PERFORMANCE ANALYSIS OF INTERIOR GATEWAY PROTOCOLS

P.Priyadhivya[1], S.Vanitha[2]

[1]Department of Electronics and Communication Engineering, SNSCT, Coimbatore (India)

[2]Assistant Professor, Department of Electronics and Communication Engineering, SNSCT, Coimbatore (India)

ABSTRACT

Routing is usually performed by a dedicated device called a router. Routing is a key feature of the internet because it enables messages to pass from one computer to another and eventually reach the target machine. Each intermediary computer performs routing by passing along the message to the next computer. The most commonly used routing protocols are RIP (Routing Information Protocol), OSPF (Open Shortest Path First) and EIGRP (Enhanced Interior Gateway Routing Protocol). These are the interior gateway routing protocols that have been developed for IP networks and it is used to exchange routing information within autonomous systems. Performance analysis of interior gateway protocols in IPv6 networks is done in terms of Convergence time and Packet loss.

Keywords: RIP, OSPF, EIGRP, IGP, Autonomous System, Routing Protocols

I. INTRODUCTION

The term IGP (Interior Gateway Protocol) is used to describe any routing protocol operating as a separate routing domain within an AS. IGPs learn about routes to networks that are internal to the AS, hence the name Interior. Within an organization's network there may be one or more routing protocols (IGPs) keeping track of the routes to subnets within the AS. Routers running a single IGP (routing protocol) only share route information with other routers running the same routing protocol. Routers running more than one IGP, like RIP and OSPF, are participants in two separate routing domains. These routers are referred to as border routers, that is, they sit on the border between two IGP routing domains. The IGP is classified into Distance vector routing protocol, Link state routing protocol, Hybrid routing protocol.

1.1 Distance Vector Routing

The distance-vector routing is a type of algorithm used by routing protocols to discover routes on an interconnected network. The primary distance-vector routing algorithm is the Bellman-Ford algorithm. Distance-vector routing refers to a method for exchanging route information. A router will advertise a route as a vector of direction and distance. Direction refers to a port that leads to the next router along the path to the destination, and distance is a metric that indicates the number of hops to the destination, although it may also be an arbitrary value that gives one route precedence over another. Internetwork routers exchange this vector information and build route lookup tables from it. Distance vector as the name suggests uses distance between remote networks to determine the best path to a remote network. The distance vector metric is typically the hop.

It's not a measure of distance as such, rather a count of number of routers in between the router and the destination network. The examples of Distance vector routing protocols are RIPv1(version1), RIPv2(version 2), RIPng(Next generation), IGRP(Interior Gateway Routing Protocol).

1.2 Link State Routing

Link state protocols are based on Shortest Path First (SPF) algorithm to find the best path to a destination. Shortest Path First (SPF) algorithm is also known as Dijkstra algorithm, since it is conceptualized by Dijkstra. Link state routing always try to maintain full networks topology by updating itself incrementally whenever a change happen in network. In Shortest Path First (SPF) algorithm, whenever a link's state changes, a routing update called a Link-State Advertisement (LSA) is exchanged between routers. When a router receives an LSA routing update, the link-state algorithm is used to recalculate the shortest path to affected destinations. Each router constructs a map of the complete network. The examples of Link state routing are Open Shortest Path First (OSPF), Intermediate system to intermediate system (IS-IS).

1.3 Hybrid Routing Protocol

Hybrid routing protocols have both the features of distance vector routing protocols and linked state routing protocols. One example is Enhanced Interior Gateway Routing Protocol (EIGRP).

II. EXISTING SYSTEM

Internet Protocol version 4 (IPv4) is the delivery mechanism used by the TCP/IP protocols. It is the fourth version in the development of the Internet Protocol (IP) Internet and routes most traffic on the Internet. IPv4 uses 32 bit addressing have maximum of 2^{32} combinations of addresses..It is an unreliable and connectionless datagram protocol – a best effort delivery service. The best effort means that IPv4 provides no error or flow control (expect for error detection on the header). IPv4 assumes the unreliability of the underlying layers and does its best to get a transmission through its destination but with no guarantees.

If reliability is important, IPv4 must be paired with a reliable protocol such as TCP. An example of a more commonly understood best effort delivery service is the post office. The post office does its best to deliver the mail but does not always succeed. If an unregistered letter is lost, it is up to the sender or would be recipient to discover the loss and rectify the problem. The post office itself does not keep track of every letter and cannot notify a sender of loss or damage.

IPv4 is a connectionless protocol for a packet switching network that uses the datagram approach. This means that each datagram is handled independently, and each datagram can follow a different route to the destination. This implies that datagram sent by the same source to the same destination could arrive out of order. Also, some could be lost or corrupted during transmission. Again, IPv4 relies in a higher level protocol to take care of all these problems. The limitations of IPv4 networks are;

- IPv4 is unreliable & connectionless datagram protocol.
- It provides no flow control or error control.
- It provides no encryption & authentication.
- It has less address space and provides less security.
- It has more delay and does not provide auto configuration facility.

III. PROPOSED SYSTEM

There are two basic IP versions: IPv4 and IPv6. Internet Protocol version 6 (IPv6) is a version of the Internet Protocol (IP). It is designed to succeed the Internet Protocol version 4 (IPv4). IPv6 is the new version of Internet Protocol that contains addressing information and some control information enabling packets to be routed in the network. IPv6 is also called next generation IP or IPng. IPv6 uses 128-bit addresses, so it supports 2^{128} addresses. The advantages of IPv6 networks are;

- IPv6 gives better QoS.
- It offers better mobility features.
- It provides better end-to-end connectivity.
- IPv6 offers ease of administration.
- It provides encryption & authentication.
- It provides less latency, supports resource allocation & has large address space.

In IPv6 networks RIP, OSPF, EIGRP protocols are enabled and it dynamically updates the routing information that helps to forward the packets from source to destination.

3.1 RIP

The Routing Information Protocol (RIP) is one of a family of IP Routing protocols, and is an Interior Gateway Protocol (IGP) designed to distribute routing information within an Autonomous System (AS).RIP is a simple vector routing protocol with many existing implementations in the field. In a vector routing protocol, the routers exchange network reachability information with their nearest neighbors. In other words, the routers communicate to each other the sets of destinations ("address prefixes") that they can reach, and the next hop address to which data should be sent in order to reach those destinations. This contrasts with link-state IGPs; vectoring protocols exchange routes with one another, whereas link state routers exchange topology information, and calculate their own routes locally.A vector routing protocol floods reachability information throughout all routers participating in the protocol, so that every router has a routing table containing the complete set of destinations known to the participating routers.

- **RIP Version 1**

RIP uses classful routing. The periodic routing updates do not carry subnet information, lacking support for variable length subnet masks(VLSM). In other words, all subnets in a network class must have the same size. There is also no support for router authentication.

- **RIP Version 2**

Due to the some deficiencies of the original RIP specification, RIP version 2 (RIPv2) was developed. It includes the ability to carry subnet information, thus supporting Classless Inter-Domain Routing (CIDR). To maintain backward compatibility, the hop count limit of 15 remained. It uses MD5 mechanism for authentication.

- **RIPng**

RIPng (RIP next generation) is an extension of RIPv2 for support of IPv6, the next generation Internet Protocol. While RIPv2 supports RIPv1 updates authentication, RIPng does not. IPv6 routers were at the time supposed to use IPsec for authentication, RIPv2 allows attaching arbitrary tags to routes, RIPng does not. RIPv2 encodes the next-hop into each route entry. RIPng requires specific encoding of the next hop for a set of route entries. The routing information protocol uses the following timers as part of its operation. They are;

Update timer

The update timer controls the time between routing updates. By default the value is 30 seconds.

Invalid timer

The invalid timer specifies how long a routing entry can be in the routing table without being updated. It is also called as expiration Timer. By default the value is 180 seconds.

Hold-down timer

The Hold Down timer tells the routers to hold down recently affected routes for some period. During this time no update can be done to that routing entry. The default value of this timer is 90 seconds.

Flush timer

The flush timer controls how long before a route is completely flushed from the routing table. By default the value is 120 seconds.

Routing Information Protocol has advantages in small networks. It is easy to understand, configure and is supported by almost all routers. Since its limited to 15 hops, any router beyond that distance is considered as infinity, and hence unreachable. RIP has very slow network convergence in large networks. If implemented in a large network, RIP can create a traffic bottleneck by multicasting all the routing tables every 30 seconds, which is bandwidth intensive. The routing updates take up significant bandwidth leaving behind very limited resources.RIP doesn’t support multiple paths on the same route and is likely to have more routing loops resulting in a loss of transferred data. RIP uses fixed hop count metrics to compare available routes, which cannot be used when routes are selected based on real-time data. This results in an increased delay in delivering packets and overloads network operations due to repeated processes. In IPv6 networks RIPng protocol is used and by modifying the update time, performance of the network is increased.

3.2 OSPF

The OSPF (Open Shortest Path First) protocol is one of a family of IP Routing protocols, and is an Interior Gateway Protocol (IGP) for the Internet, used to distribute IP routing information throughout a single Autonomous System (AS) in an IP network. The OSPF protocol is a link-state routing protocol, which means that the routers exchange topology information with their nearest neighbors. The topology information is flooded throughout the AS, so that every router within the AS has a complete picture of the topology of the AS. This picture is then used to calculate end-to-end paths through the AS, normally using a variant of the Dijkstra algorithm. OSPF supports a variable network subnet mask so that a network can be subdivided.

OSPF defines the following categories of Routers.

- **Internal router(IR)**

An Internal Router is a router that has only OSPF neighbor relationships with routers in the same area.

- **Area border router(ABR)**

Routing devices that belong to more than one area and connect one or more OSPF areas to the backbone area are called area border routers (ABRs). At least one interface is within the backbone while another interface is in another area. ABRs also maintain a separate topological database for each area to which they are connected.

- **Backbone router(BR)**

Backbone Routers are part of the OSPF backbone. This includes all area border routers and also routers connecting different areas.

- **Autonomous system boundary router(ASBR)**

Routing devices that exchange routing information with routing devices in non-OSPF networks are called AS boundary routers. They advertise externally learned routes throughout the OSPF AS. Depending on the location of the AS boundary router in the network, it can be an ABR, a backbone router, or an internal router (with the exception of stub areas). Routing devices within the area where the AS boundary router resides know the path to that AS boundary router. Any routing device outside the area only knows the path to the nearest ABR that is in the same area where the AS boundary router resides.

In addition to the four router types, OSPF uses the terms designated router (DR) and backup designated router (BDR), which are attributes of a router interface.

- **Designated router and Backup designated router**

A Designated Router (DR) is the router interface elected among all routers on a network segment, and Backup designated (BDR) is a backup for the Designated Router. Designated Routers are used for reducing network traffic by providing a source for routing updates. The Designated Router maintains a complete topology table of the network and sends the updates to the other routers via multicast. All routers in an area will form a slave/master relationship with the Designated Router.

OSPF uses the following timers;

- **Hello interval**

Routing devices send hello packets at a fixed interval on all interfaces, including virtual links, to establish and maintain neighbor relationships. The hello interval specifies the length of time, in seconds, before the routing device sends a hello packet out of an interface. This interval must be the same on all routing devices on a shared network. By default, the routing device sends hello packets every 10 seconds (broadcast and point-to-point networks) and 30 seconds (nonbroadcast multiple access (NBMA) networks).

- **Poll interval**

Routing devices send hello packets for a longer interval on nonbroadcast networks to minimize the bandwidth required on slow WAN links. The poll interval specifies the length of time, in seconds, before the routing device sends hello packets out of the interface before establishing adjacency with a neighbor. By default, the routing device sends hello packets every 120 seconds until active neighbors are detected. Once the routing device detects an active neighbor, the hello packet interval changes from the time specified in the poll interval to the time specified in the hello interval.

- **LSA retransmission interval**

When a routing device sends LSAs to its neighbors, the routing device expects to receive an acknowledgment packet from each neighbor within a certain amount of time. The LSA retransmission interval specifies the length of time, in seconds, that the routing device waits to receive an LSA packet before retransmitting the LSA to an interface’s neighbors. By default, the routing device waits 5 seconds for an acknowledgment before retransmitting the LSA.

- **Dead interval**

If a routing device does not receive a hello packet from a neighbor within a fixed amount of time, the routing device modifies its topology database to indicate that the neighbor is nonoperational. The dead interval specifies the length of time, in seconds, that the routing device waits before declaring that a neighboring routing device is unavailable. This is an interval during which the routing device receives no hello packets from the neighbor. This interval must be the same on all routing devices on a shared network. By default, this interval is four times the default hello interval, which is 40 seconds (broadcast and point-to-point networks) and 120 seconds (NBMA networks).

- **Transit delay**

Before a link-state update packet is propagated out of an interface, the routing device must increase the age of the packet. The transit delay sets the estimated time required to transmit a link-state update on the interface. By default, the transit delay is 1 second.

OSPF routing protocol has a complete knowledge of network topology allowing routers to calculate routes based on incoming requests. Additionally, OSPF has no limitations in hop count, it converges faster than RIP, and has better load balancing. A downside with OSPF is that it doesn’t scale when there are more routers added to the network. This is because it maintains multiple copies of routing information. An OSPF network with intermittent links can increase traffic every time a router sends information. This lack of scalability in OSPF makes it unsuitable for routing across the Internet.OSPFv2 is used in IPv4 networks. In IPv6 networks OSPFv3 protocol is used and by modifying the hello interval, performance is further increased.

3.3 EIGRP

Enhanced Interior Gateway Routing Protocol (EIGRP) is considered as a Hybrid Routing Protocol because EIGRP has characteristics of both Distance Vector and Link State Routing Protocols. It is designed to give all the flexibility of routing protocols such as OSPF but with much faster convergence. EIGRP shares routing table information that is not available in the neighboring routers, thereby reducing unwanted traffic transmitted through routers. It uses Diffusing Update Algorithm (DUAL), which reduces the time taken for network convergence and improves operational efficiency. EIGRP is used on a router to share routes with other routers within the same autonomous system. Unlike RIP, EIGRP only sends incremental updates, reducing the workload on the router and the amount of data that needs to be transmitted. EIGRP calculates its metrics by using bandwidth, delay, reliability and load.

IV. RESULTS

4.1 Network Topology

The network topology is created with six routers and four clouds using Graphical Network Simulator (GNS 3) software. This is considered as a Wide Area Network and it is converged with RIP or OSPF protocols and the comparisons are made between them.

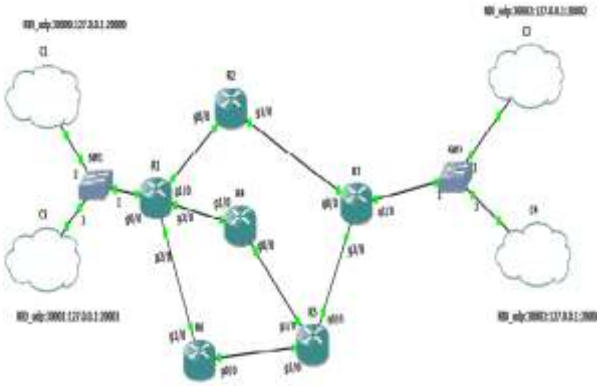

Fig. 1 IPv6 Network Topology

4.2 Convergence Time Analysis

The time taken for a packet to take alternative path when any link gets failure is termed as convergence time. The convergence time is measured in Wireshark software. While evaluating the performance of the convergence time of modified RIP and modified OSPF, modified OSPF has faster convergence than modified RIP Protocol.

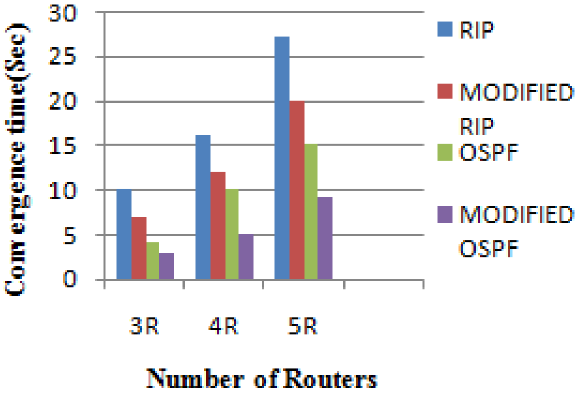

Fig. 2 Convergence Time

4.3 Packet Loss Analysis

Packet loss occurs when one or more packets of data travelling across a computer network fail to reach their destination. Packet loss is measured in VPCS (Virtual PC Simulator). While evaluating the performance of modified RIP and modified OSPF, modified OSPF has less packet loss.

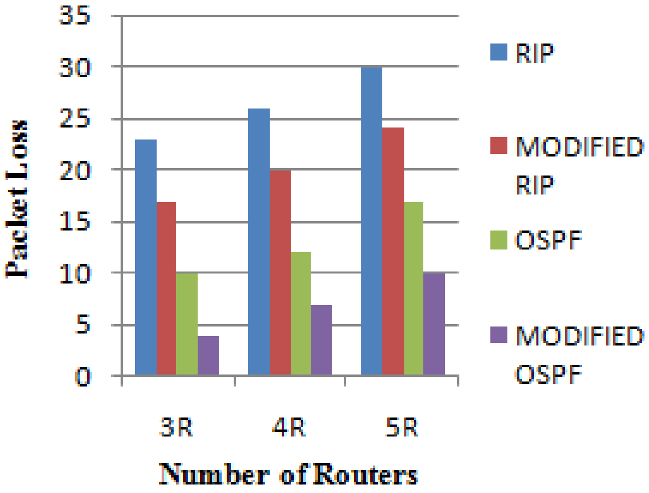

Fig. 3 Packet Loss

V. CONCLUSION AND FUTURE WORK

This project explains the need for implementing IPv6 technology to overcome some of the limitations involved in IPv4 technology. This paper also explains about different interior gateway protocols. From the simulation results compared to RIP, OSPF has faster convergence and less packet loss and it is suited well for wide area networks. The future work involves modifying the parameters of EIGRP protocol and analyzing the performance in IPv6 networks.

REFERENCES

[1] Vishal Sharma, Rajneesh Narula and Sameer Khullar "Performance Analysis of IEEE 802.3 using IGRP and EIGRP Routing Protocols" International Journal of Computer Applications(0975-8887) Volume 44-No13, April 2012.

[2] R.Rastogi, Y.Breitbart and M.Garofalakis, "Optimal configuration of ospf aggregates", IEEE/ACM transaction on networking , vol 11, April 2003.

[3] Cisco systems (2012), Enhanced Interior Gateway Routing Protocol (EIGRP) wide metrics, retrieved 14 March 2014.

[4] Ittiphon Krinpayorm and Suwat Pattaramalai, "Link recovery Comparison between OSPF & EIGRP", International Conference on Information and Computer Networks (ICICN 2012) IPCSIT Vol. 27 (2012) IACSIT Press, Singapore.

[5] Ioan Fitigau, Gavril Toderean, " Network performance Evaluation of RIP, OSPF & EIGRP Routing protocols", IEEE, 2013.

[6] Pankaj Rakheja, Prabhjot kaur, Performance Analysis of RIP, OSPF, IGRP and EIGRP Routing Protocols in a Network, International Journal of Computer Application, 2012.

[7] Dejan Spasov , Marjan Gushev, "On the Convergence of Distance Routing Protocols", ICT 2012.

[8] Poprzen, Nemanja, "Scaling and Convergence speed of EIGRPv4 and OSPFv2 dynamic routing protocols in hub and spoke network" IEEE 2009.

[9] Savage, Slice " Enhanced Interior Gateway Routing Protocol" Internet Engineering Task Force, 2013.

[10] Chandra Wijaya "Performance Analysis of Dynamic Routing Protocol EIGRP and OSPF in IPv4 and IPv6 Network", First International Conference on Informatics and Computational Intelligence, 2011.