: Proposed architecture [47]

The above topology has been implemented through Mininet, Quagga, SDN Controller-RYU. Mininet creates an OpenFlow virtual network with a controller, switches hosts, and links, and also allows to develop custom topologies using Python scripts [32] Mininet has become one of the prominent emulation tools in this context since it incorporates several elements of Software Defined Networking (SDN). Developed at Stanford University, it is an open - source, emulator that provides a programmable interface to define and build network configuration with virtualized elements. [33]. In this study, the Mininet has been installed on the Vmware 12.5.1.

The systems depicting various AS2 and AS3 has been implemented on Quagga version 1.2.4. Quagga is a network routing software suite, which provides the

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

implementation of routing protocols like Open Shortest Path Forwarding (OSPF), Routing Information Protocol (RIP), BGP.

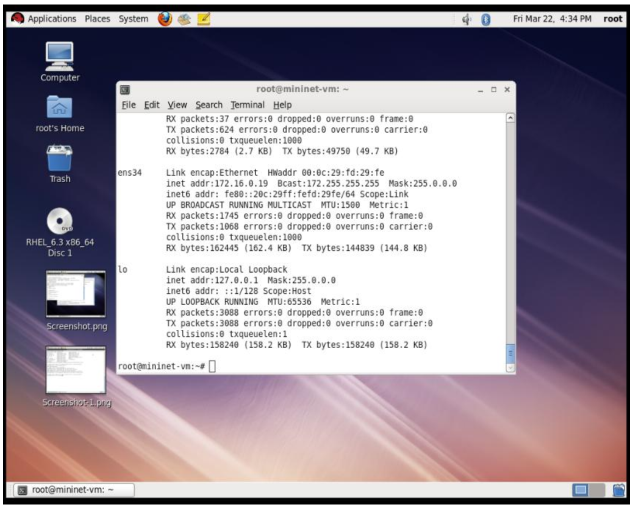


Fig. 16: Screenshot of the VMware system implementing Mininet

For the present work, the Border Gateway Protocol (BGP) has been implemented on Quagga. For the Controller purpose, SDN-Ryu supports the BGP library in Python. For this specific work, the files titled as 'bgpspeaker.py, bgpapplication.py has been used.

Table 6: Key constituents of the tested network design

Components	Device/ Interface	Count	Configuration	Description
Network Device	Router	4(Inter-AS) + 2(Intra-AS)	7200 Series Cisco Router	These routers can be configured for MPLS and BGP configurations for Inter-AS and EIGRP for Intra-AS communication.
Bandwidth	Serial Links	5	64000 Kbps	The bandwidth of a network link is the amount of data bits that can be transmitted at a time.
	Fast-Ethernet	3	100 Mbps	
Window Size	Size of a Ping request	5	56 bytes	The number of data bits that can be sent together without waiting for the acknowledgment.

VII. RESULT AND DISCUSSIONS

The graphs are shown in Fig. 17 and Fig. 18 for delay and throughput which exhibits that assimilated approach of various mechanisms is not showing much better performance as compared with BGP alone. The reason for this is that the SDN controller may add extra delay for the communication between the client node and an SDN controller which further affect throughput also. However, the SDN controller provides flexibility for customization of routing mechanisms through their built-in libraries.

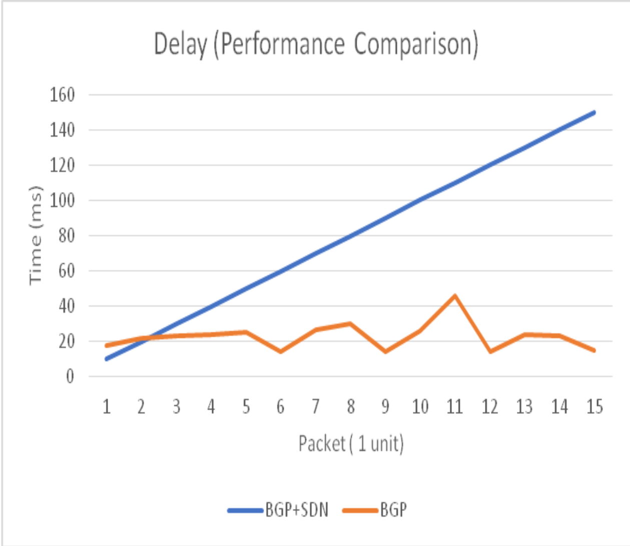


Fig 17 : Performance Comparison of BGP and BGP+SSN in terms of Delay

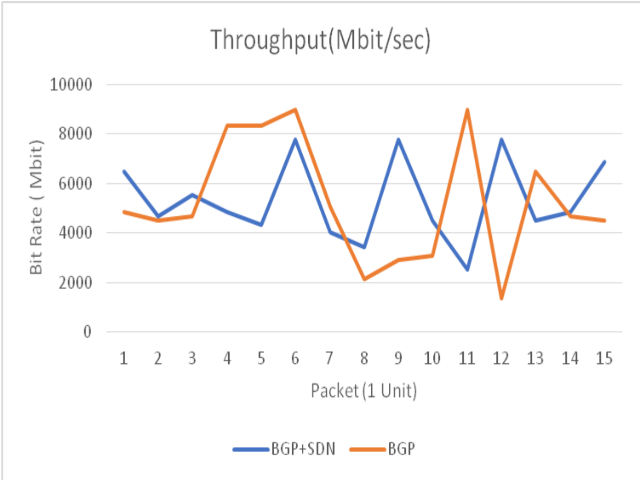


Fig. 18: Throughput (Performance Comparison)

Fig. 19 and Fig. 20 show the time taken by routers for network path restoration if one node/interface on the path towards destination fails. However, The screenshots depicted in Fig. 19 and Fig. 20 shows that the router configured with BGP alone takes much time for path restoration with much loss in packets as compared to the integrated approach. It can be retrieved from the above that SDN controller shows better results in terms of minimal packet loss during network path restoration while in case of delay and throughput the routing policy must be modified to bring more positive results in terms of less delay and high throughput.

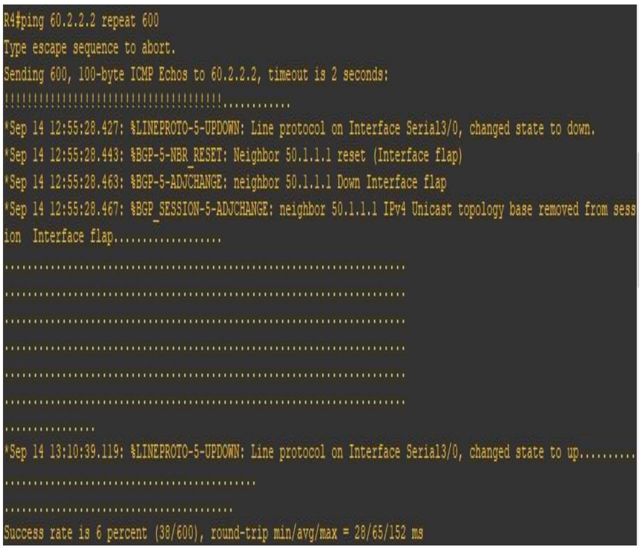


Fig. 19. Network Path Restoration with BGP

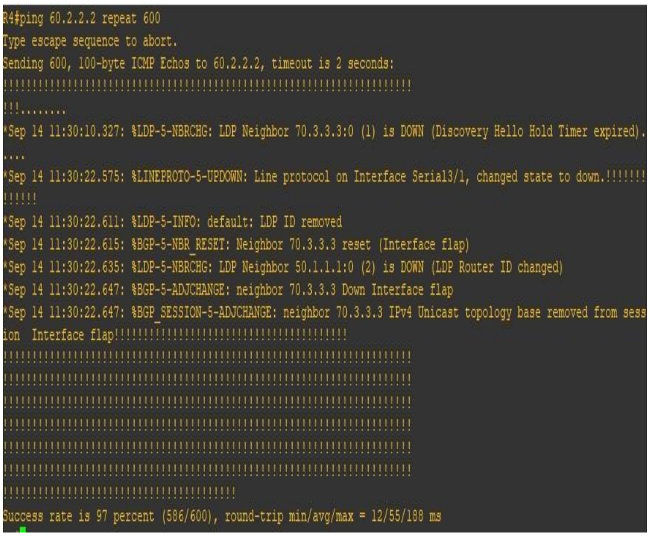


Fig. 20. Network Path Restoration with MPLS+BGP+SDN

VIII. CONCLUSION

The BGP routing protocol needs updates which are condition specific and SDN-Ryu controller has the potential to customize the behavior of BGP. The paper first explored the POX and Ryu controller of SDN through a simulation conducted in Mininet. SDN-Ryu supported BGP Libraries. The results obtained from another simulation performed in Quagga and SDN-Ryu shows that an assimilated approach of BGP and SDN mechanisms has much potential for Network Path Restoration in terms of minimal packet loss. However, to achieve less delay and high throughput, routing policies of BGP must be changed otherwise SDN controller may add an extra delay to the communication between the client node and the SDN controller that will further affect throughput as well.

REFERENCES

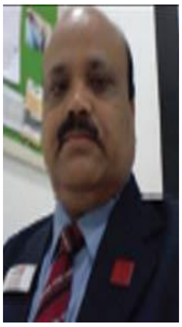
1. F. Hu, Q. Hao, and K. Bao, “A survey on software-defined network and OpenFlow: From concept to implementation,” *IEEE Commun. Surv. Tutorials*, vol. 16, no. 4, pp. 2181–2206, 2014.
2. K. Bakshi, “Considerations for Software Defined Networking (SDN): Approaches and use cases,” *IEEE Aerosp. Conf. Proc.*, pp. 1–9, 2013.
3. S. U. Masruroh, A. Fiade, M. F. Iman, and Amelia, “Performance evaluation of routing protocol RIPv2, OSPF, EIGRP with BGP,” *Proc. - 2017 Int. Conf. Innov. Creat. Inf. Technol. Comput. Intell. IoT, ICITech 2017*, vol. 2018–Janua, pp. 1–7, 2018.
4. B. Al-Musawi, P. Branch, and G. Armitage, “BGP Anomaly Detection Techniques: A Survey,” *IEEE Commun. Surv. Tutorials*, vol. 19, no. 1, pp. 377–396, 2017.
5. Y. Rekhter, “A Border Gateway Protocol 4 (BGP-4),” 1995.
6. L. Todd, *CCNA Routing and Switching Study Guide: Exams 100-101, 200-101, and 200-120*. 2013.
7. Jeff Doyle, *CCIE Professional Development Routing TCP/IP, Volume I, Second Edition*, vol. I, no. 1919. 2005.
8. R. Musunuri and J. A. Cobb, “An overview of solutions to avoid persistent BGP divergence,” *IEEE Netw.*, vol. 19, no. 6, pp. 28–34, 2005.
9. R. B. Da Silva and E. S. Mota, “A Survey on Approaches to Reduce BGP Interdomain Routing Convergence Delay on the Internet,” *IEEE Commun. Surv. Tutorials*, vol. 19, no. 4, pp. 2949–2984, 2017.
10. H. Guo, W. Su, H. Zhang, and S. Kuo, “On the convergence condition and convergence time of BGP,” *Comput. Commun.*, vol. 34, no. 2, pp. 192–199, 2011.
11. G. Huston, “The ISP Column BGP in 2013 – The Churn Report,” no. February, pp. 1–12, 2014.
12. M. Yannuzzi, X. Masip-Bruin, and O. Bonaventure, “Open issues in interdomain routing: A survey,” *IEEE Netw.*, vol. 19, no. 6, pp. 49–56, 2005.
13. D. Kreutz, F. M. V. Ramos, P. Verissimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, “Software-Defined Networking: A Comprehensive Survey,” pp. 1–61, 2014.
14. I. Akyildiz, A. Lee, P. Wang, M. Luo, and W. Chou, “A Roadmap for Traffic Engineering in Software Defined Networks,” *Comput. Networks*, no. June, pp. 1–27, 2014.
15. Y. C. Liu HP, Tsai PW, Chang WH, “Design and Development of the Reactive BGP peering in Software-Defined Routing Exchanges,” *Proc. Asia-Pacific Adv. Netw.*, vol. 44, pp. 48--53, 2017.
16. A. Jaggard and V. Ramachandran, “Toward the design of robust interdomain routing protocols,” *Network, IEEE*, no. December, pp. 35–41, 2005.
17. R. Wójcik *et al.*, “A survey on methods to provide interdomain multipath transmissions,” *Comput. Networks*, vol. 108, pp. 233–259, 2016.
18. T. G. Griffin and B. J. Premore, “An experimental analysis of BGP convergence time,” *Int. Conf. Netw. Protoc.*, pp. 53–61, 2001.
19. “No Title.” [Online]. Available: https://www.cloudflare.com/learning/security/glossary/bgp-hijacking/
20. W. Venters and E. A. Whitley, “A critical review of cloud computing: Researching desires and realities,” *J. Inf. Technol.*, vol. 27, no. 3, pp. 179–197, 2012.
21. J. Chen, X. Zheng, and C. Rong, “Survey on software-defined networking,” *IEEE Commun. Surv. Tutorials*, vol. 9106, no. 1, pp. 115–124, 2015.
22. T. Bakhshi, “State of the art and recent research advances in software defined networking,” *Wirel. Commun. Mob. Comput.*, vol. 2017, 2017.
23. T. Mizrahi and Y. Moses, “Time4: Time for SDN,” *IEEE Trans. Netw. Serv. Manag.*, vol. 13, no. 3, pp. 433–446, 2016.
24. S. Kaur, J. Singh, and N. S. Ghumman, “Network Programmability Using POX Controller,” *Int. Conf. Commun. Comput. Syst.*, p. 5, 2014.
25. P. C. Da Rocha Fonseca and E. S. Mota, “A Survey on Fault Management in Software-Defined Networks,” *IEEE Commun. Surv. Tutorials*, vol. 19, no. 4, pp. 2284–2321, 2017.
26. A. P. S. Virk and R. Boutaba, “Economical protection in MPLS networks,” *Comput. Commun.*, vol. 29, no. 3, pp. 402–408, 2006.
27. S. Sezer *et al.*, “Are We Ready for SDN? Implementation Challenges for Software-Defined Networks BACKGROUND: WHY SDN?,” *IEEE Commun. Mag.*, vol. 51, no. 7, pp. 36–43, 2013.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

28. X. Zhang, Z. Cheng, R. P. Lin, L. He, S. Yu, and H. Luo, "Local fast reroute with flow aggregation in software defined networks," *IEEE Commun. Lett.*, vol. 21, no. 4, pp. 785–788, 2017.
29. M. Anan, A. Al-Fuqaha, N. Nasser, T. Y. Mu, and H. Bustam, "Empowering networking research and experimentation through Software-Defined Networking," *J. Netw. Comput. Appl.*, vol. 70, pp. 140–155, 2016.
30. R. Jawaharan, P. M. Mohan, T. Das, and M. Gurusamy, "Empirical evaluation of SDN controllers using mininet/wireshark and comparison with cbench," *Proc. - Int. Conf. Comput. Commun. Networks, ICCCN*, vol. 2018–July, 2018.
31. E. Amiri, M. R. Hashemi, and K. Raeisi, "Policy-Based Routing in RIP-Hybrid Network with SDN Controller Policy-Based Routing in RIP-Hybrid Network with SDN Controller," no. September, 2018.
32. RvachovaNatalia, "THE COMPARISON OF NETWORK SIMULATORS FOR SDN Network," 2018.
33. D. Muelas, J. Ramos, and J. E. L. De Vergara, "Assessing the Limits of Mininet-Based Environments for Network Experimentation," *IEEE Netw.*, vol. 32, no. 6, pp. 168–176, 2018.

AUTHORS PROFILE

Vidhu Baggan graduated at Beant College of Engineering & Technology and completed her Master's Degree at NITTTR, Chandigarh. She has a teaching experience of 18 years. At present, She is pursuing her Ph.D. and is Associate Professor at Chitkara University, Punjab. In addition, She is certified as a Microsoft Certified Professional (2004), Cisco Certified Network Associate(2005 & 2016), Huawei Certified Network Associate(2018) and Huawei Certified Instructor(2018).



Surya Narayan Panda is presently working as a Director, Research in Chitkara University, Punjab. He is associated with academics for the last 23 years. His areas of research are cyber security, education system, and network security. He has guided numerous Ph.D. scholars. He has filed more than 3 patents and one of them is published in WIPO. He has worked on various consultancy projects like smart luggage tracking system and wireless solution to diesel engine tuning system. He is presently working on Millenium Alliance-funded research project. He has also been awarded an excellence award from Chitkara University in the year 2017. In addition to the above, he has 8 Patents and 1 crore plus funded projects from Ministry of Science and Technology, Govt. of India. He had also guided 7 Ph.D. under his mentorship

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication