A Comparison of OSPFv3 and EIGRPv6 in a Small IPv6 Enterprise Network

Richard John Whitfield
University of Derby

Shao Ying Zhu
University of Derby

***Abstract*—As the Internet slowly transitions towards IPv6, the routing protocols that are used to forward traffic across this global network must adapt to support this gradual transition. Two of the most frequently discussed interior dynamic routing protocols today are the IETF's OSPF and Cisco's EIGRP routing protocol. A wealth of papers have compared OSPF and EIGRP in terms of converge times and resource usage, however few papers have assessed the performance of each when implementing their respective security mechanisms. Therefore a comparison of OSPFv3 and EIGRPv6 will be conducted using dedicated Cisco hardware. This paper will firstly introduce each protocol and its security mechanisms, before conducting a comparison of OSPFv3 and EIGRPv6 using Cisco equipment. After discussing the simulation results, a conclusion will be drawn to reveal the findings of this paper and which protocol performs the best upon implementing their respective security mechanisms within a small IPv6 enterprise network.**

***Index Terms*—IPv4; IPv6; OSPFv3; IPSec; ESP; EIGRPv4; EIGRPv6; MD5**

I. Introduction

Two of the most discussed IPv6 routing protocols amongst researchers are the IETF's Open Shortest Path First Version 3 (OSPFv3) and Cisco's Enhanced Interior Gateway Routing Protocol for IPv6 (EIGRPv6). A number of papers such as [1,2,3,4] have reviewed both protocols countless times with respect to their resource usage and convergence speed. However, no comparisons have been conducted to assess the additional effects when implementing the respective authentication and encryption mechanisms of OSPFv3 and EIGPRv6.

Therefore, due to the popularity of OSPFv3 and EIGRPv6, it is critical that a through comparison is conducted to comprehensively assess both protocols when operating within a small IPv6 enterprise network.

In addition, it should also be noted that in recent years, a key drawback of EIGRP has been its proprietary nature. However, as discussed by [5], EIGRP is been opened up to the IETF and will soon no longer be a drawback.

This paper contributes to the ongoing comparisons of OSPFv3 and EIGRPv6 by testing both protocols and assessing the additional impact of both protocol's security mechanisms when they are implemented in a Cisco hardware based test environment.

II. OSPFv3

OSPFv3 is a dynamic routing protocol that uses the Shortest Path First (SPF) algorithm and has been specifically designed to run within an IPv6 environment. Compared to its IPv4 equivalent OSPFv2, OSPFv3 incorporates a number of key changes necessary to operate in an IPv6 network [6].

As discussed by [7], a key change that has been performed for OSPFv3 is that the packet header of which has been restructured. OSPFv3's packet header is now far less complex compared to that of OSPFv2 and also includes the "Instance ID" field [7]. The Instance ID field also reflects another dramatic change, in that routing protocols for IPv6 are more concerned about the links they are enabled on, rather than the nodes they are enabled on [7]. This "per-interface" concern means that multiple addresses can be configured on the same interface [8]. This is because rather than establishing neighbourship using IP subnets, OSPFv3 uses link local addresses to establish its adjacencies.

Furthermore, the changes to the OSPFv3 packet header have also had an additional effect on the OSPFv3 Hello Packet. To reflect the changes made for IPv6, the OSPFv3 Hello packet structure has been changed [8].

These changes are as follows [7]:

- The addresses of 224.0.0.5 and 224.0.0.6 are used for passing traffic between the DR and DROther routers is now FF02::5 and FF02::6.
- IPv6 addresses in OSPFv3 are located within the payload rather than the packet header.
- Network-LSA's do not contain any IPv6 addresses compared to OSPFv2.
- OSPFv3 requires that a router ID is configured before routing can begin.
- DR and BDR routers are now identifiable by their router ID's instead of their IP addresses as with OSPFv2.

In addition, a key change for OSPFv3 is the security mechanisms that the protocol uses to protect its routing updates. As discussed by [7,9], whereas OSPFv2 used MD5 authentication, OSPFv3 uses the services provided by IPsec, of which is used within an IPv6 environment [10].

III. EIGRPv6

Designed by Cisco, the Enhanced Interior Gateway Routing Protocol for IPv6 (EIGRPv6) uses the Diffusing Update Algorithm (DUAL) which is also used by EIGRP in an IPv4 environment. However, unlike OSPFv3, the majority of

EIGRP's features for IPv4 have been integrated into IPv6. As discussed by [7,11], these similarities include:

- The use of DUAL to compute EIGRP Successor and Feasible Successors.
- Using bandwidth and delay as the default metrics.
- The use of Reliable Transport Protocol (RTP).
- No periodic updates.
- EIGRPv6 implements the same authentication mechanism (MD5) as EIGRP.

However, despite the almost identical properties between EIGRP and EIGRPv6, a few changes have been implemented to prepare the protocol for routing within an IPv6 environment. As further discussed by [11], these changes include:

- The use of Link Local Addresses to establish neighbor adjacencies instead of using an IP subnet. This is also the case with OSPFv3.
- EIGRP routers will use the IPv6 multicast address FF02::10 rather than the previous 224.0.0.10 multicast address.
- Like OSPFv3, EIGRPv6 is also configured on a per-interface basis rather than been globally enabled.
- The creation of a router ID is required to successfully start routing operations.

However, unlike OSPFv3, EIGRPv6 does not incorporate the use of IPSec to encrypt its routing updates, but instead uses the MD5 authentication method that was previously used in EIGRP for IPv4 [7].

IV. Methodology

To ensure that the most relevant information can be gathered to accompany the research undertaken for this paper, a clear and concise methodology is required. Therefore, a number of specific goals will be implemented to deliver the most accurate conclusion possible. These goals include:

1) To investigate which protocol initialises quickest from a cold start-up.

2) To assess OSPFv3 and EIGRPv6's ability to recover from unforeseen failures.

3) Analyse which protocol re-converges with minimal packet drops.

4) Investigate the response times of each protocol when detecting idle link changes.

5) Examine each protocols security mechanism and implement them to compare their operational differences.

6) Observe any differences upon implementing both protocols.

Furthermore, to meet the goals designated above, a series of controlled experiments will be carried out by implementing four Cisco 1841 routers and one Cisco 2960 switch, all connected through fast Ethernet ports.

Moreover, data for this paper will be gathered by using outputs from the router's command line and packets captured in Wireshark. It should also be made clear that each test performed for either protocol will be conducted three times and then averaged to promote result reliability. In addition, each specific test will be done again to assess the additional impact upon implementing OSPFv3 and EIGRPv6's security mechanism. This test strategy ensures that the additional effects of OSPFv3 and EIGPRv6's security mechanisms can be measured, while performing each test three times to ensure result reliability.

Lastly, it should be mentioned that both protocols will be operating using the default Hello and Dead timers to ensure that the results best reflect the default behavior of both OSPFv3 and EIGRPv6.

V. Experiment Scenarios

So that a comprehensive and thorough comparison can be conducted, two test scenarios have been designed to assess the performance of OSPFv3 and EIGRPv6.

As figure 1 illustrates, test Scenario 1 implements a four router point to point test scenario. The purpose of this scenario is to assess the performance of both protocols when the routers are connected directly and not through another device such as a switch.

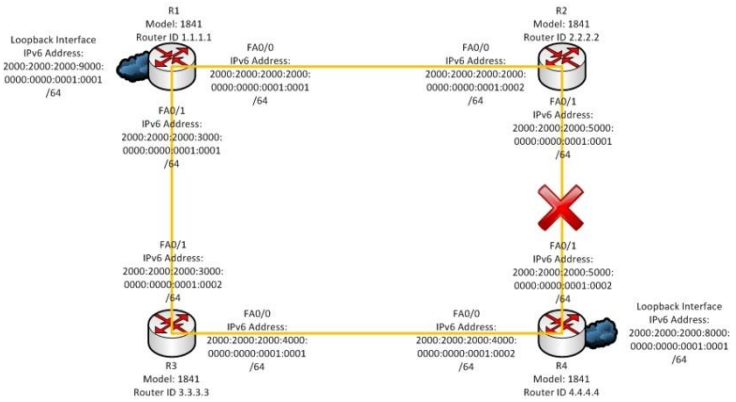

Fig. 1. Test Scenario 1

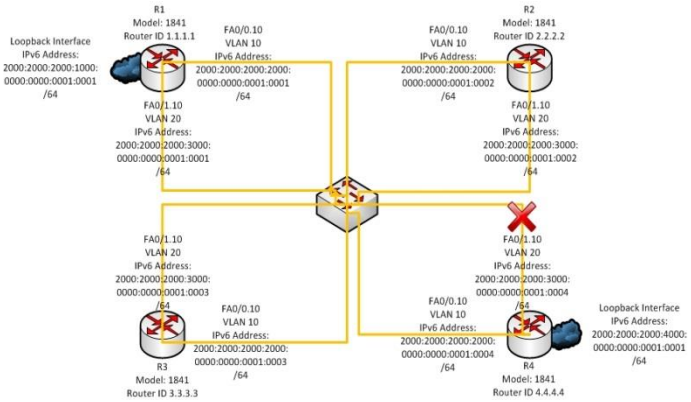

Fig. 2. Test Scenario 2

Furthermore, figure 2 demonstrates the second scenario that has been implemented to test OSPFv3 and EIGRPv6. Compared to the point to point topology of Scenario 1,

Scenario 2 implements a LAN environment where all routers connect to a switch. In Scenario 2, the switch will be configured with two VLANS to ensure the traffic for each interface is separated and kept in their own subnets. Therefore, compared to Scenario 1 where each router operates with different subnets, the routers in Scenario 2 will operate in the same subnet (one for the primary and one for the secondary link) and therefore enable an assessment of OSPFv3 and EIGRPv6's performance in a LAN environment.

Also, so that an active interface is always available to send and reply to ICMP Ping messages, a Loopback interface [12] will be implemented onto routers R1 and R4. By implementing Loopback address on R1 and R4, the traffic can be routed via another path depending on the link failed in the topology.

It should be noted for the purposes of this paper that all tests will be executed and monitored from R4's perspective and the preferred interface is FA0/1 towards R2.

VI. Scenario Results and Analysis

This section will discuss the results generated by testing OSPFv3 and EIGRPv6 and their security mechanisms, in Scenarios 1 and 2. The results are as follows:

TABLE I. Test Summary for Scenario's 1 and 2

Test Details	With Auth	Scenario 1		Scenario 2	
		OSPFv3	EIGRPv6	OSPFv3	EIGRPv6
Convergence time from a cold router start-up.		181.3s	143.4s	182.2s	163.5s
	Y	180.3s	142.4s	180.6s	163.6s
Neighbour down detection after an unexpected link failure.		9.7s	7.5s	9.1s	4.7s
	Y	9.7s	9.1s	9.3s	8.3s
Traffic re-sent after an unexpected link failure.		14.4s	8s	14.9.s	13.5s
	Y	13.6s	11.0s	14.3s	14.9s
Time for Protocol to detect neighbour down after cable removal		10.1s	7.2s	9.8s	8.2s
	Y	8s	10.3	7.9s	9.3s
Time to detect neighbourship re-establishment after cable replacement		49s	6.8s	43.5s	35.2s
	Y	50.5s	6.9s	43.4s	36.8s
Peak CPU utilisation		70%	70%	70%	70%
	Y	70%	70%	70%	70%

The first goal set in the methodology section previously was to investigate which protocol initialises the fastest from a cold start-up.

As figure 3 demonstrates, the testing performed for this paper reveals a series of key findings through testing in Scenarios 1 and 2. These findings have been extracted from table I shown earlier in this section.

As shown by figure 3 below, the startup times for EIGRPv6 are significantly faster than that of OSPFv3, irrespective of the test scenario. However, a key finding is that compared to its Scenario 1 (P2P) result, EIGRPv6 took longer to start up in Scenario 2 (LAN) test environment. In addition, figure 3 also reveals that whereas EIGRPv6 performed worse in Scenario 2, OSPFv3 performed marginally better and better still when its IPSec encryption mechanism was enabled. Interestingly, EIGRPv6's MD5 authentication mechanism affected the protocols performance in Scenario 1, but had no additional effect in Scenario 2.

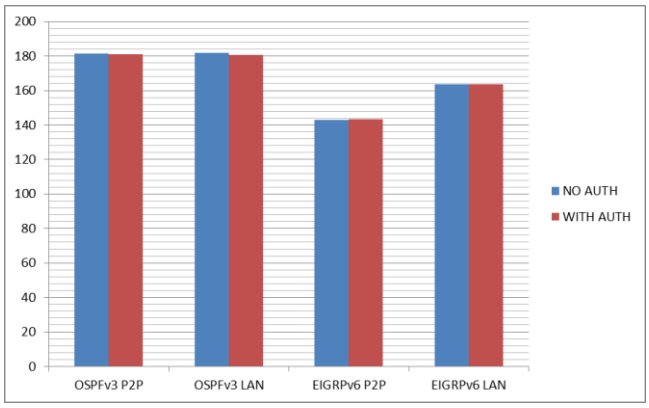

Fig. 3. OSPFv3 and EIGRPv6 Cold Start-up Time Comparison

The second and third goals that were defined in the methodology of this paper are to assess OSPFv3 and EIGRPv6's ability to recover from unforeseen failures and analyse which protocol re-converges with minimal packet drops. Therefore using the results collected in table I in addition to figures 4 and 5, this shows the averaged results from the convergence tests conducted in this paper.

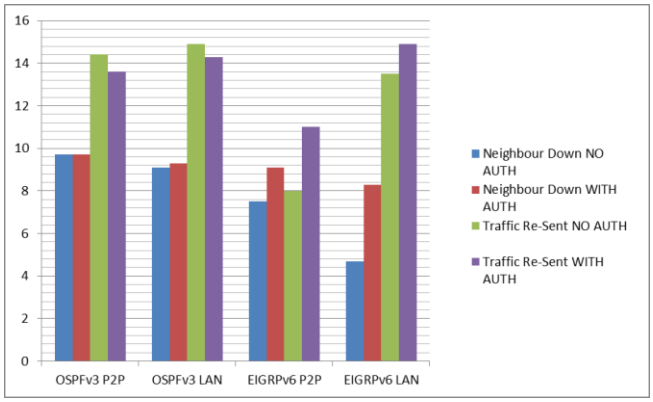

Fig. 4. OSPFv3 and EIGRPv6 Re-Convergence Times

As revealed by figure 4, a number of key findings can be found. Firstly, figure 6 continues the trend observed in figure 4 in that EIGRPv6 performance is better in Scenario 1 compared to that of Scenario 2. Although EIGRPv6 detected the neighbor was down faster in Scenario 2, it took longer to resend the traffic in Scenario 2 and also with a much bigger margin when MD5 authentication was activated.

Furthermore, figure 4 also shows that OSPFv3 performed better in Scenario 2 than Scenario 1 for neighbor detection, but was able to resend the traffic faster in Scenario 1. Moreover, when OSPFv3's IPSec encryption was configured in Scenario 2, the time taken to detect the neighbor was down increased.

However as figure 5 shows, this result may have been caused by packet drops.

Figure 5 reveals that compared to Scenario 1, OSPFv3 in Scenario 2 dropped on average more packets compared to Scenario 1. However, an interesting finding from this test is that whereas IPSec encryption improved the performance of OSPFv3, EIGRPv6's MD5 authentication adversely affected the protocols performance in both test Scenarios. In addition, figure 5 also supports the trend identified throughout this paper, in that EIGRPv6 performs better in the point to point topology of Scenario 1 compared to that of Scenario 2's LAN topology.

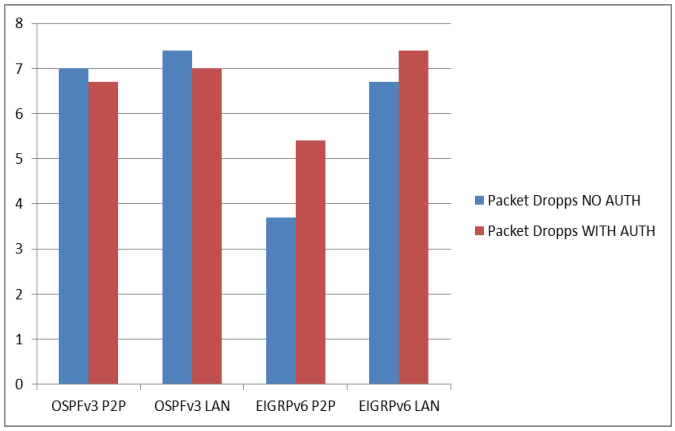

Fig. 5. OSPFv3 and EIGRPv6 Packet Drop Comparison

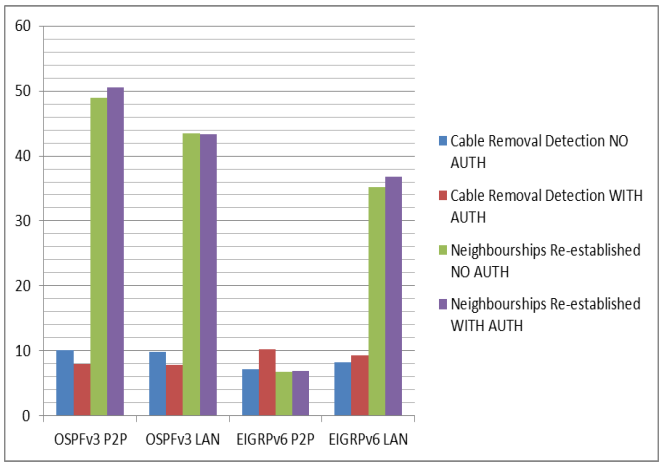

Fig. 6. Protocol Response Testing

In addition, a test to measure the responsiveness times of OSPFv3 and EIGRPv6 was carried out by deliberately failing a link over an idle link. This test differs to the convergence tests discussed earlier as the purpose is to measure the time taken for each protocol to detect and re-establish a neighbourship, rather than detecting and re-sending traffic. This test satisfies the fourth goal in the methodology which is to analyse the response times of each protocol when detecting idle link changes.

As shown in figure 6, a number of interesting findings can be found from the results extracted from table I.

Firstly, the two ongoing trends identified throughout this paper are whereas IPSec improves the performance of OSPFv3, EIGRPv6's MD5 negatively affects its performance and that EIGRPv6 performs better in the point to point environment of Scenario 1 compared to that of Scenario 2. Figure 6 also agrees with this trend with the exception of the point to point cable removal with authentication time average.

Furthermore, a packet inspection using Wireshark was performed in addition to attempting to crack the type seven passwords implemented upon encrypting the running configurations within the Cisco 1841 routers. These tests meet the criteria for the fifth goal which is to examine each protocols security mechanism and implement them to compare their operational differences.

As shown in figures 7 and 8, the results of the packet inspection can be observed when a packet is captured and analysed using Wireshark.

```
⊞ Frame 251: 130 bytes on wire (1040 bits), 130 bytes captured (1040 bits
⊞ Ethernet II, Src: Cisco_6f:da:77 (00:22:55:6f:da:77), Dst: Cisco_6f:dc:
⊟ Internet Protocol Version 6, Src: fe80::222:55ff:fe6f:da77 (fe80::222:5
  ⊞ 0110 .... = Version: 6
  ⊞ .... 1110 0000 .... .... .... .... .... = Traffic class: 0x000000e0
    .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
    Payload length: 76
    Next header: ESP (50)
    Hop limit: 1
    Source: fe80::222:55ff:fe6f:da77 (fe80::222:55ff:fe6f:da77)
    [Source SA MAC: Cisco_6f:da:77 (00:22:55:6f:da:77)]
    Destination: fe80::222:55ff:fe6f:dc53 (fe80::222:55ff:fe6f:dc53)
    [Destination SA MAC: Cisco_6f:dc:53 (00:22:55:6f:dc:53)]
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
⊟ Encapsulating Security Payload
    ESP SPI: 0x000003ea (1002)
    ESP Sequence: 4
```

Fig. 7. OSPFv3's IPSec ESP Encrypted Packet

As shown by figures 7 and 8, the major difference between the two packets is that compared to OSPFv3's ESP IPSec encrypted packet, EIGRPv6's MD5 authenticated packet makes no attempt to hide the information within the packet. Therefore as figure 8 shows, information such as the autonomous system number, the "K" values in use and the Hello times used by EIGRPv6 can be discovered by capturing one packet.

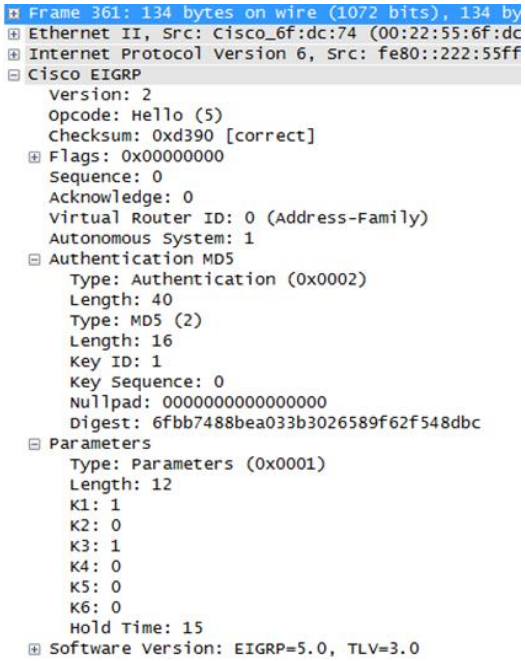

Fig. 8. EIGRPv6 MD5 Authenticated Packet

In addition using the tools provided by [13], a test was also performed to attempt to reverse the type seven passwords stored in the routers running configuration. This type seven password is used by both protocols authenticate a neighboring router and is encrypted using the "service password-encryption" command. The Cisco Type 7 Reversing tool found on [13] will be used to reverse the passwords stored in the routers running configuration file.

Upon attempting to reverse the passwords used by both protocols, it was discovered that whereas OSPFv3's passwords was only partially decrypted, EIGRPv6's MD5 authentication passwords was completely decrypted and therefore revealed the authentication password required to peer with a router in the topology. The reason for this is because whereas OSPFv3's ESP IPSec encryption requires a minimum password length of 40 characters, EIGRPv6's MD5 authentication mechanism specifies no minimum password length. Therefore, EIGRPv6 can be configured with potentially very weak passwords and making the implemented password prone to decryption as a result.

Lastly, the final goal set in the methodology was to observe any differences upon implementing both protocols.

Fig. 9. OSPFv3 Router ID Prompt

As revealed in figure 9, a key difference noticed when implementing OSPFv3 and EIGRPv6 is whereas OSPFv3 generates a router ID prompt upon first configuration, EIGRPv6 does not generate this prompt for the creation of a router ID. As discussed previously, both protocols will not begin routing traffic until a router ID is created. As a result, a network administrator may spend time debugging EIGRPv6 only to find that the protocol would not route traffic due to the lack of a router ID.

VII. Conclusion

This paper finds that upon comparing the performance of OSPFv3 and EIGRPv6 using the tests that have been conducted throughout this project, EIGRPv6 was the faster performing protocol. However aside from the overall conclusion, a series of thought provoking results have been found in this project. These include:

- That EIGRPv6 performed better in every test when it was configured for the point to point topology of Scenario 1. EIGRPv6's performance was noticeably different when it was implemented into Scenario 2's LAN environment, taking longer to recover from simulated failures and dropping considerably more packets. It can therefore be assumed from the findings that EIGRPv6 performs better within a point to point configuration, rather than a LAN environment.
- OSPFv3's performance was relatively similar when implemented into Scenarios 1 and 2, but on average performed consistently better when IPSec was enabled. By comparison, EIGRPv6's performance was always degraded when its MD5 authentication mechanism was enabled.
- However despite this degradation, EIGRPv6 still outperformed OSPFv3 in terms of sheer speed while converging and adjusting to failures and therefore wins the performance comparison.

Therefore, the principle conclusion from the results of this paper is that when comparing OSPFv3 and EIGRPv6 within a small flat IPv6 enterprise network, EIGRPv6 outperforms OSPFv3 in terms of start-up and re-convergence speed and is therefore the faster protocol. This conclusion has been generated by testing OSPFv3 and EIGRPv6 in both a point to point and LAN based network environment, where OSPFv3 took consistently longer to complete its operations than that of EIGRPv6.

However whereas the MD5 authentication mechanism used by EIGRPv6 negatively affected its performance, IPSec noticeably improved OSPFv3's performance. This therefore makes OSPFv3 an attractive option to network administrators who wish to implement a routing protocol that integrates a strong security mechanism and operates within a hierarchical network topology. By comparison, EIGRPv6 is designed to operate on a typically flat network structure which may still limit its application.

References

[1] Wijaya, C. (2011) Performance Analysis of Dynamic Routing Protocol EIGRP and OSPF in IPv4 and IPv6 Network, Informatics and Computational Intelligence (ICI), 2011 First International Conference, pp. 335-360.

[2] Thorenoor, S.G. (2010) Dynamic Routing Protocol Implementation Decision Between EIGRP, OSPF and RIP Based on Technical Background using OPNET Modeler, Computer and Network Technology (ICCNT), 2010 Second International Conference, pp. 191-195.

[3] Krishnan,Y.N., G, Shobha. (2013) Performance Analysis of OSPF and EIGRP Routing Protocols for Greener Internetworking, Green High Performance Computing (ICGHPC), 2013 IEEE International Conference, pp. 1-4.

[4] Fitigau, I., Toderean, G. (2013) Network Performance Evaluation for RIP, OSPF and EIGRP Routing Protocols, Electronics, Computers and Artificial Intelligence (ECAI) 2013 International Conference, pp. 1-4.

[5] Savage, D., Slice, D., Ng, J., Moore, S., White, R. (2013) Enhanced Interior Gateway Routing Protocol Draft-Savage-EIGRP-00, IETF, Febuary 2013.

[6] Hinds, A., Atojoko, A., Zhu, S. (2013) Evaluation of OSPF and EIGRP Routing Protocols for IPv6, International Journal of Future Computer and Communication, 2(4), pp. 287-291.

[7] Teare, D. (2010) Implementing Cisco IP Routing (Route). 4th edn. Indianapolis: Cisco Press.

[8] Coltun, R., Ferguson, D., Moy, J., Lindem, A. (2008) RFC 5340 - OSPF for IPv6, IETF, July 2008.

[9] Gupta, M., Melam, N. (2006) RFC 4552 - Authentication / Confidentiality for OSPFv3, IETF, June 2006.

[10] Wen, X., Xu, C., Guan, J., Su, W., Zhang, H. (2010) Performance Investigation of IPsec Protocol Over IPv6 Network, Advanced Intelligence and Awareness Internet (AIAI 2010), 2010 International Conference, pp. 174-177.

[11] Graziani, R. (2012) IPv6 Fundamentals. 1st edn. Indianapolis: Cisco Press.

[12] Deering, S., Haberman, B., Jinmei, T., Nordmark, E., Zill, B. (2005) RFC 4007 - IPv6 Scoped Address Architecture, IETF, March 2005.

[13] Packet Life (2008) PacketLife.net. Cisco Type 7 Reverser. [Online]. Available at: http://packetlife.net/toolbox/type7/ Date of access: (January 24th 2014).