DOI: http://dx.doi.org/10.26483/ijarcs.v8i7.4486

ISSN No. 0976-5697

Volume 8, No. 7, July – August 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

REVIEW ON HIGH AVAILABILITY AND FASTER CONVERGENCE IN IP NETWORKS

Er. Avtar Singh
Department of Computer Engineering
Punjabi University, Patiala
Punjab, India

Er. Harpreet Kaur
Assistant Professor, Department of Computer Engineering
Punjabi University, Patiala
Punjab, India

Abstract: This paper explains the importance of High Availability and Faster Convergence in today's Networks and the current set of high availability and faster convergence protocols and technologies used. Network Convergence and High Availability of IP networks are related with each other and both play a very important role in achieving the business continuity and to make IT works for any business. As Networks act as a base to transport the data from one part to other and most of the business units are dependent on IT for its functions to run, the paper includes those technologies and protocols that helps achieving best results to achieve around hundred percent business continuity with the help of networks. Through the studies it's been detected that BGP is best in ISP Edge Networks and BFD is most beneficial in the event where L2 Network is operating as a transit route for L3 Network, while LSA and SPF Pacing is effective to fasten the core Routing.

Keywords: FHRP, BGP PIC,PAGP, LINK AGGREGATION, LACP, BFD, Fast Reroute, LSA and SPF Pacing.

1. INTRODUCTION

IT is changing and it is also bringing the revolutionary shift in the Businesses Worldwide. Almost every business is connected with IT and those who are not connected will use it in future as it has become a kind of a need to compete with competitors. Technologies like Cloud and Internet-of-Things are taking the Business innovations to the entire different level where you can achieve Machine to Machine connectivity and also can connect to your applications, data and machines from any place any time. One thing that is making these all things possible is Networks. Networks are acting as the beating heart of the business continuity as network is the thing that makes all the applications accessible to the clients or employees from any part of the world. Enterprises, Individual Users are moving their data to the private and public clouds and as more and more data is shifting towards the clouds ,like Amazon AWS or Rackspace for Enterprises or Apple iCloud, Dropbox, Google Drive etc for individuals, the importance of network availability has increased with the time. Stock Markets, Enterprises, SOHO Users etc, in order to always connect with their business applications requires different technologies and protocols related to Highly Available and Faster Convergence Networks. Faster Convergence and High Availability are two different terms, but are related to each other in a manner that both are needed to make business continuity work. Convergence in Networks means at what rate the data traffic shifts to the backup link, if primary link goes down. Better the convergence, higher availability can be achieved. Sub-Second convergence is what is needed in today's networks to make the business continuity work and to make the enterprise applications always available to the users.

2. VARIOUS PARAMETERS TO MEASURE THE PERFORMANCE OF PROTOCOLS

(I) Convergence Measurement -
Time in ms taken by (Failure Detection + Event Propagation + Routing Process + FIB Update)
If we take an example, suppose a large Call Center like Dell's, which mainly uses VoIP Calling to interact with their customers has multiple internet links from different internet service providers and all the links are in use with active-active links and traffic is engineered in a way that it is divided between multiple links and suddenly one of the link goes down, then the very first thing is that the failure is detected by the router or layer 3 switch after the timer expiration of routing protocol, IP SLA Tracking or using any other faster convergence method, where multiple links are terminated from different internet service providers, then that event of link failure is propagated, after that the changes in routing-information-base(RIB) are made by routing protocol and then the changes are made to the data plane of the device, so that new link should be provided for the traffic passing over the failed link. This process of Convergence takes much more time than a application might need to be in use all the time. So to reduce the convergence time to minimum time possible.

II) Availability in terms of ISP = (MTBF - MTTR) / MTBF, where MTBF is the mean time between failure, also indicates, what, when and how does a link fails, while MTTR is known as the mean time to repair the network availability problem also known as how long does it take to repair the network availability. When buying network services from ISPs, the cost matters according to the bandwidth and the availability level that the customer selects. Below are some of the standard availability levels .

Table 1 - Availability Levels in Network. Source - Ciscolive

Availability	DPM	Downtime Per Year (24x365)		
99.000%	10000	3 Days	15 Hours	36 Minutes
99.500%	5000	1 Day	19 Hours	48 Minutes
99.900%	1000		8 Hours	46 Minutes
99.950%	500		4 Hours	23 Minutes
99.990%	100			53 Minutes
99.999%	10			5 Minutes
99.9999%	1			30 Seconds

"High Availability"

DMP—Defects per Million

3. CONVERGENCE AND HIGH AVAILABILITY PROTOCOLS

a) Bidirectional Forwarding Detection - The Bidirectional Forwarding Detection (BFD) protocol provides a mechanism to detect faults in the bidirectional path between two forwarding engines[8]. BFD is a fault detection mechanism between two layer 3 devices, if they are connected using any media that does not support any sort of failure detection on their own like Ethernet, MPLS LSPs, Tunnels etc. What BFD does is that it creates a session between two layer 3 end-points[7], in case where multiple links exist, then multiple BFD sessions can be established. It is a very lightweight protocol. It can work with almost all the routing protocols like OSPF, BGP etc, therefore the neighbor loss is detected by BFD in much faster time when compared with the non-BFD mechanism[3], where failures are detected on the basis of routing protocol timers, so in an non-BFD routing protocol neighbourship of two L3 devices over a L2 bridged network, if OSPF is used as the routing protocol, it takes the default of 40 seconds of dead-timer to detect a failure in the link and after that next proces of event propagation, RIB and FIB update is done. Below figure shows the BFD scenario :-

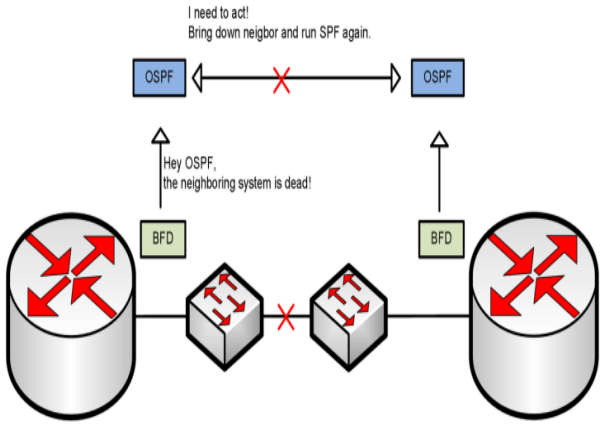

Figure 1. - BFD Scenario, Source – https://www.saidvandeklundert.nl/bfd.php

Figure 1. shows two L3 devices running OSPF routing protocol are connected over two L2 Ethernet switches and BFD is configured between the two routing nodes to make Layer 3 fast convergence.

b) LSA and SPF Pacing Timers - OSPF is the most used Interior Gateway Routing protocol in the world. Link- state advertisement (LSA) is responsible for the routing information exchange between routers[6]. OSPF uses Dijkstra's SPF algorithm to find the best path towards destination. OSPF stores every route information in the form of Link State Advertisement(LSA) and the age of every LSA is 3600 seconds or 60 minutes, which gets extended or refreshed every 1800 seconds or 30 minutes. SPF Calculation and LSA propagation are very important part of OSPF Routing Protocol and RIB and FIB update process contributes most of the convergence time where thousands of routes are calculated and added in the routing table. Therefore throttling OSPF LSAs and SPF Calculation time can help achieving faster convergence in OSPF. figure 2 depicts SPF tuning :

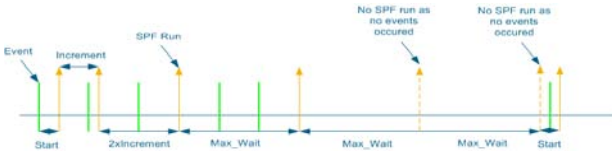

Figure 2 - SPF Schedule Tuning, Source – http://blog.ine.com/2009/12/31/tuning-ospf-performance/

c) BGP PIC - Border Gateway Protocol is the protocol that makes internet ticks. PIC abbreviated as Prefix Independent Convergence is a faster convergence protocol of the Forwarding information base. BGP is a slow protocol, it was made slow for the reason that it has hundreds of thousands of routes, where every second, some routes goes up and down, which can take lots of CPU resources and memory usage, therefore it was made in a manner, where updates were sent in a batch of 30 seconds in case of External BGP and in 5 seconds batch for every Internal BGP neighbor. it is possible to reduce the traffic loss time to sub-second for BGP Core or Edge failures by using BGP PIC[11]. BGP PIC is used to faster convergence of BGP routing Protocol in a manner which does not effect CPU resource and memory usage as it stores a backup or alternate path in the RIB and FIB and in case of failure detection, backup path immediately gets into use and automatically enables faster failover. Figure 3 shows the BGP PIC scenario :

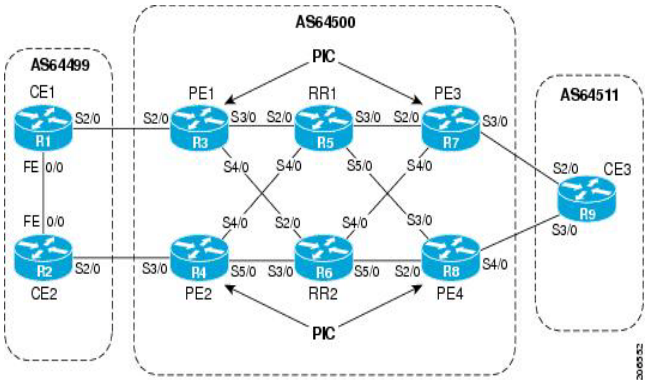

Figure 3 - BGP PIC for MPLS PE Primary-Alternate Scenario, Source - http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bgp/configuration/xe-3s/irg-xe-3s-book/irg-bgp-mp-pic.html

d) MPLS FRR - One of the key features of MPLS Traffic Engineering (MPLS-TE) is fast recovery in case of failure of

link or node[2]. MPLS Fast Reroute is a traffic engineering mechanism used to reduce the convergence time in the MPLS Backbone Networks. These mechanisms enable the re-direction of traffic onto backup LSP tunnels in 10s of milliseconds, in the event of a failure[5]. It provides a automatic mechanism to reroute traffic on a LSP, if some link or node under the LSP fails. Traffic Engineering uses Existing Link State Routing Protocols OSPF and ISIS to disseminate topology information[1]. It is achieved by pre-computing a number of protection LSPs. Figure 4 is the scenario of MPLS Fast Reroute :-

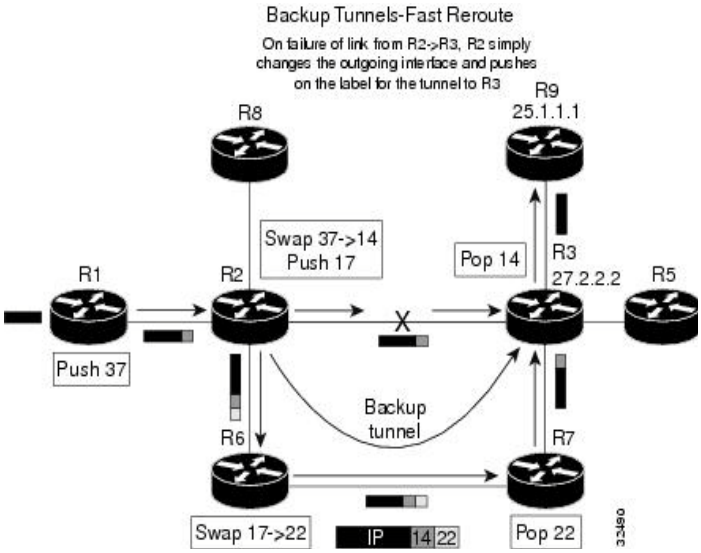

Figure 4 - MPLS FRR Mechanism, Source,http://www.cisco.com/c/en/us/td/docs/ios/12_0s/feature/guide/fslinkpt.html

High Availability is also a very important factor to achieve business continuity. Availability can be measured by using formula (Table no. 1)

e) First Hop Redundancy Protocols - FHRPs mainly comes in three variants i.e. HSRP, VRRP and GLBP. These three protocols are used for gateway redundancy and is used for high availability of networks. Hot Standby Router Protocol and Gateway Load Balancing Protocol are licensed under Cisco Systems Inc., while Virtual Router Redundancy Protocol is an Open Standard Gateway Redundancy Protocol and is defined in IETF RFC 3768. The advantage gained from using VRRP is a higher availability default path without requiring configuration of dynamic routing or router discovery protocols on every end-host[4]. In both HSRP and VRRP, HSRP provides failover services to those hosts[10]. .Load Balancing is enabled by default and in case user requires load balancing, he has to configure multiple groups, while GLBP does load balancing by default. All these protocol use the concept of virtual IP which is shared among different gateway routers and primary to backup link failure depends on the timers, which can be reduced to single second or in ms(in case of HSRP and GLBP). Figure 5 showing HSRP scenario:-

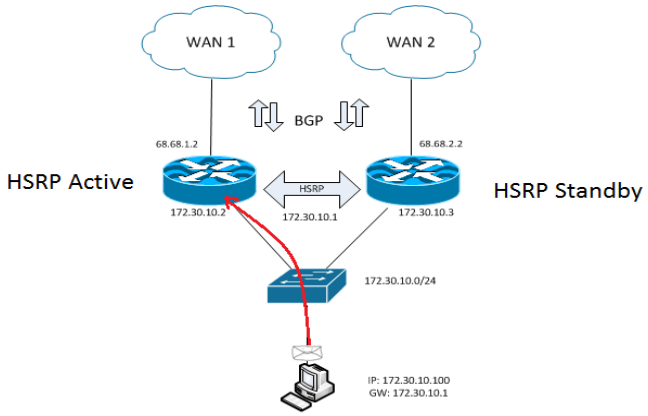

Figure 5 - HSRP Scenario - Source – https://thecciejourney.wordpress.com/2014/10/12/hsrp-no-longer-for-the-weak-of-heart/

f) Link Aggregation - LACP is a standards-based alternative to PAgP, defined in IEEE 802.3ad[9]. Also known as Ether Channels or NIC Teaming, it is used to aggregate multiple physical links to create a single logical link. Multiple 8 links can be in use. Different methods can be used to bundle multiple links like we can use static method by using On mode, or we can use dynamic method by using protocols to negotiate EtherChannel. Protocols that can be used are Port Aggregation Protocol and Link Aggregation Channel Protocol[3]. In LACP, maximum 16 links can be bundled, but a maximum of 8 wil be in use at a time. So the capacity can reach up to 80 Gbps, if we bundle 8 links of 10Gbps each. Traffic between the links can be decided on the basis of Load Sharing Algorithms used with Ether Channels. If a single address based load sharing method is used, then the BITS method, while XOR is used in case where source and destination addresses are used in load sharing mechanism. figure 6 depicts the - Link Aggregation or EtherChannel

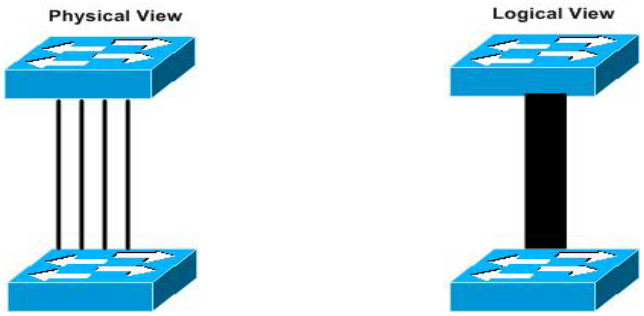

Figure 6 - Link Aggregation or EtherChannel, Source - http://ericleahy.com/index.php/etherchannels/

4. FINDINGS :-

From the studies it has been observed that BGP Works best in ISP Edge Networks and BFD is best in case where L2 Network is acting as a transit path for L3 Network, while LSA and SPF Pacing works well to fasten the Core Routing.
Feature Comparison of the discussed Protocols on the basis of Convergence time and Placement has been formulated in Table 2 as described below :-

Table 2 – Comparison of Protocols

Protocol	Convergence	Normal Placement of Protocol
Bidirectional Forwarding Detection	Less than 1 Second	L3 Neighborship over L2 Network
BGP PIC	Less than 1 Second	ISP Edge Network
LSA and SPF Pacing	Less than 1 Second	Core Routing
FHRP	Less than 1 Second	Enterprise Edge
IP SLA	1-2 Seconds	Edge Networks

5. CONCLUSION

When designing networks for current IT and business units, one of the most important things that must be designed and implemented with care is the faster convergence and high available behavior of the network. Discussion about various protocols has been carried out and Through the studies it's been detected that BGP is best in ISP Edge Networks and BFD is most beneficial in the event where L2 Network is operating as a transit route for L3 Network, while LSA and SPF Pacing is effective to fasten the core Routing. it has been concluded that networks should be made in the manner, which can provide the best possible results in achieving the business continuity as any problem in networks directly or indirectly hurts the business approach. Therefore the faster convergence and high availability technologies should be configured in order to achieve faster convergence and almost always available networks.

6. REFERENCES

[1] MPLS Traffic Engineering – Fast Reroute by Shuguftha Naveed, S. Vinay Kumar of Vasavi College of Engineering(Osmania University), Hyderabad in May, 2014 under IJSR – ISSN: 2319-7064.

[2] MPLS Recovery Schemes: An Experimental Evaluation(July 2015) by Seema Anand Ladhe and Vijay T Raisinghani of NMIMS University, Mumbai, under IJCNCS - ISSN 2410-0595.

[3] High Availability and Faster Convergence in IP Networks(September 2015) by Jashandeep Kaur and Rupinder Kaur Gurm of RIMT-IET, Punjab, under IJCST - Volume 3 Issue 5.

[4] Virtual Router Redundancy Protocol (VRRP) by R. Hinden, Ed. Of Nokia in Internet Engineering Task Force – RFC 3768

[5] Fast Reroute Extensions to RSVP-TE for LSP Tunnels by P. Pan, Ed. Of Hammerhead Systems, G. Swallow, Ed. Of Cisco Systems and A. Atlas, Ed. Of Avici Systems in IETF RFC 4090

[6] Survey on the RIP, OSPF, EIGRP Routing Protocols by V. Vetriselvan et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014, 1058-1065

[7] Bidirectional Forwarding Detection (BFD) by D. Katz and D. Ward of Juniper Networks in IETF RFC 5880.

[8] Bidirectional Forwarding Detection (BFD) on Link Aggregation Group (LAG) Interfaces by M. Bhatia of Alcatel-Lucent, M. Chen of Huawei Technologies, S. Boutros, M. Binderberger of Cisco Systems. J. Haas of Juniper Networks in IETF RFC 7130

[9] Press, Cisco. " Ccnp Routing and Switching Switch 300 - 115 Official Cert Guide." (2015).

[10] Cisco Hot Standby Router Protocol (HSRP) by T. Li and B. Cole of Juniper Networks, P. Morton and D. Li of Cisco Systems in IETF RFC 2281.

[11] BGP Prefix Independent Convergence (PIC) Technical Report by Clarence Filsfils, Pradosh Mohapatra, John Bettink, Pranav Dharwadkar, Peter De Vriendt, Yuri Tsier of Cisco Systems