ISSN 2348 - 2249
Volume-6, Issue-4, October-December, 2018
International Journal for Multi Disciplinary Engineering and Business Management
(IJMDEBM)

COMPARATIVE ANALYSIS OF DISTANCE VECTOR AND LINK STATE ROUTING PROTOCOLS

Shefali Singh
Research Scholar (M.Tech)
SVIET, Rajpura
India
shefali.birwal@yahoo.in

Rupali Zakhmi
Computer Science and Engineering Dept
SVIET, Rajpura
India
rupali2218@gmail.com

Abstract: *This paper explains the Interior Gateway Routing Protocols and their performance, security and scalability against each other to find out the best IGP between the Distance Vector and Link State Routing Protocols according to the requirements. OSPF and ISIS are the link state routing protocols and EIGRP and RIP are the distance vector routing protocols. OSPF and ISIS uses the concept of areas. EIGRP and RIP both are under a same category but uses different algorithms i.e. EIGRP uses DUAL algorithm, while RIP uses Bellman-Ford Algorithm. OSPF and ISIS use Dijkstra's Shortest Path First Algorithm. This paper provides a good research on which protocol works best in terms of scalability, performance and security. It can be used for good practices on how interior gateway routing protocols can be designed and tuned in terms of performance, scalability and security. As network is getting more and more important part of almost all the industries in order to access the cloud based applications, service provider and data center industry is acting as a transit and end point for all. IGPs define the paths in the transit and when traffic enters into cloud based data centers. The research work in this paper will provide an abstract view on the IGPs and their selection on the basis of performance, scalability and security.*

Keywords - IETF, RFC, NSFNET, FIB, DSCP, BGP, MPLS, QOS.

1.)Introduction

Sending a IP packet from one network to another needs to have a router, which is a piece of hardware running software in the form of operating system. Routers sends IP traffic from one network using a process known as routing. Routers and Layer 3 Switches can be used and they run either static or dynamic routing to do the tasks. Best Path Selection is done on the basis of Metrics and lowest metric or cost means a better path. A routing table is created using static or dynamic routing protocols which has information related to the destination network and the mask along with the exit interface and next-hop address value. By using the routing table, the decision on best path towards the destination is made. Following is the basic algorithm used for routing :-

1.1) Static vs Dynamic Routing:

There are two methods with which routing can be performed, its either Static or Dynamic :-

1.1.1) Static Routing - Static Routing is a method of routing where the paths and the best paths are defined by Network Engineer himself and he has total control over it as it does not work automatically or negotiate anything with the other routers. It consumes very less CPU resources as it do not have to send any messages or any other negotiation parameters to the adjacent routers. The problem with Static Routing is that it cannot be used in large scale routing environments and it is also not fault-tolerant so if in any case the next hop becomes unreachable, the route is still remains placed in the routing table which can be disastrous if IP SLA is not used to track the dead next-hop. It is also the most preferable one when compared with dynamic routing protocols because it has the lowest AD value.

1.1.2) Dynamic Routing - With Dynamic Routing, routing table is created and is maintained automatically by the Dynamic Routing Protocols. All Routing Protocols finds the best path towards destination by using Metric or Cost. Lower the cost or metric, better the path. These protocols shares their parameters and create neighborships with their adjacent routers running the same protocol. After the neighborship process is done, all the routers shares their routing information with each other. Using Dynamic routing results in more CPU processing or more memory usage as compared with the static routing because with dynamic routing protocols, there are different protocols created like Neighborship Table or Database Table. It also helps in faster convergence which was not possible by using Static routing without IP SLA. There are two types of dynamic routing protocols in IP based networks:

1.1.2.a.) Interior gateway protocols - IGPs are used inside an autonomous system, means they mainly runs inside an organization which can be enterprise, service provider. IGPs are used in every network environment where same AS is involved. Varios IGPs are RIP, EIGRP, OSPF, ISIS, IBGP.

1.1.2.b.) Exterior gateway protocols - EGP, abbreviated as Exterior Gateway Protocol is used to connect different Autonomous Systems. They are mainly used between different Service Providers and in those enterprises or Data Centers where full internet routing table is needed. The only EGP protocol in the world at the moment is BGP(Border Gateway Protocol), the protocol that makes Internet happens.

ISSN 2348 - 2249
Volume-6, Issue-4, October-December, 2018
International Journal for Multi Disciplinary Engineering and Business Management
(IJMDEBM)

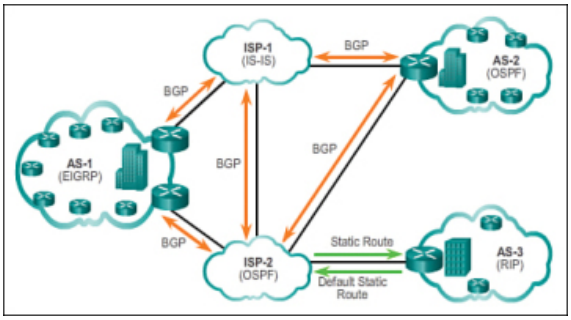

Figure 1.1 taken from pearson website shows IGPs and EGP usage in network industry.

2.) Distance Vector Routing Protocols - Based on distance and direction. Distance Vector protocols are limited with number of routers we can use. Protocols under Distance Vector Routing Protocols are –

2.1) Routing Information Protocol(RIP) -
RIP is a pure distance vector routing protocol. It uses Bellman-Ford or Ford-Fulkerson Algorithm. It is a slow protocol and has hops limited to up to 15. It is basically used in small scale environments. It is divided into three different types, RIPv1, RIPv2 and RIPng, RIPv1 and RIPv2 supports IPv4 while RIPng is used for IPv6 based RIP configurations. It was a classful protocol in its earlier version i.e. RIPv1, but now it is classless protocol. Its multicast address is 224.0.0.9 for RIPv2 and FF02::9 for RIPng. It sends its complete RIP routes every 30 seconds to its adjacent router connected with it and running RIP. RIPv2 is the only version that supports authentication.

2.2)Enhanced Interior Gateway Routing Protocol(EIGRP) - EIGRP is a advanced distance-vector routing protocol. It was created by Cisco Systems, but in February 2013, Cisco published a draft on making it open standard. It uses DUAL algorithm to find the best path towards the destination. It has a limit of up to 255 hops, by default it uses 100 hops. It uses multicast address 224.0.0.10 to send updates and hello packets and IPv6 multicast address FF02::A to send updates and hello packets. It creates three tables i.e. Neighborship Table, Topology Table and Routing Table. It uses Split-Horizon to prevent loops. Metric Calculation is done on the basis of K-values. One of the best things that EIGRP has is that it can store the backup routes in the topology table that results in Fast Convergence in case of primary link goes down. It also supports unequal-cost load balancing.

3.) Link State Routing Protocols
Link State protocols, also known as shortest path first or distributed database protocols, are built around a well-known algorithm of graph theory, E.W. Dijkstra's shortest path first algorithm. Link State protocols behave like a road map. Each router shares its link information in the form of Link State Advertisement(LSA), or Link State PDU(LSP). A link state router uses link state information to create a topology map and to select the best path to the destination in the topology. LSAs propagates to every neighbor router using protocol specific multicast address, each router that receives the LSA, updates its Link-State-Database(LSDB) and forwards the LSA to its neighbor routers within an area. SPF tree is then applied to the LSDB to find the best path to reach the destination and the best path is then added to the routing table. A example illustration showing link state routing protocols and distance vector protocol is shown below :

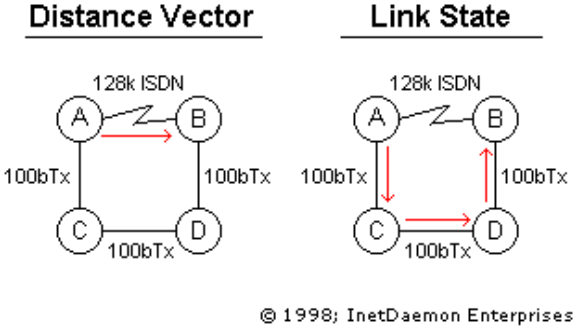

Figure 3.1 - Example of SPF within Link State Protocols
Link State Routing Protocol includes -

- **Open Shortest Path First(OSPF)**
- **Intermediate-System-to-Intermediate-System(IS-IS)**

An overview of both these protocols is given below :

3.1)IS-IS(Intermediate System to Intermediate System)
IS-IS is a link state routing protocol and is mainly used in Service Provider as an Interior Gateway Routing Protocol, it is used in ISP environment because of its scalability feature. It was not an IP routing protocol from the start and was the part of ISO's CLNS protocol stack, it was in early 1990's that it was adopted by IETF for IP based network routing. ISIS supports both IPv4 and Ipv6 routed protocols and it uses Dijkstra's Shortest Path First Algorithm to find the best path towards destination. It also uses a different addressing format, although it is used in IP routing, but one NET address is needed on every router as an identifier to create neighborship between different routers. It uses ISO's NSAP format of addressing which has the maximum size of 20 bytes and minimum of 8 bytes. It uses two "levels" of adjacencies - Level 1(L1) and Level 2(L2).

3.2) OSPF(Open Shortest Path First) - OSPF is a link state routing protocol. In OSPF, network is divided into areas with Area 0 acting as a backbone area. Area 0 always have to be in transit in order to make two non-backbone areas share their routing information. OSPF uses two multicast addresses 224.0.0.5(All SPF Router address) and 224.0.0.6(DR-BDR address) for IPv4 and FF02::5(All SPF address) and FF02::6(DR/BDR address). Routing Information is shared in the form of Link State Advertisements(LSAs). LSA Database within same area remains same on all the routers. Router that shares routing information from one are to another is known as Area Border Router(ABR), its have to have atleast one interface in Area 0. There is no limit on number of routers/hops that we can use in OSPF. So it can be used in small -to- medium and large networks.

ISSN 2348 - 2249
Volume-6, Issue-4, October-December, 2018
International Journal for Multi Disciplinary Engineering and Business Management
(IJMDEBM)

4.) RESULTS

Performance Routing Protocols are used to make control plane that helps in creating the routing table and automatically copies to the forwarding information base(FIB) and creates a data plane. Interior Gateway Routing Protocols are divided into two categories i.e. Distance Vector and Link State Routing Protocols. RIP and EIGRP comes under Distance Vector and OSPF and ISIS comes under Link State Routing Protocols. Performance is a major part of routing and as the packets move from one router to other in order to reach the destination, routing table and forwarding information base are needed in that. I have used every interior gateway routing protocol to find the best one according to performance(measured in terms of Convergence Time) and scalability. OSPF and ISIS are the protocols which are used heavily in the service provider networks and part from them both are using the same algorithm, i.e. Dijkstra's Shortest Path First algorithm in order to find the best path to reach the destination, but both these link state routing protocols still have lots of differences which can be seen clearly after looking at the results. Following are the parameters used in the topology :-

Cisco IOS 14.1
Link Bandwidth = 100Mbps
Duplex = Full

A dual stack network is used to gather the results from the topology. Dual stack network is a network which uses both IPv4 and IPv6 in the same network. As IPv4 is mostly depleted, therefore we have also used IPv6 for the configuration and results and found the difference not only between the routing protocols, but also between the routed protocols by comparing the performance and scalability.
Below is the topology used :-

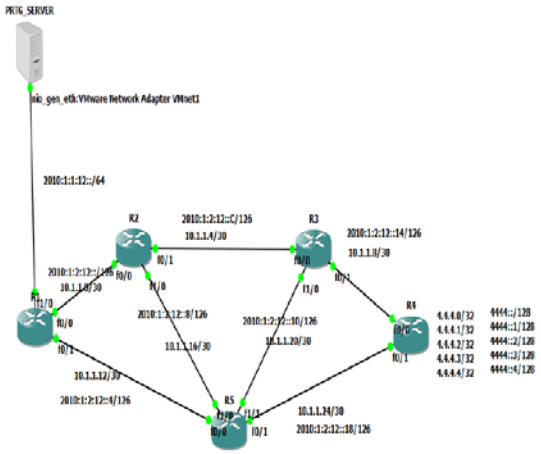

Figure 4.1 - Topology used for Project

RIP is the first protocol that I used in the topology defined above which is same for all the protocols. I have configured RIPv2 in the topology and prtg server is connected with the gns3 topology to plot a graph that shows the convergence time. RIPv2 and RIPng by default has a hold down timer of 180 seconds which is way too much for a network and applications running over it. For faster convergence, timers have been reduced to 9 seconds for flush timer. In the topology we have multiple links from R1 to loopback of R4 and if one link goes down, all the traffic shifts towards the other link automatically and convergence time it takes to shift is defined below :-

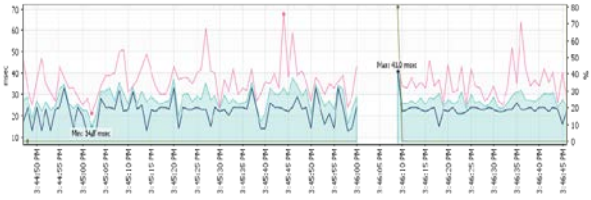

Figure 4.2–RIPs Convergence time

Above graph displays the default convergence time with reduced timers for faster convergence technology or protocol is 9 seconds, which is not good for today's network and applications. For IPv6 based RIPng, we are using a similar topology, and from R1 , we have multiple paths towards R4s 4444::1, and when one path goes down, other path automatically becomes the best path.Below Graph displays max, min, and average convergence time results:

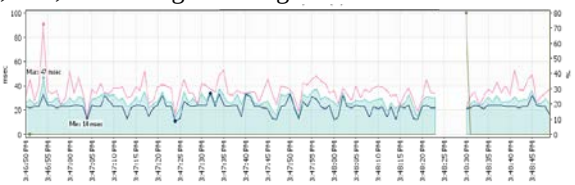

Figure 4.3 - Convergence Time in RIPng

Above graph displays that there is not much difference when we compare RIPv2 and RIPng for convergence, as both takes around 6 seconds to converge. Below is the comparison table between both types of RIP :-

Table 4.1 - RIPs Comparison table with default and tuned parameters

Protocol	Convergence Time	Convergence Time with Tuned Timers
RIPv2	180 seconds	9 seconds
RIPng	180 seconds	6 seconds

EIGRP is the other distance vector routing protocol that i used and it comes under the advanced distance vector routing protocol category. EIGRP uses different mechanism to find the best path towards destination and to does not on lesser number of hops to find the best path. Convergence time with default parameters of EIGRP is defined below in the graph where we are using the same topology that we used for RIP and graph shows the convergence time that EIGRP takes to fall from primary to backup link. Graph with EIGRP convergence times is shown below :

ISSN 2348 - 2249
Volume-6, Issue-4, October-December, 2018
International Journal for Multi Disciplinary Engineering and Business Management
(IJMDEBM)

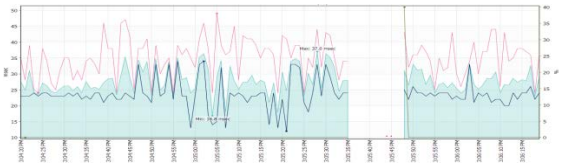

Figure 4.4 - EIGRP Convergence time with default parameters

graph displays EIGRP without any convergence time takes around 14 seconds to fall from primary to backup link, which is better than RIP. We can reduce the convergence time by using some faster convergence technology. With EIGRPv6, i have used the same topology and the algorithm used in calculation is also same with both EIGRPv4 and EIRPv6. With EIGRPv6, we have multiple paths to reach 4444::1 from R1, and if primary path goes down, backup path comes up automatically and the convergence time for that is shown below :-

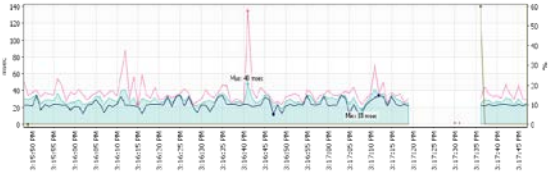

Figure 4.5 –EIGRPv6 Convergence time with default parameters

Figure 4.5 displays the convergence time taken by EIGRPv6 to shift the traffic from primary to backup link, in case of primary link failure. It takes around 15 seconds by default without any faster convergence mechanism. After tuning the DUAL algorithm for timers, below are the convergence times that we achieved :-

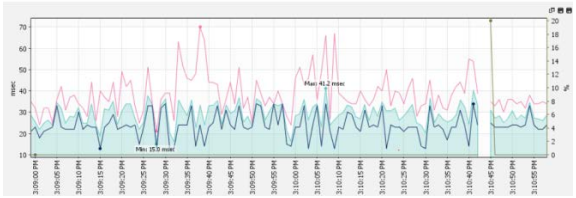

Figure 4.6 –IPv4 based EIGRP Convergence time with tuned parameters

Figure 4.6 shows the reduced convergence time to around 2 seconds. With IPv6 tuned DUAL algorithm, below is the graph showing convergence :-

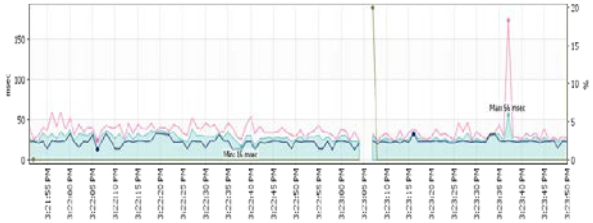

Figure 4.7 –Ipv6 based EIGRP Convergence time with tuned parameters

Comparison Table of EIGRP and EIGRPv6 on the basis of convergence time is below:

Table 4.2 –EIGRP and EIGRPv6 Convergence Table

Protocol	Convergence Time	Convergence Time with Tuned Algorithm
EIGRP with IPv4	14-15 seconds	2-3 seconds
EIGRPv6	15-16 seconds	2-3 seconds

Next Protocol that i used to examine is OSPF which is a link state routing protocol. OSPF has different version for IPv4 and IPv6. OSPFv2 is used for IPv4 and OSPFv3 is used for IPv6. I have used the same topology for OSPF which i used for RIP and EIGRP also. OSPF uses Dijkstra's Shortest Path First Algorithm and everything is divided into Areas in OSPF. We have multiple paths to reach 4.4.4.1 from R1 and convergence time OSPF takes in case of primary link failure is shown in the graph below :-

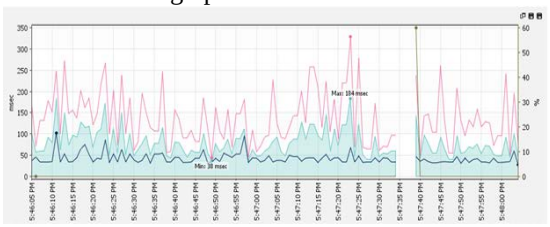

Figure 4.8- PRTG Graph showing OSPFv2 Convergence Time

As shown in Figure 4.7 graph, OSPF takes around 5 seconds to converge from primary to backup link and it is the time with the default parameters and with no Timers to convergence mechanisms tuned. OSPFv3 calculation is also made for IPv6 based OSPF. We have multiple links from R1 towards R4's 4444::1 and if primary link goes down, backup link automatically comes up and the time it takes to converge is shown below:

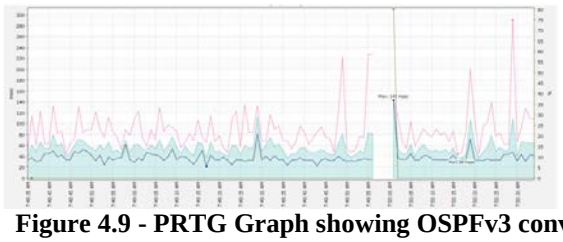

Figure 4.9 - PRTG Graph showing OSPFv3 convergence time with default parameters

Above graph clearly shows that there is not much difference between OSPF for IPv4 and OSPF for IPv6 as convergence time for IPv6 based OSPF is same as OSPFv2 i.e. 5 seconds. I have tuned the OSPF SPF algorithm to converge faster and by

ISSN 2348 - 2249
Volume-6, Issue-4, October-December, 2018
International Journal for Multi Disciplinary Engineering and Business Management
(IJMDEBM)

changing some of the parameters like "Delay which is between receiving a change to SPF calculation to 100msec", "Delay two successive SPF calculation to 100msec" and "Maximum waiting time for SPF calculations to 120msec".
After tuning the result is shown below :-

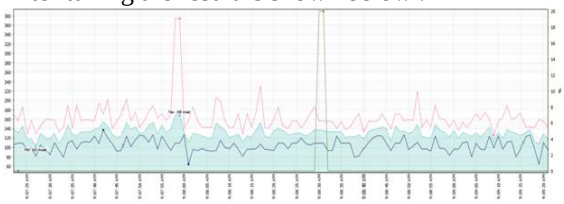

Figure 4.10 - Sub-Second convergence after tuning SPF timers

Table below displays the convergence time comparison between OSPFv2 and OSPFv3 :

Protocol	Convergence Time	Convergence with SPF Tuning
OSPFv2	4-5seconds	Within a Second
OSPFv3	4-5seconds	Within a Second

Table 4.3- Convergence Table of OSPFv2 and OSPFv3 with both default and tuned parameters

ISIS is another LSRP and it also uses the same algorithm i.e. Shortest Path First. ISIS is mainly used in the large service provider networks and i have used the same topology for ISIS also. We have multiple links to reach 4.4.4.1 from R1 and if best path goes down, backup link automatically gets into use for data plane. Convergence time it takes is shown below in the graph :-

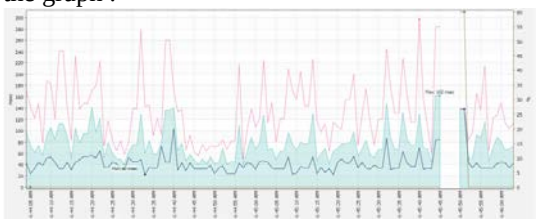

Figure 4.11- PRTG Graph showing ISIS Convergence time with default parameters.

Above graph in figure 4.10 shows that ISIS with IPv4 takes around 4 seconds to converge with default parameters and no faster convergence technology applied. ISIS with IPv6 also works same and the use of NET address is also the same. Below is the graph showing ISIS with IPv6 convergence time :-

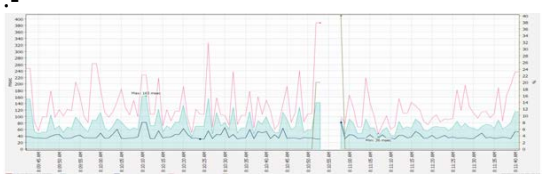

Figure 4.12- ISISv6 Convergence time with default parameters

After tuning SPF Algorithm with same parameters as we tuned in OSPF, we get the following result :-

Figure 4.13 - ISIS with SPF timers tuned.

A table comparing both ISISv4 and ISISv6 with default and tuned parameters is below:

Table 4.4- Performance Table of ISISv4 and ISISv6 with both default and tuned parameters

Protocol	Convergence Time	Convergence with SPF tuned
IPv4 based ISIS	4 seconds	Within a Second
IPv6 based ISIS	5 seconds	Within a Second

Below is the table showing the complete analysis of interior routing protocols on the basis of convergence with both default and tuned parameters, which properly shows the comparison on the basis of performance of routing protocols:

Protocol	Convergence Time	With Faster Convergence Methods
RIPv2	180 seconds	9 seconds
RIPng	180 seconds	6 seconds
EIGRP with IPv4	14-15 seconds	2-3 seconds
EIGRPv6	15-16 seconds	2-3 seconds
OSPFv2	4-5seconds	Within a Second
OSPFv3	4-5seconds	Within a Second
IPv4 based ISIS	4 seconds	Within a Second
IPv6 based ISIS	5 seconds	Within a Second

Table 4.5- IGP comparison table in terms of performance

Above IGP Comparison table with default values and algorithms tuned, shows that Faster Convergence technologies are important to maintain the data plane and control plane traffic. Link State Routing Protocols are better in terms of convergence and can even provide sub second convergence with algorithm tuned. Therefore for VoIP or any other delay sensitive traffic using Routing Protocols with faster

ISSN 2348 - 2249
Volume-6, Issue-4, October-December, 2018
International Journal for Multi Disciplinary Engineering and Business Management
(IJMDEBM)

convergence technologies is mandatory, otherwise the data plane traffic can create lot of problems.

4.2 Security Analysis of Distance Vector and Link State Routing Protocols

Routing is the core part of networking and routing protocols are used to share the control plane information between the routers. Routing Information is shared between the routers which are acting as neighbors running the same routing protocol. Authentication is an important part between the neighbors and is used between the neighbor routers to share route information in secure manner. Authentication in RIP can be used in IPv4 only as in IPv6 RIP is totally dependent on IPSEC for authentication purposes. Below is the RIP packet capture taken in wiresharkthat shows a simple plain-text password :-

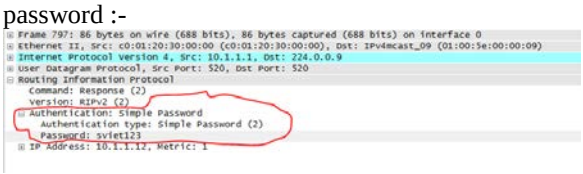

Figure 4.14- RIPv2 Packet in wireshark with Plain-Text Authentication used

Plain Text Authentication is not secure and its better to use MD5 based hashing with authentication, which makes authentication process much more secure. A packet capture showing RIPv2 MD5 based authentication mechanism is shown below:

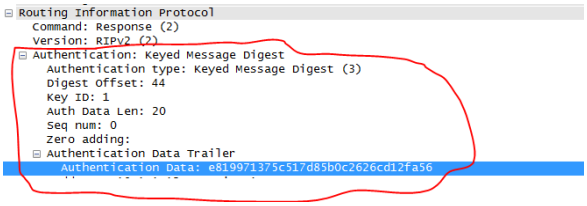

Figure 4.15- Packet captured in wireshark with MD5 based Authentication used

EIGRP mainly uses MD5 based authentication both for IPv4 and IPv6 based routing. Below are the captures taken in Wireshark with IPv4 based EIGRP and IPv6 based EIGRP :-

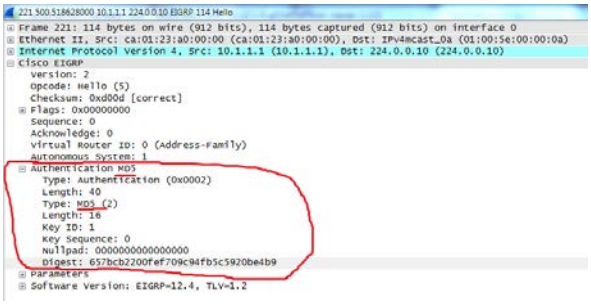

Figure 4.16- EIGRP MD5 Authentication in IPv4

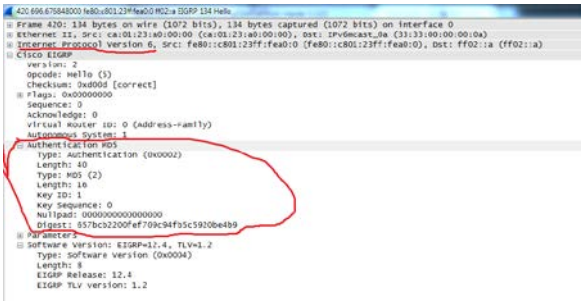

Figure 4.17- EIGRP MD5 Authentication in IPv6

OSPF uses both Text-Based and MD5 based authentication in IPv4 and below captures showsaclear plain-text password showing password "sviet123" in the wireshark, while MD5 Based authentication mechanism makes authentication more secure. Below are the Plain-Text and MD5 based password captures in OSPF :-

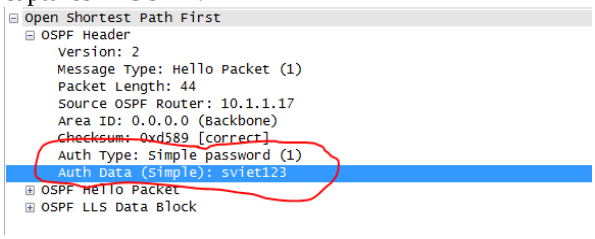

Figure 4.18 - OSPF Text Based authentication captured in Wireshark

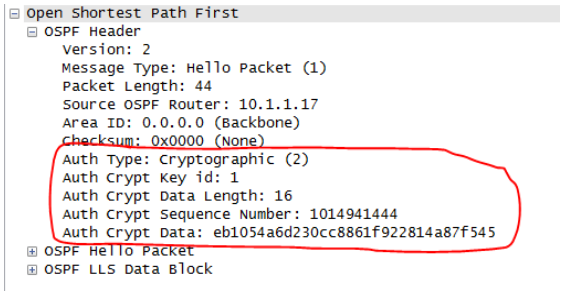

Figure 4.19- OSPF MD5 based authentication captured in Wireshark

OSPFv3 uses much better authentication mechanisms by including hashing methods like MD5 and SHA1, the best thing is that SPI i.e. Security Parameter Index is used with authentication, which is just a number but needed to be same on both the neighbors along with the password. SHA1 provides 160 bits of hashing while MD5 provides 128 bits of hashing.

Below is the wireshark capture of the OSPFv3 authentication :-

ISSN 2348 - 2249
Volume-6, Issue-4, October-December, 2018
International Journal for Multi Disciplinary Engineering and Business Management
(IJMDEBM)

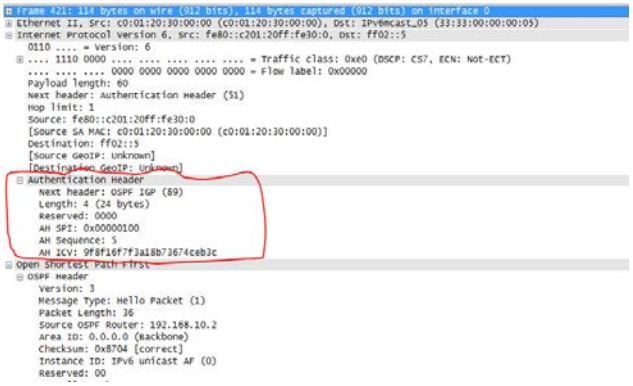

Figure 4.20- OSPFv3 authentication with MD5 technique

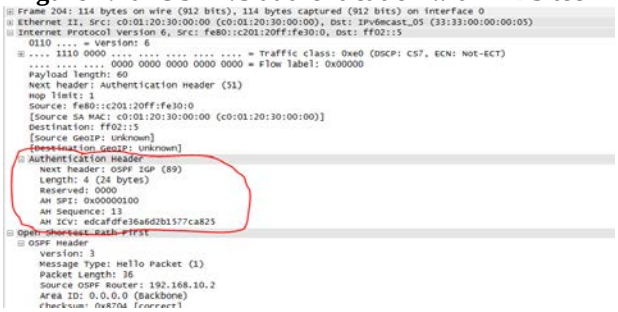

Figure 4.21- OSPFv3 authentication with SHA-1 technique

ISIS is a ISPs core routing protocol in large networks and it uses plain text and MD5 based hashing with Authentication to securely share the routing information with the neighbor core routers. Below is the wireshark packet capture of ISIS Packet with Authentication enabled :-

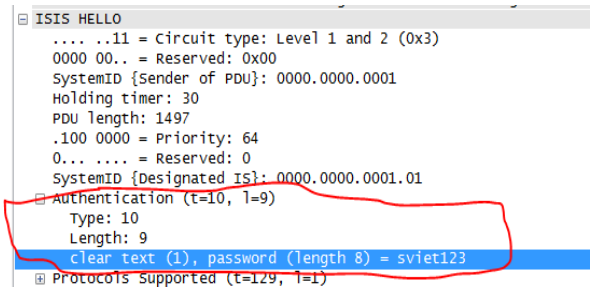

Figure 4.22 - ISIS authentication wireshark capture

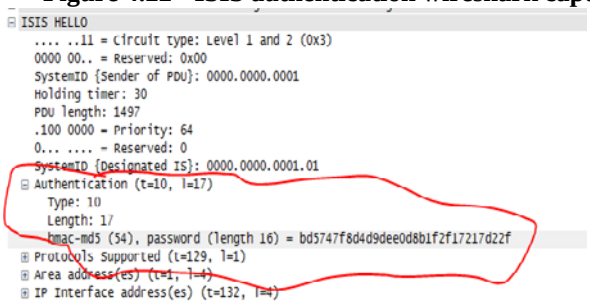

Figure 4.23 - ISIS authentication MD5 capture in Wireshark

4.3 Scalability Analysis of DVRP and LSRP

Scalability is another major factor for selecting any routing protocol and as we have four Interior Gateway Routing Protocols, categorizing them on the basis of scalability can be done on how many routers or hops a routing protocol message can be able to traverse and how a routing protocol sends its updates to the neighbors. RIP, the oldest protocol of all the four, can only traverse maximum of 15 routers, which clearly shows it is not as scalable as today's network demands. Also it sends periodic updates after every 30 seconds which added to CPU resource consumption in case the routing table size is large. On the other hand, EIGRP, other distance vector routing protocol can traverse maximum of 255 hops, which is large and technically fine as a packet life is also 255 hops which is the maximum TTL(Time to live) Value. But as it was Cisco proprietary before February 2013, lots of vendors still haven't implemented it in their network Operating System. OSPF and ISIS both can have unlimited number of hop counts that can be used and all the networks are divided in the areas, make it a better choice and more efficient and scalable. Therefore using Link State routing protocols is better in terms of scalable networks. Below is a table showing Maximum Routers each protocol can traverse and the update mechanism of each protocol.

Table 4.6 - Scalability comparison of IGPs

Protocol	Category	Maximum Routers	Updates
RIP	Distance-Vector	15	Periodic
EIGRP	Advance Distance-Vector	255	Triggered
OSPF	Link State	Unlimited	Triggered
IS-IS	Link State	Unlimited	Triggered

CONCLUSION :

Link State and Distance Vector are the two types of Interior Gateway Routing Protocols used. Link State Protocols has OSPF and ISIS and Distance Vector has EIGRP and RIP protocols categorized under them. As per performance, EIGRP is better than RIP, while ISIS and OSPF behaves almost similar, but ISIS can work better in Large scale ISP networks in terms of performance and simplicity. Performance wise, Link State Routing protocols are better than Distance Vector Routing Protocols as it can also provide sub second convergence by enhancing the SPF algorithm. From security perspective, almost all the protocols use MD5 based hashing with the authentication mechanism to securely share the routing information between the neighboring routers. Link State Routing Protocols are much more scalable than using Distance Vector Protocols as they have no limit on them, that is one of the reason they are used in large scale enterprises and service provider networks. From a total perspective, Link State Routing Protocols are better than Distance Vector Routing Protocols.

FUTURE SCOPE :

Routing is used to get the best path towards destination and routing protocols are used to achieve this and IGPs are used in

almost all the medium to large sized networks which can be enterprise, service provider or data centers. But, Software Defined Networks has started to shift the curve. Having Control plane and Data Plane work separately does the trick in centralizing the process. By using SDN, deployment and maintenance can be centralized in the controller which is controlling all the programmable switches in the southbound region. All the switches that are only data plane devices and the brain they are using of the controller are interacting with the controller by using Openflow Protocol. Enhancement can be made by having a hybrid environment running both SDN architecture and traditional IP routing protocols with slowly moving towards all SDN based environment.

REFERENCES

[1] A.Kudtarkar, R.Sonkusare, and D.Ambawade[2014], "Performance Analysis of Routing Protocol for Real Time Application", International Journal of Advance Research in compute and Comunication Engineering Vol.3, Issue 1.

[2] Anuj Gupta, NehaGrang[2014]. "Compare OSPF Routing Protocol With other Interior Gateway Routing Protocol", IJEBEA

[3] Hedrick,C., "Routing Information Protocol", RFC 1058 , Rutgers University , June 1988.

[4] Malkin, G. and R. Minnear, "RIPng for IPV6", RFC 2080, DOI 10.17487/RFC2080, January 1997.

[5] Malkin,G., "RIP Version 2", STD 56, RFC 2453, DOI 10.17487/RFC2453, November 1998.

[6] B.Albrightson, j.j Garcia-Luna-Aceves and Joanne Boyle, "EIGRP-A Fast Routing Protocol based on Distance – Vector", Cisco System, University of California.

[7] R.E. Bellman. Dynamic Programming. Princeton, New Jersey: Princeton University Press; 1957.

[8] L. R. Ford Jr. and D. R. Fulkerson. Flow in Networks. Princeton, New Jersey: Princeton University Press; 1962.

[9] Enhanced Interior Gateway Routing Protocol(EIGRP) IETF draft by D. Savage, D.Slice, J.Ng, S.Moore, and R. White of Cisco Systems.

[10] Jeff Doyle and Jennifer Carrol, "Routing TCP/IP, Volume1 Second Edition", Ciscopress.

[11] Oran, D., Ed., "OSI IS-IS Intra-Domain Routing Protocol", RFc 1142, DOI .17487/RFC119, Feburary 1990.

[12] Callon, R., "Use of OSI IS-IS for Routing in TCP/IP and dual environment", RFC 1195, DOI 10.17487/RFC1195, December 1990.

[13] Hopps, C., "Routing IPv6 with IS-IS", RFC 5308 DOI 10.17487/RFC5308, October 2008.

[14] Moy, J., "OSPF Version 2", STD 54, RFC 2328, DOI 10.17487/RFC2328, April 1998.

[15] Murphy, P., "The OSPF Not-So-Stubby Area (NSSA) Option", RFC 3101, DOI 10.17487/RFC3101, January 2003.

[16] Coltun, R., Ferguson, D., and J. Moy, "OSPF for IPv6", RFC 2740, DOI 10.17487/RFC2740, December 1999.

[17] Pillay-Esnault, Moyer, P,. Doyle, J., Ertekin, E., and M. lundberg, "OSPFv3 as a Provider Edge to customer Edge (PE-CE) Routing Protocol", RFC 6565, DOI 10.17487/RFC6565, June 2012.

[18] Moy, J., Pillay-Esnault, P., and A. Lindem, "Graceful OSPF Restart", RFc 3623, DOI 10.17487/RFC3623, November 2003.

[19] Gupta, M. and N. Melam, " Authentication/Confidentiality for OSPFv3", RFC 4552, DOI 10.17487/RFC4552, June 2006.

[20] Pillay-Esnault, P. and A. Lindem, "OSPFv3 Graceful Restart", RFC 5187, DOI 10.17487/RFC5187, june 2008

