Department of Electronics and Communications Engineering

"Comparative Analysis of Two Prominent Routing Protocols in IPv6 Network: OSPFv3 & EIGRPv6"

Prepared By

Md. Mahful Islam Sunvy
ID: 2012-2-55-046

Md. Nesar Uddin Majumder
ID: 2012-2-55-004

Supervised By

Md. Asif Hossain
Senior Lecturer, Dept. of ECE
August 2016

Letter of Transmittal

To
Md. Asif Hossain
Senior Lecturer
Department of Electronics and Communications Engineering
East West University

Subject: Submission of Project Report as (ETE-498)
Dear Sir,

I am pleased let you know that I have completed my project on "Comparative Analysis of Two Prominent Routing Protocols in IPv6 Network: OSPFv3 & EIGRPv6". Theattachment contain of the project that has been prepared for your evaluation and consideration. Working on this project has given me some new concepts. By applying those concepts we have tried to make something innovative by using my theoretical knowledge which I have acquired since last four years from you and the other honorable faculty members of EWU. This project would be a great help for us in future. I am very grateful to you for your guidance, which helped us a lot to complete my project and acquire practical knowledge.

Thanking You.
Yours Sincerely

_____
Md. Mahful Islam Sunvy
ID: 2012-2-55-046

_____
Md. Nesar Uddin Majumder
ID: 2012-2-55-004

Dept. of ECE
East West University

Declaration

This is certified that the project is done by us under the course "Project (ETE-498): Comparative Analysis of Two Prominent Routing Protocols in IPv6 Network: OSPFv3 & EIGRPv6". has not been submitted elsewhere for the requirement of any degree or any other purpose except for publication.

_____

Md. Mahful Islam Sunvy
ID: 2012-2-55-046

_____

Md. Nesar Uddin Majumder
ID: 2012-2-55-004

Acceptance

This Project paper is submitted to the Department of Electronics and Communications Engineering, East West University is submitted in partial fulfillment of the requirements for the degree of B.Sc. in ETE under complete supervision of the undersigned.

_____

Md. Asif Hossain
Senior Lecturer
Dept. of ECE
East West University

Abstract

Due to the huge demand of Internet, computer network has been transited from IPv4 to IPv6 environment. New routing protocols are also needed in IPv6 network. Among them two are very prominent: IETF's OSPF and Cisco's EIGRP. In IPv6 network, they are known as OSPFv3 and EIGRPv6 respectively. Though several researchers have worked in these area, but this paper have analyzed the comparisons between these two routing protocols more intensively. In this paper, packet loss, routing convergence speed and end to end delay have been considered as the parameters of the comparisons. The comparisons have been evaluated in Cisco's simulation environment; Packet Tracer.

TABLE OF CONTENTS

Table of Contents

CHAPTER 1: INTRODUCTION

IPv6, the latest version of Internet Protocol was first introduced in 1998. 128 bits are being used in IPv6, on the other hand, our running IPv4 is using 32 bits. Internet user is increasing day by day. Till the year 2000, 50% of total IPv4 space were used. To support upcoming generations, Internet protocol addressing system is needed to implant some up gradation [1]. By measuring these matters, IETF (Internet Engineering Task Force) started to develop another version of Internet Protocol to support IPv4 at 1994, which is known as IPv6 now. In the year 1998, the basic protocol (RFC 2460) was published [2]. There are many features in IPv6 as like [3, 4]:

1. In IPv6, IP header is better optimized by removing facultative fields by replacing them after IPv6 header. Here the IPv6 header is easily passable between the routers.
2. IPv6 has a very large addressing space with 128 bits. This is for giving the addressing and sub-netting an up gradation.
3. There might be no need of NAT (Network Address Translation) when IPv6 is fully applied.
4. For ISP (Internet Service Provider), more effective addressing and routing Infrastructure is provided.
5. With IPv6, a host can be configured automatically with the Link-local address.
6. IPSec is mandatory in IPv6. So there will be built in Internet security.
7. IPv6 is totally compatible for implementing new features by adding extension headers.

Routing IPv6 traffic is not supported by existing IPv4 routing protocols [5]. Development of IPv6 dynamic routing protocols are essential due to the importance upon reliability and scalability in many networks. Dynamic routing protocols are much better than the static routing protocol due to the ability to automatically adjust to network topological changes. These changes are included like failed components and rerouting traffic through alternative paths. There are several interior routing protocols are available for IPv6 network. Among them 2 are very prominent. One of them is OSPFv3 (Open Shortest Path First version 3) and another one is EIGRPv6 (Enhanced Interior Gateway Routing Protocol version 6).

There are several works have been done with these routing protocols. In [6], the authors have analyzed RIP and OSPF in IPv6 network. The authors in [7] have compared and discussed OSPF and EIGRP routing protocols with the IPv6 network and IPv4 network. IKram Ud Din and Saeed Mahfooz [8], shown the performance analysis of various routing protocols like RIP, OSPF, IGRP and EIGRP with the parameters such as packets dropping, traffic received, end to end delay and jitter in voice. Some other related works have been done in [9-13].

CHAPTER 2: OVERVIEW OF IPV6 ROUTING PROTOCOL: OSPFv3 & EIGRPv6

Brief History of OSPFv3

The Open Shortest Path First (OSPF) routing protocol was first conceived in the late 1980s. This was a time when the IETF was just starting to mature into an international networking standards organization. The IETF needed to develop a robust IP routing protocol suitable for larger networks. OSPF was first documented as a standard by John Moy in RFC 1131. Improvements were made in OSPF version 2, which was originally documented in RFC 1247 but later updated by RFC 2178 and then again in RFC 2328.

OSPF was then extensively modified to support IPv6. The IETF developed a new version OSPF that was specifically developed for IPv6 and was introduced in RFC 2740. Many network equipment vendors implemented OSPF for IPv6 as they developed their IPv6 products. OSPF for IPv6 (OSPF version 3) was then updated with RFC 5340. Fundamental OSPF mechanisms and algorithms unchanged but the packet and LSA formats are different in OSPFv3 because of the larger 128-bit IPv6 addresses. However, there were other subtle differences between OSPFv2 and OSPFv3 that network engineers should be aware of.

OSPFv2 and OSPFv3 Comparisons

Many aspects of the OSPF routing protocol remain the same between OSPFv2 and OSPFv3; such as the LSA flooding rules, the LSA aging mechanisms, and the interface types (broadcast, point-to-point, point-to-multipoint, among others). OSPFv3 Packet and LSA formats differ from OSPFv2. Specifically, OSPFv3 adds two new LSA types for Link (0x0008, tells neighbors about link-local addresses and IPv6 prefixes on link) and Intra-Area-Prefix (0x2009, IPv6 prefixes connected to a router). OSPFv2 has two flooding scope, AS wide and area wide but now OSPFv3 has three flooding scopes (noted with the S1 and S2 bits).

Similarities between OSPFv2 and OSPFv3:

1. Both are link-state Interior Gateway Protocol (IGP) routing protocols
2. Both use a 2-level hierarchy with Area 0.0.0.0 at the core
3. Both use Area Border Routers (ABRs) and Autonomous System Boundary Routers (ASBRs)
4. Both use the Shortest Path First (SPF) calculation within each area utilizing Edsger Dijkstra's SPF algorithm
5. Both use metrics that are based on interface bandwidth (or manual configuration)
6. Both have 5 common protocol packet types: Hello, Database description (DBD), Link-state request (LSR), Link-state update (LSU), Link-state acknowledgment (LSA)
7. They use similar interface types: Broadcast, P2P, P2MP, NBMA, and Virtual-Links
8. They have the same LSA flooding and aging timers

Differences between OSPFv2 and OSPFv3:

1. They use different address families (OSPFv2 is for IPv4-only, OSPFv3 can be used for IPv6-only or both protocols (more on this following))
2. OSPFv3 introduces new LSA types
3. OSPFv3 has different packet format
4. OSPFv3 uses different flooding scope bits (U/S2/S1)
5. OSPFv3 adjacencies are formed over link-local IPv6 communications
6. OSPFv3 runs per-link rather than per-subnet
7. OSPFv3 supports multiple instances on a single link, Interfaces can have multiple IPv6 addresses
8. OSPFv3 uses multicast addresses FF02::5 (all OSPF routers), FF02::6 (all OSPF DRs)
9. OSPFv3 Neighbor Authentication done with IPsec (AH)
10. OSPFv2 Router ID (RID) must be manually configured, which is still a 32-bit number.

Load-Balancing in OSPFv3:

When a device learns multiple routes to a specific network via multiple routing processes (or routing protocols), it installs the route with the lowest administrative distance in the routing table. Sometimes the device must select a route from among many learned via the same routing process with the same administrative distance. In this case, the device chooses the path with the lowest cost (or metric) to the destination. Each routing process calculates its cost differently and the costs may need to be manipulated in order to achieve load balancing.

OSPFv3 performs load balancing automatically in the following way. If OSPFv3 finds that it can reach a destination through more than one interface and each path has the same cost, it installs each path in the routing table. The only restriction on the number of paths to the same destination is controlled by the maximum-paths command. The default maximum paths are 16, and the range is from 1 to 64.

Addresses Imported into OSPFv3:

When importing the set of addresses specified on an interface on which OSPFv3 is running into OSPFv3, you cannot select specific addresses to be imported. Either all addresses are imported, or no addresses are imported.

OSPFv3 Customization:

You can customize OSPFv3 for your network, but you likely will not need to do so. The defaults for OSPFv3 are set to meet the requirements of most customers and features. If you must change the defaults, refer to the IPv6 command reference to find the appropriate syntax.

OSPFv3 Cost Calculation:

Because cost components can change rapidly, it might be necessary to reduce the volume of changes to reduce network-wide churn. The recommended values for S2, S3, and S4 in the second table below are based on network simulations that may reduce the rate of network changes. The recommended value for S1 is 0 to eliminate this variable from the route cost calculation.

The overall link cost is computed using the formula shown in the figure below.

Overall Link Cost Formula:

$$\text{Link Cost} = OC + BW\left(\frac{\text{Through out}_{\text{weight}}}{100}\right) + \text{Resources}\left(\frac{\text{Resources}_{\text{Weight}}}{100}\right) + \text{Latency}\left(\frac{\text{Latency}_{\text{weight}}}{100}\right) + \text{L2\_factor}\left(\frac{\text{L2\_weight}}{100}\right)$$

$$OC = \left[\frac{(\text{ospf\_reference\_bw})}{(\text{MDR})(1000)}\right]$$

Here, OSPF reference bandwidth=10^8

$$BW = \frac{(65535)\left(100 - \frac{\text{CDR}}{\text{MDR}}(100)\right)}{100}$$

$$resources = \frac{(100 - \text{resources})^3 (65535)}{1000000}$$

Latency=latency

$$\text{L2\_factor} = \frac{(100 - \text{RLQ})(65535)}{100}$$

The table below defines the symbols used in the OSPFv3 cost calculation:

Cost Component	Component Definition	
OC	The default OSPFv3 cost. Calculated from reference bandwidth using reference_bw / (MDR*1000), where reference_bw=10^8.	
A through D	Various radio-specific data-based formulas that produce results in the 0 through 64,000 range.	
A	CDR- and MDR-related formula: (2^16 * (100 – (CDR * 100 / MDR)))/100	
B	Resources related formula: ((100 – RESOURCES)^3 * 2^16 / 10^6)	
C	Latency as reported by the radio, already in the 0 through 64,000 range when reported (LATENCY).	
D	RLF-related formula: ((100 – RLF) * 2^16)/100	
S1 through S4	Scalar weighting factors input from the CLI. These scalars scale down the values as computed by A through D.The value of 0 disables and the value of 100 enables full 0 through 64,000 range for one component.	

Table 1: OSPF cost calculation component definitions

Because each network might have unique characteristics that require different settings to optimize actual network performance, these are recommended values intended as a starting point for optimizing an OSPFv3 network. The table below lists the recommended value settings for OSPFv3 cost metrics.

The default path costs were calculated using this formula, as noted in the following list. If these values do not suit your network, you can use your own method of calculating path costs.

- 56-kbps serial link—Default cost is 1785.
- 64-kbps serial link—Default cost is 1562.
- T1 (1.544-Mbps serial link)—Default cost is 64.
- E1 (2.048-Mbps serial link)—Default cost is 48.
- 4-Mbps Token Ring—Default cost is 25.
- Ethernet—Default cost is 10.
- 16-Mbps Token Ring—Default cost is 6.
- FDDI—Default cost is 1.
- X25—Default cost is 5208.
- Asynchronous—Default cost is 10,000.
- ATM—Default cost is 1.

To illustrate these settings, the following example shows how OSPFv3 cost metrics might be defined for a Virtual Multipoint Interface (VMI) interface:

```
interface vmi1
 ipv6 ospf cost dynamic weight throughput 0
 ipv6 ospf cost dynamic weight resources 29
 ipv6 ospf cost dynamic weight latency 29
 ipv6 ospf cost dynamic weight L2-factor 29
```

Force SPF in OSPFv3:

When the process keyword is used with the clear ipv6 ospf command, the OSPFv3 database is cleared and repopulated, and then the SPF algorithm is performed. When the force-spf keyword is used with the clear ipv6 ospf command, the OSPFv3 database is not cleared before the SPF algorithm is performed.

Brief History of EIGRPv6:

Enhanced Interior Gateway Routing Protocol (EIGRP) is an interior gateway protocol suited for many different topologies and media. In a well-designed network, EIGRP scales well and provides extremely quick convergence times with minimal network traffic. Some of the many advantages of EIGRP are:

- very low usage of network resources during normal operation; only hello packets are transmitted on a stable network
- when a change occurs, only routing table changes are propagated, not the entire routing table; this reduces the load the routing protocol itself places on the network
- rapid convergence times for changes in the network topology (in some situations convergence can be almost instantaneous)

EIGRP is an enhanced distance vector protocol, relying on the Diffused Update Algorithm (DUAL) to calculate the shortest path to a destination within a network.

There are two major revisions of EIGRP, versions 0 and 1. Cisco IOS versions earlier than 10.3(11), 11.0(8), and 11.1(3) run the earlier version of EIGRP; some explanations in this paper may not apply to that earlier version. We highly recommend using the later version of EIGRP, as it includes many performance and stability enhancements. A typical distance vector protocol saves the following information when computing the best path to a destination: the distance (total metric or distance, such as hop count) and the vector (the next hop). For instance, all the routers in the network in Figure 1 are running Routing Information Protocol (RIP). Router Two chooses the path to Network A by examining the hop count through each available path.

EIGRPv6 theory of operations:

Some of the many advantages of EIGRP are:

- very low usage of network resources during normal operation; only hello packets are transmitted on a stable network

- when a change occurs, only routing table changes are propagated, not the entire routing table; this reduces the load the routing protocol itself places on the network
- rapid convergence times for changes in the network topology (in some situations convergence can be almost instantaneous)

EIGRP is an enhanced distance vector protocol, relying on the Diffused Update Algorithm (DUAL) to calculate the shortest path to a destination within a network.

Major Revisions of the Protocols:

There are two major revisions of EIGRP, versions 0 and 1. Cisco IOS versions earlier than 10.3(11), 11.0(8), and 11.1(3) run the earlier version of EIGRP; some explanations in this paper may not apply to that earlier version. We highly recommend using the later version of EIGRP, as it includes many performance and stability enhancements.

Basic Theory:

A typical distance vector protocol saves the following information when computing the best path to a destination: the distance (total metric or distance, such as hop count) and the vector (the next hop). For instance, all the routers in the network in Figure 1 are running Routing Information Protocol (RIP). Router Two chooses the path to Network A by examining the hop count through each available path.

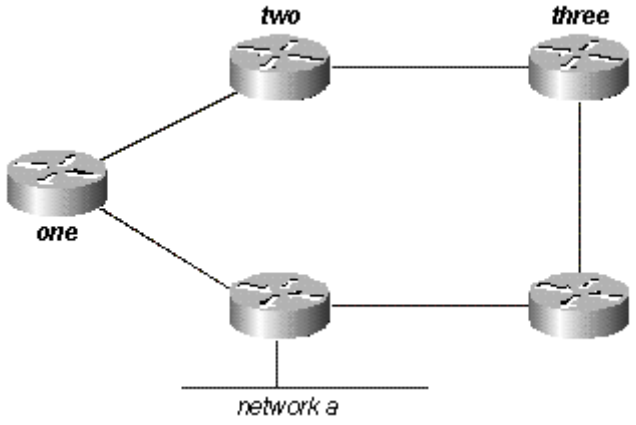

Fig. 1: Simple Network Topology

Since the path through Router Three is three hops, and the path through Router One is two hops, Router Two chooses the path through One and discards the information it learned through Three. If the path between Router One and Network A goes down, Router Two loses all connectivity with this destination until it times out the route of its routing table (three update periods, or 90 seconds), and Router Three re-advertises the route (which occurs every 30 seconds in RIP). Not including any hold-down time, it will take between 90 and 120 seconds for Router Two to switch the path from Router One to Router Three.

EIGRP, instead of counting on full periodic updates to re-converge, builds a topology table from each of its neighbor's advertisements (rather than discarding the data), and converges by either looking for a likely loop-free route in the topology table, or, if it knows of no other route, by querying its neighbors. Router Two saves the information it received from both Routers One and Three. It chooses the path through One as its best path (the successor) and the path through Three as a loop-free path (a feasible successor). When the path through Router One becomes unavailable, Router Two examines its topology table and, finding a feasible successor, begins using the path through Three immediately.

From this brief explanation, it is apparent that EIGRP must provide:

- a system where it sends only the updates needed at a given time; this is accomplished through neighbor discovery and maintenance
- a way of determining which paths a router has learned are loop-free
- a process to clear bad routes from the topology tables of all routers on the network
- a process for querying neighbors to find paths to lost destinations

We will cover each of these requirements in turn.

Neighbor Discovery and Maintenance:

To distribute routing information throughout a network, EIGRP uses non-periodic incremental routing updates. That is, EIGRP only sends routing updates about paths that have changed when those paths change.

The basic problem with sending only routing updates is that you may not know when a path through a neighboring router is no longer available. You cannot time out routes, expecting to receive a new routing table from your neighbors. EIGRP relies on neighbor relationships to reliably propagate routing table changes throughout the network; two routers become neighbors when they see each other's hello packets on a common network.

EIGRP sends hello packets every 5 seconds on high bandwidth links and every 60 seconds on low bandwidth multipoint links.

5-second hello:

- broadcast media, such as Ethernet, Token Ring, and FDDI
- point-to-point serial links, such as PPP or HDLC leased circuits, Frame Relay point-to-point sub interfaces, and ATM point-to-point sub interface
- high bandwidth (greater than T1) multipoint circuits, such as ISDN PRI and Frame Relay

60-second hello:

- multipoint circuits T1 bandwidth or slower, such as Frame Relay multipoint interfaces, ATM multipoint interfaces, ATM switched virtual circuits, and ISDN BRIs

The rate at which EIGRP sends hello packets is called the hello interval, and you can adjust it per interface with their command. The hold time is the amount of time that a router will consider a neighbor alive without receiving a hello packet. The hold time is typically three times the hello interval, by default, 15 seconds and 180 seconds. You can adjust the hold time with the ip hold-time eigrp command.
Note that if you change the hello interval, the hold time is not automatically adjusted to account for this change - you must manually adjust the hold time to reflect the configured hello interval.

It is possible for two routers to become EIGRP neighbors even though the hello and hold timers do not match. The hold time is included in the hello packets so each neighbor should stay alive even though the hello interval and hold timers do not match.

While there is no direct way of determining what the hello interval is on a router, you can infer it from the output of show ip eigrp neighbors on the neighboring router.
If you have the output of a show ip eigrp neighbors command from your Cisco device, you can use Cisco CLI Analyzer (registered customers only) to display potential issues and fixes. To use Cisco CLI Analyzer, you must have JavaScript enabled.

router# show ip eigrp neighbors
IP-EIGRP neighbors for process 1

H	*Address*	*Interface*	*Hold (sec)*	*Uptime*	*SRTT (ms)*	*RTO*	*Q Cnt*	*Seq Num*	*Type*
1	*10.1.1.2*	*Et1*	*13*	*12:00:53*	*12*	*300*	*0*	*620*	
0	*10.1.2.2*	*S0*	*174*	*12:00:56*	*17*	*200*	*0*	*645*	

```
rp-2514aa# show ip eigrp neighbor
IP-EIGRP neighbors for process 1
H   Address      Interface   Hold Uptime   SRTT   RTO  Q  Seq  Type
                             (sec)        (ms)       Cnt Num
1   10.1.1.2     Et1          12 12:00:55   12   300  0  620
0   10.1.2.2     S0          173 12:00:57   17   200  0  645
```

```
rp-2514aa# show ip eigrp neighbor
IP-EIGRP neighbors for process 1
H   Address      Interface   Hold Uptime   SRTT   RTO  Q  Seq  Type
                             (sec)        (ms)       Cnt Num
1   10.1.1.2     Et1          11 12:00:56   12   300  0  620
0   10.1.2.2     S0          172 12:00:58   17   200  0  645
```

The value in the Hold column of the command output should never exceed the hold time, and should never be less than the hold time minus the hello interval (unless, of course, you are losing hello packets). If the Hold column usually ranges between 10 and 15 seconds, the hello interval is 5 seconds and the hold time is 15 seconds. If the Hold column usually has a wider range - between 120 and 180 seconds - the hello interval is 60 seconds and the hold time is 180 seconds. If the numbers do not seem to fit one of the default timer settings, check the interface in question on the neighboring router - the hello and hold timers may have been configured manually.

Note:

- EIGRP does not build peer relationships over secondary addresses. All EIGRP traffic is sourced from the primary address of the interface.
- When configuring EIGRP over a multi-access Frame Relay network (point-to-multipoint, and so on), configure the broadcast keyword in the frame-relay map statements. Without the broadcast keyword the adjacencies would not establish between two EIGRP routers. Refer to Configuring and Troubleshooting Frame Relay for more information.
- There are no limitations on the number of neighbors that EIGRP can support. The actual number of supported neighbors depends on the capability of the device, such as:
    - memory capacity
    - processing power
    - amount of exchanged information, such as the number of routes sent
    - topology complexity
    - network stability

Building the topology table:

Now that these routers are talking to each other, what are they talking about? Their topology tables, of course! EIGRP, unlike RIP and IGRP, does not rely on the routing (or forwarding) table in the router to hold all of the information it needs to operate. Instead, it builds a second table, the topology table, from which it installs routes in the routing table.

Note: As of Cisco IOS versions 12.0T and 12.1, RIP maintains its own database from which it installs routes into the routing table.

To see the basic format of the topology table on a router running EIGRP, issue the topology command. The topology table contains the information needed to build a set of distances and vectors to each reachable network, including:

- lowest bandwidth on the path to this destination as reported by the upstream neighbor
- total delay
- path reliability
- path loading
- minimum path maximum transmission unit (MTU)
- feasible distance
- reported distance
- route source (external routes are marked)

Feasible and reported distance are discussed later in this section. If you have the output of a show ip eigrp topology command from your Cisco device, you can use Cisco CLI Analyzer (registered customers only) to display potential issues and fixes. To use Cisco CLI Analyzer, you must have JavaScript enabled.

EIGRPv6 Metrics:

EIGRP uses the minimum bandwidth on the path to a destination network and the total delay to compute routing metrics. Although you can configure other metrics, we do not recommend it, as it can cause routing loops in your network. The bandwidth and delay metrics are determined from values configured on the interfaces of routers in the path to the destination network.

For instance, in Figure 2 below, Router One is computing the best path to Network A.

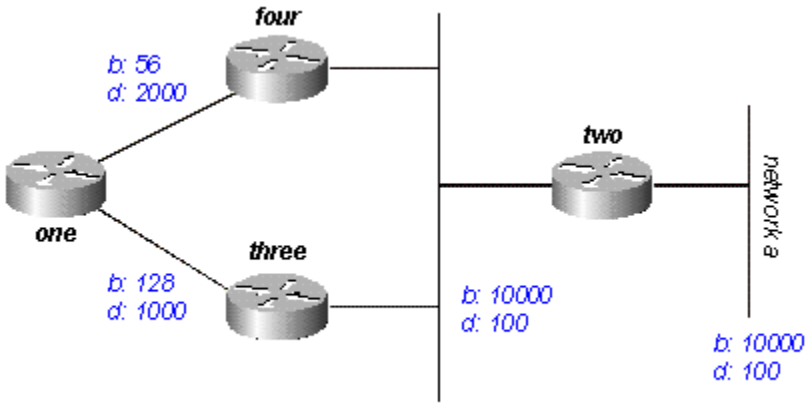

Fig. 2: Simple Network Topology

It starts with the two advertisements for this network: one through Router Four, with a minimum bandwidth of 56 and a total delay of 2200; and the other through Router Three, with a minimum bandwidth of 128 and a delay of 1200. Router One chooses the path with the lowest metric.

Let us compute the metrics. EIGRP calculates the total metric by scaling the bandwidth and delay metrics. EIGRP uses the following formula to scale the bandwidth:

- bandwidth = (10000000/bandwidth(i)) * 256

  where bandwidth(i) is the least bandwidth of all outgoing interfaces on the route to the destination network represented in kilobits.

EIGRP uses the following formula to scale the delay:

- delay = delay(i) * 256

where delay(i) is the sum of the delays configured on the interfaces, on the route to the destination network, in tens of microseconds. The delay as shown in the show ip eigrp topology or show interface commands is in microseconds, so you must divide by 10 before you use it in this formula. Throughout this paper, we use delay as it is configured and shown on the interface.

EIGRP uses these scaled values to determine the total metric to the network:

- metric = ([K1 * bandwidth + (K2 * bandwidth) / (256 – load) + K3 * delay] * [K5 / (reliability + K4)]) * 256

Note: These K values should be used after careful planning. Mismatched K values prevent a neighbor relationship from being built, which can cause your network to fail to converge.

Note: If K5 = 0, the formula reduces to Metric = ([k1 * bandwidth + (k2 * bandwidth)/(256 – load) + k3 * delay]) * 256.

The default values for K are:

- K1 = 1
- K2 = 0
- K3 = 1
- K4 = 0
- K5 = 0

For default behavior, you can simplify the formula as follows:

metric = bandwidth + delay

Cisco routers do not perform floating point math, so at each stage in the calculation, you need to round down to the nearest integer to properly calculate the metrics. In this example, the total cost through Router Four is:

In this example, the total cost through Router Four is:

minimum bandwidth = 56k

total delay = 100 + 100 + 2000 = 2200

[(10000000/56) + 2200] x 256 = (178571 + 2200) x 256 = 180771 x 256 = 46277376

And the total cost through Router Three is:

minimum bandwidth = 128k

total delay = 100 + 100 + 1000 = 1200

[(10000000/128) + 1200] x 256 = (78125 + 1200) x 256 = 79325 x 256 = 20307200

So to reach Network A, Router One chooses the route through Router Three.

Note the bandwidth and delay values we used are those configured on the interface through which the router reaches its next hop to the destination network. For example, Router Two advertised Network A with the delay configured on its Ethernet interface; Router Four added the delay configured on its Ethernet, and Router One added the delay configured on its serial.

Feasible Distance, Reported Distance, and Feasible Successor

Feasible distance is the best metric along a path to a destination network, including the metric to the neighbor advertising that path. Reported distance is the total metric along a path to a destination network as advertised by an upstream neighbor. A feasible successor is a path whose reported distance is less than the feasible distance (current best path). Figure 3 illustrates this process:

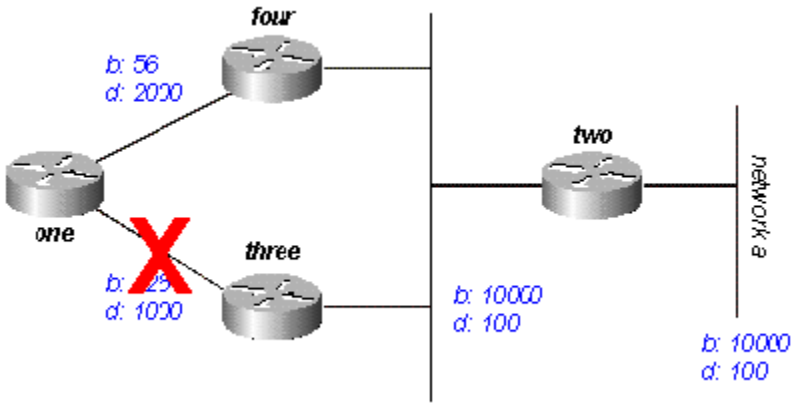

Fig 3: Path selection by distance.

Router One sees that it has two routes to Network A: one through Router Three and another through Router Four.

- The route through Router Four has a cost of 46277376 and a reported distance of 307200.
- The route through Router Three has a cost of 20307200 and a reported distance of 307200.

Note that in each case EIGRP calculates the reported distance from the router advertising the route to the network. In other words, the reported distance from Router Four is the metric to get to Network A form Router Four, and the reported distance from Router Three is the metric to get to Network A from Router Three. EIGRP chooses the route through Router Three as the best path, and uses the metric through Router Three as the feasible distance. Since the reported distance to this network through Router Four is less than the feasible distance, Router One considers the path through Router Four a feasible successor.

When the link between Routers One and Three goes down, Router One examines each path it knows to Network A and finds that it has a feasible successor through Router Four. Router One uses this route, using the metric through Router Four as the new feasible distance. The network converges instantly, and updates to downstream neighbors are the only traffic from the routing protocol.

Let us look at a more complex scenario, shown in Figure 4.

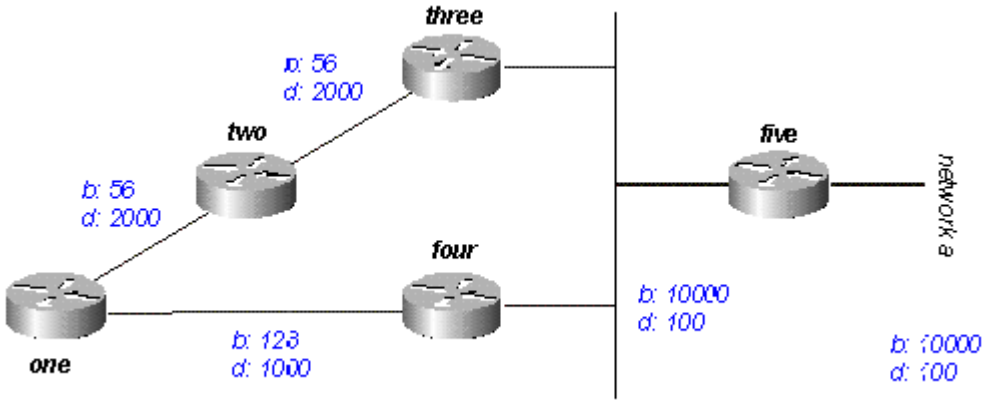

Fig 4: Complex network topology

There are two routes to Network A from Router One: one through Router Two with a metric of 46789376 and another through Router Four with a metric of 20307200. Router One chooses the lower of these two metrics as its route to Network A, and this metric becomes the feasible distance. Next, let us look at the path through Router Two to see if it qualifies as a feasible successor. The reported distance from Router Two is 46277376, which is higher than the feasible distance - so this path is not a feasible successor. If you were to look in the topology table of Router One at this point (using show ip eigrp topology), you would only see one entry for Network A - through Router Four. (In reality there are two entries in the topology table at Router One, but only one will be a feasible successor, so the other will not be displayed

in show ip eigrp topology; you can see the routes that are not feasible successors using show ip eigrp topology all-links).

Let us suppose that the link between Router One and Router Four goes down. Router One sees that it has lost its only route to Network A, and queries each of its neighbors (in this case, only Router Two) to see if they have a route to Network A. Since Router Two does have a route to Network A, it responds to the query. Since Router One no longer has the better route through Router Four, it accepts this route through Router Two to Network A.

Deciding if a path is loop-free:

How does EIGRP use the concepts of feasible distance, reported distance, and feasible successor to determine if a path is valid, and not a loop? In Figure 5, Router Three examines routes to Network A. Since split horizon is disabled (for example, if these are multipoint Frame Relay interfaces), Router Three shows three routes to Network A: through Router Four, through Router Two (path is two, one, three, four), and through Router One (path is one, two, three, four).

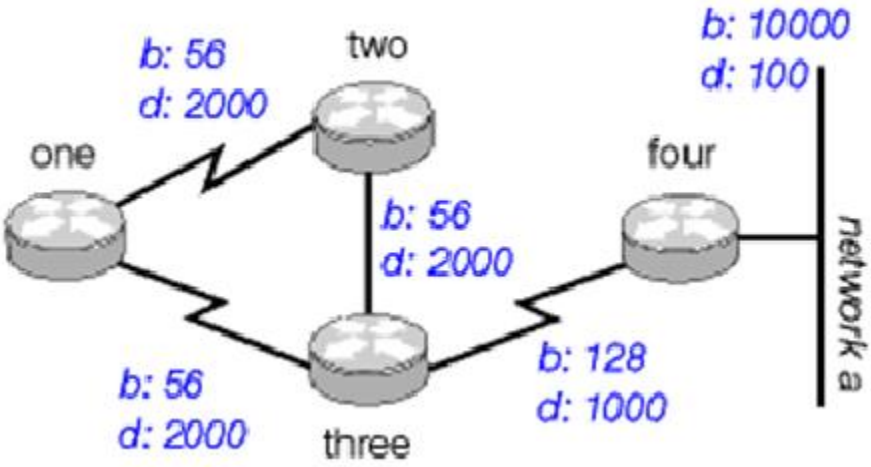

Fig 5: Loop free route

If Router Three accepts all of these routes, it results in a routing loop. Router Three thinks it can get to Network A through Router Two, but the path through Router Two passes through Router Three to get to Network A. If the connection between Router Four and Router Three goes down, Router Three believes it

can get to Network a through one of the other paths, but because of the rules for determining feasible successors, it will never use these paths as alternates. Let us look at the metrics to see why:

- total metric to Network A through Router Four: 20281600
- total metric to Network A through Router Two: 47019776
- total metric to Network A through Router One: 47019776

Since the path through Router Four has the best metric, Router Three installs this route in the forwarding table and uses 20281600 as its feasible distance to Network A. Router Three then computes the reported distance to Network a through Routers Two and One: 47019776 for the path through Router Two, and 47019776 for the path through Router One. Because both of these metrics are greater than the feasible distance, Router Three does not install either route as a feasible successor for Network A.

Suppose that the link between Routers Three and Four goes down. Router Three queries each of its neighbors for an alternative route to Network A. Router Two receives the query and, because the query is from its successor, searches each of the other entries in its topology table to see if there is a feasible successor. The only other entry in the topology table is from Router One, with a reported distance equal to the last known best metric through Router Three. Because the reported distance through Router One is not less than the last known feasible distance, Router Two marks the route as unreachable and queries each of its neighbors - in this case, only Router One - for a path to Network A.

Router Three also sends a query for Network A to Router One. Router One examines its topology table and finds that the only other path to Network A is through Router Two with a reported distance equal to the last known feasible distance through Router Three. Once again, since the reported distance through Router Two is not less than the last known feasible distance, this route is not a feasible successor. Router One marks the route as unreachable and queries its only other neighbor, Router Two, for a path to Network A.

This is the first level of queries. Router Three has queried each of its neighbors in an attempt to find a route to Network A. In turn, Routers One and Two have marked the route unreachable, and queried each of their remaining neighbors in an attempt to find a path to Network A. When Router Two receives the Router One query, it examines its topology table and notes that the destination is marked as unreachable. Router Two replies to Router One that Network A is unreachable. When Router One receives the Router Two query, it also sends back a reply that Network A is unreachable. Now Routers One and Two have both concluded that Network A is unreachable, and they reply to the original Router Three query. The network has converged, and all routes return to the passive state.

Split Horizon and poison reverse:

In the previous example, we assumed that split horizon was not in effect to show how EIGRP uses the feasible distance and the reported distance to determine if a route is likely to be a loop. In some circumstances, however, EIGRP uses split horizon to prevent routing loops as well. Before dealing with the details of how EIGRP uses split horizon, let us review what split horizon is and how it works. The split horizon rule states:

- Never advertise a route out of the interface through which you learned it.

For instance, in Figure 5, if Router One is connected to Routers Two and Three through a single multipoint interface (such as Frame Relay), and Router One learned about Network A from Router Two, it will not advertise the route to Network A back out the same interface to Router Three. Router one assumes that Router Three would learn about Network A directly from Router Two.

Poison reverse is another way of avoiding routing loops. Its rule states:

- Once you learn of a route through an interface, advertise it as unreachable back through that same interface.

Let us say the routers in Figure 4a have poison reverse enabled. When Router One learns about Network A from Router Two, it advertises Network A as unreachable through its link to Routers Two and Three. Router Three, if it shows any path to Network A through Router One, removes that path because of the unreachable advertisement. EIGRP combines these two rules to help prevent routing loops.

EIGRP uses split horizon or advertises a route as unreachable when:

- two routers are in startup mode (exchanging topology tables for the first time)
- advertising a topology table change
- sending a query

Let us examine each of these situations.

Startup Mode:

When two routers first become neighbors, they exchange topology tables during startup mode. For each table entry a router receives during startup mode, it advertises the same entry back to its new neighbor with a maximum metric (poison route).

Topology Table Change

In Figure 6, Router One uses variance to balance the traffic destined to Network A between the two serial links - the 56k link between Routers Two and Four, and the 128k link between Routers Three and Four (see the "Load Balancing" section for a discussion of variance).

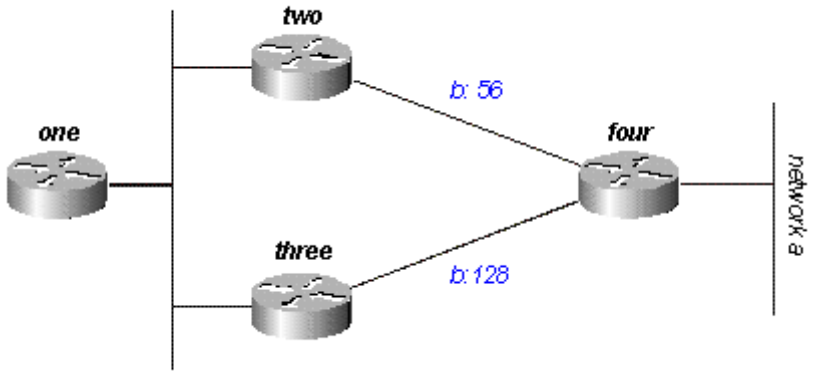

Fig 6: Load balancing scenario

Router Two sees the path through Router Three as a feasible successor. If the link between Routers Two and Four goes down, Router Two simply re-converges on the path through Router Three. Since the split horizon rule states that you should never advertise a route out the interface through which you learned about it, Router Two would not normally send an update. However, this leaves Router One with an invalid topology table entry. When a router changes its topology table in such a way that the interface through which the router reaches a network changes, it turns off split horizon and poison reverses the old route out all interfaces. In this case, Router Two turns off split horizon for this route, and advertises Network A as unreachable. Router One hears this advertisement and flushes its route to Network A through Router Two from its routing table.

Table 2: Comparison between OSPFv3 & EIGRPv6:

Point	OSPFv3	EIGRPv6
Protocol Type	Link-State	Hybrid
Protocol Number	89	88
Default Metric	Path Cost	Bandwidth/ Delay
Algorithms	Dijkastra	DUAL
Update Operation	In every 30 mins, LSA (Link-State Advertisement) table is updated	Only at time of occurring changes
Updating address	244.0.0.5 & 244.0.0.6 (DR & BDR)	244.0.0.10
Hop-Count (Limit)	None	244 (100 default)
VLSM Supporting	Yes	Yes
Convergence	Fast	Faster
Administrative distance	110	External=170, Internal=90
Updating Part	Only Changes	Only Changes

CHAPTER 3:

SIMULATION MODEL

For the analysis of the performance between the routing protocols, Packet Tracer 6.2.2 has been used. For the simulation purposes, Cisco's router, switch and general computers have been used. Standard IPv6 addresses have been used in these topologies.

OSPFv3:

For the simulation purpose of OSPFv3, the following topology has been used:

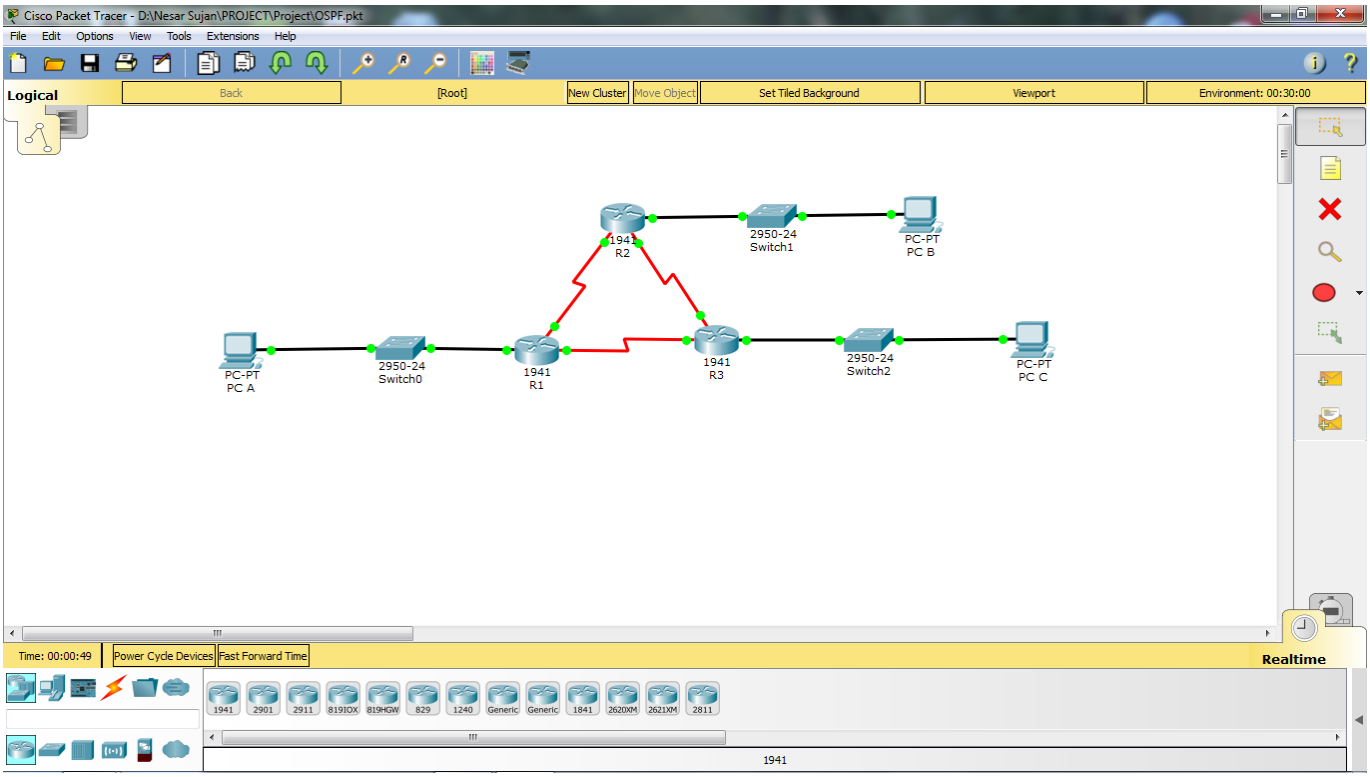

Fig 7: OSPF Routing Topology

Table 3: Packet Tracer Code for the OSPFv3 Simulation (summarized)

For Router 1	For Router 2	For Router 3
ipv6 unicast-routing *ipv6 router ospf 10* *router-id 1.1.1.1* *exit* *int g0/0* *ipv6 ospf 10 area 0* *int s0/0/0* *ipv6 ospf 10 area 0* *int s0/0/1* *ipv6 ospf 10 area 0*	*ipv6 unicast-routing* *ipv6 router ospf 10* *router-id 2.2.2.2* *exit* *int g0/0* *ipv6 ospf 10 area 0* *int s0/0/0* *ipv6 ospf 10 area 0* *int s0/0/1* *ipv6 ospf 10 area 0*	*ipv6 unicast-routing* *ipv6 router ospf 10* *router-id 3.3.3.3* *exit* *int g0/0* *ipv6 ospf 10 area 0* *int s0/0/0* *ipv6 ospf 10 area 0* *int s0/0/1* *ipv6 ospf 10 area 0*

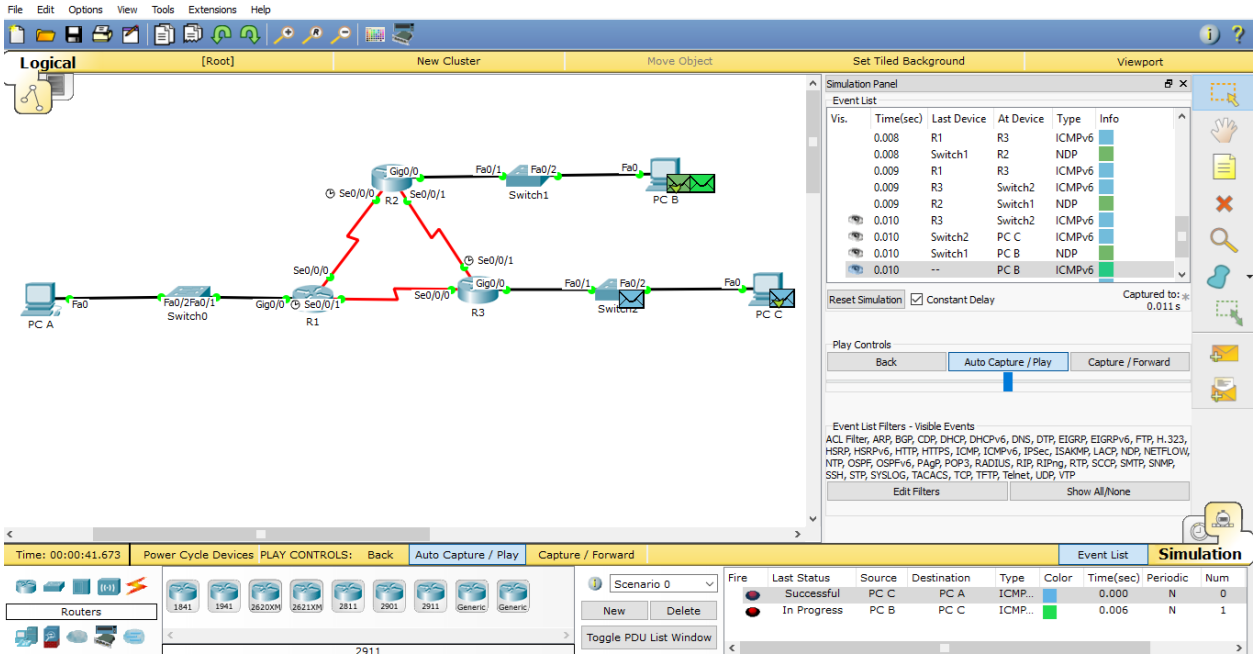

Fig 8: Simulation of the OSPFv3 Routing Protocols

EIGRPv6

For the simulation purpose of EIGRPv6, the following topology has been used:

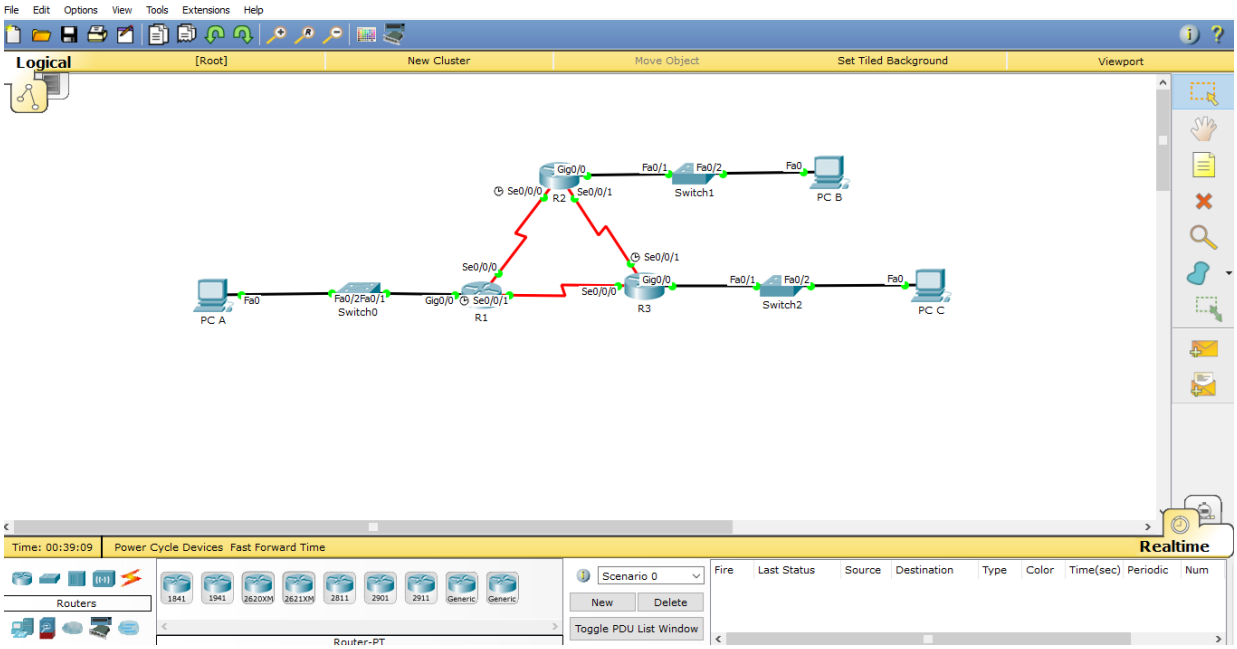

Fig 9: EIGRPv6 Routing Topology

Table 3: Packet Tracer Code for the EIGRPv6 Simulation (summarized)

For Router 1	For Router 2	For Router 3
ipv6 unicast-routing *ipv6 router eigrp 1* *no shut* *eigrp router-id 1.1.1.1* *exit* *int g0/0* *ipv6 eigrp 1* *int s0/0/0* *ipv6 eigrp 1* *int s0/0/1* *ipv6 eigrp 1*	*ipv6 unicast-routing* *ipv6 router eigrp 1* *no shut* *eigrp router-id 2.2.2.2* *exit* *int g0/0* *ipv6 eigrp 1* *int s0/0/0* *ipv6 eigrp 1* *int s0/0/1* *ipv6 eigrp 1*	*ipv6 unicast-routing* *ipv6 router eigrp 1* *no shut* *eigrp router-id 3.3.3.3* *exit* *int g0/0* *ipv6 eigrp 1* *int s0/0/0* *ipv6 eigrp 1* *int s0/0/1* *ipv6 eigrp 1*

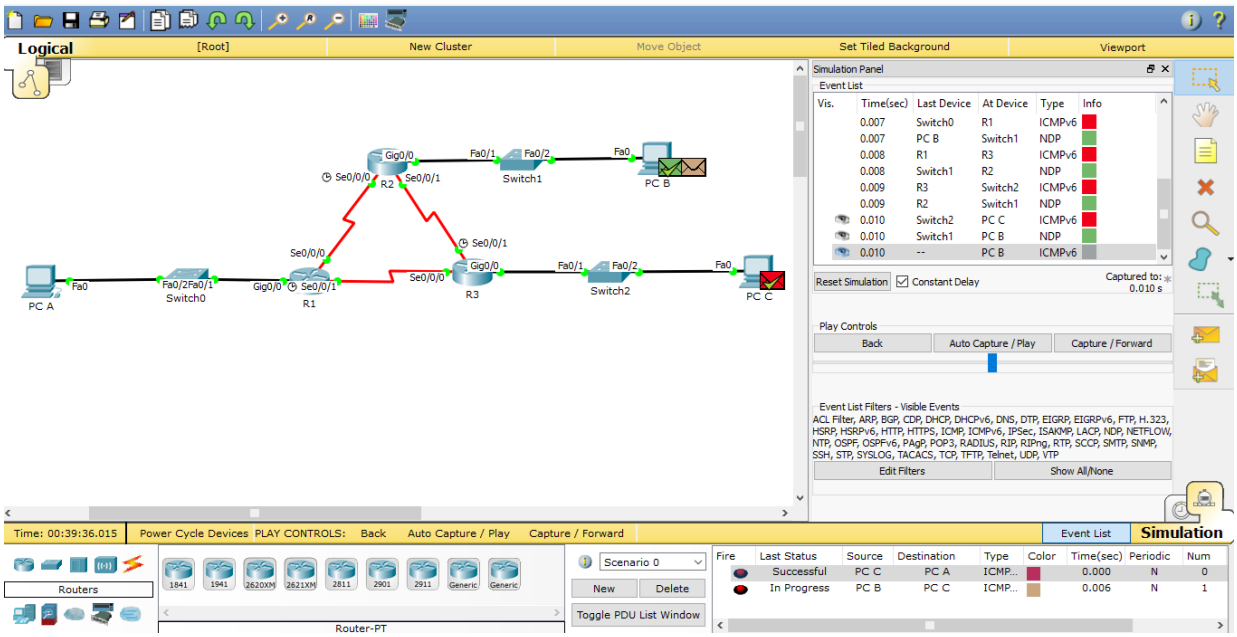

Fig 10: Simulation of the EIGRPv6 Routing Protocols

CHAPTER 4:

RESULTS ANALYSIS

In this section, the results got from the above simulations have been analyzed. In our simulation we have used complex 'ping' packet.

Analysis of packet loss comparison:

In the first analysis, we have increased the transmitted packet size for both the topologies. Packet loss occurs when one or more packets of data travelling across a computer network fail to reach their destination. Packet loss is typically caused by network congestion failed to choose the alternative paths immediately. It has been found that, increasing the packet size will result the increasing the number of packet loss. In Fig. 11, it is shown that the packet loss is more for the OSPFv3 network than the EIGRPv6 network. So, for the packet loss perspective, EIGRPv6 performs much better than OSPFv3.

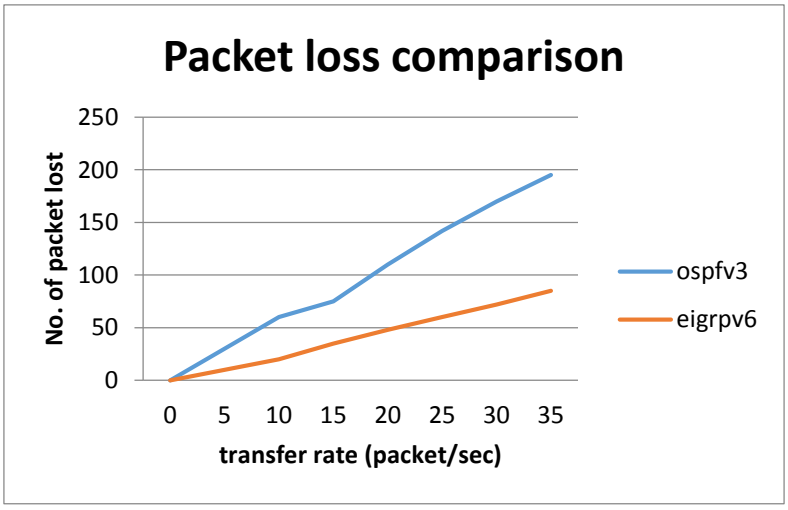

Fig 11: Packet loss comparison between OSPFv3 and EIGRPv6

Analysis of end to end delay comparison:

End-to-end delay is referred as the time taken for a packet to be transmitted across a network from source to destination. It is a common term used in IP network monitoring. In Fig. 12, it is shown that increasing the packet size will increase the end to end delay, because the increasing of congestion and the routing delay. In this Fig.12. OSPFv3 has more end to end delay than EIGRPv6. So here also EIGRPv6 performs the better.

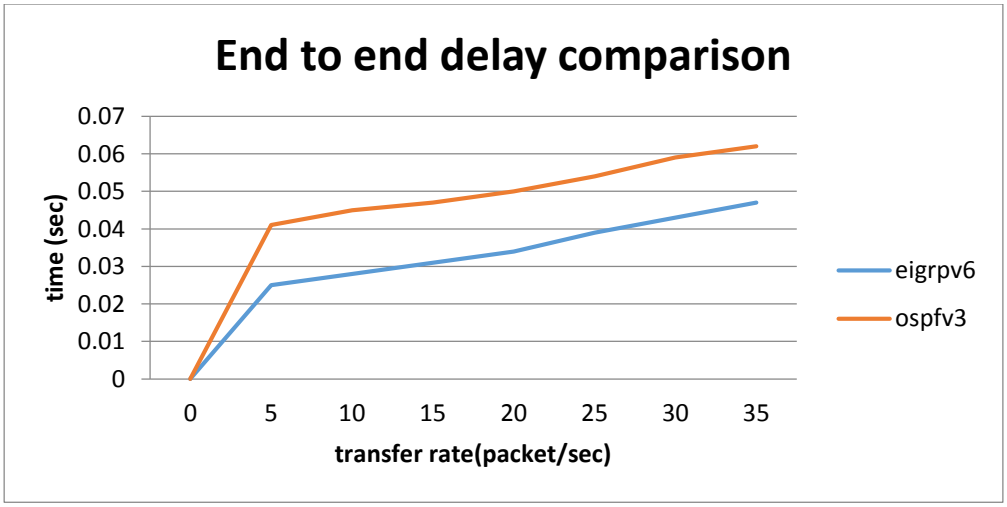

Fig 12: End to end delay comparison between OSPFv3 and EIGRPv6

Analysis of convergence time comparison:

Convergence is the state of a set of routers that have the same topological information about the internetwork in which they operate via the implemented routing protocol. In Fig. 13, we have found that OSPFv3 takes around 9 seconds while EIGRPv6 takes 6 seconds. So, in the case of convergence time, EIGRPv6 is also the faster than the OSPFv3.

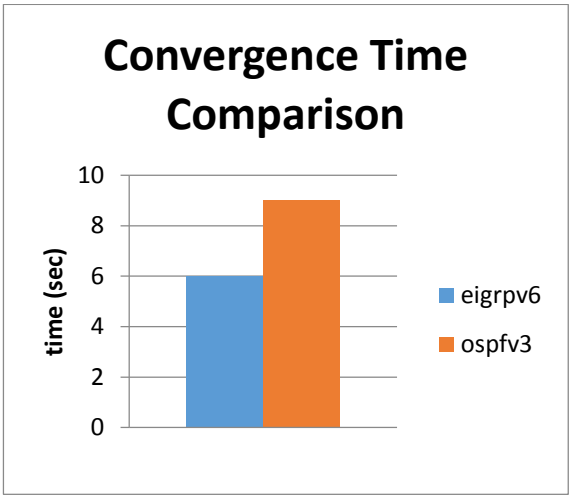

Fig 13: Convergence time comparison between OSPFv3 and EIGRPv6

This is due to EIGRP uses DUAL to provide fast convergence whilst OSPF detects topology changes using hello timers and interface changes. This triggers LSA to update neighbors, optimizations to convergence in OSPF are done by changing timer values.

CHAPTER 5:
CONCLUSION

The paper has been discussed two eminent interior routing protocols. Their performances have been analyzed considering the parameters of packet loss, end to end delay and convergence timing. In our analysis, we have found that EIGRPv6 performs much better that OSPFv3 in all these three cases. So our recommendation is to use EIGRPv6 as interior routing protocols in IPv6 network. But the main disadvantage of EIGRPv6 is that, these routing protocols can only be used in the Cisco's routers only. In this case, OSPFv3 is the best alternative. In future, we will compare these routing protocols with considering the security issues of IPv6. The work will be also extended to the real life devices.

REFERENCES

[1] Geoff Huston, Telstra, "IPv4: How long do we have?‥", Internet Protocol Journal, Vol. 6, No. 4, pp.2-15, 2003

[2] RFC 2460: https://www.ietf.org/rfc/rfc2460.txt

[3] "European IPv6 Task Force", IPv6 TF-SC Consortium, Workshop Industry Focus, Paris, June, pp.27-28, 2006.

[4] Gregory R. Schloz, Clint Evans, Jaime Flores, Mustafa Rahman, "Internet protocol version 6", Internet Protocol Journal, Vol. 16, Issue 3, pp. 197 - 204, March 2001.

[5] D. Genkov, "An approach for finding proper packet size in IPv6 networks," in Proc. of 12th International Conference on Computer Systems and Technologies, Vienna, Austria, pp. 442-447, 2011.

[6] Narula, Rajneesh, and Pallavi Aggarwal. "Performance Evaluation of RIP And OSPF In IPv6 Using Opnet 14.5 Simulator." International Journal of Technical Research and Applications, Vol. 2, Issue 6, PP. 37-41, 2014.

[7] Alex Hinds, Anthony Atojoko, and Shao Ying Zhu, "Evaluation of OSPF and EIGRP Routing Protocols for IPv6,"International Journal of Future Computer and Communication vol. 2, no. 4 pp. 287-291, 2013.

[8] IKram Ud Din, Saeed Mahfooz and Muhammad Adnan, "Analysis of the routing protocols in the Real Time Transmission: A Comparative study", Global Journal of Computer Science and Technology, Vol. 10, Issue 5, Ver. 1.0, pages 18-22, July 2010.

[9] V.Vetriselvan, Pravin R. Patil, M.Mahendran,"Survey on the RIP, OSPF, EIGRP Routing Protocol", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5(2), pp.1058 1065, 2014

[10] Saubhagya Das, Santosh Subedi and N. Shekar V. Shet, "Network Performance Analysis of Dynamic Routing protocols real time applications", International Journal of Modern Engineering Research, Vol.4, Issue 5, pp. 49-57, May 2014.

[11] N, Ayub, F. Jan, T. Mustafa, W. J. Rana, M. Y. Saeed, and S. Ullah, "Performance analysis of OSPF and EIGRP routing protocols with respect to the convergence," European Journal of Scientific Research, vol. 61, no. 3, pp. 434-447, 2011

[12] Krishnan,Y.N., G, Shobha, "Performance Analysis of OSPF and EIGRP Routing Protocols For Greener

Internetworking", Green High Performance Computing (ICGHPC), 2013 IEEE International Conference, pp. 1-4, 2013.

[13] Dey, Golap Kanti, Md Mobasher Ahmed, and Kazi Tanvir Ahmmed. "Performance Analysis and Redistribution Among ripv2, EIGRP & OSPF Routing Protocol." 2015 International Conference on Computer and Information Engineering (ICCIE). IEEE, 2015.

[14] Whitfield, Richard John, and Shao Ying Zhu. "A Comparison of OSPFv3 and EIGRPv6 in a Small IPv6 Enterprise Network." Editorial Preface 6.1, 2015.

[15] Routing Protocol in IPv6 Network." arXiv preprint arXiv: 1305.4311, 2013.

[16] A. Riesco and A. Verdejo, "Implementing and analyzing in Maude the Enhanced Interior Gateway Routing Protocol," Electronic Notes in Theoretical Computer Science, pp. 249–266, 2009.

[17] B. Albrightson, J. J. G. L. Aceves, and J. Boyle. "EIGRP – A Fast Routing Protocol Based on Distance Vectors," in Proc. of Networld/Interop, pp.1-13, April 1994.

APPENDIX

This project was submitted to the journal of International Journal of Computer (IJC) and accepted for the publication.

Paper Overview:

Md. Asif Hossain, Md.Mahful Islam Sunvy, Md. Nesar Uddin Majumder "Comparative Analysis of Two Prominent Routing Protocols in IPv6 Network: OSPFv3 & EIGRPv6", International Journal of Computer (IJC), Vol:22, No:1, 2016.

Online Link: http://ijcjournal.org/index.php/InternationalJournalOfComputer/article/view/678/400