

## Convergence Routing Analysis in IPv6 Networks

S.Arun Kumar<sup>1</sup> and S.Mari Rajan<sup>2</sup>

PG Student, Communication Systems, Department of ECE, Valliammai Engineering College, Tamilnadu<sup>1</sup>  
Assistant Professor, Department of ECE, Valliammai Engineering College, Tamilnadu<sup>2</sup>  
arunkumar030393@gmail.com<sup>1</sup>, eceमारirajan@gmail.com<sup>2</sup>

---

**Abstract:** Internetworking is widely spread and used for different applications and in all domains. Their growth continues at an amazing rate sustained by its high penetration in both home networks and mobile markets. The internet is a worldwide publicly accessible system of interconnected computer networks, since IPV4 in network enables data sharing between two or more computers which minimize time and energy wastages. The exhaustion of available IPV4 addresses and other scale issues like routing table's explosion will occur in a near future. Routing is the heartbeat of the Internet. Several routing protocols exist nowadays but the most common ones are Routing Information Protocol (RIP) and Enhanced Interior Gateway Routing Protocol (EIGRP). Due to limitation of dynamic protocol, converging time may differ whenever modification occurs in the network. As a result, loss of packets more or less based properties of converging time that decrease the network performance. In order to overcome this, IPv6 network is proposed in this project with enabling the RIP and EIGRP open source dynamic protocols that dynamically update the routing information that helps to forward the packet from source to destination. The prime objectives of this project are to investigate the consequences of deploying RIP and EIGRP simultaneously on a network and the performance can be analysed and that can be implementing in the network to increase the QoS.

**Index term:** IPV4, IPV6, RIP, EIGRP.

---

### I. INTRODUCTION

The goal of this paper is to investigate the behaviour of routing convergence. It begins with an explanation of IP addressing. The paper discusses the two routing protocols: Routing Information Protocol (RIP) and Enhanced Interior Gateway Routing Protocol (EIGRP) into great detail. The paper then examines the structure of a routing table and the route selection process. In order to be practical in the investigation of the routing convergence, we perform an experiment that involved routers. It is assumed that an end customer requires redundancy for its Wide Area Network (WAN) connection. The customer purchases WAN connectivity from two different ISPs that are, running two different routing protocols hence routing information must be redistributed. We conduct the experiment such that network convergences under different failure situation are examined. We will also modify the timers of RIP and OSPF to inspect any improvement.

Routing protocols [8] are based on routing algorithms, which rely on various metrics to find the best path to transmit data across networks. Metrics include cost, bandwidth, maximum transmission unit (MTU), packet delay, and hop count. Routing protocols utilize a routing table to store the results of these metrics. Routing is the process of selecting paths in a network. In packet switching networks, routing directs traffic forwarding of logically addressed packets through intermediate nodes from their source to their ultimate destination. Routing protocols are designed to select and determine the best path to each router in the network. Routers should learn the next hop to send the packets. Forwarding data should be efficient and effective. Consequently, the routing decision of a protocol is very important for network performance. Among many routing protocols such as RIP and EIGRP, have been most widely used. In this paper, we use GNS 3 to simulate performance of the RIP and EIGRP routing protocols. We collected, compared, and analysed simulation results in the terms of network convergence, throughput, latency and packet loss. In this paper, we compare performance of RIP and EIGRP using GNS 3 simulator.

### II. DYNAMIC ROUTING PROTOCOLS OVERVIEW

Dynamic routing protocols play an important role in today's networks. They are used to facilitate the exchange of routing information between routers. They dynamically share information between routers, automatically update routing table when topology changes, and determine the best path to a destination. Compared to static routing, dynamic routing protocols have better scalability and adaptability and require less administrative overhead. Dynamic routing protocols allow routers to dynamically advertise and learn routes, determine available routes and identify the most efficient routes to a destination. Dynamic routing protocols

have the capability to maintain the network operation in case of a failure or when network configuration or topology change.

“Distance vector” [6][7] and “link state” [4] are used to describe routing protocols used by routers to forward packets. There are two groups of routing protocols, based on whether the routing protocol selects the best routing path based on a distance metric (the distance) and an interface (the vector) or selects the best routing path by calculating the state of each link in a path and finding the path with the lowest total metric to the destination. Distance vector protocols evaluate the best path based on distance, which can be measured in terms of hops or a combination of metrics calculated to represent a distance value. The IP Distance vector routing protocols in use today are RIP and IGRP. In link state routing, every node constructs a map of the connectivity to the network in the form of a graph showing connectivity of the nodes to each other. Each node then independently calculates the next best logical path to every possible destination in the network. The collection of best paths forms the node's routing table. Link state protocols have the routers announce their closest neighbours to every router in the network. Only a part of the table pertaining to its neighbours is distributed. EIGRP, OSPF [1][5], and Intermediate System Intermediate System (IS-IS)[1] are link state routing protocol.

### **III. ROUTING INFORMATION PROTOCOL (RIP)**

RIP is a distance vector dynamic routing protocol that employs the hop count as a routing metric. RIP[6] is implemented on top of the User Datagram Protocol (UDP) as its transport protocol. It is assigned the reserved port number 520. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from the source to a destination. The maximum number of permitted hops is 15. Hence a hop count of 16 is considered an infinite distance. This hop number limits the size of networks that RIP may support. RIP selects paths that have the smallest hop counts. However, the path may be the slowest in the network. RIP is simple and efficient in small networks. However, it may be inefficient in larger networks. Every RIP router broadcasts to other routers the best path based on its 2 calculation. Each router updates its own routing table by communicating with neighbouring routers. RIP router transmits full updates every 30 seconds. RIP may take 30–60 seconds to converge based on the features of distance vector protocols. RIP has lower power consumption and memory than some other routing protocols. RIP may be implemented in all types of routing devices. Consequently, it is a better choice in a multiband, mixed network.

Database each RIP router on a given network keeps a database that stores the following information for every computer in that network:

- IP Address: The Internet Protocol address of the computer.
- Gateway: The best gateway to send a message addressed to that IP address.
- Distance: The number of routers between this router and the router that can send the message directly to that IP address.
- Route change flag: A flag that indicates that this information has changed, used by other routers to update their own databases.

The RIP algorithm works like this Update. At regular intervals each router sends an update message describing its routing database to all the other routers that it is directly connected to. Some routers will send this message as often as every 30 seconds, so that the network will always have up-to date information to quickly adapt to changes as computers and routers come on and off the network. Propagation. When a router X finds that a router Y has a shorter and faster path to a router Z, then it will update its own routing database to indicate that fact. Any faster path is quickly propagated to neighbouring routers through the update process, until it is spread across the entire RIP network.

Each hop in a path from source to destination is assigned a hop-count value, which is typically 1. When a router receives a routing update that contains a new or changed destination network entry, the router adds one to the metric value indicated in the update and enters the network in the routing table. The IP address of the sender is used as the next hop.

### **IV. ENHANCED INTERIOR GATEWAY ROUTING PROTOCOL (EIGRP)**

EIGRP [6] is a Cisco proprietary routing protocol. It is based on a new route calculation algorithm called the Diffusing Update Algorithm (DUAL) [2]. It has features of both distance vector and link state protocols. EIGRP metrics are based on reliability, MTU, delay, load, and bandwidth. Delay and bandwidth are the basic parameters for calculating metrics. EIGRP collects data from three tables. The first is the neighbours' table, which stores data about neighbouring routers that are directly accessible through interfaces that are connected. The second is the topology table, which contains the aggregation of the routing tables that are gathered from all neighbours that are directly connected. It contains a list of destination networks in the EIGRP routed network and their respective metrics. The third routing table stores the actual routes to all destinations.

EIGRP differs from most distance vector protocols because it does not rely on periodic route dumps. Hence, it is capable of maintaining its topology table. Information that is to be routed is only exchanged when the new neighbours adjacency is established. The EIGRP router maintains its own routing table and tables of its neighbours [3]. The EIGRP router broadcasts to other neighbours if it cannot locate a router based on its routing database.

Diffusing Update Algorithm (DUAL) is given by

*Feasible Distance (FD)*: The lowest cost needed to reach the destination is usually termed as the feasible distance for that specific destination.

*Reported Distance (RD)*: A router has a cost for reaching the destination and it is denoted as reported distance.

*Successor*: A successor is basically an adjacent router which determines the least-cost route to the destination network.

*Feasible Successor (FS)*: It is an adjacent router which is used to offer a loop free [2] backup path to the destination by fulfilling the conditions of feasible condition.

*Feasible Condition (FC)*: After the condition of FD is met, FC is used in order to select the reasonable successor.

## V. SCENARIO DESIGNED

The network topology has been designed in GNS 3 (Graphical Network Simulator 3). I have designed a RIP (Routing Information Protocol) and EIGRP (Enhanced Interior Gateway Routing Protocol) implemented in IPv6 network. Fig 1 shows the network topology,

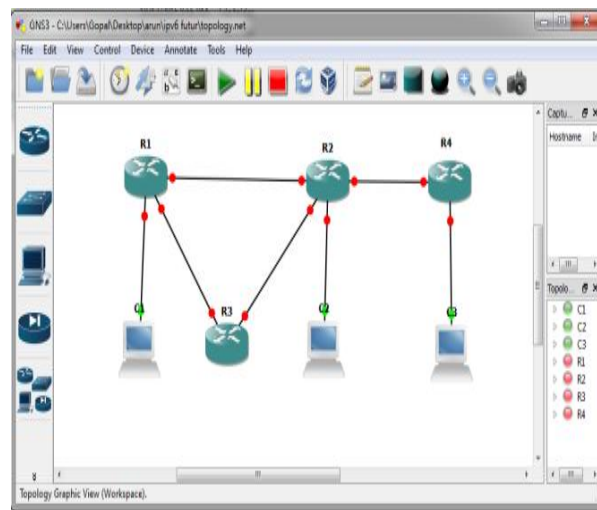


Fig 1:Network Topology

GNS3 is an excellent complementary tool to real labs for network engineers, administrators and people want to study for certifications such as Cisco CCNA, CCNP, CCIP and CCIE as well as Juniper JNCIA, JNCIS and JNCIE. It can also be used to experiment features of Cisco IOS, Juniper JunOS or to check configurations that need to be deployed later on real routers.

This is an open source, free program that may be used on multiple operating systems, including Windows, Linux, and MacOS X.

In RIP protocol, if any changes occurs in the network means it starts losing packets and it takes more time to regains its path, in between more number of packets get lost. Fig 2 and 3 shows the packet loss scenario,

```

Virtual PC Simulator for Dynapics/GNS3
58 2001:2222::2 171.600 ms 171.601 ms 156.000 ms
59 2001:2222::2 171.600 ms 140.401 ms 171.600 ms
60 2001:2222::2 156.000 ms 140.400 ms 171.601 ms
61 2001:2222::2 171.600 ms 124.800 ms 124.801 ms
62 2001:2222::2 124.800 ms 156.000 ms 140.400 ms
63 2001:2222::2 140.401 ms 124.800 ms 171.600 ms
64 2001:2222::2 312.001 ms 187.200 ms 171.600 ms

UPCS[1] > trace 2001:7777::2

trace to 2001:7777::2, 64 hops max
1 2001:1111::1 62.400 ms 62.400 ms 31.200 ms
2 2001:2222::2 109.200 ms 78.000 ms 62.400 ms
3 2001:4444::1 124.801 ms 109.200 ms 109.200 ms
4 2001:5555::2 156.000 ms 109.201 ms 124.800 ms
5 2001:7777::2 140.400 ms 124.800 ms 187.201 ms

UPCS[1] > ping 2001:7777::2 -c 500

2001:7777::2 icmp6_seq=1 ttl=58 time=327.600 ms
2001:7777::2 icmp6_seq=2 ttl=58 time=140.400 ms
2001:7777::2 icmp6_seq=3 ttl=58 time=140.400 ms
2001:7777::2 icmp6_seq=4 ttl=58 time=124.800 ms
2001:7777::2 icmp6_seq=5 ttl=58 time=109.200 ms
2001:7777::2 icmp6_seq=6 ttl=58 time=109.200 ms
2001:7777::2 icmp6_seq=7 ttl=58 time=109.201 ms
2001:7777::2 icmp6_seq=8 ttl=58 time=124.800 ms
2001:7777::2 icmp6_seq=9 ttl=58 time=109.200 ms
2001:7777::2 icmp6_seq=10 ttl=58 time=156.000 ms
2001:7777::2 icmp6_seq=11 ttl=58 time=124.801 ms
2001:7777::2 icmp6_seq=12 ttl=58 time=124.800 ms
2001:7777::2 icmp6_seq=13 ttl=58 time=140.400 ms
2001:7777::2 icmp6_seq=14 ttl=58 time=93.600 ms
2001:7777::2 icmp6_seq=15 timeout
*2001:1111::1 icmp6_seq=16 ttl=64 time=62.400 ms <ICMP type:1, code:0, No rou
to destination>
*2001:1111::1 icmp6_seq=17 ttl=64 time=46.800 ms <ICMP type:1, code:0, No rou
to destination>
*2001:1111::1 icmp6_seq=18 ttl=64 time=62.401 ms <ICMP type:1, code:0, No rou
to destination>
*2001:1111::1 icmp6_seq=19 ttl=64 time=31.200 ms <ICMP type:1, code:0, No rou
to destination>
*2001:1111::1 icmp6_seq=20 ttl=64 time=46.800 ms <ICMP type:1, code:0, No rou

```

Fig 2: packet loss scenario

```

Virtual PC Simulator for Dynapics/GNS3
2001:7777::2 icmp6_seq=340 timeout
2001:7777::2 icmp6_seq=341 timeout
2001:7777::2 icmp6_seq=342 timeout
2001:7777::2 icmp6_seq=343 timeout
2001:7777::2 icmp6_seq=344 timeout
2001:7777::2 icmp6_seq=345 timeout
2001:7777::2 icmp6_seq=346 timeout
2001:7777::2 icmp6_seq=347 timeout
2001:7777::2 icmp6_seq=348 timeout
2001:7777::2 icmp6_seq=349 timeout
2001:7777::2 icmp6_seq=350 timeout
2001:7777::2 icmp6_seq=351 timeout
2001:7777::2 icmp6_seq=352 ttl=56 time=140.400 ms
2001:7777::2 icmp6_seq=353 ttl=56 time=140.400 ms
2001:7777::2 icmp6_seq=354 ttl=56 time=140.400 ms
2001:7777::2 icmp6_seq=355 ttl=56 time=171.601 ms
2001:7777::2 icmp6_seq=356 ttl=56 time=171.600 ms
2001:7777::2 icmp6_seq=357 ttl=56 time=140.400 ms
2001:7777::2 icmp6_seq=358 ttl=56 time=140.400 ms
2001:7777::2 icmp6_seq=359 ttl=56 time=156.000 ms
2001:7777::2 icmp6_seq=360 ttl=56 time=156.000 ms
2001:7777::2 icmp6_seq=361 ttl=56 time=140.400 ms
2001:7777::2 icmp6_seq=362 ttl=56 time=156.001 ms
2001:7777::2 icmp6_seq=363 ttl=56 time=140.400 ms
2001:7777::2 icmp6_seq=364 ttl=56 time=124.800 ms
2001:7777::2 icmp6_seq=365 ttl=56 time=156.000 ms
2001:7777::2 icmp6_seq=366 ttl=56 time=140.400 ms
2001:7777::2 icmp6_seq=367 ttl=56 time=124.800 ms

```

Fig 3: Packet takes another path once the link gets failed

In EIGRP protocol, if any changes occurs in the network means it starts losing packets and it takes lesser of time to regains its path, in between less number of packets get lost when compared to RIP protocol. So EIGRP is the better protocol in IPv6 network when compared to RIP protocol. Fig 4 shows the packet loss scenario,

```

UPCS[1] ping 2001::2 -c 500
2001::2: icmp6_seq=1 ttl=58 time=140.400 ms
2001::2: icmp6_seq=2 ttl=58 time=140.400 ms
2001::2: icmp6_seq=3 ttl=58 time=140.401 ms
2001::2: icmp6_seq=4 ttl=58 time=140.400 ms
2001::2: icmp6_seq=5 ttl=58 time=140.400 ms
2001::2: icmp6_seq=6 ttl=58 time=140.400 ms
2001::2: icmp6_seq=7 ttl=58 time=140.401 ms
2001::2: icmp6_seq=8 ttl=58 time=140.400 ms
2001::2: icmp6_seq=9 ttl=58 time=124.800 ms
2001::2: icmp6_seq=10 ttl=58 time=140.400 ms
2001::2: icmp6_seq=11 ttl=58 time=187.200 ms
2001::2: icmp6_seq=12 ttl=58 time=140.400 ms
2001::2: icmp6_seq=13 ttl=58 time=140.400 ms
2001::2: icmp6_seq=14 ttl=58 time=140.401 ms
2001::2: icmp6_seq=15 ttl=58 time=140.400 ms
2001::2: icmp6_seq=16 timeout
2001::2: icmp6_seq=17 timeout
2001::2: icmp6_seq=18 timeout
2001::2: icmp6_seq=19 timeout
2001::2: icmp6_seq=20 timeout
2001::2: icmp6_seq=21 timeout
2001::2: icmp6_seq=22 timeout
2001::2: icmp6_seq=23 timeout
2001::2: icmp6_seq=24 timeout
2001::2: icmp6_seq=25 timeout
2001::2: icmp6_seq=26 timeout
2001::2: icmp6_seq=27 timeout
2001::2: icmp6_seq=28 timeout
2001::2: icmp6_seq=29 ttl=56 time=234.001 ms
2001::2: icmp6_seq=30 ttl=56 time=156.000 ms
2001::2: icmp6_seq=31 ttl=56 time=171.600 ms
2001::2: icmp6_seq=32 ttl=56 time=156.000 ms
2001::2: icmp6_seq=33 ttl=56 time=171.601 ms
2001::2: icmp6_seq=34 ttl=56 time=171.600 ms
2001::2: icmp6_seq=35 ttl=56 time=171.600 ms
    
```

Fig 4 : Packet takes another path once the link gets failed

## VI. RESULTS

The significance of time parameters on network performance is crucial since it decides the overall characteristics of the network both in time domain and in terms of packet loss. When there is a change in the network, the information is updated quickly and the optimal route is selected with minimum cost. In RIP the variation of timers results in reduction of packet loss and faster convergence time, where as in EIGRP the varying timers information has little impact on packet loss and convergence time. Also when there is a change in the network like addition or deletion of nodes and link failures occurrence the information will update automatically at that time.

The parameters here used is

- Convergence time
- Packet Loss
- Throughput

### A. Convergence time:

Convergence time is a measure of how fast a group of routers reach the state of convergence. Convergence occurs as a result of a change in network topology, i.e., a link becoming available or unavailable. The time required before all of the routers can reach a destination regarding the new topology i.e., a link gets failed in the current topology. The EIGRP has the fast convergence time as compared to RIP.

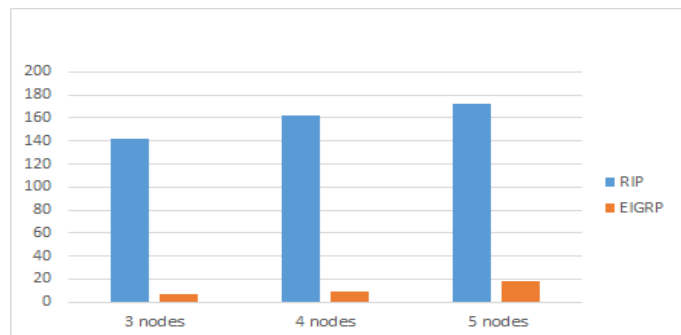


Fig.5 Graph for convergence time

**B. Packet Loss:**

Packet loss is the failure of one or more transmitted packets to arrive at their destination. The losses are usually due to congestion on the network. In EIGRP (Enhanced Interior Gateway Routing protocol) the packet loss will be less when compared to RIP (Routing Information protocol).

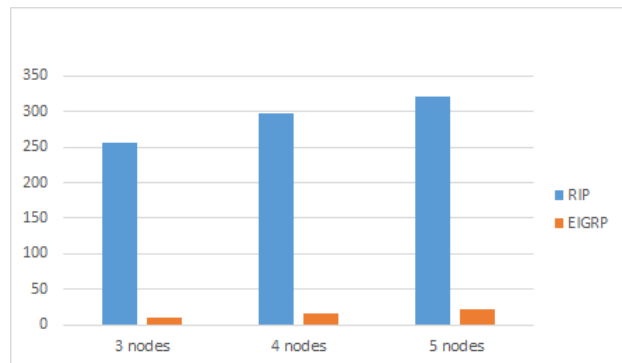


Fig. 6 Graph for packet loss

**C.Throughput:**

Throughput is the measure of how many units of information a system can process in a given amount of time. It is applied broadly applied to system ranging from various aspects of computer and network systems to organizations. Related measures of system productivity include, the speed with which some specific workload can be completed, and response time. The amount of time between a single interactive user request and receipt of the responses.EIGRP protocol has the higher throughput when compared to RIP protocol.Throughput = packet size / latency

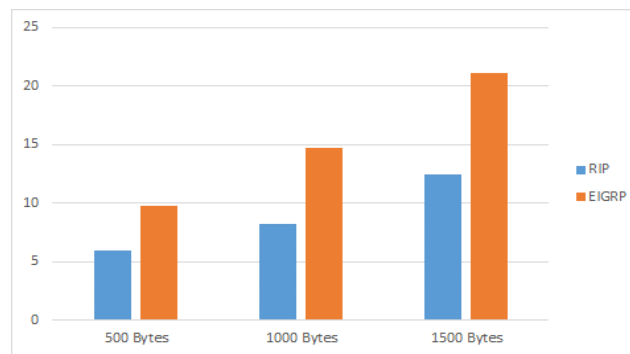


Fig. 7 Graph for Throughput

**VII. CONCLUSION**

In this paper we are implementing the RIP (Routing information Protocol) and EIGRP (Enhanced Interior Gateway Routing Protocol) open source dynamic protocols, that dynamically update the routing information that helps to forward the packet from source to destination. The prime objectives of this project are to investigate the consequences of deploying RIP and EIGRP simultaneously on a network and the performance can be analyzed and that can be implement in the network to increase the QoS.With these we are getting that EIGRP has the less packet loss when compared to RIP protocol and also it has better convergence time and throughput than the RIP protocol.

**REFERENCES:**

- [1]. Franck Le and João Luís Sobrinho, *Member, IEEE*, "Interconnecting Routing Instances", IEEE/Acm Transactions On Networking, Vol. 22, No. 2, April 2014.
- [2]. M. Goyal, M. Soperi, E. Baccelli, G. Choudhury, A. Shaikh, H. Hosseini, and K. Trivedi, "Improving convergence speed and scalability in ospf: A survey," *IEEE Commun. Surveys Tut.*, vol. 14, no. 2, pp.443–463, 2nd Quart., 2012.
- [3]. C. Filsfils, P. Francois, M. Shand, B. Decraene, J. Uttaro, N. Leymann, and M. Horneffer, "Loop-free alternate (LFA) applicability in service provider (SP) networks," Internet Engineering Task Force, RFC 6571 (Informational), Jun. 2012 [Online]. Available: <http://www.ietf.org/rfc/rfc6571.txt>

- [4]. A. Kvalbein, A. F. Hansen, T. Čičić, S. Gjessing, and O. Lysne, "Multiple routing configurations for fast IP network recovery," *IEEE/ACM Trans. Netw.*, vol. 17, no. 2, pp. 473–486, Apr. 2009.
- [5]. P. Francois and O. Bonaventure, "Avoiding transient loops during the convergence of link-state routing protocols," *IEEE/ACM Trans. Netw.*, vol. 15, no. 6, pp. 1280–1292, Dec. 2007.
- [6]. P. Francois, M. Shand, and O. Bonaventure, "Disruption free topology reconfiguration in OSPF networks," in *Proc. IEEE INFOCOM*, Anchorage, AK, USA, May 2007, pp. 89–97.
- [7]. O. J. S. Parra, A. P. Rios, and G. L. Rubio "IPV6 and IPV4 QoS mechanisms," in Proc. of International Organization for Information Integration and Web-based Application and Services, , pp. 463-466, ,2011.
- [8]. Thorenoor S.G," Dynamic Routing Protocol Implementation Decision between EIGRP, OSPF and RIP based on Technology Background Using OPNET Modeler ",IEEE Conference on Computer and Network Technology (ICCNT), pp. 191-195, 2010.