INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

(Volume2, Issue6)

Available online at: www.Ijariit.com

Behavior Analysis of OSPF and ISIS Routing Protocols with Service Provider Network

Vikasdeep Kaur[1]
CSE, PTU/ Bahra Group of Institutes
Patiala, Punjab, India
vickygosal_11@ymail.com

Jaspreet Kaur[2]
CSE, PTU/Bahra Group of Institutes
Patiala, Punjab, India
jaspreetkaur.rb@gmail.com

Harpreet Kaur[3]
CSE, PTU/Bahra Group of Institute
Patiala, Punjab, India
preet.harry11@gmail.com

Abstract: OSPF is mainly designed for IP networks from scratch and runs in almost all sorts of environments like enterprise, data centers, or service providers, while ISIS, which was mainly designed by ISO was not intended to run for IP based networks from scratch and IETF in the early 1990's adopted ISIS for its advantages. As a scalability purpose ISIS is better than OSPF, but when we have a large database or a large service provider, with only a single level design inside the service provider Both the routing protocols have different authentication mechanisms with ISIS providing key chain based mechanism and provides both plain-text and MD5 based integration with it, while OSPF also provide MD5 and SHA1 hashing based authentication when used with IPv6. Multiprotocol label switching technology (MPLS) is used to transfer the data in service provider network. Apart from Interconnecting Data Centers, L2VPNs are also used for Inter-AS service provider's connectivity and connecting various Enterprise Branch offices with each other. Selection of right L2VPN technology is very important as wrong technology can harm the network. The main focus of this technique to give the solutions for slow speed, quality of service, lack of traffic engineer, less security and problem in trouble shouting. The motive is to improve the speed, high security, easily trouble shoot, high quality in terms of packet transformation and better results for traffic engineering.

Keywords: MPLS, ISIS, OSPF, Dijkstra's Shortest Path algorithm, BGP, EIGRP.

I. Introduction

A) IP Routing: When using network packets are exchanged from one device to another device is known as routing. All the hosts in the internetwork the logical network address, such as IP addresses are configured after. Basically, two types of dynamic routing protocol in internet protocol based networks:

1.Interior Gateway Protocols – Interior gateway protocols are that protocols which are used within an autonomous system for IP routing.

2. Exterior Gateway Protocols – Exterior gateway protocols which are used to interact or share the routes between the different autonomous systems.

B) Distance Vector Protocol:

Distance vector protocols are based on two algorithms that are Bellman-Ford or Ford-Fulkerson. The distance vector protocols choose the best path to a remote network by judge the distance. To be the best route each time least number of hops (routers) is determined.

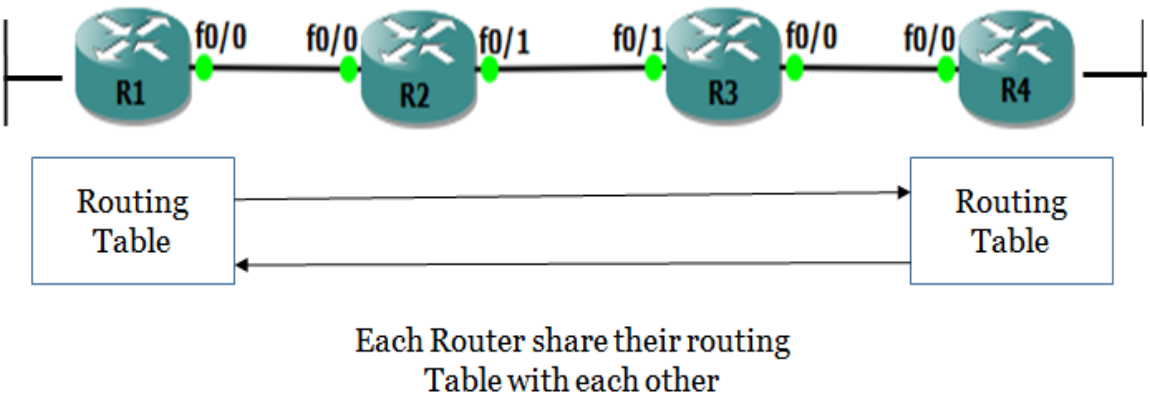

Figure 1: Distance vector routing protocol

C) Link State Routing Protocols:

Link State protocols are also called shortest path first (SPF) or distributed database protocols, are build approximately a well-known algorithm of graph theory, E.W. Dijkstra's shortest path first algorithm. In the form of Link State Advertisement (LSA) each router shares its link information. Link state information is used by a link state router to generate a topology map and in the topology to choose the finest path to the destination. SPF tree is then applied to the LSDB to reach the destination to find the best path and the best path is then added to the routing table.

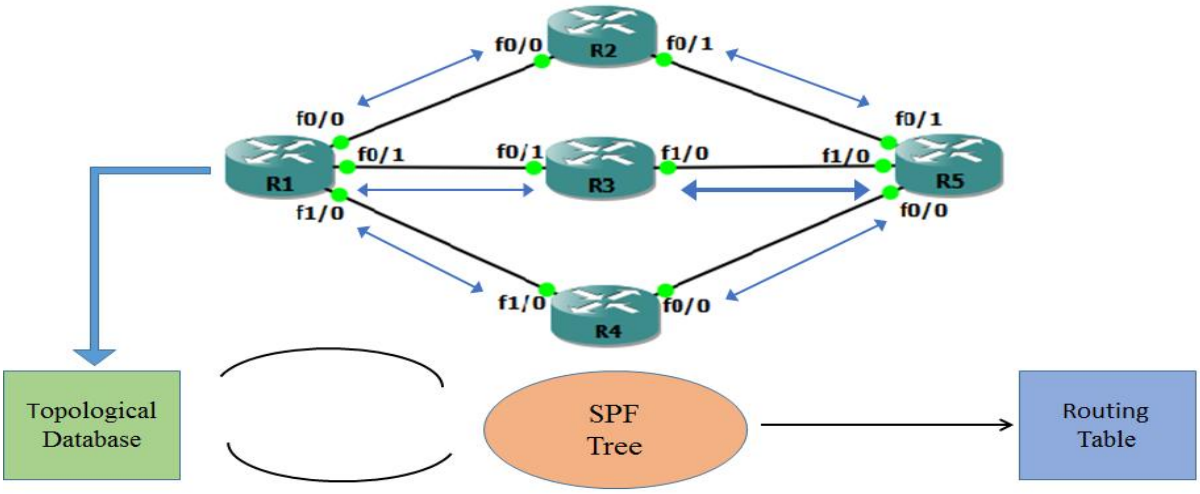

Figure 2: Example of SPF within Link State Protocols

II. MATERIAL and METHOD

Open Shortest Path First (OSPF):

OSPF is a type of link state routing protocol developed by IETF. It works for both with IPv4 and IPv6. IPv4 is used by OSPFv2 and IPv6 is used by OSPFv3. To find the best path from source to destination, OSPF uses Dijkstra's Shortest Path First Algorithm. OSPF has its own transport mechanism and OSPF does not use TCP or UDP. On the network OSPF packets are exchanged only between the neighbor devices. Networks defined within areas in OSPF. With area 0 it creates a hierarchical type of design, acting as the backbone area without non-backbone area can connect with each other by default.

Intermediate-System-to-Intermediate-System (IS-IS):

IS-IS is a type of link state routing protocol which uses same algorithm as OSPF. It is created by ISO and uses by default CLNP addressing. Recently ISIS mainly uses IP addressing but CLNP addresses are also required to be in routing process.To exchange protocol information, IS-IS uses PDUs (Protocol Data Units). It is a part of CLNS stack, Integrated IS-IS is an IP extension of IS-IS and was not an IP protocol originally. It uses both IPv4 and IPv6. To find the best path, IS-IS uses Dijkstra's Shortest Path First algorithm.

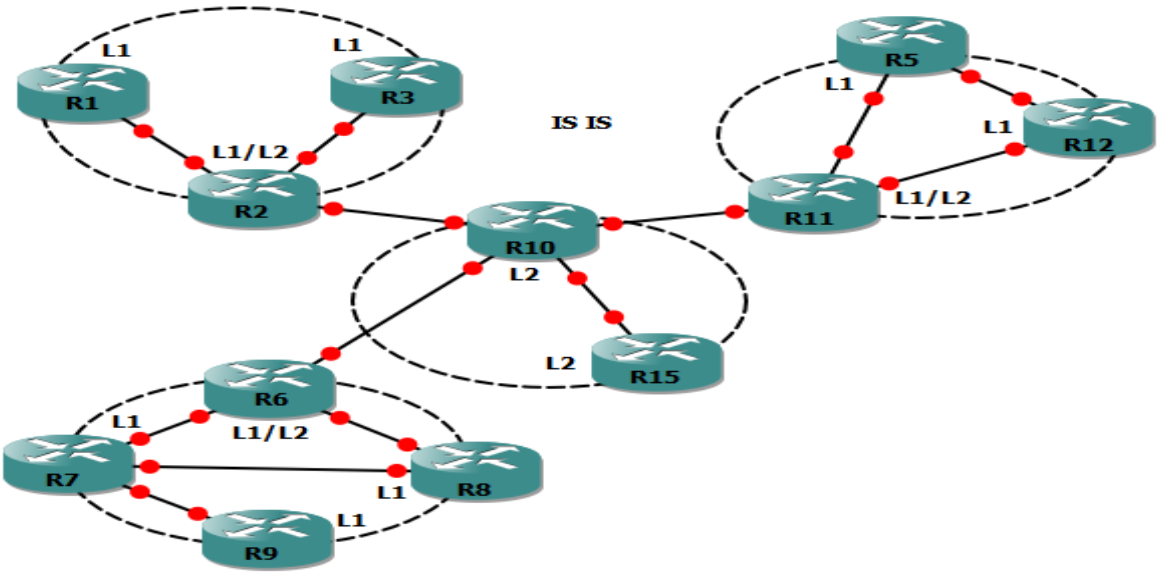

Figure 3: Basic Integrated IS-IS implementation

D) Multiprotocol label switching (MPLS):

The major technology that uses the labels to forward the packets is Multiprotocol Label switch (MPLS). Labels square measure connected to the packets. If the labeled packet does not reached from one provider edge router to completely different provider edge router then a label mapping does not complete.

Within the MPLS Label Distribution protocols are used for distribution of labels and replace the labels from one router to another router. Label Distribution Protocol (LDP) is that the defaulting and most usually used protocol, for distribution of labels. RSVP is employed to distribute the labels for Traffic Engineering. Multiprotocol Label Switch (MPLS) has the superior capability to promote traffic on the basis of labels rather than target (destination) informatics address that helps in removal of discrimination Border Gateway protocol (BGP) within the core of Service Provider networks.

E) Enhanced Interior Gateway Routing Protocol (EIGRP):

Enhanced Interior Gateway Routing Protocol (EIGRP) is a sophisticated distance-vector routing protocol that is used on a computer network for automating routing decisions and configuration. Partial capability of EIGRP changed into transformed to an open standard. EIGRP is used on a router to percentage routes with other routers in the equal self sufficient gadget. Unlike different well known routing protocols, along with RIP, EIGRP only sends incremental updates, decreasing the workload on the router and the quantity of data that wishes to be transmitted.

III. Literature Reviews

Amanpreet Kaur, Dinesh Kumar [] has represented OSPF and ISIS, utilize the similar algorithm to decide the finest (best) path. With default parameters ISIS behaves much better, and in 3 seconds it converges the network while OSPF takes around five seconds. When SPF timers are reduced to milliseconds then the convergence time also reduced to sub-second for both protocols. For security analysis, neighbor authentication passwords for secure allocation of IP packets between both the routing protocols have used.

C. Hopps [] it describes a technique for exchanging IPv6 routing information with the IS-IS routing protocol. To allot the essential IPv6 information during a routing domain this technique utilizes two new TLVs: reachability TLV and an interface address TLV.

*D. Oran []*has shown statistics change among structures IS to IS Intra-area routing change over protocol to be used together with the Protocol for provided that the Connectionless- mode community service technologies.

J. Moy [] represents implementation internally to a single Autonomous System. In Autonomous System's topology each OSPF router possesses an equal database. By construct a SP tree we can determine (calculate) a routing table from this database.

J. Moy, et al. [] has presented an improvement to the OSPF routing protocol and even as its OPSF software is re-executed OSPF router can continue on the forwarding path.

JP. Vasseur, etal.[] it describes the setup of a full network of Multi-Protocol Label Switching (MPLS) traffic Engineering (TE) Label Switched Paths (LSP) along with a fixed of Label switch Routers (LSR) is a regular place use state of interaction of MPLS traffic Engineering both for bandwidth optimization, bandwidth ensures or fast rerouting with MPLS rapid Reroute.

K. Ishiguro, etal. [] it describes extensions to OSPFv3 to retain intra-area traffic Engineering (TE). It extends OSPFv2 TE to address IPv6 networks. A new TLV and a number of new sub-TLVs are described to maintain IPv6 networks.

M. Chen, etal. [] it describes extensions to the OSPF version 2 and 3 protocols to maintain Multiprotocol Label Switching (MPLS) and Generalized MPLS (GMPLS) Traffic Engineering (TE) for multiple Autonomous Systems (ASes).

M. Shand, L. Ginsberg[] it describes a method for a restarting router to signal to its neighbors that it is restarting, allowing them to restore their adjacencies without cycling during the down state, whereas still appropriately initiating database synchronization.

P. Murphy [] has presented a non-compulsory kind of Open Shortest path First (OSPF) location this is reffered to as "not-so-stubby" area (or NSSA). NSSAs are connected to the accessible OPSF stub place configuration selection however has the extra capacity of importing AS external routes in an inadequate fashion.

P. Pillay-Esnault, A. Lindem [] it describes the OSPFv3 graceful restart. The OSPFv3 graceful restart is identical to that of OSPFv2. These differences include the format of the grace Link State Advertisements (LSAs) and other considerations.

R. Callon [] has provided an integrated routing protocol, on the basis of OSI Intra-domain IS-IS Routing Protocol, which may be utilized as an IGP to keep TCP/IP in addition to OSI. This allows a single routing protocol to be used to assist pure IP environments, pure OSI environments, and dual environments.

R. Coltun, et al. [] has presented the modifications to OSPF to help version 6 of the internet Protocol (IPv6). The basic mechanisms of OSPF (flooding, targeted Router (DR) election, area aid, SPF calculations, and so forth.

T. Li, H. Smit [] has offered extensions to the Intermediate device to report Intermediate machine (IS-IS) protocol to keep up traffic Engineering (TE). This extends the IS-IS protocol with the aid of specifying latest information that an Intermediate gadget (router) can set in link state Protocol data units (LSP).

IV. Objectives

Check the performance related terms, speed, security, scalability, Quality of service (QoS), and their role in traffic engineering and various case studies will be done:

To determine the performance of IS-IS and OSPF routing protocols into the service provider network.

To determine the scalability of IS-IS and OSPF routing protocols into the service provider network.

To determine the security of IS-IS and OSPF routing protocols into the service provider network.

To determine which the best Link State routing protocol is, when it comes to work in ISPs MPLS backbone according to their network design.

V. Methodology/ Planning of Work

To revise (observe) a spread of Layer 2 MPLS preferred document that are used with varied companies on the same time as developing their devices and network working machine.

Imposing OSPF, IS-ARE protocols and MPLS technologies in simulation surroundings and draw conclusions based on an expansion of parameters.

Implementation of all of the parameters of OSPF, IS-IS protocols and MPLS on real Cisco devices and an end may be drawn from the output.

A deep packet assessment will be made via evaluating the phrases of OSPF, IS-IS protocols and MPLS the usage of Wire shark visitors Analyzer.

For monitoring functions, simple network management Protocol (SNMP) might be used among network monitoring device and Routers/Switches.

A tracking tool like Paessler Router traffic Grapher (PRTG) can be used to draw output graphs in order to help us comparing exceptional outputs.

VI. Result and Discussion

Performance Analysis of OSPF and ISIS protocol using default parameters:

OSPF and ISIS are the two link state routing protocols used in Service Provider Industry. Both are used inside the service provider for internal routing purposes. In both these routing protocols, one of the common thing is the algorithm they use, i.e. Dijkstra's Shortest Path First Algorithm. Service Providers mainly use single area OSPF or ISIS design to reduce the complexity and for better traffic engineering results. A service provider topology running MPLS in the core with OSPF as the interior gateway routing protocol is show below in figure taken from Graphic Network Simulator:

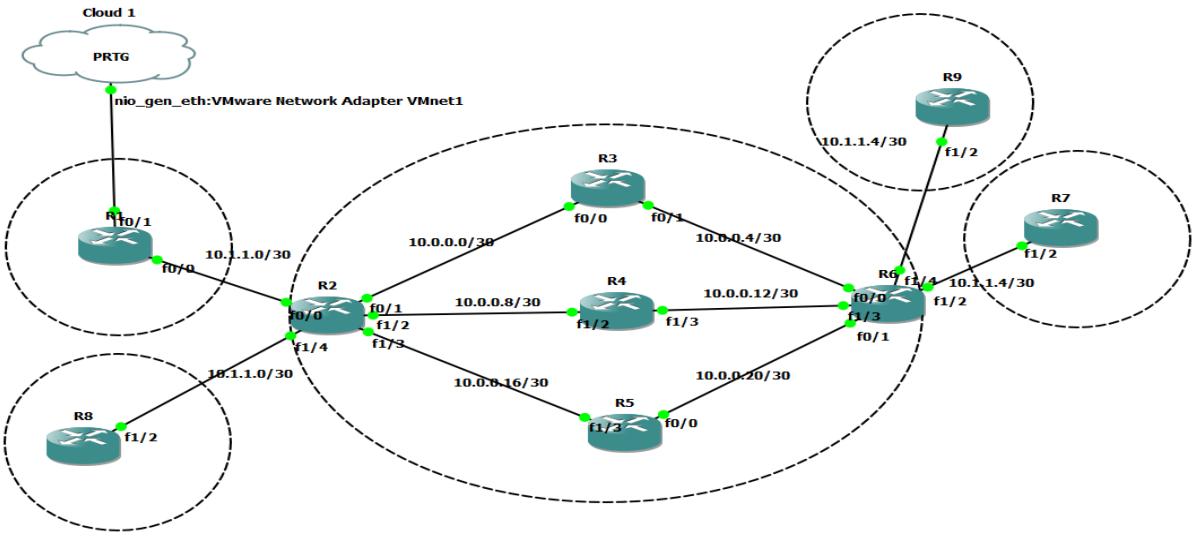

Figure 4 : MPLS Backbone Network with OSPF running in the service provider

In the above topology, Routers R2-R3-R4-R5-R6 are running in the service provider. R2 and R6 are the provider edge routers connected with the Customer Edge devices i.e. R1-R9-R8-R7. R3-R4-R5 are the provider routers. All the routers running inside service provider are running MPLS and OSPF is used as the interior gateway routing protocol for routing inside service provider. MP-BGP is running from Provider Edge to other Provider Edge for Customer VPN routes. R1 is sending the traffic towards R9 over the service provider, Service provider has three provider links, out of which it is sending traffic via R1-R4-R6, and when the link between R1 and R4 goes down, all the traffic is shifted to the other link. With no parameter or any other change in the protocol, below is the graph taken via PRTG that is showing the convergence time and delay:-

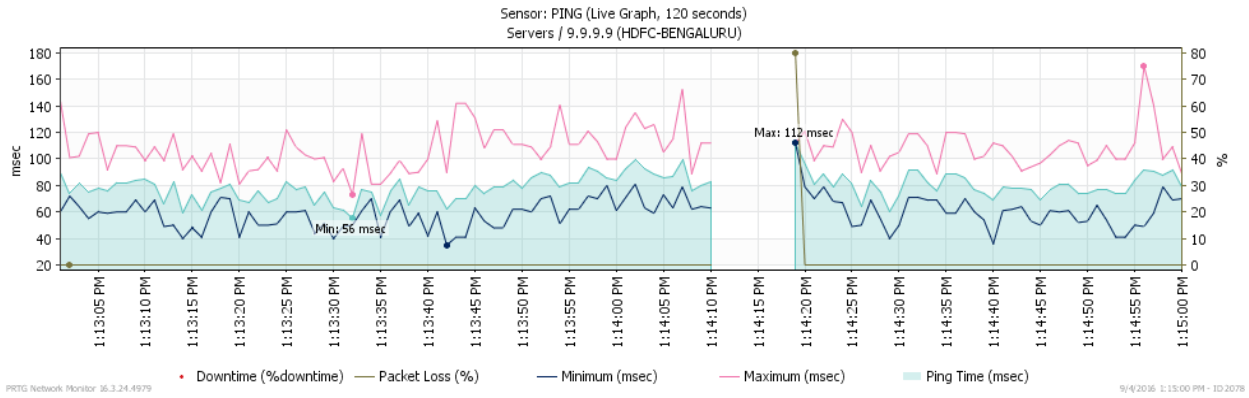

Figure 5 : PRTG Graph shows the amount of time it takes to converge the link from primary to secondary link

Above graph shows that during convergence from one link to another, OSPF takes around 9 seconds when running inside an MPLS service provider environment. This amount of convergence time is huge when we talk about service provider networks. It can easily destroy any real time applications of the customer like VoIP. Maximum delay is 112 msec and minimum delay is 56 msec.

ISIS is also used in large extent in service provider networks, It is created by ISO and in not intended for IP based networks when first created, but with the popularity of IP based networks in early 1990s, ISIS is also extended for IP by IETF and is called Integrated ISIS. Same topology as used in OSPF based service provider topology is used with ISIS in service provider networks, the only change in the topology is that ISIS is used in place of OSPF in Service Provider. Below is the topology running MPLS Backbone Service Provider network with ISIS running inside the service provider:-

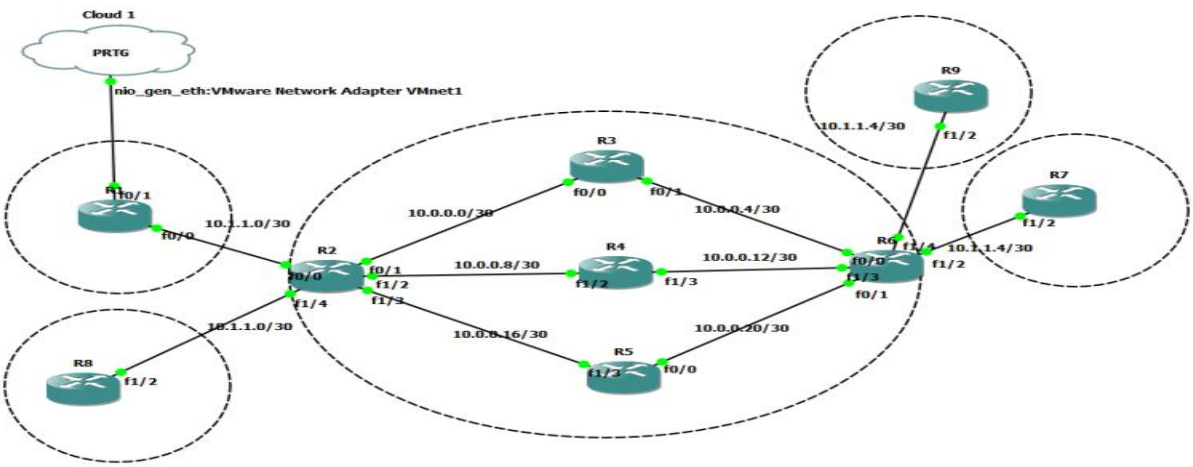

Figure 6 : Integrated IS-IS Topology

In the above topology, all the traffic from one customer site to other customer site is going via R2-R5-R6, and when the link between R2-R5 goes down, the time taken for traffic shift from one link to another is around 6 seconds, but still it is not up to the standards of the service providers, as it is also not great for real time applications like VoIP. So all in all what we saw till now is that without changing any parameters related to timers or the algorithm, a service provider cannot traverse real time application traffic over its environment, the graph showing convergence time taken by to shift the traffic from primary to backup link is shown below :-

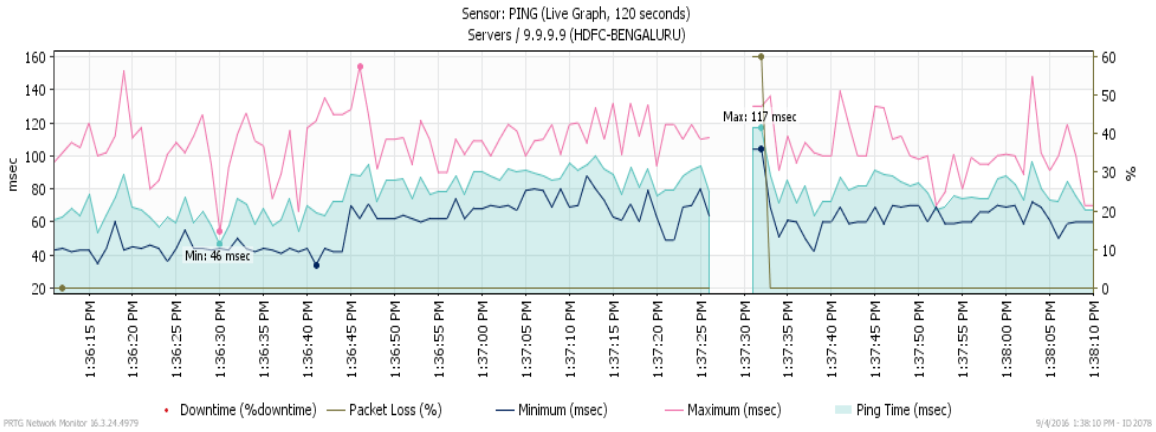

Figure 7 : IS-IS Convergence time graph in PRTG

Now as shown above, IS-IS gives much lesser downtime as compared to OSPF.

IS-IS, when use same area for its entire network has a much lesser convergence time by default, i.e. 6 seconds. IS-IS protocol supports a two level hierarchy to scale routing in large networks.

Table 1: Displays default convergence difference between ISIS and OSPF

Protocol	Convergence Time	Maximum Delay	Minimum Delay
OSPF	9 seconds	112 msec	56 msec
Int. IS-IS	6 seconds	117 msec	46 msec

As we can see in the above table, 9 seconds and 6 seconds are the convergence time that OSPF and IS-IS can have with default parameters, in case if the primary link goes down and convergence needs to happen towards Backup Link. As both OSPF and ISIS runs Dijkstra's SPF algorithm, what I have done in this topology is that I tuned the algorithm to calculate at much faster rate than the normal, which have produced significant improvement in the convergence time of OSPF and ISIS routing protocol, that one can see in the resulted graph shown below:-

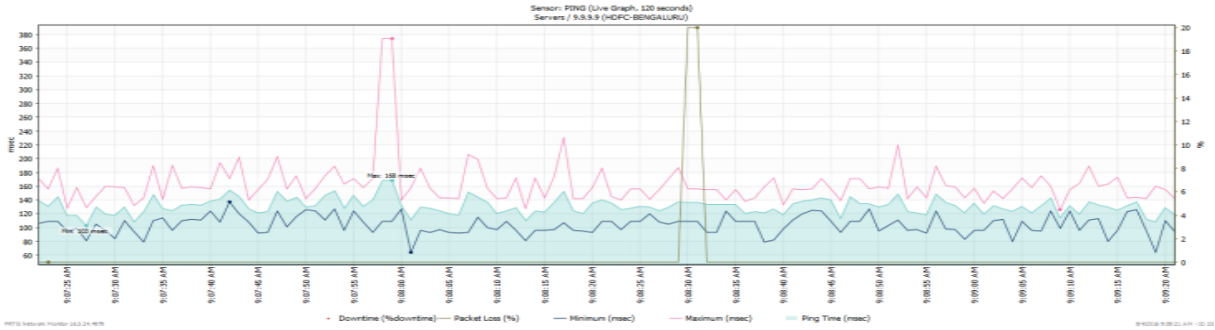

Figure 8 : OSPF Convergence Time after fasten the process of Dijkstra's SPF Algorithm

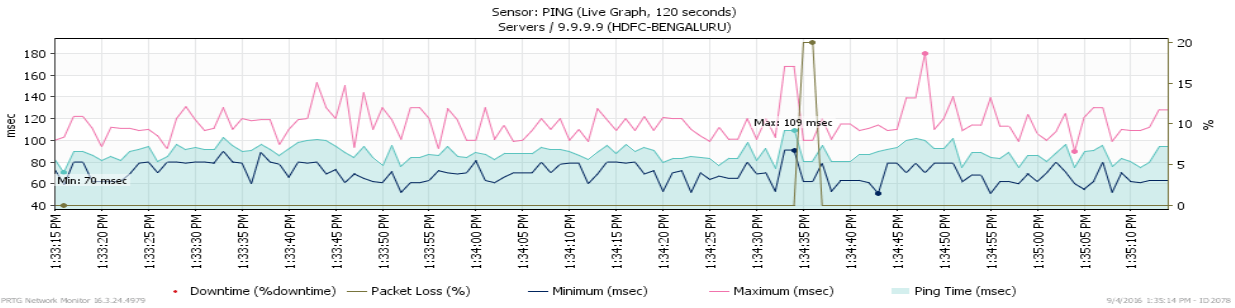

Figure 9 : ISIS Convergence Time after fasten the process of Dijkstra's SPF Algorithm

As we can see from the above graph, after tuning Dijkstra Algorithm, convergence time has decreased to sub-second, which is much better than the default timers. Both ISIS and OSPF can give sub-second convergence after tuning SPF timers.

Table 2: Display convergence time difference between OSPF and ISIS

Protocol	Convergence Time (Default Parameters)	Convergence Time (With SPF timers tuned)
OSPF	9	Sub-Second
ISIS	6	Sub-Second

Scalability Analysis of OSPF and IS-IS Protocol:

Scalability is one of the largest parameter in the service provider networks as service provider networks are large and are always expanding. Average CPU load that one protocol uses is a important process. Below is the processes that OSPF uses when running in service provider network from a provider router :-

```
AIRTEL-P2#sh processes cpu | sec OSPF|SPF|LSA|LSU
  3          60         286         209  0.16%  0.01%  0.00%   0 OSPF-1 Hello
 53           0           1           0  0.00%  0.00%  0.00%   0 DSPFARM DSP READ
129         292         604         483  1.88%  0.15%  0.03%   0 OSPF-1 Router
AIRTEL-P2#
```

Figure 10: OSPF Processes runs on Service Provider Router

In the above output taken from Cisco 1841 series router, I have filtered my output and only processes running OSPF are shown. Below is the same output when we are running ISIS in the topology of the service provider network:-


```
AIRTEL-P3#
AIRTEL-P3#show process cpu | sec ISIS
   3        2768       7497         369  0.08%  0.06%  0.08%   0 ISIS Adj
 158        2408       3596         669  0.00%  0.05%  0.05%   0 ISIS Upd
AIRTEL-P3#
AIRTEL-P3#
```

Figure 11: ISIS Processes runs on Service Provider Router

As you can see that ISIS uses less resource when compared with OSPF in normal circumstances. ISIS Adj is the process that sends hello packets to the neighboring routers running ISIS and ISIS Upd is the process that is used to send the updates that router has any of ISIS to the neighboring ISIS devices.

Both the routing protocols shares the routes between the neighboring devices in the form of LSA(Link State Advertisement) and LSPdu(Link State Protocol Data Unit). Both protocols uses SPF and creates a database table that holds the Link State database created by the routing table. ISIS divides database in two forms, one is LEVEL 1 and other is LEVEL 2, Only the routers that are at the edge of any area have to run both L1/L2, all the internal routers inside the area can run only L1 and routes coming from other areas then cannot enter the LK1 only area and a default route is originated at the L1/L2 edge routes which is at the edge of the area, that helps in reducing the size of database table of ISIS and automatically reduces the routing table size by having all the routes from other areas reached via a single default route, but this cannot be done if the area is a transit area, otherwise that area becomes the black hole for all the traffic. For all the areas that are not transit, this results in reduced size of routing and database table. Below is the output of ISIS database table taken from Cisco Router running in service provider network :-

```
R5
AIRTEL-P3#sh isis database detail

IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
AIRTEL-PE-DELH.00-00  0x0000000F   0x298F        435               0/0/0
  Area Address: 49.0000
  NLPID:        0xCC
  Hostname: AIRTEL-PE-DELHI
  IP Address:   2.2.2.2
  Metric: 10         IP 10.0.0.0 255.255.255.252
  Metric: 10         IP 10.0.0.8 255.255.255.252
  Metric: 10         IP 10.0.0.16 255.255.255.252
  Metric: 10         IP 2.2.2.2 255.255.255.255
  Metric: 10         IS AIRTEL-P2.01
  Metric: 10         IS AIRTEL-P3.01
AIRTEL-P1.00-00       0x00000009   0x6BE4        394               0/0/0
  Area Address: 49.0000
  NLPID:        0xCC
  Hostname: AIRTEL-P1
  IP Address:   3.3.3.3
  Metric: 10         IP 10.0.0.4 255.255.255.252
  Metric: 10         IP 3.3.3.3 255.255.255.255
  Metric: 10         IS AIRTEL_PE_BENG.01
AIRTEL-P2.00-00       0x0000000D   0x2273        974               0/0/0
  Area Address: 49.0000
  NLPID:        0xCC
  Hostname: AIRTEL-P2
  IP Address:   4.4.4.4
  Metric: 10         IP 10.0.0.8 255.255.255.252
  Metric: 10         IP 10.0.0.12 255.255.255.252
  Metric: 10         IP 4.4.4.4 255.255.255.255
  Metric: 10         IS AIRTEL-P2.01
AIRTEL-P2.01-00       0x00000006   0x99AD        1006              0/0/0
  Metric: 0          IS AIRTEL-P2.00
  Metric: 0          IS AIRTEL-PE-DELH.00
AIRTEL-P3.00-00     * 0x00000009   0x07D7        950               0/0/0
  Area Address: 49.0000
  NLPID:        0xCC
  Hostname: AIRTEL-P3
  IP Address:   5.5.5.5
  Metric: 10         IP 10.0.0.20 255.255.255.252
  Metric: 10         IP 10.0.0.16 255.255.255.252
  Metric: 10         IP 5.5.5.5 255.255.255.255
 --More--
```

Figure 12 : Output of ISIS Database in Cisco Router

In ISIS, as there are two types of routes, L1 and L2, if we create both L1/L2 neighbor ship between the routers, then the database table gets increase in size, otherwise if we use only L1 in our inside network, then it behaves like a stub zone and does not add any L2 LSPdu'sthat helps in reducing the size of database table. On the other hand when we see the OSPF database table, it has different types of LSAs present inside the OSPF database table. It is little bit complex than ISIS which has only two types of LSPdu's. OSPF

does not have the stub like feature by default as it is in ISIS; we have to explicitly configure it to reduce the size of LSA database of OSPF. OSPF has 11 types of LSAs and all of them represent different features with different scope levels. Below is the output of OSPF database table in Cisco Router:-

```
AIRTEL-P2#show ip ospf  database rou
AIRTEL-P2#show ip ospf  database router

            OSPF Router with ID (4.4.4.4) (Process ID 1)

                Router Link States (Area 0)

  LS age: 180
  Options: (No TOS-capability, DC)
  LS Type: Router Links
  Link State ID: 2.2.2.2
  Advertising Router: 2.2.2.2
  LS Seq Number: 80000006
  Checksum: 0x3EC8
  Length: 72
  Number of Links: 4

    Link connected to: a Stub Network
     (Link ID) Network/subnet number: 2.2.2.2
     (Link Data) Network Mask: 255.255.255.255
      Number of TOS metrics: 0
       TOS 0 Metrics: 1

    Link connected to: a Transit Network
     (Link ID) Designated Router address: 10.0.0.18
     (Link Data) Router Interface address: 10.0.0.17
      Number of TOS metrics: 0
       TOS 0 Metrics: 1

    Link connected to: a Transit Network
     (Link ID) Designated Router address: 10.0.0.9
     (Link Data) Router Interface address: 10.0.0.9
      Number of TOS metrics: 0
       TOS 0 Metrics: 97

    Link connected to: a Transit Network
     (Link ID) Designated Router address: 10.0.0.2
     (Link Data) Router Interface address: 10.0.0.1
      Number of TOS metrics: 0
       TOS 0 Metrics: 10

 --More--
```

Figure 13: Output of OSPF Database in Cisco Router

All in all, when we talk about scalability within link state routing protocols, ISIS is better when we compared with OSPF. For larger service provider networks, ISIS performs much better with functionality like shorter database table.

Security Analysis of Link State Routing Protocols:

Routers running Link State Routing Protocols when share link state information with neighbor routers, needed to be secured which can be done with the help of authentication between routers acting as neighbors. Routes can be shared between the routers running OSPF or ISIS only if passwords on both the ends match. OSPF and ISIS, both uses both plain-text and MD5 based hashing mechanism. OSPF, when used with IPv6 have multiple options with hashing mechanism, i.e. MD5 and SHA1 can be used to protect the route or link state information sharing. To secure IP traffic in the best possible manner, IPSec can be used to secure both IPv4 and IPv6 data traversing over the network. When using IPSec, between the Provider Edge devices to secure the traffic over the service provider, there is little burden that we put on the provider edge devices as they will have to do extra processing by encrypting and decrypting packets which are formerly sent with plain text. Below is the snapshot taken after configuring IPSec from PE-PE devices :-

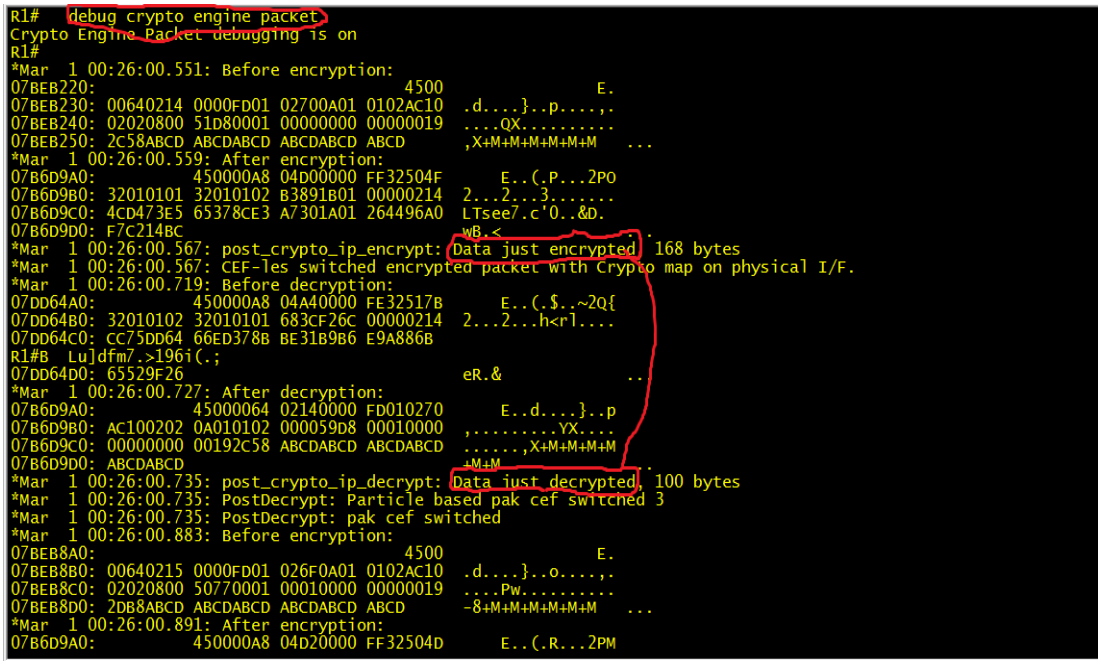

Figure 14 : IP Traffic flow between service provider after applying IPSec

Table 3: Performance table of Link State Routing Protocols

Protocol	Convergence Time	Maximum Delay	Minimum Delay
OSPF	9 seconds	112 msec	56 msec
Integrated IS-IS	6 seconds	117 msec	46 msec
OSPF	Sub-Seconds	104 msec	49msec
Integrated IS-IS	Sub-Seconds	109 msec	40 msec

VII. Conclusion

OSPF and ISIS, both are the protocols in the link state routing category and the most used routing protocols for the internal routing purpose in the service provider networks. Both these protocols use the Dijkstra's SPF algorithm. OSPF is mainly designed for IP networks from scratch and runs in almost all sorts of environments like enterprise, data centers, or service providers, while ISIS, which was mainly designed by ISO was not intended to run for IP based networks from scratch and IETF in the early 1990's adopted ISIS for its advantages. Both ISIS and OSPF, when runs with default parameters, ISIS provides better performance than OSPF in terms of convergence and delay and when we enhance the dijkstra's algorithm to fasten the process, then both ISIS and OSPF provides sub-second convergence and minimal delay. On the basis of scalability also, ISIS is better than OSPF, but when we have a large database or a large service provider, with only a single level design inside the service provider. It consumes less CPU resources because in the time of route flapping, full SPF calculation is not done inside ISIS , like in OSPF. ISIS also is much easily extendable than OSPF. In terms of security, both the routing protocols have different authentication mechanisms with ISIS providing key chain based mechanism and provides both plain-text and MD5 based integration with it, while OSPF also provide MD5 and SHA1 hashing based authentication when used with IPv6. The best that one can do to achieve the security from one service provider edge to other is to use IPSEC.

Acknowledgement

This paper has been made possible through the constant encouragement and helps from my parents and guide. I would like to thank my guide Er. Jaspreet Kaur asstt. Professor of CSE deptt. And Er. Harpreet Kaur HOD and AP of CSE deptt. for their generous guidance, help and useful suggestions.

References

[1]Amanpreet Kaur, Dinesh Kumar,"*Comparative Analysis of Link State Routing Protocols OPSF and IS-IS"*,IJCST, vol-3, issue-4, july-aug 2015.

[2]C. Hopps, *"Routing IPv6 with IS-IS of Cisco Systems"*,IETF, RFC 5308, oct2008.

[3]D. Oran, *"OSI IS-IS Intra-domain Routing Protocol of Digital Equipment Corporation"*, IETF, RFC 1142, feb 1990.

[4]J. Harrison , J. Berger, M. Barlett*," IPv6 Traffic Engineering in IS-IS"*, IETF, RFC 6119, feb2011.

[5]J. Moy, *" OSPF Version 2"*,Internet Engineering Task Force(IETF), RFC 2328, 1998.

[6]J. Moy, P. Pillay-Esnault, A. Lindem, *" Graceful OSPF Restart"*, IETF, RFC 3623, nov2003.

[7]JP. Vasseur, Ed. , S. Previdi, P. Psenak, JL. Leroux, Ed., S. Yasukawa, P. Mabbey, *"Routing Extensions for Discovery of Multiprotocol (MPLS) Label Switch Router (LSR) Traffic Engineering (TE) Mesh Membership",*IETF, RFC 4972, july2007.

[8]K. Ishiguro, V. Manral, A. Davey, A. Lindem, Ed., *"Traffic Engineering Extensions to OSPF Version 3"*, IETF, RFC 5329, sept2008.

[9]M. Chen, R. Zhang, X. Duan, *"OSPF Extensions in Support of Inter-Autonomous System (AS) MPLS and GMPLS Traffic Engineering"*, IETF, RFC 5392, jan2009.

[10]M. Shand, L. Ginsberg, *"Restart Signaling for IS-IS"*, IETF, RFC 5306, oct2008.

[11]P. Murphy,*"The OSPF Not-So-Stubby Area (NSSA) Option"*, IETF, RFC 3101, 2003.

[12]P. Pillay-Esnault, A. Lindem,*"OSPFv3 Graceful Restart"*, IETF, RFC 5187, july2008.

[13]R. Callon, *" Use of OSI IS-IS for Routing in TCP/IP and Dual Environments"*, IETF, RFC 1195, dec1990.

[14]R. Coltun, D. Ferguson, J. Moy, A. Lindem, Ed., *" OSPF for IPv6"*, IETF, RFC 5340, july2008.

[15]T. Li, H. Smit, *"IS-IS Extensions for Traffic Engineering"*, IETF, RFC-5305, October 2008.

