***Original Research Article***

# PERFORMANCE COMPARISON OF OSPFV3 AND EIGRP WITH IPV6 NETWORK


## Abstract

A collection of interconnected devices that deal with communication protocols that are common to share resources provided by nodes of a network over digital interconnections is a computer network. The process of determining the most efficient route from a source to a given target is called routing. Cisco's Enriched Internal Routing Gateway Protocol for IPv6 and the IETF's OSPFv3 (First Version 3 of Open Shortest Path) are two of the most frequently studied IPv6 routing protocols among researchers (EIGRPv6).As a result of the popularity of EIGRPv6 and OSPFv3, it is necessary to undertake a thorough contrast of the two protocols once working inside a minor enterprise network on IPv6. Thus, the study analysed the performance comparison of OSPFV3 and EIGRP with IPv6 networks with regards to convergence time, end-to-end delay, and packet loss. Packet Tracer 6.2.2 was used to compare the performance of routing protocols of different kinds. In the simulation, Cisco routers, switches, and generic computers were employed in the test. In these topologies, standard IPv6 addresses have been used. The findings of the study revealed that EIGRPv6 outperforms OSPFv3. As a result, we advocate using EIGRPv6 as an internal routing protocol in a network of IPv6.



Keywords: OSPFV3, EIGRP, IPv6, performance, network and internet


## Introduction

A computer network is a collection of interconnected devices such as laptops, servers, desktops, tablets, and smartphones that deal with communication protocols that are common to share resources provided by nodes of a network over digital interconnections (Fuzi, Abdullah, Abd Halim, & Ruslan, 2021). The process of determining the most efficient route from a source to a given target is called routing (Sinthia, Nasir, Paul, Rashid, & Adnan, 2021). It can be done in real time by utilising routing protocols based on various routing algorithms. EGRP (Exterior Gateway Routing Protocols) and IGRP (Interior Gateway Routing Protocols) are two types of routing protocols (Odom, 2013). EGRPs include proteins like BGP. All types of IGRP (Essah, Senior, & Anand, 2021) are all types of IGRP (Essah, Senior, & Anand, 2021). RIP, EIGRP, ISIS, and OSPF are the most popular IGRPs. Convergence, or the ability to adapt quickly to network changes, the ability to identify the best path among multiple paths, and the volume of traffic routing created, are all features that separate different routing protocols (Sankar & Lancaster, 2010). For network success, protocols for routing play a decisive role. Every day, the Internet expands around the world (Ashraf & Yousaf, 2017).

A variety of devices are joining the Internet every day (Jain, Payal, & Jain, 2021). For communication over the network, all of these devices require an IP address. IP (Internet Protocol) is the most widely used routing protocol on the Internet, according to Chauhan and Sharma (2015).IP comes in two flavors: IPv4 and IPv6. IPv6 will be the focus of this study. The IETF (Internet Engineering Task Force) created the protocol IPv6 in 1990. (Deering & Hinden, 1998). The 128-bit addressing technique is used in IPv6. 2013; Ashraf).It will progressively phase out IPv4 as the days go by. IPv4 is relatively simple to set up, while IPv6 is more difficult

due to its complex address structure (Li et al., 2014). However, the Cisco Enriched Internal Gateway Routing Protocol for IPv6 and the IETF OSPFv3 (Open Shortest Path First Version 3) are two of the most frequently studied IPv6 routing protocols among researchers (EIGRPv6) (Jain, Payal, & Jain, 2021).

These are just a few of the articles that have compared the convergence speed and resource utilisation of both protocols.Though no contrasts were made to analyse the extra implications of deploying OSPFv3 and EIGPRv6's respective authentication and encryption techniques (Whitfield & Zhu, 2021). As a result of the popularity of EIGRPv6 and OSPFv3, it is necessary to undertake a thorough contrast of the two protocols once working inside a minor enterprise network on IPv6 (Samaan & Lecturer, 2018). It should also be noted that one of EIGRP's major flaws was its proprietary nature (Abidin, Fiade, Aripiyanto, & Handayani, 2021).Though, as Savage, Slice, Ng, Moore, & White (2013) point out, EIGRP was released to the IETF and will quickly be obsolete. By analysing the two protocols and examining the added security measures' influence of the two protocols once deployed in a Cisco hardware-centred assessment environment, this article adds to the continuing contrasts of EIGRPv6 and OSPFv3 (Pal, Kushwaha, Tomar, & Tripathi, 2021). These routing protocols have been the subject of several studies.

The authors of Rajneesh & Aggarwal (2014) looked at OSPF and RIP in a network of IPv6. Hinds, Zhu, & Atojoko (2013) examined and discussed the routing protocols EIGRP and OSPF

with IPv4 and IPv6 networks. Din, Adnan, and Mahfooz (2010) examined numerous routing protocols' performance, such as OSPF, RIP, EIGRP, and IGRP, with regards to traffic received, packet loss, jitter in voice, and end-to-end delay. Other related work has been completed (Vetriselvan et al., 2014; Sathyasri, Janani, & Mahalakshmi, 2021; Sadat, 2021; Das, Das et al., 2014). In addition, a study by Jain & Payal (2020), who analysed the IS-ISv6 performance comparison with the IPv6 network, proposed that a performance comparison with alternative routing protocols should be completed for IPv6. To bridge the gap in the literature, the study sought to analyse the performance comparison of OSPFV3 and EIGRP with IPv6 networks with regards to packet loss, end-to-end delay, and convergence time.

**EIGRPv6**

Enhanced Internal Gateway Routing Technology (EIGRP) is a protocol that Cisco developed (Essah, Senior, & Anand, 2021). It's a protocol of hybrid routing since it combines distance vector and link state routing protocols (Tersianto, Hidayat, & Nurwasito, 2020). EIGRP was first presented in 1993 and supports IPv4 (Vesel, Rek, & Ryav, 2015). EIGRPv6 is a more advanced version that supports IPv6. It functions as part of the AS (autonomous system). An AS is a comparable router collection that shares routes and is managed by the same administrator (Savage et al., 2016). It is a classless routing protocol that enables Variable Length Subnet Mask (VLSM). VLSMs allow you to granularly assign essential bits of the host. The main characteristic of the routing protocol is its unequal load balancing (Okonkwo & Emmanuel, 2020). The routing protocol of EIGRPv6 has 3 tables that aid in routing decisions (Julia, Suseno, Wardhani, Khairani, Hulliyah, & Muharram, 2020). tables for neighbors, topology, database, and

routing. EIGRPv6's default metrics for determining the optimum path are "bandwidth and latency," but dependability, load, and MTU can also be employed (Ordabayeva, Othman, Kirgizbayeva, Iztaev, & Bayegizova, 2020). It transmits "welcome mails" to its neighbours every five seconds on FDDI networks and Ethernet, and every minute on SMDS links and Frame Relay (Tarasiuk et al., 2016). It is 90 kilometres away, administratively. Instead of broadcasting, it employs multicast updates. The address FF02::A is a multicast address (Ashraf, 2013).

EIGRP is a distance vector protocol that uses the Diffused Update Algorithm (DUAL) to find the shortest path to a network endpoint (Hossain, Ali, Akter, & Sajib, 2020). Versions 0 and 1 are the two major iterations of EIGRP. Some explanations in this paper may not apply to Cisco IOS versions prior to 10.3 (11), 11.0 (8), and 11.1 (3), which run an earlier version of EIGRP. We strongly advise you to use the latest version of EIGRP, which offers numerous performance and stability improvements (Jain & Payal, 2020). When calculating the optimum path to a destination, a common distance vector protocol saves the following information: the distance (total metric or distance, such as hop count), and the vector (the next hop) (Jain, Payal, & Jain, 2021). For example, all of the routers in Figure 1's network run the Routing Information Protocol (RIP). Router Two determines the best path to Network A by counting the number of hops on each accessible path.



**EIGRPv6 theory of operations:**

Some of the many advantages of EIGRP are:

- Only hello packets are transmitted on a stable network during normal operation;

- 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 a distance vector protocol that uses the Diffused Update Algorithm (DUAL) to find the shortest path to a network endpoint (Rasel, 2020).

**Major Revisions of the Protocols:**

Versions 0 and 1 are the two major iterations of EIGRP. Some explanations in this paper may not apply to Cisco IOS versions prior to 10.3(11), 11.0(8), and 11.1(3), which run an earlier version of EIGRP (Biradar, 2020). We strongly advise you to use the latest version of EIGRP, which offers numerous performance and stability improvements.

**Basic Theory:**

When calculating the optimum path to a destination, a common distance vector protocol saves the following information: the distance (total metric or distance, such as hop count) and the vector (the next hop) (Triasari, Tulloh, & Iqbal, 2020). For example, all of the routers in Figure 1's network run the Routing Information Protocol (RIP). Router Two determines the best path to Network A by counting the number of hops on each accessible path.

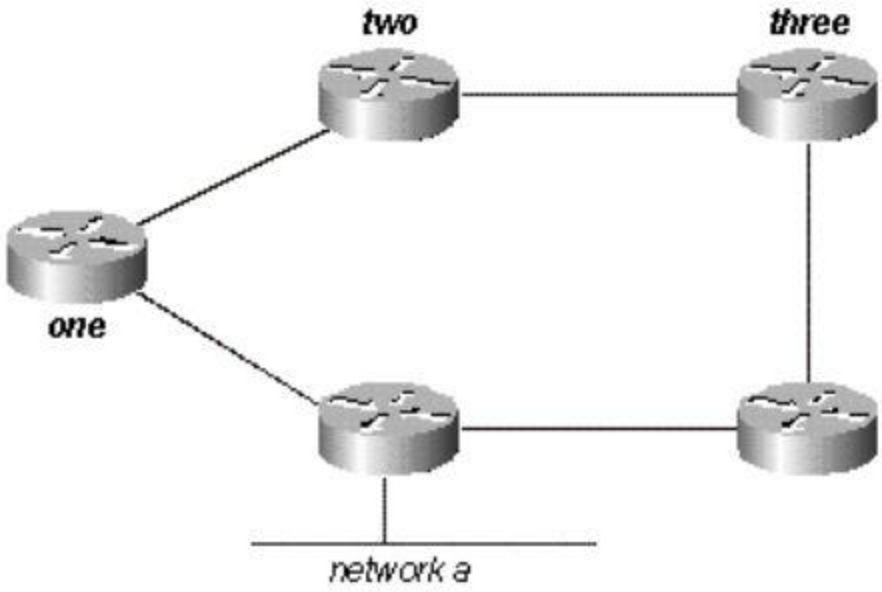



*Figure 1: Simple Network Topology*

Router Two chooses the path through One and discards the information it learned through Router Three because the road through Router Three is three hops and the path through Router One is two hops. Router Two loses all communication with this destination if the path between Router One and Network A goes down until Router Three times out the route in its routing database (three update periods, or 90 seconds) and Router Three re-advertises the route (which occurs every 30 seconds in RIP) (Muhammad, Trisnawan, & Amron, 2020). Router Two will take between 90 and 120 seconds to transition the path from Router One to Router Three, not including any hold-down time. Instead of relying on full periodic updates to re-converge, EIGRP creates a topology database from each of its neighbors' advertising (rather than discarding the data) and converges by either searching the topology table for a likely loop-free route or asking its neighbors if none exist (Sakib, & Singh, 2020). Router Two keeps track of the data it receives from Routers One and Three. It selects the path through One as the best (successor) and the way through Three as the loop-free path (a feasible successor). When Router One's path becomes

unavailable, Router Two reviews its topology database and, if a viable successor is found, instantly switches to Router Three's path. From this brief explanation, it is clear that EIGRP must provide: a system that provides only the updates that are required at any given moment; this is accomplished through neighbor discovery and maintenance; and a method of determining which loop-free paths a router has learnt. A method for querying neighbors to locate paths to lost destinations a process for clearing faulty routes from the topology tables of all routers on the network we will take a look at each of these prerequisites one by one.

**Neighbor Discovery and Maintenance:**

EIGRP employs non-periodic incremental routing updates to provide routing information throughout a network. That is, EIGRP only transmits routing updates for changing pathways when those paths change. The primary issue with merely providing routing updates is that you may not be aware when a way through a neighboring router is no longer accessible (Fuzi, Abdullah, Abd Halim, & Ruslan, 2021). You can't time out routes and expect your neighbors to send you a new routing table. To properly disseminate routing table updates throughout the network, EIGRP relies on neighbor relationships; two routers become neighbors when they see each other's hello packets on the same network. On high-bandwidth networks, EIGRP sends hello packets every 5 seconds; on low-bandwidth multipoint links, hello packets are sent every 60 seconds.

**5-second hello:**

• Ethernet, Token Ring, and FDDI are examples of broadcast medium.

• PPP or HDLC leased circuits, Frame Relay point-to-point sub interfaces, and ATM point-to-point sub interfaces are examples of point-to-point serial links.

• multipoint lines with high bandwidth (higher than T1), such as ISDN PRI and Frame Relay

**60-second hello:**

- T1 bandwidth or slower multipoint lines, such as Frame Relay multipoint interfaces, ATM multipoint interfaces, ATM switched virtual circuits, and ISDN BRIs The hello interval is the pace at which EIGRP broadcasts hello packets, and it can be adjusted per interface using their command. The hold time is how long a router considers a neighbor alive if it hasn't received a hello packet. The hold period is usually three times the hello interval, which is 15 seconds by default and 180 seconds by default (Jain, Payal, & Jain, 2021). The IP hold-time EIGRP command can be used to change the hold time. If you alter the hello interval, the hold time does not automatically adapt to reflect the new interval; you must manually adjust the hold time to match the new hello interval. Even if the hello and hold times of two routers do not match, they can become EIGRP neighbors. The hold duration is included in the hello packets, thus even if the hello interval and hold timings don't match, each neighbor should stay alive. While there is no direct way to determine the hello interval on a router, the output of show IP EIGRP neighbors on the surrounding router can be used to infer it. You can use Cisco CLI Analyzer (registered customers only) to display potential issues and fixes if you have the result of a show IP EIGRP neighbors command from your Cisco equipment. JavaScript must be enabled in order to utilize Cisco CLI Analyzer. Over secondary addresses, EIGRP does not establish

peer associations. All EIGRP communication originates from the interface's main address.

- Configure the broadcast keyword in the frame-relay map statements when configuring EIGRP over a multi-access Frame Relay network (point-to-multipoint, etc.). The adjacencies between two EIGRP routers would not establish without the broadcast keyword. For further information, see Configuring and Troubleshooting Frame Relay (Pal, Kushwaha, Tomar, & Tripathi, 2021).
- EIGRP has no restrictions on the number of neighbors it can support. The number of supported neighbors is determined by the device's capabilities, such as memory capacity, processing power, the amount of transmitted information, such as the number of routes sent, topology complexity, and network stability.

**Building the topology table:**

What are these routers talking about now that they've started communicating to each other? Of course, their topological tables! Unlike RIP and IGRP, EIGRP does not rely on the router's routing (or forwarding) table to store all of the information it need to function. Instead, it creates a second table, the topology table, from which routes are installed in the routing table. Note: Starting with Cisco IOS 12.0T and 12.1, RIP has its own database from which it inserts routes into the routing table (Sathyasri, Janani, & Mahalakshmi, 2021). Issue the topology command on an EIGRP router to see the basic format of the topology table. The topology table contains the information needed to construct a set of distances and vectors to each reachable network, including: • the 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 (external routes are marked). Later in this section, we'll talk about feasible and reported distances. You can use Cisco CLI Analyzer (registered customers only) to display potential issues and fixes if you have the output of a show IP EIGRP topology command from your Cisco device. JavaScript must be enabled in order to utilize Cisco CLI Analyzer.

**EIGRPv6 Metrics:**

To compute routing metrics, EIGRP employs the minimum bandwidth on the path to a destination network and the total latency. Other metrics can be configured, however we don't encourage it because it can generate routing loops in your network (Sadat, 2021). Values configured on the interfaces of routers in the path to the target network are used to calculate bandwidth and delay metrics. Router One, for example, is calculating the optimum path to Network A in Figure 2.

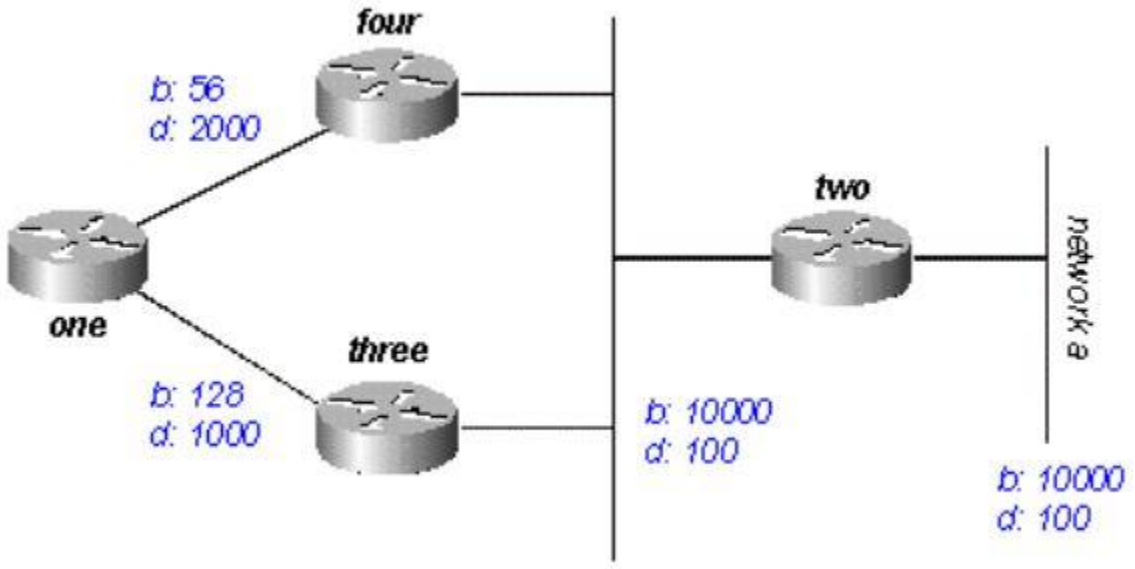



*Figure 2: Simple Network Topology*

It begins with two advertisements for this network: one via Router Four, with a minimum bandwidth of 56 and a total delay of 2200; and the other via Router Three, with a minimum bandwidth of 128 and a delay of 1200. The path with the lowest metric is chosen by Router One.

**Startup Mode:**

During startup mode, two routers exchange topology tables when they first become neighbors. A router broadcasts the same table entry to its new neighbor with a maximum metric for each table entry it receives during startup mode (poison route) (Essah, Senior, & Anand, 2021).

**Topology Table Change**

Figure 3 shows Router One balancing traffic destined for Network A across the two serial lines - the 56k link between Routers Two and Four and the 128k link between Routers Three and Four - using variance (see the "Load Balancing" section for a discussion of variance).

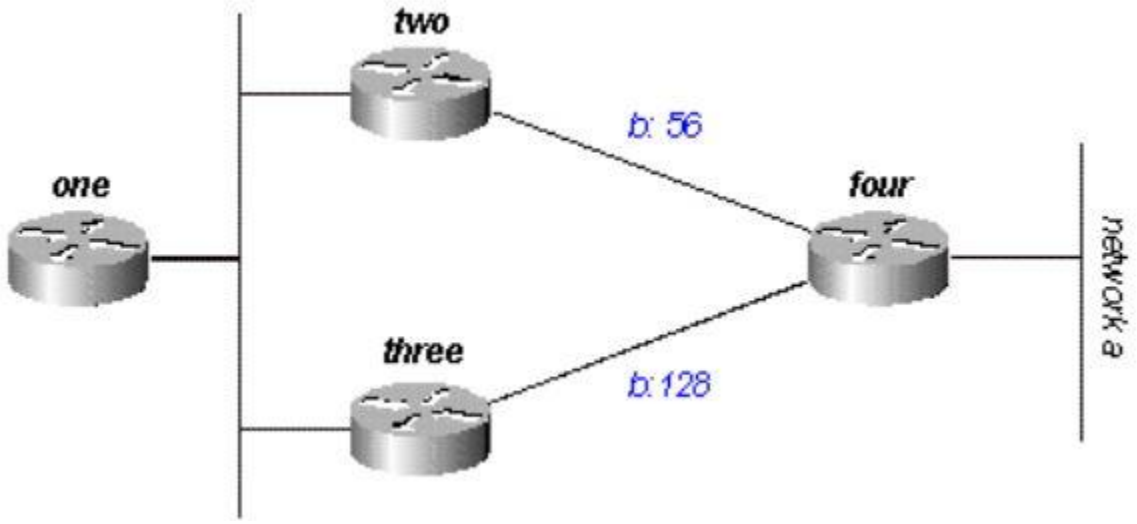



*Figure 3: Load balancing scenario*

Router Two considers Router Three's approach to be a viable replacement. Router Two simply re-converges on the way through Router Three if the link between Routers Two and Four fails. Router Two would not ordinarily send an update since the split horizon rule stipulates that you should never publicize a route out the interface via which you learned about it. Router One, on the other hand, is left with an invalid topology table entry. When a router modifies its topology table in such a way that the interface via which it connects to a network changes, it disables split horizon and poisons all interfaces, reversing the former path (Tersianto, Hidayat, & Nurwasito, 2020). Router Two disables split horizon for this route and marks Network A as inaccessible in this situation. When Router One hears this advertisement, it clears its routing table and flushes its route to Network A via Router Two.

**OSPFv3**

OSPF is a routing protocol of link state that first prioritizes the shortest pathway. In 1988, it is the greatest widely used routing protocol and open standard created by Task Force of Internet Engineering (TFIE). In 1999, the IETF released an updated OSPFv3 version for IPv6. It's known for its scalability and stability. Its specification is freely available due to the open standard (Tarasiuk et al., 2016). The network is divided by it in zones in order to bring together comparable routers for easier control. When there are many zones, one of them is referred to as a "backbone area." “Area 0” refers to the backbone area. Virtual linkages connect a number of different places to the backbone. It also supports VLSM and is a classless routing mechanism (Krishnan & Shobha, 2013). It also has the ability to load balance up to sixteen equivalent pathways. Cost is the metric used to decide the finest pathway. It is 110 kilometers away administratively. There are three tables in OSPFv3 as well. Tables for neighbors, topologies, and

routing. “Link State Advertisement” carries the topological information (LSAs). LSAs come in a variety of shapes and sizes.

Some of these are commonly applied. LSA type 1 (Router link LSA) defines interfaces of router's state, LSA type 2 (network link LSA) defines the connected routers to LAN and signifies a LAN broadcast, and LSA type 3 (network summary LSA) defines the routers linked to LAN (ABRs), Border Router of Autonomous System (BRAS) summary LSA (LSA type4), LSA type5 (external LSA) and LSA type7 (NSSA (Not So Stubby Area) external LSA) (Goyal et. al., 2012). Five types of packets: The OSPFv3 protocols Hello, LSACK (Link State Acknowledgement), LSU (Link State Update), LSR (Link State Request), and DBD (Database Description) are utilized in normal operation (Jian & Fang, 2011). It establishes and maintains a friendship with its neighbor by sending “hello messages” every 10 seconds. The manner of sending Hello packets has changed in OSPFv3. Before sending the Hello packet, the interface ID must be copied into the Hello packet (Coltun, Ferguson, Moy & Lindem, 2008).

A neighbor is declared dead if he or she does not respond in forty seconds (lifeless interval period). It's possible that your next-door neighbor lives in a different state. Init, Down, ExStart, 2Way, Full, Loading, and Exchange are the seven states of OSPFv3 (Gough, 2003). It serves as a “Backup Designated Router” in a multi-access network (BDR) or “Designated Router” (DR). BDR/DR routers in OSPFv3 are identifiable by their router IDs rather than their IP addresses. On a multi-access network, the DR is in charge of creating adjacencies with all neighbors (for example FDDI or Ethernet). The BDR protocol is applied to offer network idleness. The BDR takes over as the novel DR once DR fails. To communicate with one another, multicast LSAs are

employed. At FF02::6, LSAs are transmitted to the BDR/DR, and at FF02::5, LSAs are sent to other routers (Ashraf, 2013).

OSPF allows network builders to divide big networks into smaller ones called Areas using hierarchical network design. The amount of routing information that can be propagated at one time is reduced when larger networks are divided into sections. The network's convergence time is reduced as a result of this. Furthermore, any network issue can be traced to each individual location inside the network (Lammle, 2007). OSPFv3 is an open standard routing protocol implemented by many network providers, rather than a proprietary technology.

**Changes for OSPFv3**

One of the key changes in OSPFv3 is that the protocol's header has been changed, as Teare (2010) points out. In comparison to OSPFv2, the header is no longer as complex. An instance ID field has been added to the header. In IPv6, routing is done per–interface rather than per–subnet. Each IPv6 routing protocol is more concerned with the link, not the subnet, on which it is configured. As a result of the addition of the new instance ID field to the protocol structure, several OSPFv3 instances or addresses can now be enabled on the same link. The instance ID is set to 0 by default. It is increased when there is an additional occurrence. A unique instance ID is assigned to each OSPF instance. In addition, the instance ID has just a local link relevance. This means that OSPFv3 routers must have identical instance IDs before they can become neighbors. When a router receives a packet with an instance ID that differs from its own, for example, it simply discards the packet. The greeting packet structure has also been modified as a result of

the revised OSPFv3 header (Coltun et al, 2008). According to Teare (2010), the OSPFv3 has undergone the following changes:

The multicast addresses reserved for all SPF or link state routers and all designated routers in OSPFv3 are now FF02::5 and FF02::6, respectively, instead of 224.0.0.5 and 224.0.0.6 as in OSPFv2.

- IPv6 addresses are not permitted in the OSPFv3 packet header. Rather, the IPv6 address is carried in the link state update packet's payload.
- IPv4 addresses are carried by network LSAs in OSPFv2, but IPv6 addresses are not carried by network LSAs in OSPFv3.
- Before routing can begin, the router ID must be enabled when configuring OSPFv3 on routers.
- The router's ID is used to identify the designated router and backup designated router in OSPFv3, rather than its IP address as in OSPFv2.

Another major difference in OSPFv3 is the security technique it employs to safeguard routing data. The main security technique used to safeguard routing information in OSPFv2 is Message Digest 5. This is not the case in OSPFv3. In OSPFv3, routing information is secured using IPsec, which is part of the IPv6 protocol (Wen et al, 2010). The OSPFv3 packet structure is shown in Figure 4.

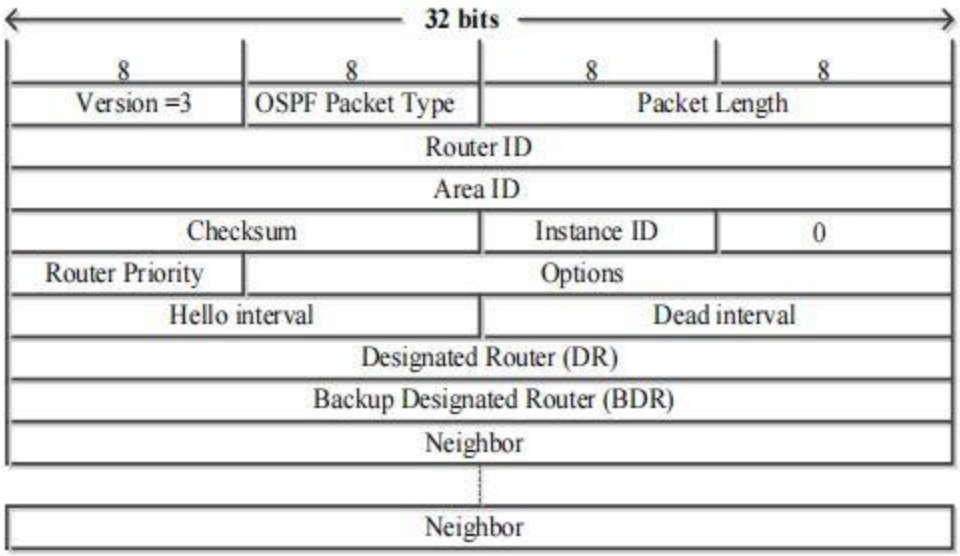



*Figure 4:* ***OSPFv3 Packet structure***

**Features of OSPFv3**

**Hello protocol**

OSPF routers use the Hello protocol to dynamically discover and maintain neighbor relationships. The Hello protocol includes a specific packet known as the Hello packet, which is sent out on a regular basis by each router on every OSPF–enabled interface to establish and confirm neighbor connections with other routers before routing information may be exchanged (Okonkwo, & Emmanuel, 2020). The OSPF Hello packet is primarily used for:

- finding neighbors
- establishing two–way communication between neighbors
- electing the DR and the BDR

When sent, the Hello packet includes information about the OSPF interface and the router sending the packet. The router ID, area ID, router priority, hello interval, dead interval,

designated router, and backup designated router are all included in this data. A list of all neighbors and other optional sending router capabilities are also included in the Hello packet metadata. The hello interval specifies how frequently the router delivers a Hello packet to its neighbor. The dead interval is the duration after which a router can deem a neighbor dead if it does not receive any Hello packets from that neighbor during that time. The hello interval on a broadcast media is set to ten seconds by default, whereas the dead interval is set to forty seconds (Hossain, Ali, Akter, & Sajib, 2020). Hello packet can be used as a keep alive message to determine if a neighbor is still communicating thanks to the dead interval. A router drops a neighbor from its local neighbor table if it has not received any Hello packets from that neighbor within the chosen dead period. Router priority is used to elect or disqualify a router as the designated router or backup designated router. The designated and backup designated router fields are also used to indicate whether or not the neighbor has been elected as the DR or BDR. When an OSPF router receives a Hello packet from another router, it compares the information in the packet to the information on the interface that received the message. The routers are considered neighbors if the information on both interfaces is the same (Rasel, 2020). The router ID field is used to facilitate two–way communication between two interfaces. This field holds a list of all the router IDs with whom the sender router has communicated. A receiving interface looks through the list of router IDs to see whether it can find its own router ID. If this data is found, a two–way communication channel between the sending and receiving interfaces is formed.



**OSPF Neighbors**

Open the shortest route. The first neighbors are routers that share a network interface. The Hello packet, which is sent frequently from each router, is used for neighbor finding in OSPF. For two routers to be considered neighbors, they must have the same information on their interfaces:

- Area ID
- Optional capabilities
- Hello interval
- Dead interval
- This information is stored into the neighbor table if it is the same for both interfaces. The neighbor ID and the neighbouring router's priority are both stored in a typical neighbor table. The following information is also included in the neighbor table:
- **State**: used to indicate if communication with the neighbor is still active and whether the neighbor is attempting to establish two–way communication with the router issuing the Hello packet. State is also used to indicate whether the neighbor has attained full adjacency and is sharing its link–state information.
- **Dead time:** used to indicate how long it has been since the neighbor has sent a Hello packet.
- **Link–local IPv6 address**: used to denote the link–local IPv6 address of a neighbor.
- **Local interface**: This is the router interface that was utilized to receive this neighbor's Hello packet.
- **Designated router**: indicates if a neighbor has been designated as the DR or BDR.

When a router gets the initial Hello packet from a new neighbor, it enters the init state and adds that neighbor to the neighbor table. The neighbor state transforms to a two–way state after the router and this neighbor initiate two–way communication. The exstart and exchange states

follow the two–way state, where both routers will now exchange their link–state database. The neighbor enters the full state, denoting full adjacency, once all of these are completed. If the neighbor does not send any Hello packets during the dead interval, the neighbor is moved to the down state and no longer considered adjacent. The benefits of establishing neighbor connections in OSPF are numerous. It is used to determine whether a router is active or inactive. Neighbor relationships are also utilized to streamline communication results because when all routers' topology databases are the identical, only periodic updates will be transmitted to neighbors when the network topology changes (Cisco, 2016).

**Adjacency**

Following the establishment of a neighbor relationship via the Hello packet, neighbors communicate routing updates. The topology database or table stores network information, from which the optimum path to each destination is computed and recorded in the routing table. When all neighbor routers' topology databases are synchronized, the neighbors become totally adjacent. A router must deliver the Hello packet on a regular basis to guarantee that the neighbor relationship is maintained and the content of the topology tables is accurate and up–to–date. As long as they continue to receive the Hello packet, all receiving routers can keep the transmitting router and its networks in their topology tables. The term "adjacency" does not apply to all neighbors. Adjacency formation is determined by the network type and how the routers are configured. OSPFv3 uses three separate packets to establish adjacency. Database description (DBD), link state request (LSR), and link state update (LSU) packets are the three types of packets. Only LSA headers from the neighbor's link–state database are included in the DBD packet. When a local router receives these LSA headers, it compares them to the header of its

own link–state database to determine which LSAs are new or up–to–date. If some of the LSAs need to be updated, the local router sends LSR packets to its neighbors, requesting that they give this information. When the neighbors get the LSR packets, they respond with an LSU packet containing LSA update information. The routers keep exchanging information until they all have the same link–state information. Because the neighbor of a router collects information about the network and sends it to other neighbors directly linked to it, OSPF neighbor relationship and adjacency are important components of the protocol. Furthermore, the establishment of both relationships between routers is utilized to regulate the distribution of OSPF packets, allowing the network to converge more quickly (Leahy, 2011).

**Link State Advertisement**

OSPF builds its routing table using a special packet called Link State Advertisement (LSA) in addition to the Hello packet. The LSA protocol is the most basic way for OSPF to communicate a router's local routing topology to other routers in the same area. Following the establishment of adjacency between OSPF routers, neighbor routers exchange LSAs so that all routers have identical link–state databases. A typical LSA includes information on the state, the cost of each link, and any other details about a neighbor. Each router generates LSAs for each connection connecting to it and then floods these LSAs to other routers via every OSPF–enabled interface. Once the content of all routers' link–state databases is equal, all routers use the SPF method to generate their routing tables, which include the shortest path to each destination network for efficient packet routing. OSPFv3 uses different LSA types for diverse purposes rather than a single LSA packet. The following LSA kinds are available:

- Type 1 or Router LSA: Each router in an area floods this LSA. The Type 1 LSA comprises a list of all links associated to each router flooding the LSA (together with their statuses and charges). SPF re–computation is caused by Type 1 LSA.
- Type 2 LSAs, also known as Network LSAs, are designed for multi-access networks that require DR and BDR. These LSAs are generated by the DR or BDR, which then flood all of the multi–access networks connected to it. A list of all routers in the multi–access network is included in network LSAs. The SPF is also re–computation due to Type 2 LSA.
- **Type 3 or Inter–Area Prefix LSA:** For every destination within the local area, the area border router (ABR) floods these LSAs to exterior areas. The cost of the link from the ABR to the local destination is included in the Inter–Area Prefix LSAs.
- **Type 4, or Inter–Area Router LSA:** The ABR generates this LSA, which is then forwarded to exterior regions. The autonomous system border router (ASBR) is the sole place where Type 4 LSA is used to advertise the cost of the link.
- **Type 5 or AS External LSA:** The ASBR floods Type 5 LSA. The cost of a link to a destination in an external autonomous system is included in Type 5 LSAs. The autonomous system is saturated with these LSAs.
- **Type 7 LSA:** The ASBR generates Type 7 LSA, which is only flooded in an NSSA. Type 7 LSA includes the cost of a link to a destination within an external autonomous system.
- **Type 8 or Link LSA:** Every router floods this LSA. To send this LSA, each router employs a link– local flooding scope. Link LSAs include the link–local address and IPv6 prefixes for that link in the link–local flooding scope.

- **Type 9 or Intra–Area Prefix LSA:** Every router floods this LSA. When the state of links changes, an update is delivered to a local area using the intra–area prefix LSA. Intra– area prefix LSA does not induce the re–computation of the SPF algorithm.
- **Type 11 or Grace LSAs:** Grace LSAs are used to resume OSPFv3 gracefully. A router that is restarting sends these LSAs. The router broadcasts this LSA using a link–local flooding scope every time it restarts (Cisco, 2016).

**Flooding and LSA Group Pacing**

- Depending on the LSA type, OSPFv3 floods LSAs to different segments of a network. The procedure employs three distinct flooding scopes:
- Link–local, which floods LSAs only on links immediately connected to the router's interface. Link LSA and Grace LSA are sent using this flooding scope.
- Area–local, in which LSAs are flooded only within a single OSPF area. This flooding scope is used to flood LSA types 1, 2, 3, 4, and 9.
- LSAs are only flooded within a single routing domain in AS scope. The AS External LSAs are sent using this flooding scope (Cisco, 2016). The use of OSPF flooding scope ensures that all routers in the network have the same routing information. Depending on the OSPFv3 area's configuration, LSAs are flooded. The LSAs are sent based on the time it takes for the link–state to refresh. By default, link– state refresh time is every 30 minutes even if all LSAs do not have the same link–state refresh time. The LSA group pacing feature of OSPF can be used to limit the rate at which LSAs are flooded in the network. High router CPU use is considerably decreased when OSPF LSA group pacing

is used. Instead of flooding numerous LSAs with the same link–state refresh time, OSPFv3 uses the group pacing feature to merge them into a single routing update.

**Link–State Database (LSDB)**

This database is used to hold all of the LSAs that each router collects. The LSDB contains information on all network paths. OSPF calculates the optimum path to each destination using information from the LSDB. The LSDB stores the optimal paths, which are then inserted into the routing table and utilized to find remote networks. OSPF uses a time interval called MaxAge to remove LSAs whose updates have not been received, in order to maintain the content of LSDB up to date. Every 30 minutes, OSPF routers flood LSA updates to prevent accurate link–state information from aging out in the LSDB.

**OSPF Areas**

OSPF Area is a feature that can be used to limit memory and CPU requirements that the protocol can put on routers. OSPF sends routing updates to other routers by flooding them via links, and one approach to control this is to divide the network into logical pieces called Areas. LSA flooding is confined to an area by partitioning the network into areas, and LSDB generation is thus limited to links inside areas. The area ID is used to identify routers that are connected in a group. This area ID must be consistent across all routers. In addition, all routers in a given area use the same topology table. Because a router might belong to more than one area at a time, an area ID is issued to a specific interface on the router. There must be an area 0 reserved area established on any router that comprises the network's backbone when configuring more than one OSPF area. The ability to design the network in a hierarchical manner using areas is an

added benefit because it improves OSPF scalability (Lammle, 2007). Area ID remains a 32–bit value in OSPFv3 and can be written as a decimal number or in dotted decimal notation. Area 0 can, for example, be configured as Area 0.0.0.0. (Islam et al., 2010). When an OSPF area is used in a routing domain (autonomous system), it is possible to designate some routers for specific tasks. When a network is separated into various sections, these routers are utilized. OSPF router types, according to Rousinnos (2014), include the following:

- **IR (internal router)**: An IR is a router that has all of its interfaces belonging to the same area.
- **ABR (area border router)**: A router that connects at least one area to the backbone is known as an ABR. Each region to which an ABR links is considered a member of that area. For each location to which it is connected, it stores numerous copies of LSAs. Type 3 LSAs are forwarded from one region to the backbone area by the ABR. ABR2 and ABR1 will, for example, send type 3 LSAs from areas 1 and 2 to the backbone area in Figure 5. (Area 0). The ABR is also used by the backbone area to deliver summarized information about one region to another. In Figure 5, for example, Area 0 will transmit Area 1 summarized information on Area 2.
- **Backbone router (BR)**: A backbone router is one whose interface is connected to the backbone network.
- **ASBR (autonomous system border router)**: An ASBR is a router that connects one OSPF region to another autonomous system. This allows OSPF to redistribute its routing information into that autonomous system or receive redistributed routes from it.

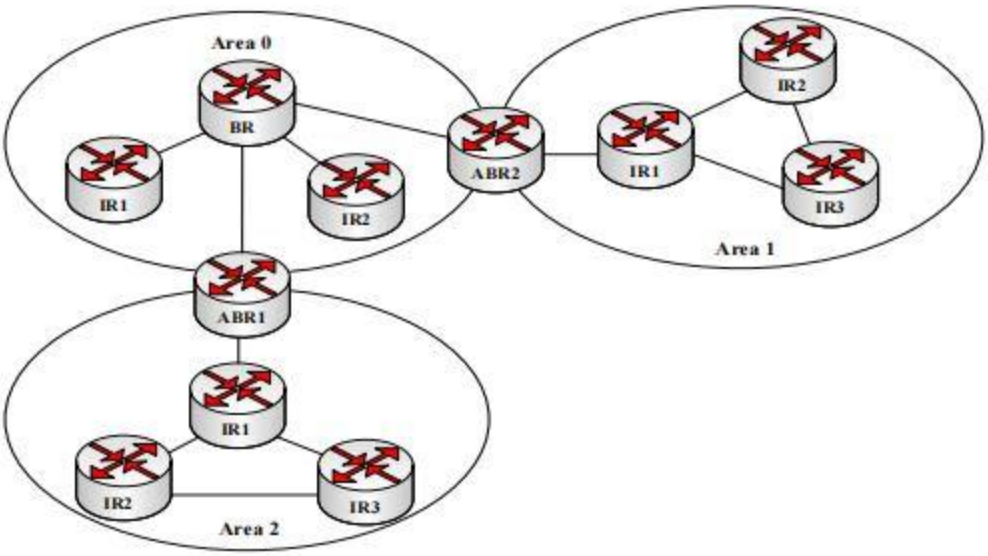



*Figure 5:* ***OSPF area structure***

Source: **Kaur & Kumar, 2015**

Depending on the needs of a network, OSPFv3 supports many sorts of areas. These are the areas in question:

- **Normal Area**: One or more area border routers connect the normal area, also known as regular area, to the backbone area. The Inter–Area– Prefix LSAs and AS External LSAs are the link state advertisement (LSA) types that are exchanged between a normal area and the backbone area. In regular areas, ASBRs are employed.
- **Stub Area**: A stub area can be designed to decrease the quantity of external routing information that is inundated in a given area. A stub Area connects to the autonomous system's backbone Area by one or more ABRs, but it does not allow the usage of internal ASBRs or the flooding of AS External LSAs, which are generally flooded across the autonomous system to distribute external route information. For any routing information

that needs to be provided via the backbone area to the external autonomous system, a stub area employs Inter–Area–Prefix LSA as the default route. This LSA's prefix length is set to 0 for IPv6.

- **NSSA (Not–So–Stubby–Area):** NSSA is similar to a stub area. However, in an NSSA, ASBR is utilized to redistribute autonomous system external routes into the NSSA. The ASBR redistributes the external routes and subsequently generates type 7 LSAs that are flooded within the NSSA. In NSSA, Type 5 LSA is not allowed. However, an ABR can be designed to connect the NSSA to other locations in order to convert type 7 LSAs to type 5 LSAs, which are then flooded throughout the autonomous system (Cisco, 2016).

**Designated Router (DR) and Backup Designated Router (BDR)**

OSPF has a variety of challenges when it comes to managing different sorts of networks. A network could be point–to–point or a multiple access network, with numerous routers communicating over a shared media. If each router floods the network with LSAs in a multiple access network, the same information regarding a link condition will be relayed from numerous sources, resulting in a significant amount of router CPU load and bandwidth usage. OSPF uses a single router called the designated router (DR) to manage how LSAs are flooded in a multi–access network. The DR's aim is to reduce the number of adjacencies produced so that all router topology tables may be synchronized. In the same network type, a backup designated router (BDR) is a hot standby router for the DR. LSA packets and routing updates are received by the BDR from OSPF neighboring routers, however the LSA updates are not flooded. The BDR is only useful if the DR has failed. In a multiple access network, each router establishes a connection with the DR and the BDR. The DR and BDR are elected depending on information in

the Hello packet. When OSPF transmits a Hello packet to other routers across an interface, it will set the priority of the DR and BDR fields if it knows which routers are the DR and BDR. If no routers proclaim themselves to be the DR or BDR, the routers will use an election mechanism based purely on which router interfaces have the highest priority. The DR is chosen as the router with the highest priority interface. By default, the highest router priority is 1. This means that changing the value of a router interface to 0 prohibits that router from being chosen as the DR or BDR. If the routers have the same router priority, the router ID is utilized to break the tie. Instead of flooding every path with LSA packets whenever a link status changes, OSPFv3 only sends updates to the DR, who then distributes the update to all the other routers in its network segment using the IPv6 multicast address FF02::5. In the event that the DR fails or ceases to function, the BDR is elected as the new DR, and OSPF elects a new BDR (Cisco, 2016).

**Shortest Path First Algorithm**

Consider the AS in Figure 6 with link–state information. The arabic numbers in the picture represent the cost metric (CST) assigned on each router interface to each network (NET), indicating the choice of using that interface. Each router is expected to receive a valid LSA from its network neighbors in order to form an LSDB from which the shortest path to every network can be determined. Before the LSDB is constructed, each router will send an LSA to all of the networks that are directly connected to it, carrying link–state information (cost). When a router receives an LSA from another router, it forwards it to its neighbors. Each router in the AS illustrated in Figure 6 will have the LSDB shown in Table 1 when the network is converged.

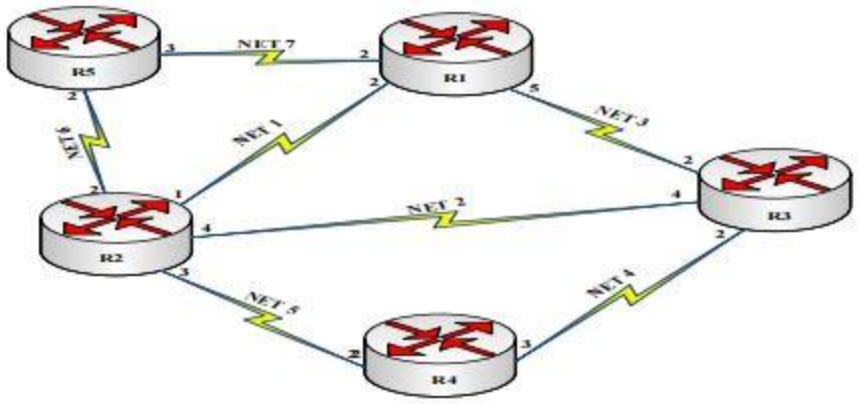



*Figure 6:* ***Autonomous System with link–state information***

Source: **Lemma et al, 2009**

Following the creation of the LSDB, each router employs the SPF algorithm to create a shortest path tree from which the least cost path to each network is calculated and saved in the routing table. R1's SPF tree is displayed in Figure 7 as it was built from the AS in Figure 6.

***Table 1: AS Link–State Database***

| Router | Connected network and Costs |
|---|---|
| R1 | NET7;CST=2, NET3;CST=5, NET1;CST=2 |
| R2 | NET6;CST=2, NET5;CST=3, NET2;CST=4, NET1;CST=1 |
| R3 | NET3;CST=2, NET4;CST=2, NET2;CST=4 |
| R4 | NET5;CST=2, NET4;CST=3 |

| | |
|---|---|
| R5 | NET6;CST=2, NET7;CST=3 |

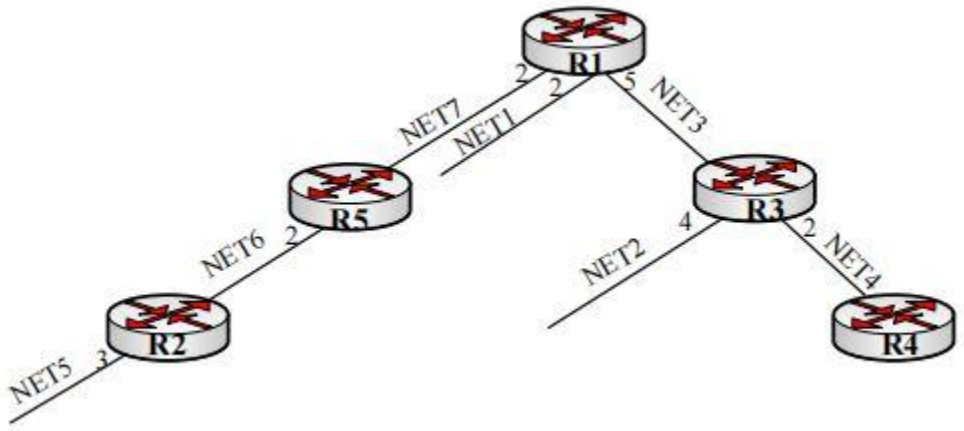
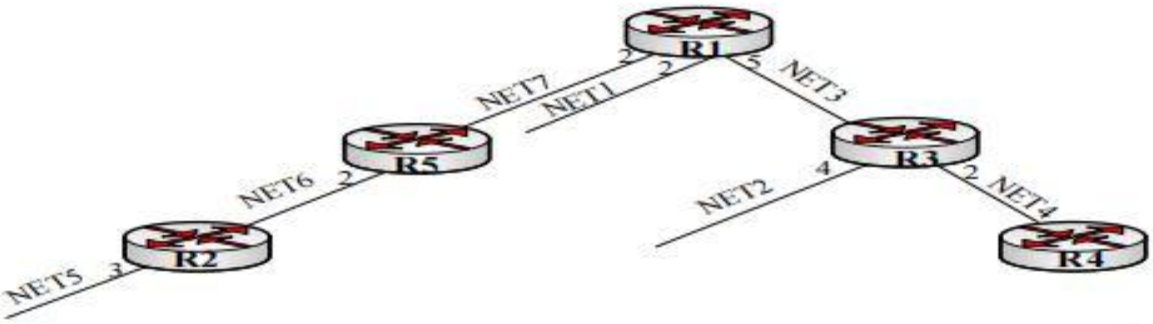



*Figure 7:* ***SPF tree constructed by R1***

Following the construction of the SPF tree, OSPF constructs routing table entries based on the information collected from the SPF tree. Each destination network built within the AS has a separate cost in the SPF tree. The routing table entries built from the SPF tree illustrated in Figure 7 are presented in Figure 8.




| Network | Forwarding Router | Metric |
|---|---|---|
| 7 | - | 2 |
| 3 | - | 5 |
| 6 | R5 | 4 |
| 5 | R2 | 5 |
| 1 | - | 2 |
| 2 | R2 | 6 |
| 4 | R3 | 7 |

*Figure 8:* ***R1 routing table entries***

**OSPF Cost**

OSPF employs cost as the primary metric for calculating the shortest path to a destination. The interface through which the router forwards LSAs has a cost associated with it. The interface with the lowest cost to the destination is chosen as the one to utilize for traffic forwarding (Lemma et al, 2009). The bandwidth on an interface is used to calculate the cost of that interface. The SPF algorithm is used by each OSPF router to build the shortest–path tree between itself and every subnetwork in its area. RFC 2328, on the other hand, does not specify how a router should calculate the cost of an associated network; the manufacturer must make this decision (Malhotra,

2002). Cisco utilizes the following calculation (Graziani et al, 2008) to compute the cost of an associated network using cumulative bandwidth at each router:

$$\text{Cost} = \frac{10^8}{bandwith\ in\ bps}$$

The cited bandwidth is the value of 108. Bits per second is the unit of measurement (bps). The referenced bandwidth is set to 100000000 by default. Cost is inversely proportional to bandwidth, as can be shown from this calculation. As a result, a link with a higher bandwidth will have the lowest cost and will be used to forward traffic more frequently.

**OSPF Convergence**

Consider the network depicted in Figure 9, which has OSPF enabled on all routers. R3 will detect the link failure and send an LSA to its neighbors R2 and R5 if the link between R3 and R4 fails. Any traffic routing is interrupted due to a change in the network topology. R2 and R5 swiftly update their topology databases, replicate the new LSA from R3, and bombard R1 and R4 with information. R1 and R4 update their topology databases when they get the new LSA, ensuring that all routers have the same topology database. The network is converged when all routers get the updated LSA and update their topology databases.

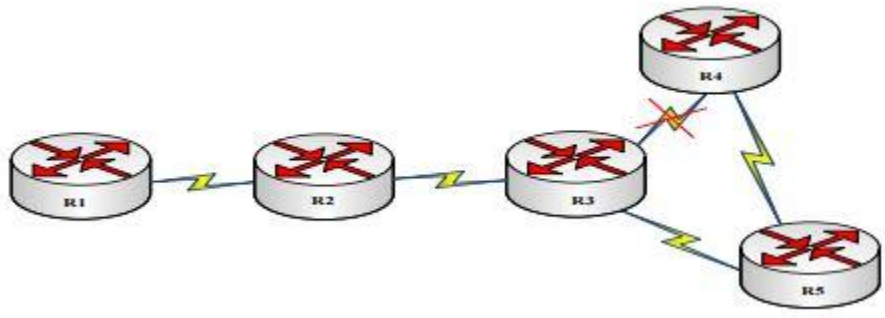



*Figure 9:* ***OSPF convergence***

Source: **Islam et al., 2010**

### 2.2.5 Advantages of OSPF

- Because OSPF is an open standard protocol, it can be used by multiple vendors.
- OSPF is more scalable, making it ideal for big networks.
- OSPF maintains many routes to a single destination with the same cost.
- OSPF minimizes routes and reduces the size of routing tables by defining regions, and any changes in network topology are immediately shared across routers.

### 2.2.6 Disadvantages of OSPF

Despite the fact that OSPF controls the flooding mechanism, it nevertheless consumes network resources (Pavani et al., 2014).

### Environment of testing

Many characteristics of EIGRPv6 and OSPFv3 are alike: the two enable CIDR ("Classless Inter-Domain Routing") and VLSM. Prefix routing is another name for CIDR. It simply host IDs and in the network indicates many bits. The two employ router IDs that are 32 bits long. Both of them have 3 tables. The two transmit incomplete updates of routing whenever there is a change rather than on a regular basis (Fiţigău & Toderean, 2013). Route summarization and redistribution are supported by both. Because of CISCO proprietary, EIGRPv6 is supported only on routers of CISCO, but OSPFv3 is an exposed standard that can be aligned on any brand, which is the reason to be likewise called industry standard (Hinds, Atojoko & Zhu, 2013). EIGRPv6 often employs a variety of measures to determine the optimum path, whereas OSPFv3 just uses one metric: cost. EIGRPv6 has an administrative distance of 90, while OSPFv3 has a

distance of 110. If two protocols of routing are functioning on similar device, a lower administrative distance signifies a higher priority.

OSPFv3's hierarchical architecture gives it a benefit over EIGRPv6. OSPFv3 is aimed for big flat networks, whereas EIGRPv6 is built for flat networks. EIGRPv6 configuration is straightforward, however OSPFv3 configuration is tough since there are many different areas kind and it works in areas, individual of which can be not so transit, transit, or stubby. Variances in these regions and their goals might enhance configuration complexity and the level of understanding required (Li et. al., 2014). Below are some comparisons based on their configuration. In interface mode, the two protocols (OSPFv3 and EIGRPv6) are aligned the same way. The two protocols are configured in global configuration mode and require 32-bit router IDs. Before configuring OSPFv3, you must first input your router ID, but configuring EIGRPv6 does not require you to submit your router ID. In the two protocols, route redistribution is aligned in worldwide mode of configuration. Route summarization in OSPFv3 is aligned in worldwide mode of configuration, but it is aligned in EIGRPv6 in mode of interface.

**What is expected from this experiment**

Xu & Trajkovi (2012) found that since it is an easy routing protocol that depends on distance vector methods, simulation findings show that RIP accomplishes well with regards to voice packet latency. When compared to EIGRP and OSPF, RIP creates less protocol traffic, specifically in the medium-sized simulated networks in this experiment. In larger networks, shortcoming of RIP is its time of slower convergence. This flaw can lead to erroneous routing

entries and, on rare occasions, routing metrics or loops nearing endlessness. In networks with less than 15 hops, RIP is favored.

With regards to Ethernet delay, routing traffic, and network convergence, EIGRP outperforms. When compared to OSPF protocol and RIP, EIGRP has distance vector and link state protocols' properties, in addition to less routing protocol traffic, lower RAM and CPU use, and enhanced network convergence. Because just hello packets are sent during regular operation, EIGRP uses extremely little network resources. When a routing table is changed, the time it takes for it to converge is short, which minimizes bandwidth use. Because a Cisco proprietary protocol is EIGRP, it cannot be used on a non-Cisco router network.

OSPF executes well for video conferencing, with regards to packet end-to-end delay and HTTP page time of reply. When updating the routing table, OSPF has a significant protocol overhead. OSPF consumes extremely little bandwidth if the network does not change. OSPF is a widely used open standard protocol that can handle massive networks. Its disadvantage is that, in comparison to RIP and EIGRP, it uses a more sophisticated algorithm that takes longer to converge when generating the routing table, resulting in more protocol traffic. OSPF requires increased processing and memory in a medium-sized simulated network, as well as a substantial bandwidth amount for the packet flooding of first link-state.

Vetriselvan, Mahendran, & Patil, (2014) found that EIGRP, IGRP, and RIP all have lower transmission costs than OSPF. IGRP has the most overhead in terms of router overhead, tracked by RIP, OSPF, and EIGRP. According to the findings depicted, OSPF followed by IGRP, RIP,

and EIGRP has the maximum throughput; for queuing delay, EIGRP followed by RIP, IGRP, and OSPF has the shortest delay; and for link utilization, EIGRP followed by IGRP, RIP, and OSPF has the highest link application.

Rakheja, Sharma, Gupta, & Kaur, (2012) found that after examining the transmission cost, throughput, router overhead, link utilization, and queuing delay of various routing protocols such as OSPF, RIP, EIGRP, and IGRP in a scenario for transmission cost, throughput, router overhead, queuing delay, and link utilization, Rakheja, Kaur, Gupta, & Sharma can conclude that OSPF has the top overall performance because it has the lowest transmission cost, the highest throughput among every queuing delay and routing protocol, and the lowest router overhead after RIP. Then EIGRP works well since its transmission costs are just slightly higher than OSPF's, and it has the best router overhead and complete performance with regards to link utilization, queuing latency, and throughput. So, OSPF outperforms competing protocols in terms of throughput, queuing latency, utilization, and overhead for best-effort service, such as data packet transfer.

Pavani, Lakshmi & Kumar (2014) found that when we compare the results of simulations of several protocols, such as RIP, EIGRP, and OSPF, for throughput, convergence, queuing delay, and link usage, we can conclude that EIGRP has the highest performance of all. After EIGRP, OSPF comes in second with the second greatest link utilization and throughput. It can be tough to choose between the two protocols, OSPF and EIGRP. As a result, we can infer that EIGRP performs better in the above circumstances, but OSPF can be a viable alternative when additional criteria such as lowest cost of transmission and lower router overhead are taken into account.

According to the findings of the convergence activity by Deng, Wu & Sun (2014), when it comes to initializing, failing, and recovering, EIGRP is certainly the fastest routing protocol among all tree protocols. OSPF is the slowest when it comes to initialization (since it has to introduce every router separately), which corresponds to their findings. RIP's performance is comparable to EIGRP on small networks, however when Deng, Wu, & Sun scale out to a larger network, convergence speed of RIP is the slowest. Deng, Wu, & Sun may deduce from the bytes/sec (traffic send) that EIGRP and OSPF profit from bandwidth, whereas RIP floods the network with comprehensive information, wasting capacity. Deng, Wu, & Sun can conclude from all simulation results' examination that EIGRP is the top alternative for networks that are small and large as it efficiently consumes bandwidth and has the fastest convergence. However, according to their research, EIGRP was just recently introduced by enterprises other than CISCO, and the structure is complex. Based on EIGRP's features, OSPF will be large networks' second choice. Because RIP performs poorly on vast networks, it is best suited to small, simple networks.

When a link fails, Anveshini, & Shetty (2016) discovered that the dynamic protocol of routing must identify the converge and failure on a novel topology to keep the operational segment network. This work investigates the case of a connection failure and recovery, as well as the duration of convergence. With little network traffic, EIGRP scales converges and well speedily. When a change occurs, EIGRP spreads only table changes of routing rather than the routing table which is complete to reduce network demand. According to the results of the experiments, OSPF has the longest network convergence time while EIGRP has the shortest.

**Methodology**

Packet Tracer 6.2.2 was used to compare the performance of different routing protocols. Cisco routers, switches, and generic computers were employed in the simulation (see Figure 11 and 13). In these topologies, standard IPv6 addresses have been used (see Figure 10 and 12).

**OSPFv3**

Below topology was utilized for OSPFv3 simulation purposes:

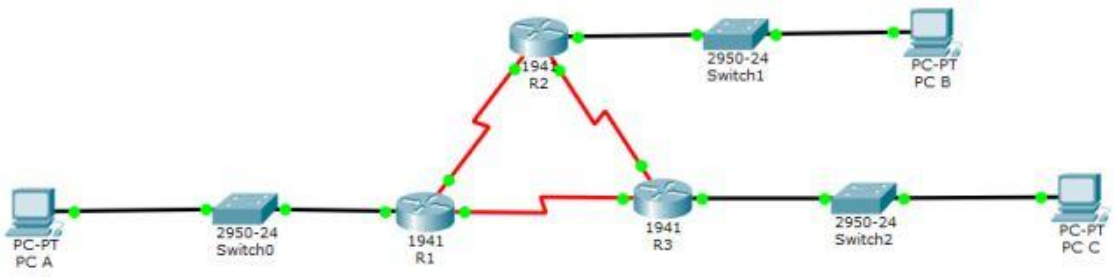



*Figure 10: OSPFv3 Topology*

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

| | | |
|---|---|---|
| *int s0/0/1* | *int s0/0/1* | *int s0/0/1* |
| *ipv6 OSPF 10 area 0* | *ipv6 OSPF 10 area 0* | *ipv6 OSPF 10 area 0* |

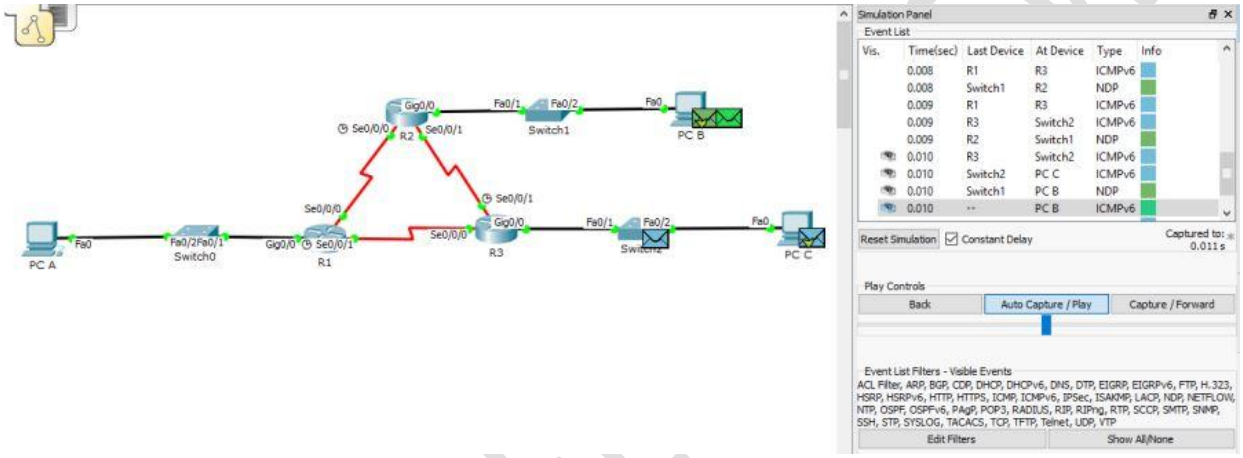



*Figure 11: Routing protocols simulation for OSPFv3*

**EIGRPv6**

For EIGRPv6 simulation purpose, topology below was applied:

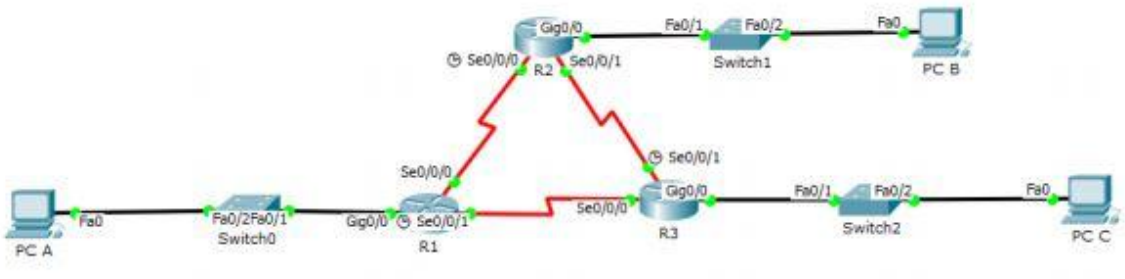



Figure 12: EIGRPv6 Topology

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

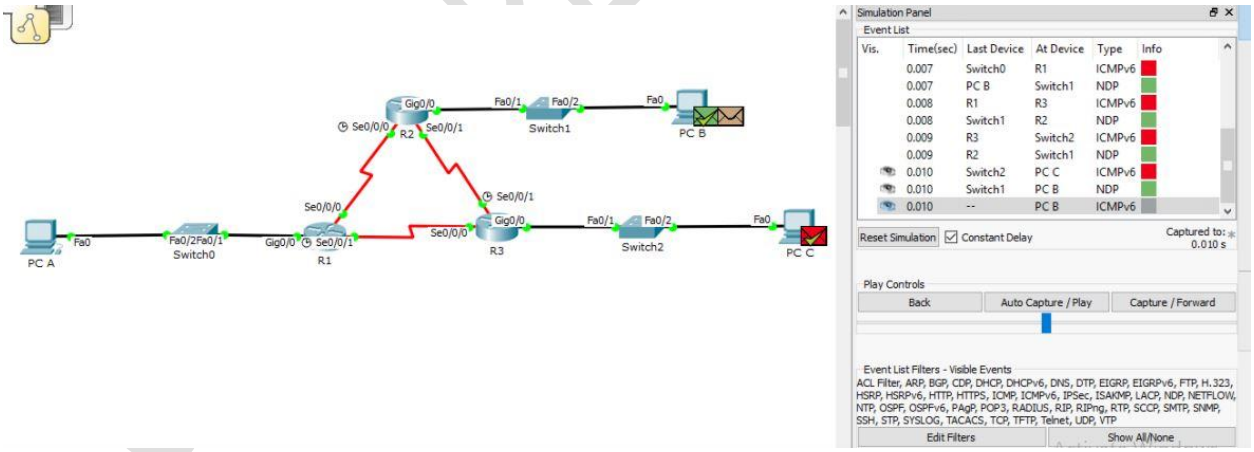



Figure 13: Routing protocols simulation for EIGRPv6

**Results and Analysis**

**Analysis of packet loss comparison**

We improved the packet size transmitted for the two topologies in the first analysis. Once more or one data migrant packets fail over a computer network to meet target, loss of packet happens. Network congestion is the most common cause of packet loss since the alternate channels were not chosen quickly enough. It was discovered that packet increasing size increases many packet losses. The packet loss of OSPFv3 network is higher than EIGRPv6 network, as illustrated in Figure 14. As a result, EIGRPv6 outperforms OSPFv3 when it comes to packet loss.

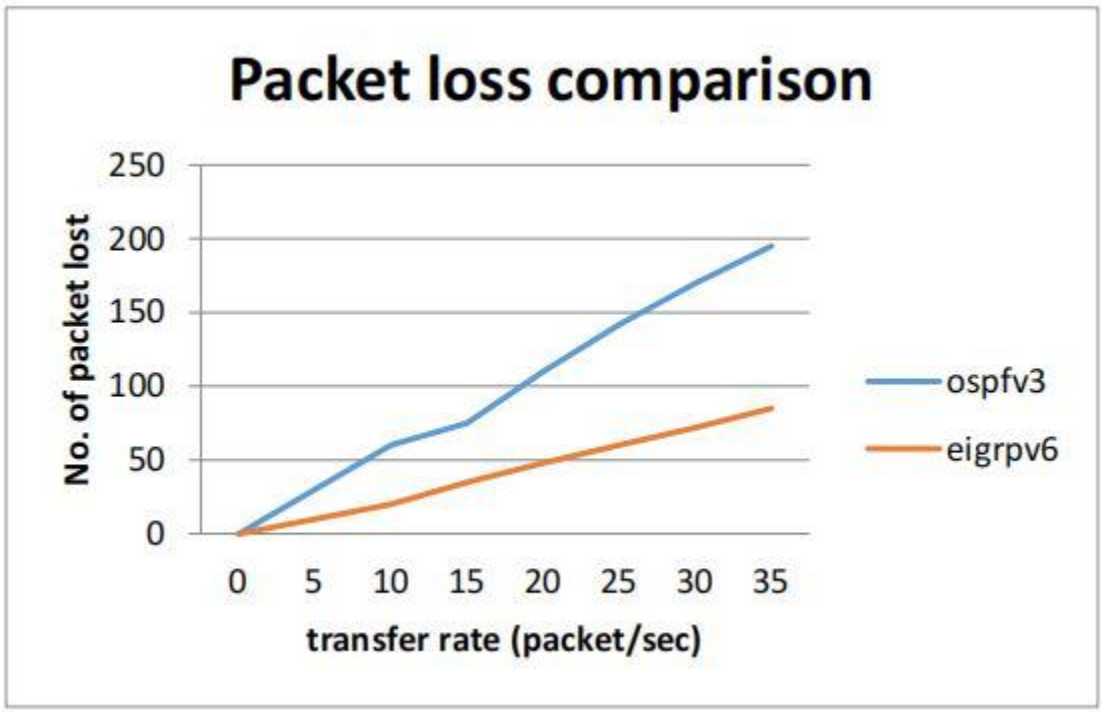



Figure 14: Comparison of packet loss between EIGRPv6 and OSPFv3

**Analysis of end to end delay comparison:**

The time it takes for a packet to go from source to destination across a network defines end-to-end delay. It's a term that's commonly used in IP network monitoring. Figure 15 shows that increasing packet size increases end-to-end delay due to congestion and routing delays. This is

seen in Figure 15. In comparison to EIGRPv6, OSPFv3 has a longer end-to-end delay. As a result, EIGRPv6 outperforms EIGRPv4.


*Figure 15: End to end delay comparison between OSPFv3 and EIGRPv6*

**Convergence time comparison analysis:**

Convergence is the state of many routers that share similar topological knowledge about the internetwork in which they function thanks to the routing protocol that has been implemented. Figure 16 shows that OSPFv3 takes about nine seconds, whereas EIGRPv6 takes approximately 6 seconds. As a result, EIGRPv6 is faster than OSPFv3 in terms of convergence time.

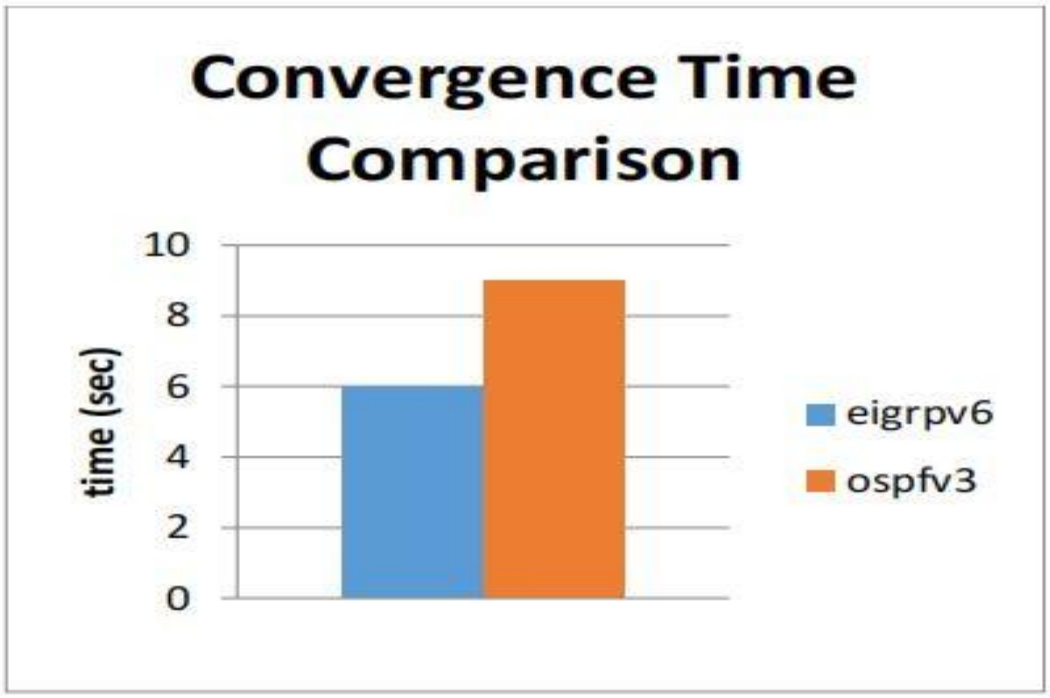



*Figure 16: Comparison of convergence time between EIGRPv6 and OSPFv3*

This is because EIGRP employs DUAL to offer quick convergence, whereas OSPF uses hello timers and interface modifications to detect topology changes. This causes LSA to update neighbors, and OSPF convergence optimizations are accomplished by modifying timer values.

**Conclusion**

Two prominent internal routing protocols are explored in this work. The characteristics of convergence timing, end-to-end delay, and packet loss were used for performance evaluation. In all three scenarios, EIGRPv6 outperforms OSPFv3 according to our findings. As a result, we advocate using EIGRPv6 as an internal routing protocol in a network of IPv6. However, the most significant drawback of EIGRPv6 is that it can only be utilized in Cisco routers. OSPFv3 is the

best option in this circumstance. In the future, we'll compare these routing protocols while taking IPv6 security into account. The project will be expanded to include real-world gadgets.

**Reference**


Abidin, N. Z., Fiade, A., Aripiyanto, S., & Handayani, V. (2021, September). Performance Analysis of POX and RYU Controller on Software Defined Network with Spanning Tree Protocol. In *2021 9th International Conference on Cyber and IT Service Management (CITSM)* (pp. 1-5). IEEE.

Ashraf, Z., & Yousaf, M. (2017). Optimized Routing Information Exchange in Hybrid IPv4-IPv6 Network using OSPF V 3 & EIGRPv6. *(IJACSA) International Journal of Advanced Computer Science and Applications*, *8*(4), 220–229.

Ashraf, Z. (2013). IPv6 Routing: A Practitioner Approach: Lap Lambert Academic Publishing GmbH KG.

Biradar, A. G. (2020, December). A Comparative Study on Routing Protocols: RIP, OSPF and EIGRP and Their Analysis Using GNS-3. In *2020 5th IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE)* (pp. 1-5). IEEE.

Chauhan, D. & Sharma, S. (2015). Performance Evaluation of Different Routing Protocols in IPv4 and IPv6 Networks on the basis of Packet Sizes. *Procedia computer science*, 46, 1072-1078.

Coltun, R., Ferguson, D., Moy, J. & Lindem, A. (2008). RFC 5340, OSPF for IPv6. *IETF*. 24(7).

Das, S., Subedi, S. & Shekar, N. V. S. (2014). Network Performance Analysis of Dynamic Routing protocols real time applications. *International Journal of Modern Engineering Research*, 4(5), 49-57.

Deering, S. E. & Hinden, R. (1998). *RFC 2640, Internet Protocol, version 6 (IPv6) Specification*. IETF RFC 2460.

Din, I. U., Mahfooz, S. & Adnan, M. (2010). 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.

Essah, R., Senior, I. A. A., & Anand, D. (2021). Assessing the Performance Analysis of OSPFV3 and EIGRP in Applications in IPV6 Analysis for Articles Published in Scopus between 2016 and 2021.

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

Fiţigău, I. & Toderean, G. (2013). Network performance evaluation for RIP, OSPF, and EIGRP routing protocols. *in Electronics, Computers and Artificial Intelligence (ECAI), 2013 International Conference*, pp. 1-4.

Fuzi, M. F. M., Abdullah, K., Abd Halim, I. H., & Ruslan, R. (2021). Network Automation using Ansible for EIGRP Network. *Journal of Computing Research and Innovation*, *6*(4), 59-69.

Gough, C. (2003). *CCNP BSCI Exam Certification Guide: CCNP Self-study*: Cisco Press.

Goyal, M., Soperi, M., Baccelli, E., Choudhury, G., Shaikh, A., Hosseini, H. et al., (2012). Improving convergence speed and scalability in OSPF: a survey. *IEEE Communications Surveys & Tutorials,* 14, pp. 443-463.

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

Hossain, M. A., Ali, M. M., Akter, M. S., & Sajib, M. S. A. (2020). Performance Comparison of EIGRP, OSPF and RIP Routing Protocols using Cisco Packet Tracer and OPNET Simulator. *Global Journal of Computer Science and Technology*.

Jain, N., & Payal, A. (2020). Performance Evaluation of IPv6 Network for Real-Time Applications IS-ISv6 Routing Protocol on Riverbed Modeler. *Procedia Computer Science: International Conference on Smart Sustainable Intelligent Computing and Applications under ICITETM2020, 173*, 46–55. https://doi.org/10.1016/j.procs.2020.06.007

Jain, N., Payal, A., & Jain, A. (2021). Effect of data packet size on the performance of RIP and OSPF routing protocols in hybrid networks. *International Journal of Pervasive Computing and Communications*.

Jain, N., Payal, A., & Jain, A. (2021). Effect of data packet size on the performance of RIP and OSPF routing protocols in hybrid networks. *International Journal of Pervasive Computing and Communications*.

Jain, N., Payal, A., & Jain, A. (2021). Performance analysis of routing protocols on IPv4 and IPv6 addressing networks. *Journal of Web Engineering*, 1327-1366.

Jian, S. & Fang, Y. Y. (2011). Research and implement of OSPFv3 in Ipv6 Network. *in Proceedings of the CSQRWC, Conference on Cross Strait Quad-Regional Radio Science and Wireless Technology Conference*, p. 746.

Julia, I. R., Suseno, H. B., Wardhani, L. K., Khairani, D., Hulliyah, K., & Muharram, A. T. (2020, October). Performance Evaluation of First Hop Redundancy Protocol (FHRP) on VRRP, HSRP, GLBP with Routing Protocol BGP and EIGRP. In *2020 8th International Conference on Cyber and IT Service Management (CITSM)* (pp. 1-5). IEEE.

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

Krishnan, Y. N. & Shobha, G. (2013). Performance analysis of OSPF and EIGRP routing protocols for greener internetworking. *in Green High Performance Computing (ICGHPC), 2013 IEEE International Conference*, pp. 1-4.

Li, F., Yang, J., Wu, J., Zheng, Z., Zhang, H. & Wang, X. (2014). Configuration analysis and recommendation: Case studies in IPv6 networks," Computer Communications, vol. 53, pp. 37-51.

Muhammad, P., Trisnawan, P. H., & Amron, K. (2020). Analisis Perbandingan Kinerja Protokol Routing OSPF, RIP, EIGRP, dan IS-IS. *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer e-ISSN*, *2548*, 964X.

Okonkwo, I. J., & Emmanuel, I. D. (2020). Comparative study of EIGRP and OSPF protocols based on network convergence. *International Journal of Advanced Computer Science and Applications*, *11*(6), 39-45.

Ordabayeva, G. K., Othman, M., Kirgizbayeva, B., Iztaev, Z. D., & Bayegizova, A. (2020, September). A systematic review of transition from IPv4 to IPv6. In *Proceedings of the 6th International Conference on Engineering & MIS 2020* (pp. 1-15).

Pal, R., Kushwaha, R., Tomar, R. S., & Tripathi, R. (2021, July). Comparison of Three Routing Protocols in terms of Packet Transfer Using IPv6 Addressing. In *2021 8th International Conference on Smart Computing and Communications (ICSCC)* (pp. 164-169). IEEE.

Rajneesh, N. & Aggarwal, P. (2014). Performance Evaluation of RIP And OSPF In IPv6 Using Opnet 14.5 Simulator. *International Journal of Technical Research and Applications*, 2(6), 37-41.

Rasel, A. N. (2020). Performance Analysis of IPv6 vs IPv4 Using Dynamic routing OSPF.

Sadat, M. A. (2021). Lab Implementation of IPv6 in Enterprise NetworkUsing Cisco Packet Tracer. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(10), 6564-6580.

Sakib, M., & Singh, J. (2020). Simulation based performance analysis of IPSec VPN over IPv6 networks. *International Journal of Electronics Engineering*, *12*(2), 92-104.

Samaan, S. S., & Lecturer, A. (2018). Performance Evaluation of RIPng , EIGRPv6 and OSPFv3 for Real Time Applications. *Journal of Engineering*, *24*(1), 111–122.

Sathyasri, B., Janani, P., & Mahalakshmi, V. (2021). Redistribution of Dynamic Routing Protocols (ISIS, OSPF, EIGRP), IPvfi Networks, and Their Performance Analysis. *Recent Trends in Communication and Intelligent Systems: Proceedings of ICRTCIS 2020*, 179.

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

Savage, D., Slice, D., White, R., Ng, J., Paluch, P. & Moore, S. (2016). RFC 7868, Cisco's Enhanced Interior Gateway Routing Protocol (EIGRP).

Sinthia, F. Z., Nasir, A., Paul, B., Rashid, M. R. A., & Adnan, M. N. (2021). Implementation of OSPFv3 in IPv4 and IPv6 for Establishing a Wide Area Network. In *ICT Systems and Sustainability* (pp. 473-481). Springer, Singapore.

Tarasiuk, H., Hanczewski, S., Kaliszan, A., Szuman, R., Ogrodowczyk, Ł., Olszewski, I. et al., (2016). The IPv6 QoS system implementation in virtual infrastructure. *Telecommunication Systems*, vol. 61, pp. 221-233.

Tersianto, R. F., Hidayat, N., & Nurwasito, H. (2020). Studi Komparasi Kinerja dari Adaptive Routing Protocol OSPFv3, RIPng, EIGRP IPv6, dan IS-IS pada Jaringan IPv6. *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer e-ISSN*, *2548*, 964X.

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

Triasari, B. E., Tulloh, R., & Iqbal, M. (2020). Implementasi Dan Analisis Perbandingan Performansi Routing Protocol Eigrp, Is-is, Dan Ospfv3 Pada Ipv6 Untuk Layanan Triple Play. *eProceedings of Applied Science*, *6*(3).

Veselý, V., Rek, V. & Ryšavý, O. (2015). Enhanced Interior Gateway Routing Protocol with IPv4 and IPv6 Support for OMNeT++," in Simulation and Modeling Methodologies, Technologies and Applications, ed: Springer, pp. 65-82.

Vetriselvan, V., Patil, P. R. & Mahendran, M. (2014). Survey on the RIP, OSPF, EIGRP Routing Protocol. *(IJCSIT) International Journal of Computer Science and Information Technologies*, 5(2), 1058 1065.

Whitfield, R., & Zhu, S. Y. (2021). A Comparison of OSPFv3 and EIGRPv6 in a Small IPv6 Enterprise Network. *(IJACSA) International Journal of Advanced Computer Science and Applications*, *6*(1), 1–7. Retrieved from http://hdl.handle.net/10545/620915

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