International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Comparative Analysis of IP Network for High Performance and Rapid Integration Techniques

Priyanka Singla

Assistant Professor, Multani Mal Modi College
Email: *priyankagarg7385[at]gmail.com*

Abstract: ***In the event of a primary link breakdown, this article covers the many approaches for faster convergence and higher availability that allow today's fast-paced networks get things done. In just a few milliseconds, the secondary connection can converge to the primary link. It describes methods for achieving high availability in networks that are employed in the real world. Additionally, a comparison of a few faster convergence and high availability approaches is done in this work.***

Keywords: VRRP, LACP, BFD, SPF, OSPF, SPF Tuning

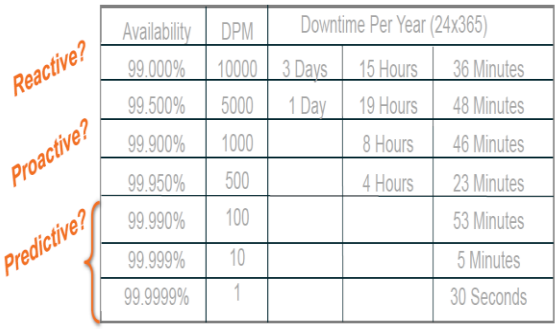
1. Introduction

The lifeblood of the IT industry is networking. In the modern world, we cannot imagine living without the Internet. Businesses are moving toward e-commerce solutions. All data is moving to clouds, which are essentially large numbers of servers at data centers. Our calling and video solutions in the workplace and in our daily lives are moving toward the new IP age. All of these applications have one thing in common that they need to succeed with: high availability and faster convergence. Whether we are designing "Enterprise Networks," "Service Provider Networks," or "Data Center Networks," the most crucial element in any network design is "high availability and faster convergence." Convergence can be measured using the formula below:

Failure Detection + Event Propagation + Routing Process + FIB Update

High Availability and Faster Convergence both work together in a way that faster the convergence higher the availability. A great example that one can take is of an e-commerce company like Amazon.com, if Amazon.com becomes unreachable for 5 minutes from his customers, how much bad impact (financial and reputation) does it make. Sub-Second convergence is what is needed when you are using VoIP in the network as VoIP uses User Datagram Protocol (UDP) for transporting Voice and Video traffic and delay can end the Voice or Video connection instantly. On the other hand, High Availability is measured using the following formula.

Availability = (MTBF-MTTR)/MTBF
where **MTBF** is mean time between failure means "What, when, why and how does it fail ?" and **MTTR** is mean time to repair means "How long does it take to fix ?"



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

Figure 1.1: High Availability Measurement Table

Above high availability measurement table shows availability of networks in terms of percentage and downtime per year and in today's network era, 99.999% and 99.9999% are termed as highly available networks.

A highly available or predictive network needs to have:
- There should not be single points of failures.
- Fault, performance and workflow process tools.
- Excellent consistency is needed with Hardware, Software, Configuration and design.
- Consistent processes for fault, security and performance.

High Availability and Faster Convergence Techniques:

Virtual Router Redundancy Protocol
VRRP is an open standard high availability protocol defined in IETF RFC 3768 defines a First-Hop Redundancy Protocol in which one router acts a Master, and other acts as Backup. A virtual IP and MAC is shared among Master and Backup Routers, which is used as a gateway address for end-points. By default, VRRP provides 3 seconds convergence from primary link to secondary link, in case of primary link or primary router failure. Example showing VRRP deployment is given below:

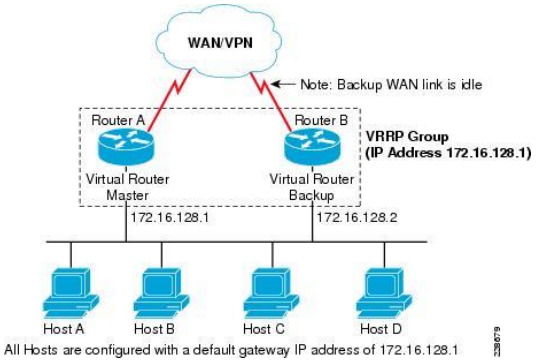


Figure 2.1: VRRP Deployment

Link Aggregation Channel Protocol

Defined in IEEE802.3ad, LACP is a protocol used to create Ether Channels. LACP packets are exchanged by switches over an Ether Channel. With LACP Ether Channel, we can bundle from 2 to 8 physical links to a single logical link, which can provide all-all forwarding links even in Layer 2 Networks. Load Sharing is done with hashing algorithm. If for load sharing algorithm, only source address, or source port address is used, then switch forwards each frame by using only single low-order bit. XOR operation is performed in case when two Addresses or Port Numbers are used. Example of LACP is shown is figure below:

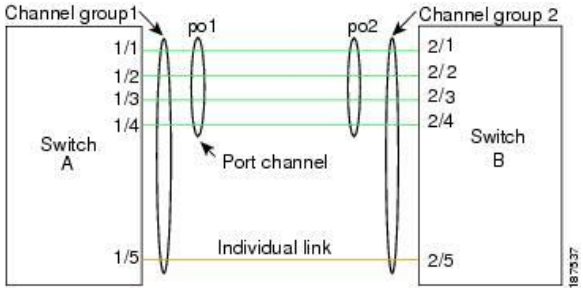


Figure 2.2: Link Aggregation example

IP Event Dampening

It prevents routing protocol churn which is caused by constant interface state changes taking lots of CPU resources. It is supported by static routing and all the dynamic routing protocols like RIP, EIGRP, OSPF, IS-IS, BGP. It also supports HSRP. It cannot be applied on sub-interfaces and can work on physical interfaces only. IP event dampening has taken the idea from route-flap dampening feature of BGP. When applied on interfaces, it tracks interface flapping or state change, and applies penalty to the flapping interface and if the penalty reaches threshold tolerance, then it put the interface in down state and if penalty is decreased below threshold level, then it brings interface to UP state again.

Bidirectional Forwarding Detection

BFD is a lightweight hello protocol. BFP runs in distributed manner and can scale to lower number of hello intervals and higher number of sessions. Any routing protocol like EIGRP, OSPF, BGP etc integrated with BFD and is notified as soon as BFD recognizes a neighbor loss. Normally, when a failure occurs in the L2 bridged network, L3 routers rely on routing protocol timers to detect the failures, but with BFD, it can be detected in less than a second. Figure below shows a scenario where BFD can be used:

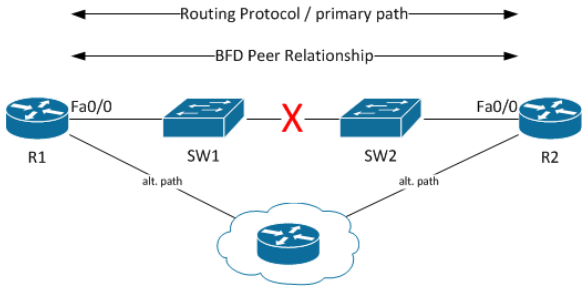


Figure 2.3 - Bi-directional Forwarding Detection Example

LSA Group Pacing:

OSPF produce large bursts of LSA Flooding traffic every 30 minutes, while individual aging do fragmentary re-flooding. LSA group pacing feature would help in controlled bursting. For example if we change the group pacing timer to 10 minutes, small batches of LSAs that are close to be aged-out are processed together. A figure below shows LSA group pacing effect:

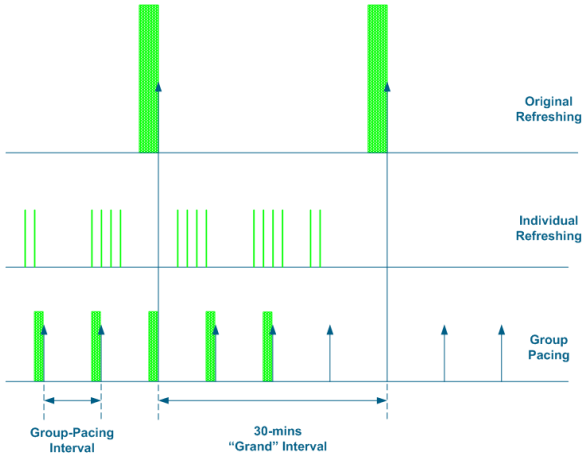


Figure 2.4: LSA Group Pacing in OSPF

2. Literature Survey

MPLS Traffic Engineering – Fast Reroute [1] by Shuguftha Naveed, S. Vinay Kumar of Vasavi College of Engineering (Osmania University), Hyderabad in May, 2014 under IJSR – ISSN: 2319-7064 draws a conclusion that in the event of link failure, traditional recovery technologies takes unacceptable time in case of VoIP and Video based critical solutions, while MPLS traffic engineering Fast Reroute meets the requirements of real-time applications with fast recovery that facilitate high availability to converge. The research shows that MPLS Fast Reroute method provides great performance in case of link failure as compared with traditional IP networks.

Virtual Router Redundancy Protocol (VRRP) [2] by R. Hinden, Ed. Of Nokia in Internet Engineering Task Force – RFC 3768 defines a First-Hop Redundancy Protocol in which one router acts a Master, and other acts as Backup. A virtual IP and MAC is shared among Master and Backup Routers, which is used as a gateway address for end-points.

Fast Reroute Extensions to RSVP-TE for LSP Tunnels [3] by P. Pan, Ed. Of Hammerhead Systems, G. Swallow, Ed. Of Cisco Systems and A. Atlas, Ed. Of Avici Systems in IETF RFC 4090 defines RSVP-TE extensions to establish backup

label-switched path (LSP) tunnels for local repair of LSP tunnels. These mechanisms enable the re-direction of traffic onto backup LSP tunnels in 10s of milliseconds, in th event of failure.

Survey on the RIP, OSPF, EIGRP Routing Protocols [4] by V. Vetriselvan et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2), 2014, 1058-1065, specifies a performance evaluation of various routing protocols with certain criteria's like Jitter, Convergence Time, end to end delay.

Bidirectional Forwarding Detection (BFD) [5] by D. Katz and D. Ward of Juniper Networks in IETF RFC 5880 describes a protocol intended to detect faults in the bidirectional path between two forwarding engines, including interfaces, data link(s), and to the extent possible the forwarding engines themselves, with potentially very low latency. It operates independently of media, data protocols, and routing protocols. Bidirectional Forwarding Detection (BFD) on Link Aggregation Group (LAG) Interfaces [6] 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 defines a mechanism to run Bidirectional Forwarding Detection (BFD) on Link Aggregation Group (LAG) interfaces.

Graceful OSPF Restart by J.Moy of Symacore Networks, P. Pillay-Esnault of Juniper Networks and A . Lindem of Redback Networks in IETF RFC 3623 [7] describes where an OSPF router can stay on the forwarding path even as its OSPF software is restarted. This process is called "graceful restart" or "non-stop forwarding".

3. Problem Definition

- High Availability in Networks is one of the major goals of every company. Large Downtime of network in a company creates big loss in companies (data centers, ISPs, Enterprises, E-commerce Companies). Various High availability protocols can be used, but all of them are used according to a specific network design. A specific set of protocols are used for different layers, all of them have different requirements, both economically and infrastructure wise.
- Same is the case with Faster convergence as if not properly implemented, the results can be severe.
- So designing a highly available and faster converging network is a very difficult task with set of different protocols trying to achieve the same.
- As world is diving towards VoIP and Video solutions, that needs high bandwidth and low delay, faster convergence has become much more important.

4. Objectives

- Comparative analysis of High Availability technologies and Faster Convergence Technologies (VRRP, LACP, FR, Tuning SPF Timers, LSA Pacing Timers, OSPF Fast Hello Mechanism, Graceful Restart, IP Event Dampening, Bi-direction Forwarding Detection) will be done.
- Selection of best High Availability and Faster Convergence method in Medium to Large Service Providers.
- Selection of best High availability and faster convergence methods that generates minimum delay for VoIP based networks
- Tools that will be used are Graphic Network Simulator (GNS3), Wireshark Packet Analyzer and Cisco 2821, 1841 series routers will be used.

5. Results

Faster Convergence with VRRP -
VRRP comes under category of first hop redundancy protocol provides default gateway redundancy. As we all know, we can give only a single default-gateway in our LAN Card to reach Internet or External Network.

Now, suppose we are large organization with 1000 employees Working in our branch office, For Internet Services, we have taken services from ISP, and for high availability at our end, we have used two internet routers connected with ISP.

One with Internal IP – 10.1.1.1
Other with Internal IP – 10.1.1.2,

500 employees are using 10.1.1.1 as Default-Gateway, and other 500 are using 10.1.1.2, now what if our Router with IP 10.1.1.1 goes down. What'll happen????

Even though the backup link is in working condition, but the gateway will not let them use the backup link, to use backup link, we need to change the default gateway on all the 500 machines, which is a very time consuming task and can create a large downtime.

Now that's where, VRRP comes for a rescue, What VRRP will do is, it'll help us create a Virtual IP, which can be shared between both the Internet Routers, and we'll give that Virtual IP as the default-gateway to our machines. Topology that we have used for testing Availability with VRRP is shown below:

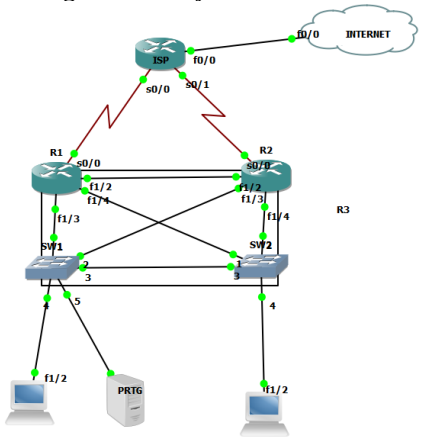


Figure 6.1- VRRP Topology used for testing

Above VRRP topology has two internet routers connected with ISP for redundant links, a virtual IP 10.1.1.10 is shared between Internet routers which is provided as default gateway to all the host machines.

Graph below shows the downtime from primary to backup link monitored by PRTG:

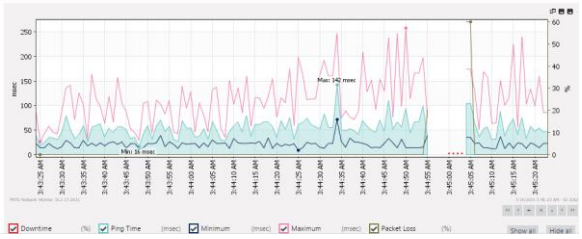


Figure 6.2: Convergence time between Primary to Backup link for Host machines

So the convergence time is around 8 seconds which is much faster in comparison with if we have to change default gateway on around 500 machines in the network manually. In this topology, we made R1 as Master by assigning with high priority of 110, and R2 as a Backup Router, having a default priority of 100, now if R1 to ISP link goes down, it will decrement the priority value of 110 to 95, as we have configured it that way, with which R2 will become master and becomes the gateway. After R1 to ISP link goes down, the process from Master to backup is shown below:

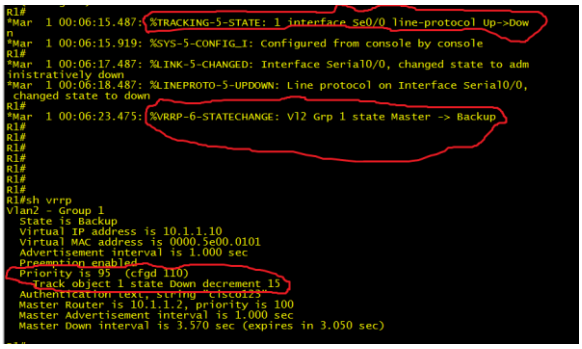


Figure 6.3: Output of master to backup conversion of a backup router.

Also the packets lost under VRRP is shown below with PRTG PC is having a continuous ping towards internet:

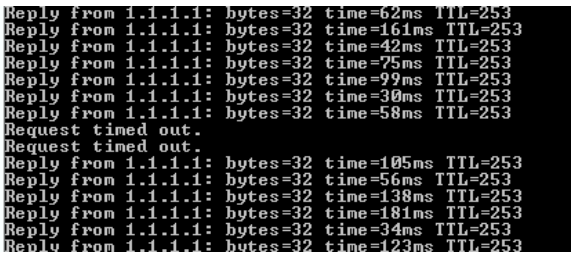


Figure 6.4: Data Packets lost with VRRP

Link Aggregation Channel Protocol

LACP is used to increase bandwidth and link redundancy, with LACP we can bundle from 2 to 16 physical links to a single logical channel. Atmost 8 links will be active at a single time, and others will become standby.

Topology used for LACP is shown below:

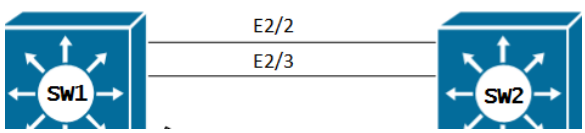


Figure 6.5: LACP Topology

In the above topology, two Ethernet physical links are bundled in a single logical channel, creating a 20 Mbps logical channel and also provides redundancy with active-active links. A port-channel is created with these links e2/2 and 2/3. Output showing port-channel is shown below:

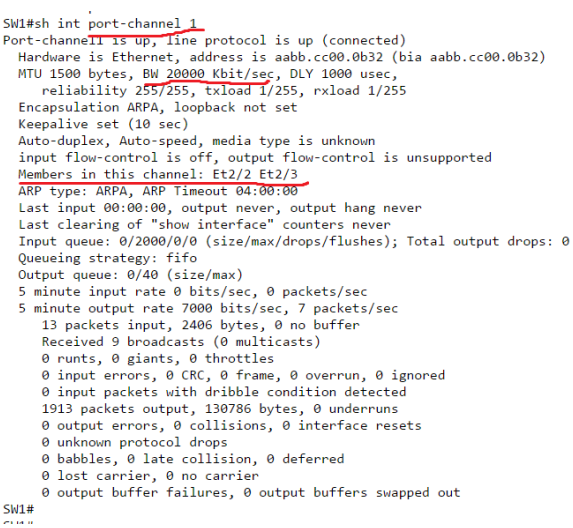


Figure 6.6: Port-channel and Bundled Physical Ports

LACP uses XOR based algorithm to load-balance traffic between multiple physical links. I used Src-Dst-IP based algorithm. Also more output grabbed from a Cisco Switch is shown below:

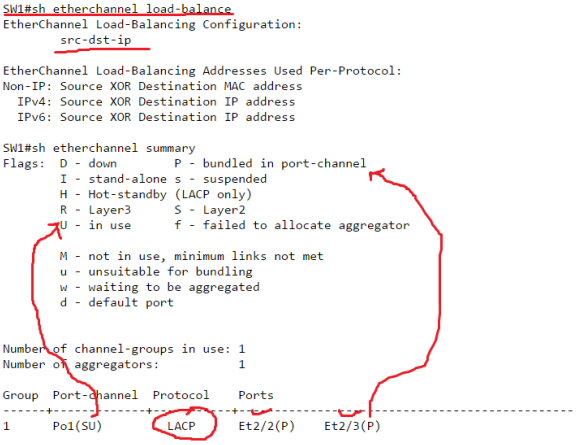


Figure 6.7: Load-Balance and LACP etherchannel output

Now if the traffic from Source to Destination is going from the e2/2 link, and the e2/2 link goes down, then traffic will shift from e2/2 to e2/3 straightway.

Bidirectional Forwarding Detection (BFD) -

BFD provides fall hellos at Layer 2.5. The main purpose is to use a single fast-hello to check if adjacent neighbor is present or not. Routing Protocols can be made to converge in much faster way with BFD. They are mainly helpful when we have two routers having a Layer 3 adjacency with any routing protocol say like OSPF, EIGRP, IS-IS, BGP etc and both the routers are connected with the help of a L2 network inbetween them like the topology we have used :

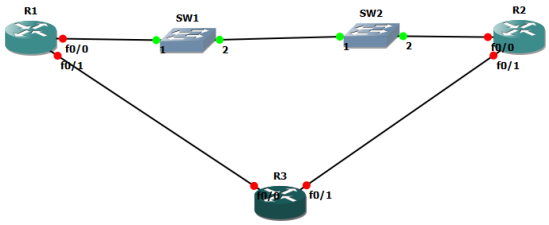


Figure 6.8: BFD Topology for testing

In the above topology, R1 and R2 are having neighborship with two switches coming inbetween them. R1 and R2 also has another path via R3 with which they can connect and share the routes. I have used OSPF in the topology. First i have dropped the link between SW1 and SW2

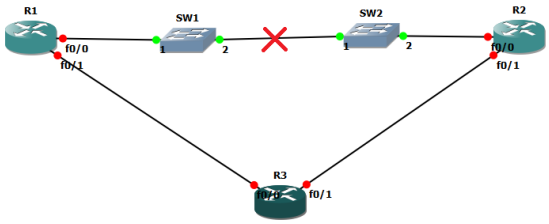


Figure 6.9: L2 link down between Routers

When link between SW1 and SW2 link goes down, R1 and R2 will have a downtime of around 40 seconds or i can say the dead timer assigned to OSPF routers. Resulted graph is shown below:

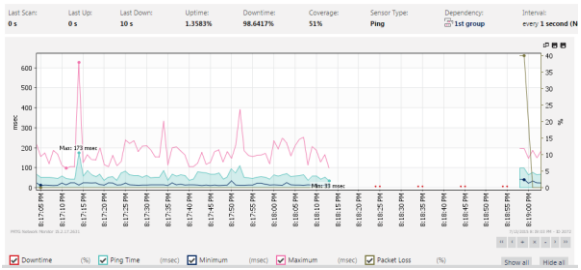


Figure 6.10: Routing Protocol Convergence without BFD with L2 link between Routers.

With BFD got applied in the routers and on interfaces of Routers R1 and R2, result is shown below:

Figure 6.11: Convergence with BFD

Not a single packet loss happened with BiDirectional Forwarding Detection is used in the network. Above output shows, that in the continuous ping, i have plugged out the cable between the two switches or we can say that the L2 link goes down while traffic is going between R1 and R2, and zero downtime occurs, which is quite good when compared to downtime of 40 seconds.

Tuning SPF Timers -

SPF is the algorithm used in Link State routing protocols, Service Provider Networks uses only Link State routing protocols for their IGP routing, so for faster convergence between Core of Service Provider, we can tune the SPF timers , in order to converge at much better speed. Three timers that are tuned with SPF tuning are spf-start, which is the initial SPF schedule delay in milliseconds, spf-hold, which is the minimum hold-time between two successive SPF calculations, spf-max-wait, which is the maximum wait time between two SPF calculations. I have used a MPLS topology of service provider to test SPF tuning in Service Provider, Topology is shown below:

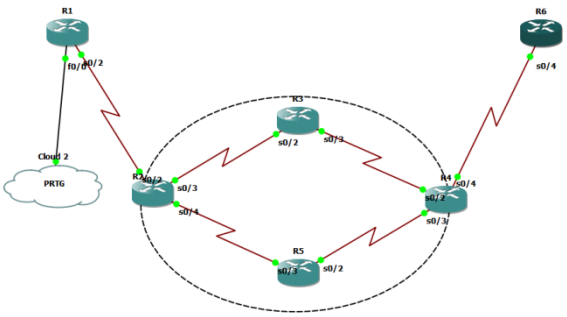


Figure 6.12: MPLS Topology used in testing

In the above topology, we are sending data traffic from Cloud (PRTG) to R6, traffic is using the path Cloud-R1-R2-R5-R4-R6 as the primary path, when link between R2 and R5 goes down, the convergence time between default parameters is shown below:

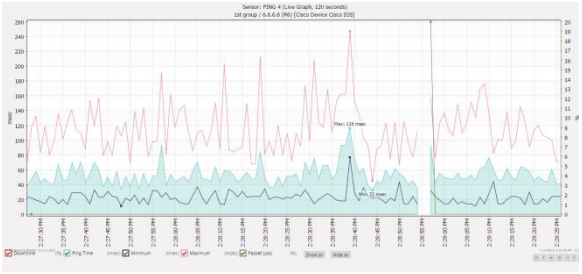


Figure 6.13: MPLS Convergence time with default parameters.

After tuning SPF timers, the convergence time is shown below:

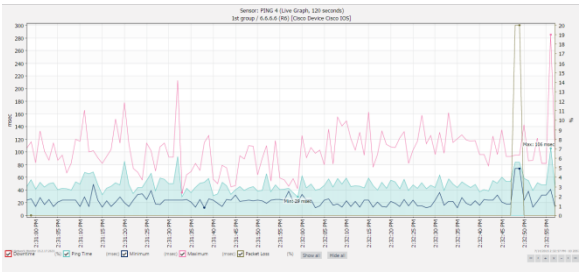


Figure 6.14: Convergence Time after SPF tuning

After SPF tuning convergence time drops down to milliseconds, which was around 3-4 seconds with default parameters.

6. Conclusion

The two main objectives of the network industry are high availability and faster convergence, which is necessary given

the volume of voice and video traffic that exists today. In my paper, I compared several protocols for faster convergence and high availability. Default Gateway redundancy is provided by VRRP, fast convergence is ensured in the event that two adjacent routers have Layer 2 links, redundant active-active physical links between switches are provided by LACP, and where Link State Routing protocols are used, fast convergence can be achieved by tuning SPF timers and the Fast-Hello mechanism.

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] Virtual Router Redundancy Protocol (VRRP) by R. Hinden, Ed. Of Nokia in Internet Engineering Task Force – RFC 3768
[3] 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
[4] 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
[5] Bidirectional Forwarding Detection (BFD) by D. Katz and D. Ward of Juniper Networks in IETF RFC 5880.
[6] 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
[7] Graceful OSPF Restart by J.Moy of Symacore Networks, P. Pillay-Esnault of Juniper Networks and A. Lindem of Redback Networks in IETF RFC 3623.
[8] Ramanpreet Kaur, Anantdeep Kaur (2014), "Black Hole Detection In MANETs Using Different Techniques: A Survey", INTERNATIONAL JOURNAL FOR MULTI-DISCIPLINARY ENGINEERING & BUSINESS MANAGEMENT, Vol 2, No. 1, pp. 33-35.
[9] Sheetal, Kanamaljeet Singh Saini (2014), "A Secure and Energy Efficient AODV Protocol Using Reliable Delivery Models", INTERNATIONAL JOURNAL FOR MULTI-DISCIPLINARY ENGINEERING & BUSINESS MANAGEMENT, Vol 2, No. 3, pp. 51-56.
[10] Akanksha Gupta, Anuj Kumar Gupta (2014), "PROVIDING SECURITY TO WIRELESS SENSOR NETWORKS FROM WORMHOLES UTILIZING REACTIVE PROTOCOLS", INTERNATIONAL JOURNAL FOR MULTI-DISCIPLINARY ENGINEERING & BUSINESS MANAGEMENT, Vol 2, No. 3, pp. 138-144.