JOURNAL OF TRANSACTIONS IN SYSTEMS ENGINEERING

Journal of Transactions in Systems Engineering
https://ijitis.org/index.php/JTSE
ISSN: 2806-2973
Volume 1, Issue 2
DOI: doi.org/10.15157/JTSE.2023.1.2.73-103
Received: 12.04.2023; Accepted: 29.07.2023

TULTECH

A Comparative Analysis of OSPF and EIGRP Routing Protocol Evaluation

Noelia Karamela[1] and Dimitrios A. Karras[1,2*]

[1] Canadian Institute of Technology, Tirana, Albania
[2] National and Kapodistrian University of Athens (NKUA), Greece
***Dimitrios.karras@gmail.com, Dimitrios.karras@cit.edu.al**

Abstract

In recent decades, technology has advanced quickly in every area of human life, but network data communications have grown at a particularly rapid rate. New terms like "Internet of Things," "Cloud" services, or "Bring your own devices (BYOD)" have been used to describe new ways of working, communicating, and socializing. The evolution of routing protocols has taken a similar course; simple distance vector protocols gave rise to the development of link state and hybrid protocols. Business demands for managing public and private cloud services, as well as the quick convergence of data centres to meet redundancy needs, have led to this progression. In order to accomplish their objective, routing protocols choose the best routes for transferring data from one node to another and define how routers communicate with one another. Exterior Gateway Protocol (EGP) and Interior Gateway Protocol (IGR) are the two primary kinds of routing protocols. The goal of this article is to evaluate the behaviour of OSPF and EIGRP, two IGR protocols that now control the market for industry standards in this area. Both function inside an autonomous system, and despite differences in how they build associations between attributes, how they respond to changes, and how they organize themselves topologically, they both succeed in delivering the same outcome in strong routing and network stability. Network convergence and communications timing, as well as packet delay variations regarding two distinct typologies, are evaluated as performance aspects in this paper. The first typology offers a basic framework for comparison, while the second looks at how scale affects both protocols.

Keywords: *OSPF, EIGRP, network convergence time, variation of packet delay in a video conference call, IP voice jitter, CPU utilization, dynamic routing protocols, Cisco Packet Tracer*

INTRODUCTION

Routing comprises sets of algorithms used by routers in the network communication processes for the data to be transmitted to known destinations by forwarding them from the configured origin. As a result of the extensive expanse of contemporary networks, corporations, businesses, and internet service providers rely on routing protocols, both internal and external. These protocols aid routers in identifying neighbouring routers, retaining connection details, acquiring knowledge of new routers, and promptly recuperating from the loss of a connection or line between routers. This demonstrates very clearly why selecting the routing protocol requires careful consideration; a bad choice of routing protocol may severely impact performance, resulting in inferior service. Before we can select a suitable routing protocol, we need to establish whether this protocol will be used within a self-governing system, which is a network managed by a common group, or between independent self-governing systems. Furthermore, other decisive factors such as network magnitude, hierarchical configuration, connection bandwidth, etc., must be taken into account. If the latter situation applies, we must utilize an external routing mechanism. The pace at which routing tables are generated in response to modifications, the amount of traffic the protocol delivers to fulfil requests, the CPU, and, of course, the memory usage all contribute to discussions and alternative conclusions that ultimately result in convergence.

Since the beginning of the Internet, there has been consistent development in the protocols used for routing. Since RIPv1, RIPv2, and IGRP, which exhibited severe limits in what are dubbed "classless networks" and discontinuous typologies, numerous attempts have been undertaken. This is because of the constraints that were shown (Fortz). What was first noticed was the need to use optimal algorithms in order to establish the best routing networks. This was initially noticed. In order to generate "loop-free" network diagrams, these methods should set speed and efficiency requirements. Because of this, the Open Shortest Path First (OSPF) protocol and its hierarchical structure were developed. It is important to keep in mind that a multi-area OSPF will install a "backbone," to which all of the other areas will need to be linked. This maintains uniformity throughout networks, and when combined with the right design, it prevents anomalies or instability from spreading to new regions [1].

Even though OSPF is a full protocol, which means that it takes into account all of the connections in a network and has knowledge of the network's whole topology, it requires additional processing in the event that any of the links in the network become unavailable. As a consequence of this, a distance-vector protocol was developed that, by making an assumption, simulates the "loop-free" choice that is taken by OSPF. This assumption, often referred to as a "feasibility requirement," was validated by means of simulation tests in line with Cisco [2]. These trials required each router to validate the information that it had received from its surrounding routers.

There have been a lot of studies that have analysed the behaviour of these two protocols, particularly in a comparative context, showing how various routing practices might impact the flow of data [3]. After analysing a variety of factors, including convergence and delay caused by network failures or link disconnections, our experiments have led us to the conclusion that EIGRP generates superior results, but the outcomes of other experimental investigations are more variable [4, 5]. This is one of the motivations for the work that was done for this paper, namely, to investigate the behaviour of these two protocols inside a scaled typology using a hierarchical design that is not very cautious. It is not an abstract scenario but rather one that may be produced by the merger of several organized autonomous systems, such as the merging of various businesses. In circumstances in which there is a double load or unexpected breakdowns in network connectivity, this will be appreciated more than usual.

It is said by [6] that EIGRP is more beneficial than OPFG when the re-routing procedure and retransmission time to reach the ultimate destination in the event of disconnection are included. This claim is based on previous research that compared the performance of EIGRP and OSPF dynamic routing protocols. In addition, [7] broadened the scope of this investigation by including real-time video streaming applications. Again, when compared to OSPF, EIGRP proved to be superior because of the criteria that were considered. This conclusion was reinforced by [8], who, among other things, highlighted the fact that EIGRP makes far less of a demand on the system's resources. In [8], we came to the conclusion that EIGRP requires less bandwidth and memory usage, which results in a better convergence time compared to OSPF. He reached this conclusion by using the same metrics that were mentioned above.

To continue with the extensive research on comparing these two protocols based on overall performance, it should be noted that in [9], after examining OSPF in terms of network scalability, we came to the conclusion that the Open Shortest Path First Protocol exhibits problems with memory and CPU usage. This was the conclusion reached after the researchers examined OSPF in terms of network scalability. In [10], the authors utilized the same simulation methodology as this study in their investigation of the performance of VOIP on three different protocols: RIP, EIGRP, and OSPF. When compared to OSPF and EIGRP, RIP is far behind the times. This is to be anticipated. EIGRP, on the other hand, is not as successful as OSPF in circumstances in which we have link failures due to the absence of a "feasible successor." During the process of computing the new routing, OSPF continues to maintain a performance that is both efficient and adaptable. Last but not least, it is important to note that in [11], it is noted that the choice of the protocol that will be employed in certain circumstances is determined by a number of different elements. They are certain that this is the case and that there is no methodology that can satisfy what is required from each of the factors.

When it comes to the performance of these two procedures, there are many ideas that have been offered, and these theories are based on the reports that scientists and analysts have made over the years. The comparison conducted in this paper will, however, become more accurate as technology continues to advance and more sophisticated simulation tools are developed. These tools will have a greater range of capabilities. The fact that EIGRP has several drawbacks that need to be taken into account is the primary justification for why this line of study has to be carried on even if it is well accepted that OSPF is a more effective routing protocol than EIGRP.

Objectives of the study

This paper compares the various aspects of the performance of two of the most popular protocols for IPv4: OSPF and EIGRP. By achieving the following goals, this will be possible:

- Constructing two typologies in a simulated setting, the first typology will be one simple typology, which will present us with the fundamental comparative controls of traits and behaviours of each protocol studied. Depending on the simulation environment, the second typology will be more complicated and show the scaling implications of each technique.
- Analysing diverse timer implementation approaches that may be utilized to emphasize the routing process, namely the convergence duration and packet delay.
- Examining the default actions of protocols in urban non-hierarchical topologies; The two stages of the protocol comparison are as follows:

First phase: Based on how they function and the behaviour of convergence, protocols are introduced, examined, and carefully explained. The way they operate on the same typology differs because they use distinctive algorithms called SPF and DUAL and utilize various metrics based on cost (OSPF) and bandwidth, reliability, and load (EIGRP).

Second phase: Experiments are utilized in the simulation environment to demonstrate how each operation operates. Although it is common knowledge that careful EIGRP design yields superior results, the purpose of this research is to illustrate that this is not always the case, especially during network convergence if a large network lacks a hierarchical structure.

Based on the experimental results of [3] and [5], there were some facts raised that will serve as a basis for the comparison of the results achieved by the conducted experiments, and they are as follows:

OSPF protocol convergence will occur quicker in basic topologies than EIGRP protocol convergence. In contrast to OSPF, the EIGRP protocol will converge more slowly in non-hierarchically scaled typologies. Regarding packet delay variation in video conference calls, the variability in EIGRP packet latency will be comparable to or somewhat less than that of OSPF, resulting in higher effective throughput. On IP voice jitter, EIGRP's IP voice jitter will be less than that of OSPF. CPU Usage and Utilization: In comparison to EIGRP, OSPF will require more computing power in simpler typologies, and in topologies that are not hierarchically scaled, EIGRP will require a greater amount of processing resources compared to OSPF.

METHODOLOGY

Access to scientific and technical information online, namely that which is powered by IEEE and CISCO, allowed for the design of this paper to be completed successfully. Also, a significant portion of the knowledge has profited from the careful selection of the information included within the research engines on the internet, as well as inside online newspapers and conferences, printed publications, and online bibliographic databases. In computer networks, speedy response is achieved by utilizing pertinent terms like OSPF, EIGRP, network convergence duration, variation in packet delay, IP voice fluctuation, CPU usage, data transfer rate, active routing mechanisms, and Cisco Packet Tracer.

INTERNAL ROUTING PROTOCOLS

The majority of individuals begin the process of establishing a network by initially connecting end devices (computers, tablets, smartphones, servers, and printers) to switches or wireless access points through Network Interface Cards (NICs). LANs are constructed in this way, and they operate on the OSI model's second tier, known as the data connection layer. The Data Link Layer [12].

On the other hand, the question of how distinct local area networks connect to one another emerges. The creation of routing is a reaction to the requirement for a solution to this challenge. Routers, servers, and layer 3 switches are equipment found in the third layer of the OSI network architecture. The process of routing entails determining the most efficient and effective approach to a certain place. When data packets are processed and "routed" to their ultimate destination, the destination address is taken into account.

Router operating mode. Routers first link to many networks. Upon receiving a transmission through any of its interfaces, the router verifies if the transmission is intended for the same network as that interface. If it is, the package is disregarded. Conversely, if the package is meant for a different network, the router performs a lookup operation by scanning its routing tables, also referred to as its local database, to identify an outgoing interface that can transport the packet. Subsequently, the router undertakes two processes: a "lookup procedure" to locate a route in the routing table and a "switch operation" to receive a packet from one interface, repackage it, and transmit it to another interface. These two procedures are commonly known as the "lookup process" and the "switch operation" respectively.

The most important component of the routing process is the process of constructing routing tables. Initially, routers would add to these tables all functioning networks to which they are directly connected through a connection formed with them. Static routing instructions are then utilized to route traffic to each of the networks selected by the administrator. Finally, if we have developed a dynamic protocol, the router will save all of the routes it has learned by utilizing this protocol in its routing database. If all of these procedures are followed, the routing table will be dynamic and will adapt itself anytime the network topology is modified or updated [13].

It is possible to classify dynamic protocols into several subgroups depending on where they are used—within or outside of autonomous systems (interior or exterior gateway protocols, respectively) and on whether they utilize the distance-vector protocol or the link-state protocol. A set of routers that share administrative control and operate under this administration constitutes an autonomous system. This kind of system also includes several routing devices. RIPv1, RIPv2, RIPv4, RIPv6, EIGRP, OSPF, and IS-IS are our internal routing protocols, whereas BGP is the industry standard protocol for outside routing. The Routing Information Protocol's initial version was RIPv1, and the fourth version was RIPv2 [13, 14].

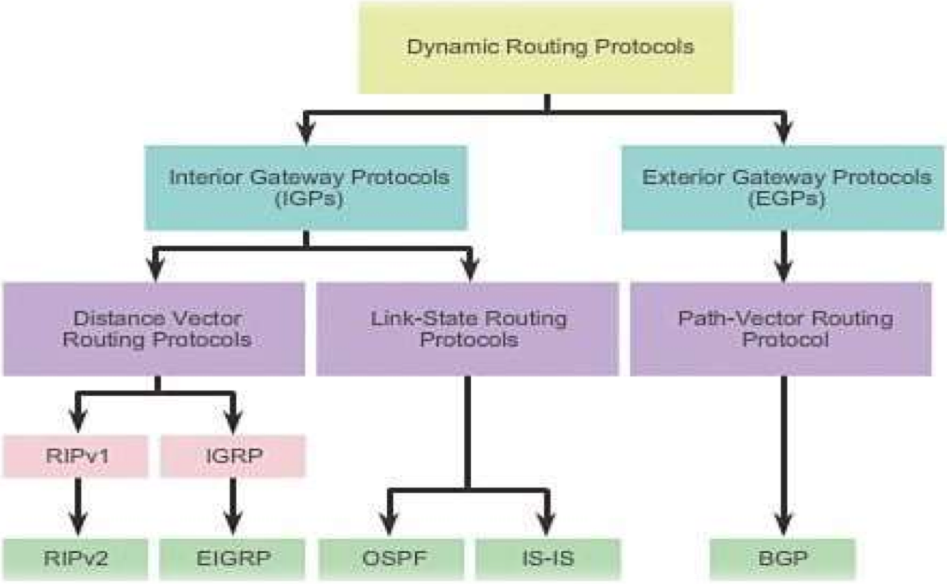

Dynamic Routing Protocols
Interior Gateway Protocols (IGPs)
Exterior Gateway Protocols (EGPs)
Distance Vector Routing Protocols
Link-State Routing Protocols
Path-Vector Routing Protocol
RIPv1
IGRP
RIPv2
EIGRP
OSPF
IS-IS
BGP

Figure 1. Hierarchy of routing protocols

Routing Distance vector

The usage of this phrase implies that routing choices are made depending on the distance between two nearby routing devices' routing pathways. It is true that routers that utilize distance-vector routing do not have knowledge about the whole network topology; rather, they only know the distance to the target network and the direction traffic should be sent. This category includes the routing protocols RIPv1, RIPv2, IGRP, and EIGRP [15].

Direction relates to how a route is discovered by a router's interface, while distance refers to the "cost" of reaching the destination network. This "cost" is measured in hops for the RIP protocol; however, for IGRP and EIGRP, it is a composite metric that takes into account aspects such as bandwidth, latency, load, and dependability [16].

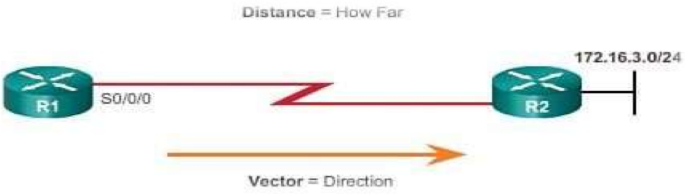


Figure 2. Understanding the distance-vector protocol

Consistent dissemination of revisions to every interface is a prime feature of distance-vector routing. These changes can impact either the complete routing table or a portion of it. Upon receipt of such an update, a participating router matches it against the data already present in its table, revises the table with the fresh data, and subsequently circulates it to other routers within the vicinity. When there are several routes that send to the same destination, this sort of routing creates routing loops. Distance vector routing is also known as "rumour routing." Each router only carries information about its adjacent router, and since it lacks knowledge about the network's typology, it relies on the information provided by this router. Numerous strategies, such as counting to infinity, splitting the horizon, and poison reversal, have been developed to overcome this challenge. These won't be investigated further since they are not the topic of this research [16].

Link-State Routing

Link-State Routing indicates that routing decisions are made independently at each router based on the network graph that is maintained in memory. This graph depicts every relationship between the nodes of an autonomous system. This typology information enables each router to compute the optimum route or routes to various networks in the system, which are subsequently stored in routing tables. A fundamental feature of this approach is that the router does not need to update nearby routers on a regular basis but only when an event happens (such as the discovery of a new router or an unexpected connection failure). Routing protocols pertaining to this category include OSPF and IS-IS [17].

Link-state routing starts with the neighbour router discovery phase, during which each router sends hello packets to find and keep all neighbouring routers connected. Then, for all routers in the system to be aware of these linkages and who creates them, each router displays the links to which it is linked. Each router maintains its own topology table, which contains all of these connections. Together with the adjacent router table, this table provides a network topology view [18].

The link cost parameter is used in the last step of algorithm execution, which creates the shortest route to each network connection. The router generates a network graph and then starts executing the shortest possible path algorithm by positioning itself at the bottom of the output tree. The final result of the algorithm, which operates separately on every router, fills up the autonomous system's routing tables. A feature of the method is that changes in the typology cause re-calculation and, as a result, memory and CPU usage [19]. This style of routing has a small benefit over distance-vector routing in that routing loops are less likely to arise since the routers are familiar with the network topology.

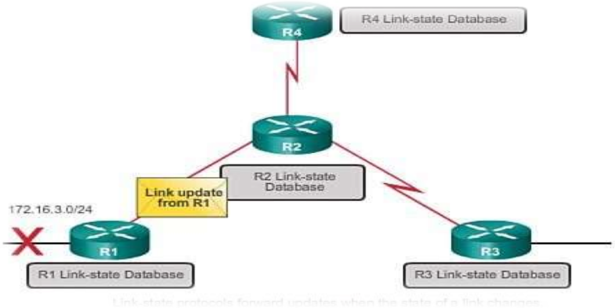


Figure 3. Link-state protocol operation

OSPF protocol

OSPF, or Open Shortest Path First, is an interior gateway routing protocol that was created in the early 1970s by a group from the Internet Engineering Task Force (IEFT), and it has been implemented in various ways on the Arpanet. This routing protocol is used by autonomous systems to send routing information. It is important to note that the name of the protocol has two features. The word "open" suggests that the protocol was created using open and public RFC (Request for Comments) methods, while "SPF" (Shortest Path First) refers to Dijkstra's well-known algorithm that identifies the shortest path dynamically in a network. The first version (OSPFv1) was developed in 1989, and drafts were created in 1131. The second version (OSPFv2) was written in 1991 and revised in RFCs 1583, 2178, and 2328. Finally, in 1997, RFC 2740 introduced OSPFv3 for IPv6.

OSPF protocol Message Encapsulation

Usually, an OSPF message is enclosed in a packet, as shown in Table 1 [20].

Table 1. Encapsulated OSPF message

Data Link Frame Header	IP Packet Header	OSPF Packet Header	OSPF packet type
1. Source Mac address (address to send interface). 2. Destination Mac address (Multicast address :01-00-5E-00-00-05 or 01-00-5E-00-00-06)	1.IPv4 source address 2. IPv4 destination address (Multicast:224.0.0.5 /224.0.0.6 and protocol field 89)	Type Code 1. Router ID 2. Area ID	1. Hello package 2. Description of the database 3. Link state request 4. List state update 5. Recognition (acceptance) State list

Every OSPF packet contains the OSPF Packet Header, which is encapsulated in an IP packet with protocol field 89 and a destination address of either 224.0.0.5 or 224.0.0.6. The OSPF packet header is shown in Table 2 [20, 21].

Table 2. OSPF Header packets

Version Number V.2 for IPv4 V.3 for IPv6	**Type** Hello, DBD, LSR, LSU, LSAck	**Package Length** The size in bytes of the OSPF packet, comprising the conventional OSPF header.
Router ID We have the ID of the source router		
Checksum It is used to check the integrity and ensure that the OSPF packet is not corrupted during transmission, including the header.	**AuType** Describes OSPF packet authentication type 0-> no authentication 1-> Simple authentication, plain text password 2-> MD5 encrypted message	
Authentication This 64-bit field is used to authenticate the OSPF packet in order to participate in the routing domain.		

Furthermore, OSPF employs five distinct sorts of packets. Each performs a distinct function [21]. They are as follows, see Table 3 and 4:

Table 3. OSPF Packet Types

1.Hello Packet
2.DataBase Description (DBD)
3.Link State Description (LSR)
4.Link State Update (LSU)
Link

a. Hello Packet is used to find and share routing databases with surrounding routers. This packet "advertises" certain parameters, and after its task is done, the nearby router becomes a neighbour. Hello packets are used to signal if the connection between the routers is "alive." Hello packets are transmitted to nearby routers on a regular basis to preserve bidirectional connections. If a router does not receive this Hello packet within a certain time period (dead interval), it is termed "dead," and all information transferred between routers is invalid. Hello packets are used to select designated (DR) and backup designated routers in broadcast or NBMA networks (BDR).

Table 4. OSPF Hello Packets

<table>
<tr><td colspan="3">**Network Mask**
The network mask of the originating interface is 32 bits and describes how it is connected to the receiving interface</td></tr>
<tr><td>**Hello Interval**
Interval between routers while exchanging data (default 10 seconds). The retransmission interval is set at 5 seconds (by deafult)</td><td>**Options Router priority**
Define the following capacity and optional capabilities: E-bit (flag bit) indicating what sort of region the interface works in (1=normal, 0=stub).</td><td>**Router priority**
This variable is used to determine DR and BDR selection in Broadcast and NBMA networks depending on the top priority number. When the priority is set to 1, the router with the greatest priority is chosen as the DR. When the priority is equal to zero, the correspondent is excluded from the selection process. This field is regarded as unimportant.</td></tr>
<tr><td colspan="3">**Router Dead Interval**
The timer indicates that the adjacent routers are inactive or dead. It is the time between Hello packets being received by the nearby router (by default 40 seconds)</td></tr>
<tr><td colspan="3">**Designated Router (DR)**
This router's identifier is linked to the DRs' RID.</td></tr>
<tr><td colspan="3">**Backup Designated Router (BDR)**
Following the selection of the DR, the RID of the BDR is added to this field.</td></tr>
<tr><td colspan="3">**List of Neighbor(s)**
The IDs of nearby routers from whom Hello packets were received during the previous dead interval.</td></tr>
</table>

b. When a pair is constructed, database description packets (OSPF packets of type 2) are sent, allowing the link state database to include typological information. Using a poll-response technique, the receiving router verifies the link state database collected from the master and slave routers.

c. Link State Seek Packets (OSPF Type 3 packets) are used to seek further typology database information after exchanging database description packets with adjacent routers. This is the last stage in establishing connectivity between routers.

d. List State Update Packets (OSPF packets of type four) are used for advertising. A single link state update contains that many link state changes.

e. List State Acknowledgement Packets (OSPF Type 5 packets) are sent and collected to transmit and receive many link state advertisements through dependable LSU packets.

Table 5 summarizing Link State advertising

Table 5. LSAs

Types of Link State Advertisement (LSA)	Description
1	*Router LSAs*
2	*Network LSAs*
3, 4	*Summary LSAs*
5	*Autonomous System External LSAs*

Designated Routers create Network LSAs (Type 2) that specify how all routers are linked to a specified network segment.

Area Border Routers (ABRs) create summary LSAs (Types 3 and 4) to advertise routers inside the area to other areas of the autonomous system. Type 3 communications (Summary Links) aggregate routers connecting distinct regions, while type 4 messages specify the routers that may reach the ASBR. Using this kind of message, all routers are notified of the routers transmitting messages outside the autonomous system.

External LSAs (Type 5) are created by ASBRs to notify all routers about routes that are not inside the autonomous system. In OSPF, these routes are redistributed and transmitted everywhere except the end areas.

Routing Metrics – Cost

The cost of the interface is used as a statistic by the OSPF protocol. This is inversely proportional to the interface's bandwidth. It is commonly known that the lower the cost, the greater the bandwidth of an interface, see equation (1).

$$cost = \frac{10^8}{bandwidth\ in\ bps} \tag{1}$$

A value of 10^8 equals 100,000,000 bps and the interface cost is determined based on bandwidth by default.

Algorithm and mode of Operation

OSPF is a Link State routing protocol that uses the shortest route 1st algorithm to identify the cheapest route to the destination. Dijkstra's method is used to determine this distance, which yields the best calculated decision. The following are the major algorithm processes:

- Each connection has a cost, and each router's goal is to have a full database of all the linkages in the network.
- The router generates a link-state advertising whenever there is a change in the nearby network or during startup.
- LSAs are shared between all routers during the 'flooding process.' Before distributing the received link-state update to other routers, each router stores it in its link-state database.
- When the link-state database in every router, where Dikjstra's algorithm is executing, is full, the shortest path tree is constructed for each of its endpoints.
- If anything changes in the network, such as link charges, this protocol notifies all routers, enabling them to be alerted at any time [21].

Each router generates its own routing tables using the neighbour router table, topology data, and the shortest-path algorithm. It takes itself as the starting point and uses the SPF algorithm to generate a 'loop-free' topology, analysing all of the information received in turn. The diagram below depicts the transformation of a physical type into a tree.

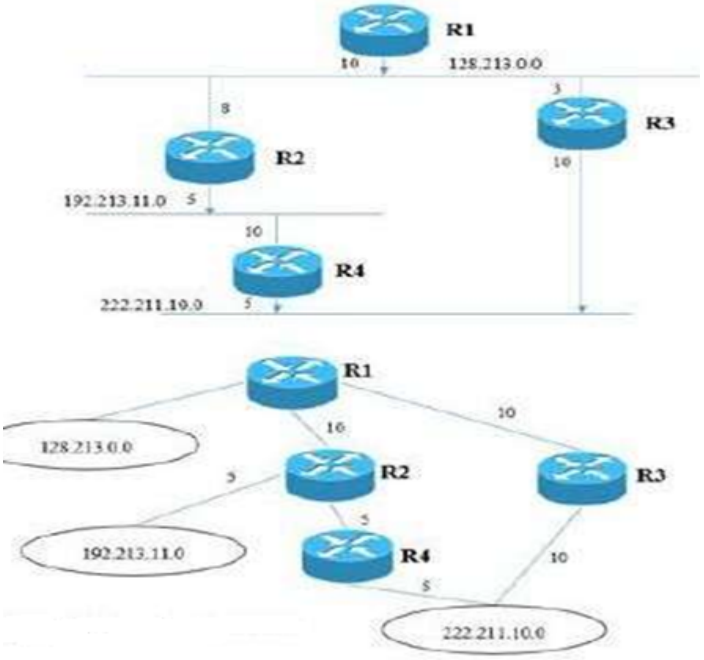


Figure 4. Algorithm and mode of operation

Convergence

The OSPF protocol's convergence time is exceptionally rapid when compared to other internal protocols. It consists of four factors that must be considered while constructing an OSPF network. These are:

- ➢ Type change detection - the time it takes OSPF to notice a change in interface, connection, or, in the worst-case scenario, failure.
- ➢ Stabilizing a new connection or cancelling a current one in reaction to a network change.
- ➢ Change propagation in the network entails the production of LSA messages as well as their transmission in a specific region or network.
- ➢ This is the time required for each router to conduct the SPF algorithm and produce a topology without loops.
- ➢ The time it takes for the router to generate a routing table is referred to as the forwarding table creation time.

As a result, the time it takes OSPF to converge is:

Convergence time = Propagation time + SPF execution time plus Time to create a routing table+ Time to discover a failure

In a common convergence environment, it takes less than one second for a router to broadcast Link State ads and execute the SPF algorithm. Meanwhile, the default time to re-execute (delay time) for the SPF algorithm is 5 seconds. This is the OSPF protocol's lowest limit of convergence under default parameters. Criteria such as network size, typology database size, and, of course, the kind of failure establish the upper limit. In the worst-case scenario, a connection breaks with no other routing path, necessitating a 40-second delay for the protocol (dead timer time).

DRs and BDRs

The OSPF procedure can lead to the designation of DR (designated router) and BDR (backup designated router) based on the network topology, particularly in multi-access networks. These duties act as the primary communication link between routers. Any A router that is not a DR or BDR only links to DR or BDR routers on a network segment and shares information exclusively with these two types of routers. As a result, the DR's objective is to disseminate updated information to all routers on the same network segment, leading to a significant reduction in routing traffic. Two multicast IP addresses are employed: All routers on a segment employ 224.0.0.6 to notify DR and BDR of any typology changes, but DR employs 224.0.05 to transmit Link State Update to all routers in the segment. The following criteria influence which router "wins" the DR/BDR selection process:

1. In a multi-access segment, the router with the greatest priority becomes the DR. By default, all routers have a priority of 1, and a router with a priority of 0 cannot participate in the selection process.

2. The router, whose ID is highest, is designated as the RD. It should be noted that the Router ID is calculated based on the relevance of the router:

- Commend router id, which changes Router ID to a given value.
- The largest IP address of the loopback interface of a router.
- The largest IP address of a router's active interface.

The router with the second highest priority is designated as the BDR. To ensure the consistency of the OSPF procedure:

- We have a new election method to pick a new BDR when a BDR becomes a DR.
- When choosing a new BDR, the variables outlined above are always taken into account.
- If a router is added to the network and has the highest priority after DR and BDR selection, it is not possible to be chosen unless one of the DR or BDR routers fails [22].

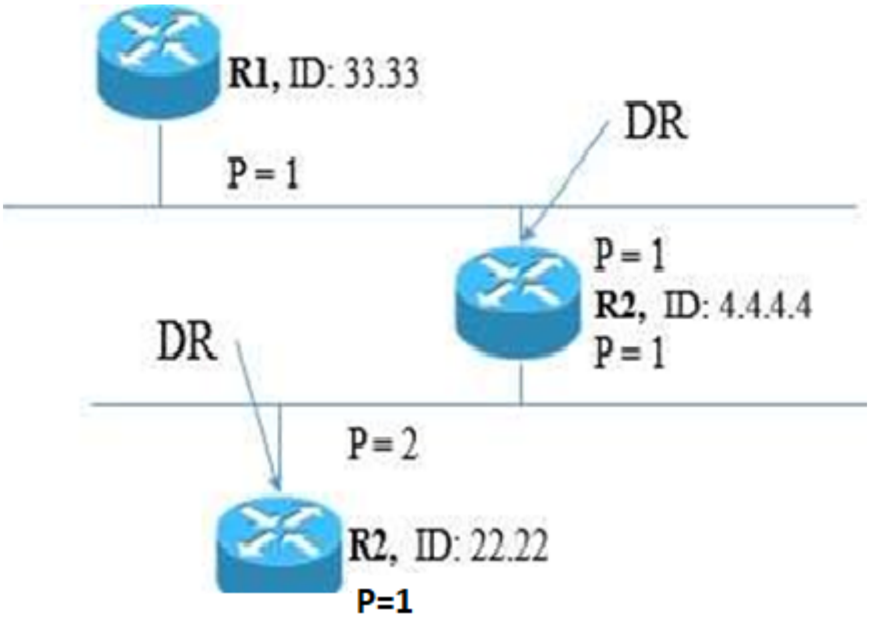


Figure 5. OSPF DR

Hierarchical Structure Operation

OSPF is a hierarchical routing system that divides the network into more manageable segments. These are logical groupings of routers that allow for less volatility, typology updates, and shorter routing tables. It should be noted that the OSPF protocol has several drawbacks when a network has more than one region. OSPF is made up of a "centrally controlled backbone network," also known as Area 0, that connects all lower areas in the hierarchy. To share routing information, all of these regions must be physically linked in this "backbone area." (Each region has its own link-state database.) This section transfers information to other areas, reducing traffic between various portions of the autonomous system. The IP address format (0.0.0.0) or the decimal format may be used to implement Area 0. A virtual connection must be set up if an area is not physically linked to Area 0.

Different sorts of zones are established in order to improve protocol configuration. These are the:

i. **Backbone Area**

Due to its location positioned in the center, the backbone region represents the fundamental physical and logical structure of a network and is always deemed acceptable and accessible for the dissemination of information in all areas. Because of the significance of this area, it must be robust and maintained throughout virtual link setup; each area must be directly linked to the Backbone area, either via virtual connections or through physical links.

ii. **Stub Area**

Because the stub region is only used to receive external routing advertising from the autonomous system (AS), the database size is significantly less. The stub area, on the other hand, obtains network information from other areas in the same OSPF domain. Some Stub Area characteristics are shown below:

- The stub area provides access in and out of the region.
- The stub region prevents external LSAs from arriving.
- Within the stub region, the default path is specified.
- OSPF routes must be setup as stub routes inside the stub area.

iii. **Not-So-Stubby Area (NSSA)**

A Not-So-Stubby, Expanded Stub Area is an extension of the Stub Area that allows the penetration of routes from autonomous system external sources into the stub area by forwarding them to other areas but does not receive external routes from other areas or import external addresses. Some important characteristics:

- The router at the autonomous system border injects type 7 external addresses (LSAs).
- In the NSSA, these LSAs are transformed to Type 6 LSAs, which are subsequently distributed to other regions.
- NSSA also permits summary LSAs.
- NSSA forbids external LSAs.

iv. **Totally Stubby Area**

It is a stub area since it is actually attached to the backbone area, which provides the default route. This region communicates with other networks through the default route, which is the only one where LSAs of type 3 are published.

Some crucial attributes:

- In a completely stubby region, Inter-area (IA) routes and other summary routes are not authorized.
- Intra-area routes are not permitted in the completely stubby region.
- Since the routing processor enables fewer routing choices, as a summary route, the default route is authorized, decreasing the utilization of system resources.

v. Totally (NSSA) Not-So-Stubby Area

It is a hybrid of TSA and NSSA in which just one default route from the backbone area (0.0.0.0) is permitted and external information is injected into the local area using ASBR and traversal. Main features;

- Totally NSSA does not cover summarized routes Type 3, 4, or 5 LSAs.
- Except for the default route as route summary, external routes are not permitted.
- Type 7 LSAs at the area border router are transformed to Type 5 LSAs in the NSSA before being routed to other areas [23].

vi. Transit area

A transit area is made up of two or more OSPF border routers that move network traffic from one region to the next.

A Table 6 summarizing OSPF areas and their constraints.

Table 6. OSPF areas

Areas	**Limited**
Normal	Doesn't have
Stubb	External Type 5 LSAs are not permitted.
NSSA	External Type 5 LSAs are forbidden. In NSSA, ABR type 7 LSAs that have been converted to type 5 LSAs are permitted.
Totally Stub	Except for the default summary route, LSAs of types 3, 4, and 5 aren't allowed.
NSSA Totally Stub	Except for the default summary route, LSAs of types 3, 4, and 5 are not permitted. In NSSA, ABR type 7 LSAs that have been converted to type 5 LSAs are permitted.

Advantages and Disadvantages

The Table 7 highlights the benefits and drawbacks of the OSPF protocol.

Table 7. Advantages and Disadvantages of OSPF

Advantages	**Disadvantages**
In comparison to other protocols such as EIGRP, the OSPF protocol is an open protocol.	OSPF configuration is difficult to accomplish.
OSPF always defines loop-free routes.	We have scalability challenges that are mostly caused by the influx of LSAs.
When changes occur in the network, they are immediately forwarded.	The SPF algorithm necessitates a high load and CPU use.
It uses multicasting 224.0.0.5 to transmit hello packets on a regular basis to test the functionality of the connection without transferring the whole routing table, hence conserving network capacity.	We have a greater use of memory as it is necessary to maintain the connection between routers, routing tables and typologies.
Through manual summary, Variable Length Subnet Masks (VLSM) and CIDR are supported.	It is not possible to sustain uneven load cost balancing.

OSPF is a hierarchical protocol with the highest point of the hierarchy being area 0 (Autonomous System).	
Cost can be used as a measure.	
It is better suited for major networks, i.e. those of a considerable scale.	
It has a limited bandwidth.	
There are several paths available.	
The area design reduces the number of route exchanges and the size of routing databases.	
OSPF has no hop count restrictions.	
IP header 89 denotes an OSPF packet..	
The Services field type determines how packets are routed.	

EIGRP protocol

EIGRP is a protocol developed by Cisco for dynamic routing in networks that use Internet Protocol (IP), IPX, and Appletalk. This protocol was created in 1992 at the University of California, Santa Cruz, and was originally proprietary. However, in 2013, CISCO made EIGRP an open standard. EIGRP is considered the most advanced distance-vector routing technology because it is highly scalable in medium- to large-scale network systems. Despite being a distance-vector protocol, EIGRP has some link-state protocol features, making it a hybrid protocol. It is primarily used to distribute information within an autonomous system, providing incremental updates and reducing the workload on each router as well as the amount of data transmitted. EIGRP's most notable feature is its use of equivalent load balancing (ECLB) and unequal cost load balancing (UCLB). ECLB distributes traffic logically and evenly across networks that have multiple paths to the same destination at the same cost. EIGRP is the only protocol that performs non-strict equal and unequal distributions, thanks to its use of the variance parameter. This protocol can also combine successful paths with viable successor routes (i.e., routes that appear in the topology table) to perform unequal-cost load balancing [26, 27].

EIGRP protocol Message Encapsulation

The encapsulation of an EIGRP packet in a Data link frame is shown in the Table 8.

Table 8 Message encapsulation in EIGRP

Data Link Frame Header	***Header***	**EIGRP Packet Header**	***TLV***
1.Mac Address of Origin (Sending Interface Address). 2. Mac address of destination (Multicast address: 01-00-5E-00-00-0A)	1.Source IPv4 Address (Sending Interface Address). 2. IPv4 address of destination (Multicast address 224.0.0.10 and protocol field 88)	Autonomous System EIGRP packet type number Opcode	TVL Types in General IP Specific TLV Types 0x0001=EIGRP Parameters 0x0003=Sequence 0x0004=Software Version 0x0005=Next Multicast Sequence 0x0102=Route internal 0x0103=IP External route.

In particular, the EIGRP packet header is encased in an IP packet with the protocol field 88 and the destination address 224.0.0.10. The below Table 9 explains the EIGRP packet header [28].

Table 9. EIGRP Packet Headers

<table>
<tr><th>The version number</th><th><i>Opcode (Operation Code)</i></th><th><i>Checksum</i></th></tr>
<tr><td>Version 1 for IPv4 &amp; IPv6</td><td>Indicates the protocol packet type, where 1 means update, 2 means reserved, 3 means query, and 4 means reply.
5=Hello,6=IPX-SAP, 10=SIA Query, and 11=Reply Query.</td><td>Estimated for the entire EIGRP packet except the IP header.</td></tr>
<tr><td colspan="3"><b>Flags</b>
Two flags are stored in a 32-bit field:
The 1st bit (0x00000001), known as the initialization bit (init), indicates that a new connection with the neighbor has been established.
In the patented reliable multicasting technique, the second bit (0x00000002) is known as the 'conditional receiver bit.</td></tr>
<tr><td colspan="3"><b>Sequences</b>
The Realizable Transport Protocol employs a 32-bit field (RTP).</td></tr>
<tr><td colspan="3"><b>Recognition (acceptance)</b>
It ensures the dependability and security of message delivery.</td></tr>
<tr><td colspan="3"><b>AS number</b>
The EIGRP domain has been determined. Because a gateway might be used in more than one AS, routing tables are linked with each one, no matter how clearly described.</td></tr>
<tr><td colspan="3"><b>Type/Value/Length</b>
This field contains type information (binary alphanumeric code) and specifies that a variable field is specified by the value type as well as the frame length.</td></tr>
</table>

Furthermore, EIGRP has six distinct packet types, each serving a distinct function, see Table 10. This is mentioned at [24, 25].

Table 10. Packet types in EIGRP

Hello	**Multicast message sent to detect neighbors (unreliable)**
Acknowledgment	Unicast message sent to confirm the safe delivery of EIGRP packets (unreliable)
Updates	They are transmitted using RTP&Unicast to communicate the arrival of the destination (reliable).
Queries	They are transmitted over Multicast&RTP, seeking routing information, as well as the state of the route for quick (reliable) convergence.
Replies	In response to query packets, RTP and unicast packets are sent (reliable)
Requests	They are broadcast through multicast or unicast to collect unique and distinct details about neighbours (unreliable).

Routing metric-Composite metric

EIGRP offers six distinct vector metrics, although only four of them are used to construct the composite metric.

Table 11 depict EIGRP metrics

Table 11 EIGRP metrics

Bandwidth	The route's minimum bandwidth from the router to the endpoint
Loads	A number between 1 and 255
Total delay	The total path delay between the router and the destination.
Reliability	A number between 1 and 255
MTU	The maximum transmission unit is never utilized in metric calculations.
Hop count	The number of network pathways that a packet traverse. Metric calculations do not make use of this term.

To choose the best route, EIGRP produces routing metrics based on the lowest bandwidth on the way to the endpoint as well as the overall latency. Other vector measures, such as load and dependability, are also used. The parameters defined in router interfaces on the destination path are used to calculate the minimum bandwidth and total latency, see equation (2).

$$metric = \left[\left(K1 * \frac{10^7}{bandwidth_{min}} + \frac{K2 * bandwidth_{min}}{256 - load} + K3 * \sum delays\right) * \frac{K5}{K4 + reliability}\right] * 256 \tag{2}$$

K1=1, K2=0, K3=1, K4=0, K5=0 are the default values for each of the K weights.

Given that the weights of K2, K4, and K5 are all 0 by default, the EIGRP formula assumes the following form.

(bandwidth+delay)*256

Where bandwidth and latency are included into the calculations:

Interface command value Bandwidth=10^7/Bandwidth (creates the connection using the least amount of bandwidth).

Delay= The delay interface command value (measured in milliseconds and increasing when a route travel through a large number of routers).

Algorithm and Operation

EIGRP supports IPv4 classless addressing and generates the routing table using the DUAL algorithm. The approach and data structure (adjacency table and typology table) will be discussed in further detail below:

Adjacency table

EIGRP routers receive information about the status and IP addresses of their neighboring routers. Whenever a new neighbor router is discovered, its IP address and interface details are collected and saved in the neighbour database. The neighbor sends out Hello packets with Dwell Time to check if the neighbouring router is reachable and operational. It is essential to note that the ASN (Autonomous System Number), subnet number, and K values must match to establish a neighbour connection. Hello packets are sent to the multicast address every 5 seconds on the LAN interface and every 60 seconds on the WAN interface to confirm the connection's functionality. If the hold time period (default 15 seconds) lapses due to the absence of a hello packet, the DUAL algorithm is activated to respond to topology changes. Additionally, the neighbour table provides information needed by the RTP (Reliable Transport Protocol) mechanism to match acknowledgments with the appropriate data packets. Trip counts are recorded in the neighbor tables to estimate the optimal retransmission interval.

Diffusion Update Algorithm (DUAL)

i. **EIGRP** uses DUAL (Diffusing Update Algorithm) or DUAL FSM (finish-state machine) to guarantee that each route is computed loop-free, hence avoiding routing loops. This algorithm reacts swiftly to changes in routing patterns and dynamically updates the routing tables. The following elements influence the 'free loop routing' mechanism:

ii. The best EIGRP metric or the lowest cost of a route to the target network that incorporates the routing metric supplied by a neighbour in the routing table is called **the Feasible Distance (FD).**

iii. The entire cost of routing disclosed by the neighbour and required on the route to the destination network **(Reported Distance (RD)/Advertised Distance (AD))**

iv. **Successor,** often known as the present Successor (or the primary route), is the lowest feasible distance route that provides a loop-free path to the target. In order to forward packages, successor routes are used to create the routing table.

v. **The Feasible Successor (FS)** is the backup route that is said to be lower in distance than the feasible route. The FS's FD is more than the Successor's FD, but the advertised distance (AD) must be less than the Successor's. When the Successor route fails, these routes are preserved in the typology tables and promoted.

vi. **The Feasibility Condition (FC)** enables the achievement of loop-free methods towards the goal via Successor and Feasible Successor routes. As per this condition, a route can be considered feasible only if the reported distance is lower than the likely distance [RD FD].

Typology Table

The EIGRP topology database includes all routes to the destination disclosed by adjacent routers. Paths and their metrics, successors and probable successors, and locally connected subnets are all kept in the topology database. It should be noted that the pathways in the typology table may be used by the router only if they are active in the routing tables or have a higher AD than the comparable route. For each available network, the typology table includes the overall latency, dependability, and load of the route, the lowest bandwidth (the weakest link), the reported distance and the feasible distance, and finally the source of the route [29].

Convergence

Convergence starts when two routers become neighbours. During the exchange of greeting packets, dynamic learning occurs (the default hello timing on high-bandwidth connections is 5 seconds and 60 seconds on slower networks). As a consequence of this neighbour discovery, neighbour tables containing all of the attributes learned in earlier sections are created. At this phase, nearby routers exchange data and construct their associated typology tables. The DUAL method is then used to determine the reported and probable distances, as well as the successor and prospective successor routes. If the possibility requirement is fulfilled, these routes may exist, allowing alternatives that are loop-free for the successor route.

The availability of potential successor routes is crucial for EIGRP convergence. When a successor (i.e., the principal route) fails, the EIGRP mechanism is triggered:

- If a likely successor is discovered, it is promoted to a successor and added to the routing table.
- In the event that a reliable replacement is not present, the EIGRP algorithm designates the unsuccessful route as active in its topographical database and begins transmitting inquiry packets to all adjacent routers in an effort to locate an alternative route for the failed network. Since these adjacent routers do not possess any other routes, they

classify this route as active in their topology tables and forward inquiry packets to their own neighbouring routers, and so on. If a router is cognizant of an alternate route, it answers inquiry packets, and all routers converge in a recursive manner. If no routers respond, this router keeps this route active until the corresponding EIGRP timer "expires," after which they all become stuck-inactive (SIA).

The previously described convergence mechanism provides a danger when growing the EIGRP network arbitrarily. When there are hundreds of routers in an EIGRP network, being stuck in an active state may be devastating. A tighter design should be established in this scenario, both in the organizational and routing structure. To recap all of the above factors, a network designer needs the following in order to speed convergence:

- Shorter timers should be used. Routers can create connections quicker and identify neighbours more efficiently this way.
- Summary routing across the hierarchical network structure is enabled. When a query reaches to an EIGRP router with a summary route, it immediately replicates the query, thereby ending the stuck-in-active status.
- Configure route filtering such that when an EIGRP query is received, the router instantly replies with an inaccessible response message, completing SIA again and assisting in the removal of non-existent routes from all routing tables.
- Configure trunk routes at distant sites so that central routes do not send requests to them.

Advantages and Disadvantages

The Table 12 illustrates the advantages and disadvantages of the EIGRP protocol

Table 12. Advantages and disadvantages of EIGRP

Advantages	Disadvantages
It employs multicasting 224.0.0.10 to deliver hello packets that check the link's functionality without transferring the whole routing database, hence lowering network traffic.	By default, EIGRP automatically summarizes routes at class borders. This functionality may be recreated without the use of the automated summary command.
Because of the possibility condition, there is a loop-free route.	As of 2013, just a portion of the Cisco protocol is open source.
Support for Variable Length Subnet Masks (VLSM) and CIDR enables the network to automatically summarize routes.	Managing huge hierarchical networks is difficult.
Simple to set up.	Due to the fact that routers from other organizations cannot use EIGRP, protocol redistribution must be configured inside the autonomous system.
Rapid Convergence Because of the Dual Algorithm. To swiftly adapt to alternative routes, the EIGRP router keeps all neighbor tables.	When the network increases greatly in size due to an arbitrary design, stuck-in-active situations might cause sluggish convergence.
EIGRP relies on the Reliable Transport Protocol (RTP) to ensure that EIGRP packets are delivered correctly to nearby routers.	Triggers should be saved using summation.
The IP 88 header identifies EIGRP packets.	
It constantly backs up prospective Successor routes (FS).	

When changes occur in the network, trigger updates inform you.	
It provides summarization on each interface, which reduces the routing table size.	
Efficient traffic use using equal cost multipath (ECMP) and unequal cost load balancing.	
Many networks layer 3 protocols, including IP, IPX, and AppleTalk, are supported by EIGRP.	
Scaling is superior for big dynamic multipoint (DM) distributions.	

A summary of the comparative study based on the criteria

Some fundamental traits are shared by the dynamic routing protocols EIGRP and OSPF. Both of these protocols have Variable Length Subnet Mask (VLSM) and Classless Inter-Domain Routing (CIDR). They are also designed to achieve quick convergence and backup routing paths in case one fails. In addition, OSPF and EIGRP are capable of managing their own routing tables and transmitting partial updates when changes occur to save network traffic.

Given the fact that these protocols give these possibilities, a comparative evaluation will, at the very least, show the advantages and disadvantages of each methodology.

Routing metrics

EIGRP uses several metrics to calculate the routing estimate. Unlike OSPF, which decides the path to the destination network based on expense, EIGRP relies heavily on bandwidth and latency, with load, dependability, and MTU as additional factors. This indicates that EIGRP has a competitive advantage over OSPF in managing network traffic.

Convergence to typology changes

In case of alterations in the network topology, every protocol needs to re-evaluate the path leading to the destination for achieving faster convergence. According to simulations, EIGRP outperforms OSPF by taking about six seconds less time to converge. Nevertheless, OSPF appears to be more effective in terms of the administrator interface time values.

Exit

It is clear which protocol produces the most throughput on the network. It is well known that EIGRP, being a hybrid protocol, may act as both a distance vector and a link state based on the network type and the DUAL algorithm. In [30] claims that EIGRP utilizes several times more CPU and has greater control based on the protocol's features. In a related study, experts stated and affirmed that OSP has superior network performance than EIGRP following simulation experiments. Because the network architecture in each test differs, it is difficult to conclude which protocol is superior in this regard.

Scaling on large networks

Due to the fact that each node must carry the routing table, the EIGRP routing protocol is designed to perform better in networks with flat topologies, while the hierarchical OSPF protocol increases CPU memory use in these networks. OSPF, on the other hand, is regarded as a more resilient protocol that, with proper design, may lower the size of the routing table and react with continuity in the event of a scalable network architecture. What is presented theoretically is intended to be shown by tests and simulations.

DESIGNING THE SIMULATIONS

Simulation tool

Cisco Systems' Packet Tracer is a cross-platform visual simulation application that enables users to develop network topologies and emulate current computer networks. Using a simulated command line interface, users may replicate the setup of Cisco routers and switches. Packet Tracer is a drag-and-drop user interface that allows users to add and delete virtual network devices as needed. The program is primarily aimed at Cisco Networking Academy students as an instructional tool to assist them in learning key CCNA principles. Students enrolled in a CCNA Academy program could previously freely download and utilize the tool for instructional purposes.

Key Features

Workspaces in Cisco Packet Tracer: There are two workspaces in Cisco Packet Tracer: logical and physical. Users may create logical network topologies by inserting, connecting, and clustering virtual network devices in the logical workspace. The physical workspace represents the logical network's graphical physical dimension, providing a sense of size and positioning in how network components like as routers, switches, and hosts would appear in a real-world context. The physical view also includes geographic representations of networks, such as cities, buildings, and wire closets.

Packet Tracer Modes: Cisco Packet Tracer has two operating modes for visualizing network behaviour: real-time mode and simulation mode. The network functions like a genuine device in real-time mode, with instantaneous real-time reaction to all network activity. The real-time mode provides students with a suitable alternative to real-world equipment and enables them to practice setup before working with real-world equipment.

The user may examine and manage time intervals, the inner workings of data transmission, and data propagation over a network in simulation mode. This assists students in grasping the core ideas behind network operations. A thorough knowledge of network principles may aid in the speed with which you learn about related ideas.

Cisco Packet Tracer is a network-capable program featuring a multiuser peer-to-peer mode that enables collaborative building of virtual networks over a real network. The multiuser function allows for interesting collaborative and competitive interactions, as well as the ability to advance from individual to social learning. It also includes options for collaboration, competitiveness, remote instructor student interactions, social networking, and gaming.

The Activity Wizard enables users to create their own learning activities by configuring scenarios with instructive text, as well as building starting and end network topologies and preconfigured packets. Grading and comments are also available via the Activity Wizard.

Design and analysis in Cisco Packet tracer

It is critical to carefully follow all of the procedures of running the Cisco Packet Tracer tool in order to obtain the required comparison between the two protocols.

The following is the order of these phases:

- We define the network model we wish to create.

- We create the situations and choose the traffic variations.
- We carry out the simulation procedure.
- We examine the outcomes.

Designing typologies of networks

For performance evaluation, two network typologies and 4 scenarios have been implemented. The first typology is a basic (simple) typology composed of 4 routers, while the scaled one is composed of 7 routers, see Figures 6 and 7.

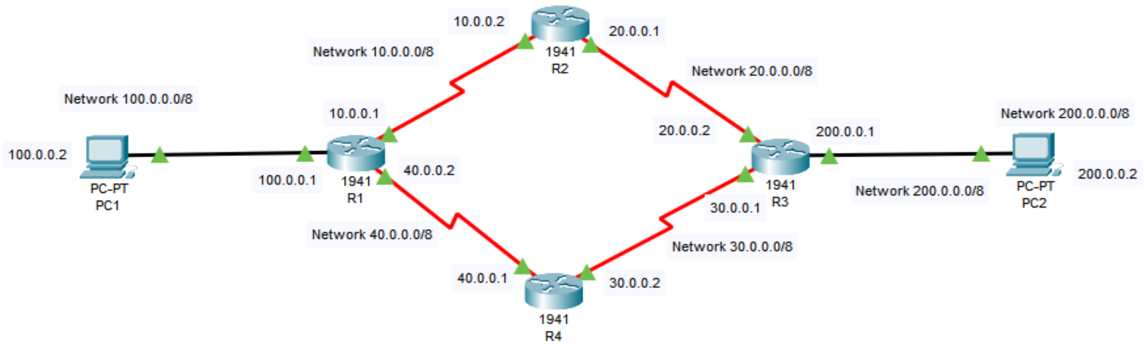


Figure 6. Basic typology

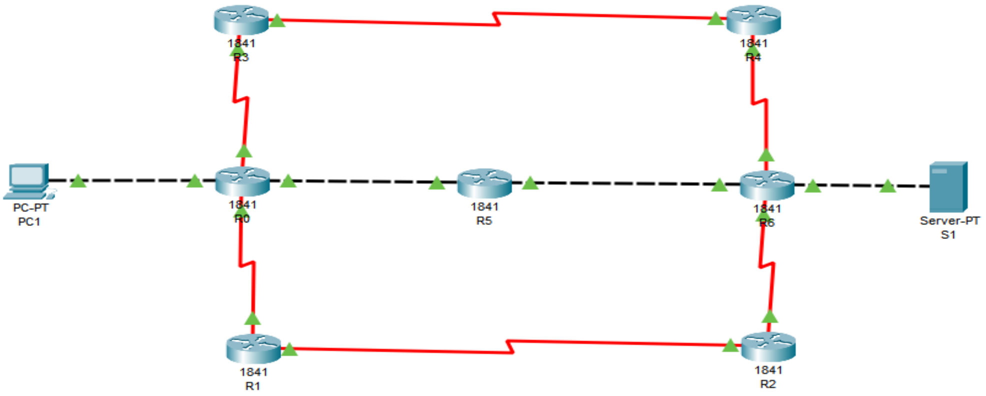


Figure 7. Scaled typology

IMPLEMENTATION OF SIMULATIONS AND RESULTING OUTCOMES

For performance evaluation, two network typologies were built. The same typologies were built for both cases.

The first typology

It is a basic (simple) typology composed of 4 routers, built in a Logical layout with multiuser clients on both sides. The duration of the simulation is set to 6 minutes. The simulation tool used is Cisco Packet Tracer.

The topology has 4 routers connected to each other through the Serial DCE cable. First, I set up the routers and PCs. Then we configured one OSPF and the other EIGRP. The plot is the same. Specific metrics are selected to measure performance as well as provide an assessment of the protocol's behaviour in each scenario as can be seen in Figure 8.

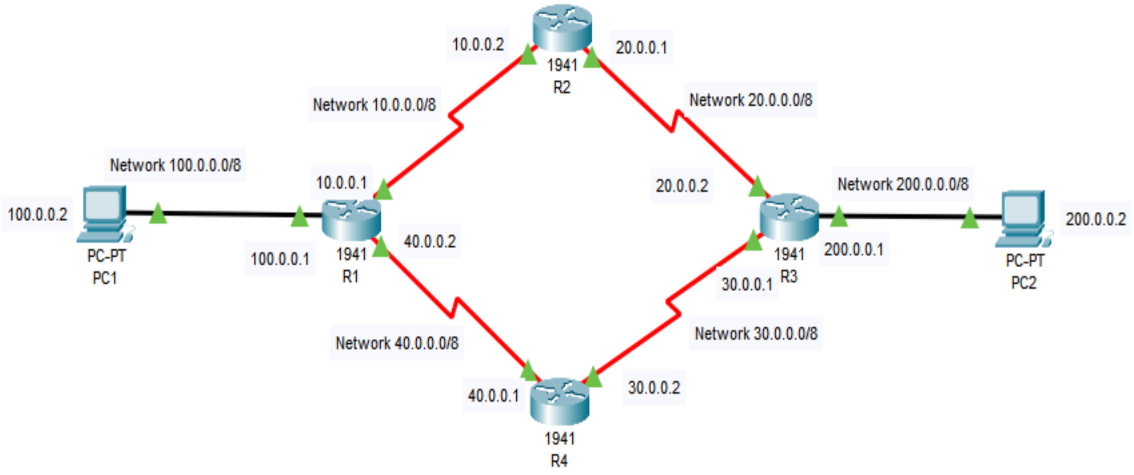


Figure 8. Basic typology

The second typology

It is a scaled typology based on the basic typology composed of 7 routers, in such a way that they create a slightly more complex structure, see Figure 9.

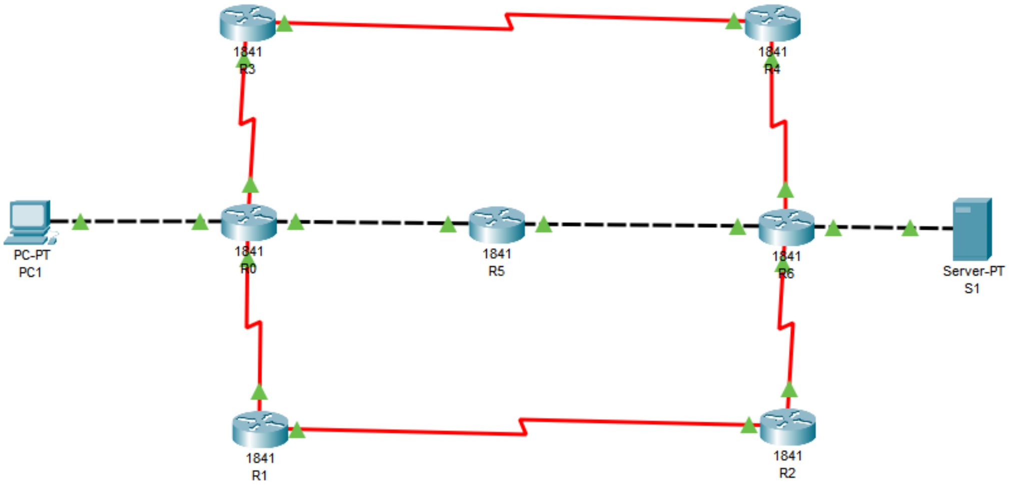
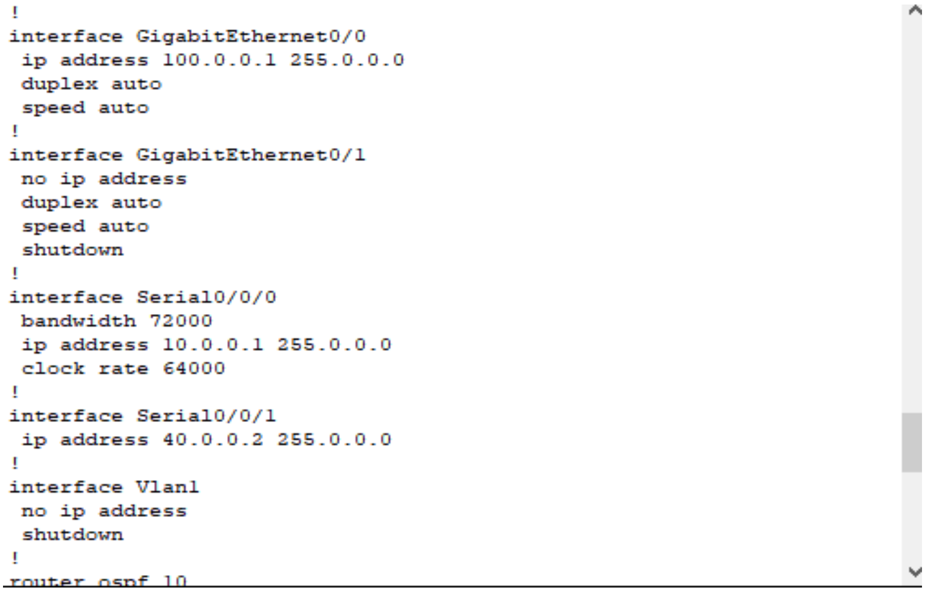


Figure 9. Scaled typology

Basic typology

OSPF.

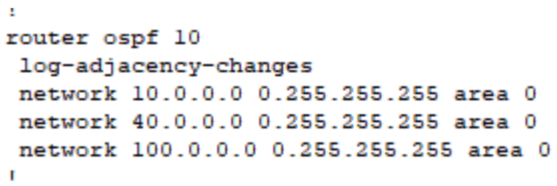
Firstly, the routers and the end devices were configured and were interconnected. In the Figures 10 until 28 are shown all the configurations of our simulations results.



```
!
interface GigabitEthernet0/0
 ip address 100.0.0.1 255.0.0.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 bandwidth 72000
 ip address 10.0.0.1 255.0.0.0
 clock rate 64000
!
interface Serial0/0/1
 ip address 40.0.0.2 255.0.0.0
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 10
```

Figure 10. Router confirmed in R1

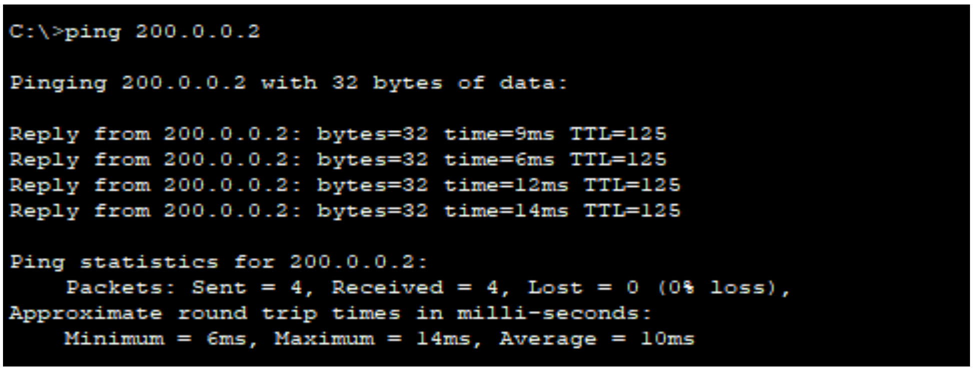
Here is the OSPS configuration for the first router:



```
!
router ospf 10
 log-adjacency-changes
 network 10.0.0.0 0.255.255.255 area 0
 network 40.0.0.0 0.255.255.255 area 0
 network 100.0.0.0 0.255.255.255 area 0
!
```

Figure 11. OSPF configuration in R1

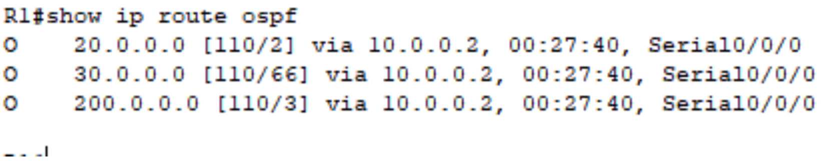
This shows that the end devices are connected and can communicate with each other:



```
C:\>ping 200.0.0.2

Pinging 200.0.0.2 with 32 bytes of data:

Reply from 200.0.0.2: bytes=32 time=9ms TTL=125
Reply from 200.0.0.2: bytes=32 time=6ms TTL=125
Reply from 200.0.0.2: bytes=32 time=12ms TTL=125
Reply from 200.0.0.2: bytes=32 time=14ms TTL=125

Ping statistics for 200.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 14ms, Average = 10ms
```

Figure 12. End devices communication, see communications timing

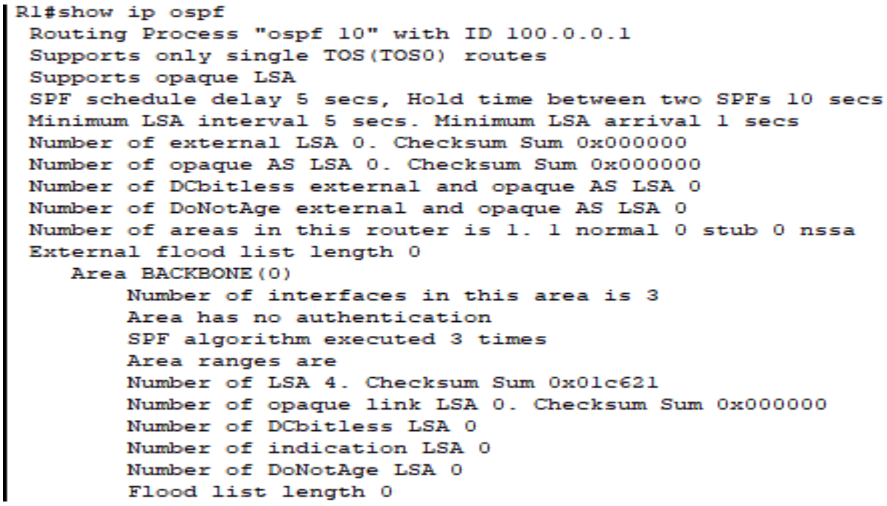
Here is shown the route OSFP follows for this topology:



```
R1#show ip route ospf
O    20.0.0.0 [110/2] via 10.0.0.2, 00:27:40, Serial0/0/0
O    30.0.0.0 [110/66] via 10.0.0.2, 00:27:40, Serial0/0/0
O    200.0.0.0 [110/3] via 10.0.0.2, 00:27:40, Serial0/0/0
```

Figure 13. Route the OSPF follows

Here is the relevant information regarding OSPF simulation regarding the aforementioned basic topology. Note the times needed in running the algorithm:

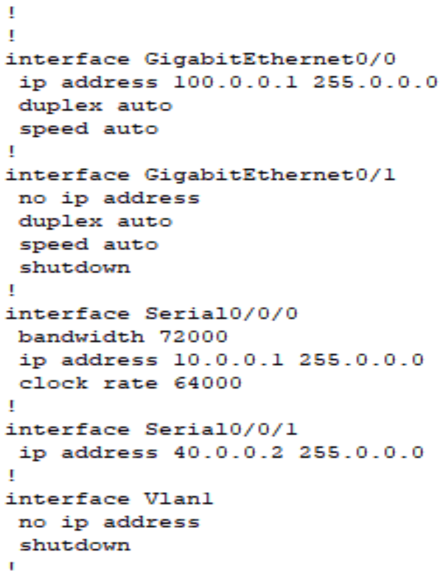


```
R1#show ip ospf
 Routing Process "ospf 10" with ID 100.0.0.1
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 External flood list length 0
    Area BACKBONE(0)
        Number of interfaces in this area is 3
        Area has no authentication
        SPF algorithm executed 3 times
        Area ranges are
        Number of LSA 4. Checksum Sum 0x01c621
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

Figure 14. OSPF information for the basic topology

EIGRP

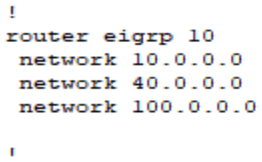
Firstly, we confirmed all the routers and end devices, then connected them together:



```
!
!
interface GigabitEthernet0/0
 ip address 100.0.0.1 255.0.0.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 bandwidth 72000
 ip address 10.0.0.1 255.0.0.0
 clock rate 64000
!
interface Serial0/0/1
 ip address 40.0.0.2 255.0.0.0
!
interface Vlan1
 no ip address
 shutdown
!
```

Figure 15. Router confirmed in R1

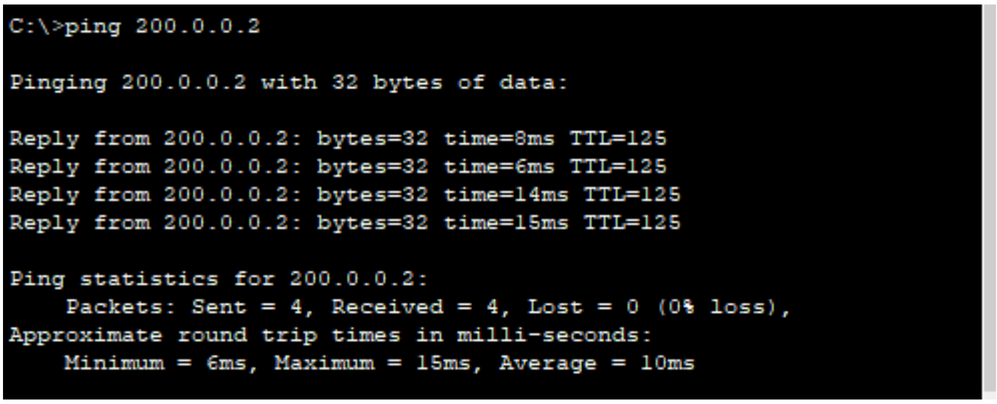
Here is the EIGRP configuration in the first topology:



```
!
router eigrp 10
 network 10.0.0.0
 network 40.0.0.0
 network 100.0.0.0

!
```

Figure 16. EIGRP configuration in R1

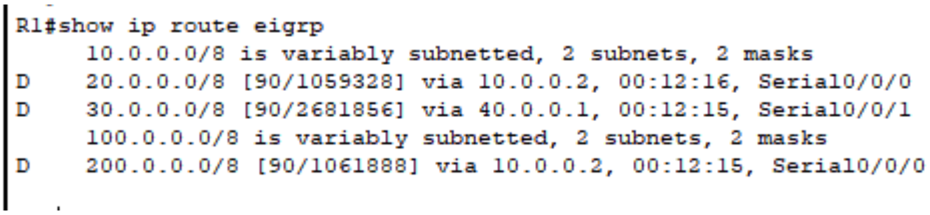
End devices are connected with each other and can communicate:



```
C:\>ping 200.0.0.2

Pinging 200.0.0.2 with 32 bytes of data:

Reply from 200.0.0.2: bytes=32 time=8ms TTL=125
Reply from 200.0.0.2: bytes=32 time=6ms TTL=125
Reply from 200.0.0.2: bytes=32 time=14ms TTL=125
Reply from 200.0.0.2: bytes=32 time=15ms TTL=125

Ping statistics for 200.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 15ms, Average = 10ms
```

Figure 17. End devices communication, see communications timing

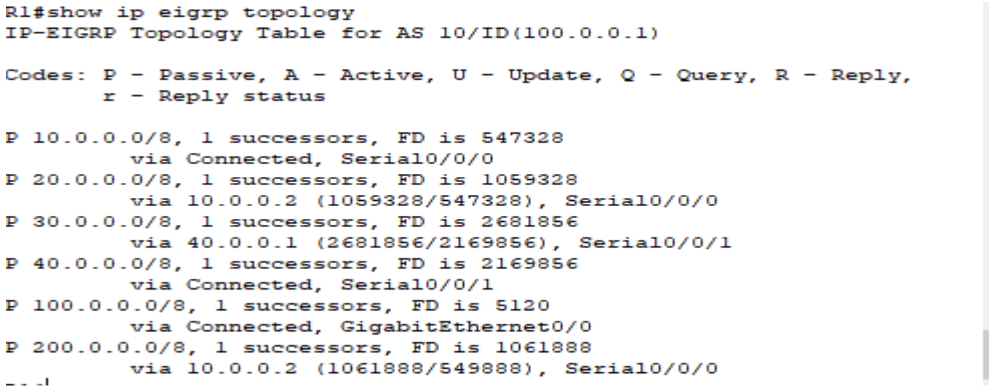
These are the best possible routes EIGRP follows in this protocol:



```
R1#show ip route eigrp
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D    20.0.0.0/8 [90/1059328] via 10.0.0.2, 00:12:16, Serial0/0/0
D    30.0.0.0/8 [90/2681856] via 40.0.0.1, 00:12:15, Serial0/0/1
     100.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D    200.0.0.0/8 [90/1061888] via 10.0.0.2, 00:12:15, Serial0/0/0
```

Figure 18. Route the EIGRP follows

Here shows how many devices are succesfully connected with EIGRP:



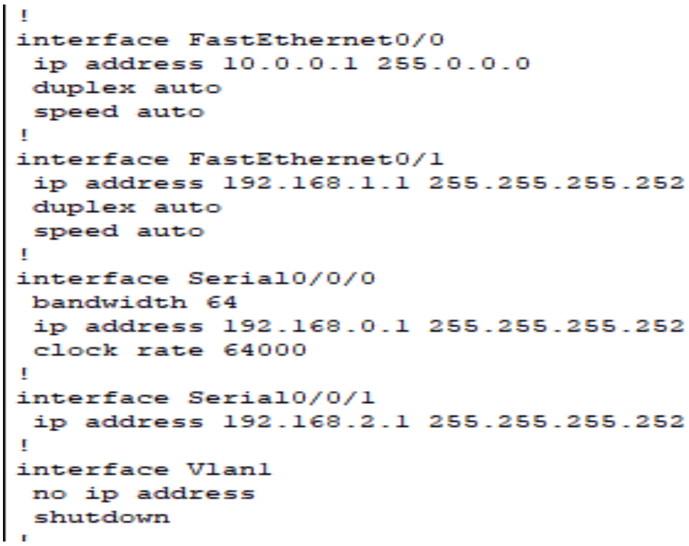
```
R1#show ip eigrp topology
IP-EIGRP Topology Table for AS 10/ID(100.0.0.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 10.0.0.0/8, 1 successors, FD is 547328
         via Connected, Serial0/0/0
P 20.0.0.0/8, 1 successors, FD is 1059328
         via 10.0.0.2 (1059328/547328), Serial0/0/0
P 30.0.0.0/8, 1 successors, FD is 2681856
         via 40.0.0.1 (2681856/2169856), Serial0/0/1
P 40.0.0.0/8, 1 successors, FD is 2169856
         via Connected, Serial0/0/1
P 100.0.0.0/8, 1 successors, FD is 5120
         via Connected, GigabitEthernet0/0
P 200.0.0.0/8, 1 successors, FD is 1061888
         via 10.0.0.2 (1061888/549888), Serial0/0/0
```

Figure 19. Devices connected with EIGRP

Scaled typology

OSFP.

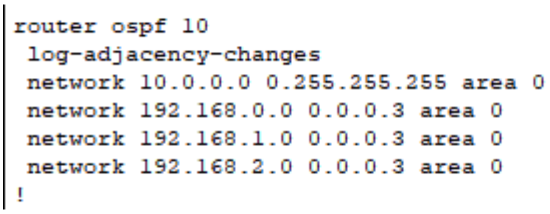
Of course, firstly all the routers and end devices were configured and connected:



```
!
interface FastEthernet0/0
 ip address 10.0.0.1 255.0.0.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.1.1 255.255.255.252
 duplex auto
 speed auto
!
interface Serial0/0/0
 bandwidth 64
 ip address 192.168.0.1 255.255.255.252
 clock rate 64000
!
interface Serial0/0/1
 ip address 192.168.2.1 255.255.255.252
!
interface Vlan1
 no ip address
 shutdown
!
```

Figure 20. Router confirmed in R0

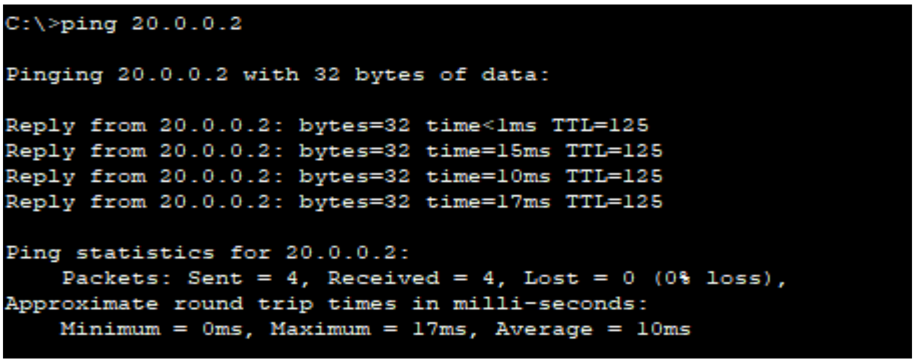
Here are shown the OSPF configuration in R0:



```
router ospf 10
 log-adjacency-changes
 network 10.0.0.0 0.255.255.255 area 0
 network 192.168.0.0 0.0.0.3 area 0
 network 192.168.1.0 0.0.0.3 area 0
 network 192.168.2.0 0.0.0.3 area 0
!
```

Figure 21. OSPF configuration in R0

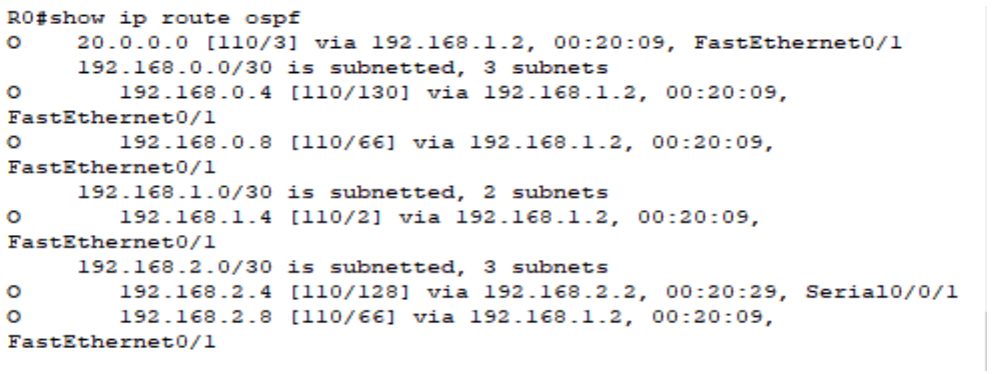
The end devices can communicate with each other through OSPF:



```
C:\>ping 20.0.0.2

Pinging 20.0.0.2 with 32 bytes of data:

Reply from 20.0.0.2: bytes=32 time<1ms TTL=125
Reply from 20.0.0.2: bytes=32 time=15ms TTL=125
Reply from 20.0.0.2: bytes=32 time=10ms TTL=125
Reply from 20.0.0.2: bytes=32 time=17ms TTL=125

Ping statistics for 20.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 17ms, Average = 10ms
```

Figure 22. End devices communication, see communications timing

Here are all the routes OSPF follows:

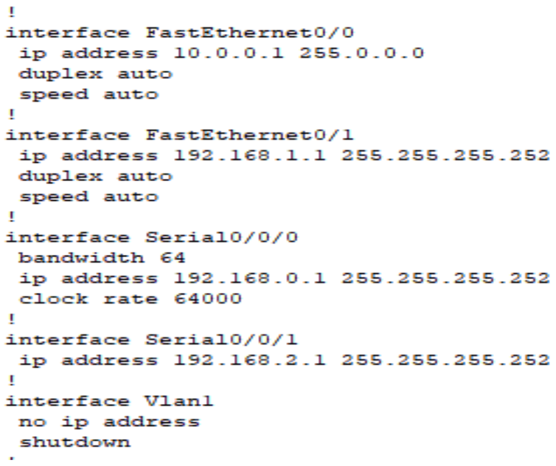


```
R0#show ip route ospf
O    20.0.0.0 [110/3] via 192.168.1.2, 00:20:09, FastEthernet0/1
     192.168.0.0/30 is subnetted, 3 subnets
O       192.168.0.4 [110/130] via 192.168.1.2, 00:20:09,
FastEthernet0/1
O       192.168.0.8 [110/66] via 192.168.1.2, 00:20:09,
FastEthernet0/1
     192.168.1.0/30 is subnetted, 2 subnets
O       192.168.1.4 [110/2] via 192.168.1.2, 00:20:09,
FastEthernet0/1
     192.168.2.0/30 is subnetted, 3 subnets
O       192.168.2.4 [110/128] via 192.168.2.2, 00:20:29, Serial0/0/1
O       192.168.2.8 [110/66] via 192.168.1.2, 00:20:09,
FastEthernet0/1
```

Figure 2.3 OSPF routes

EIGRP.

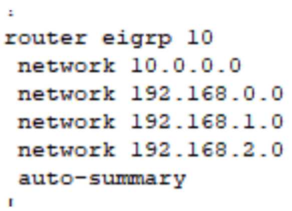
Firstly, the routers and end devices were confirmed.



```
!
interface FastEthernet0/0
 ip address 10.0.0.1 255.0.0.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.1.1 255.255.255.252
 duplex auto
 speed auto
!
interface Serial0/0/0
 bandwidth 64
 ip address 192.168.0.1 255.255.255.252
 clock rate 64000
!
interface Serial0/0/1
 ip address 192.168.2.1 255.255.255.252
!
interface Vlan1
 no ip address
 shutdown
.
```

Figure 24. Router confirmed in R0

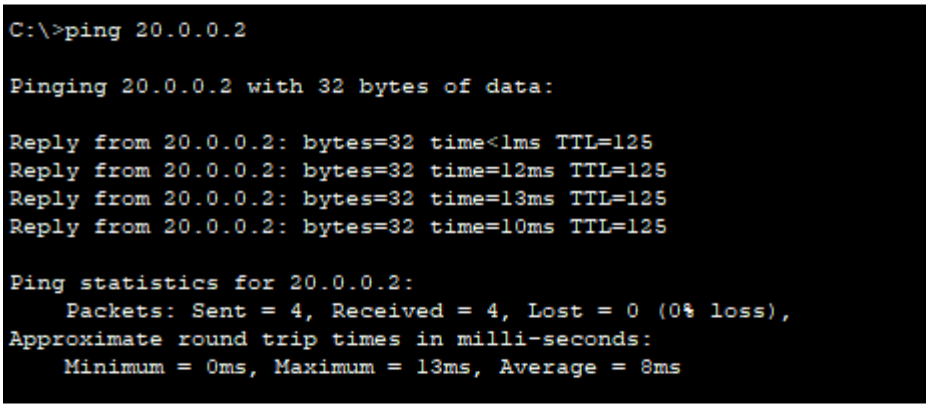
Furthermore, the configuration with EIGRP was made:



```
:
router eigrp 10
 network 10.0.0.0
 network 192.168.0.0
 network 192.168.1.0
 network 192.168.2.0
 auto-summary
'
```

Figure 25. EIGRP configuration in R0

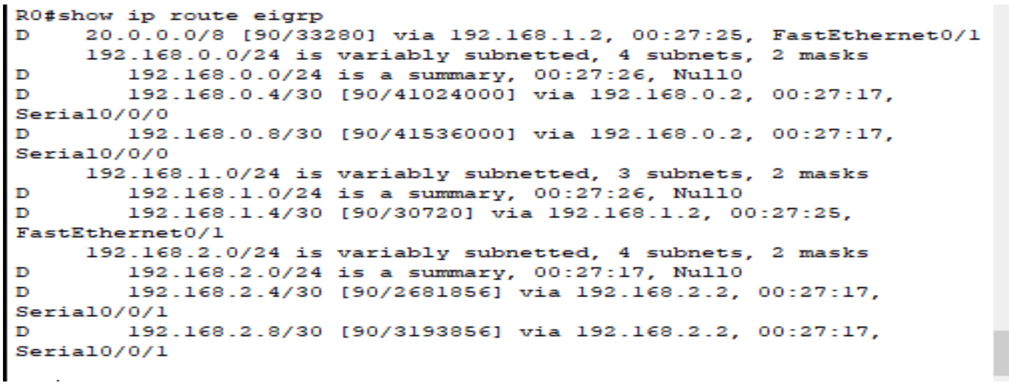
End devices can communicate with each other:



```
C:\>ping 20.0.0.2

Pinging 20.0.0.2 with 32 bytes of data:

Reply from 20.0.0.2: bytes=32 time<1ms TTL=125
Reply from 20.0.0.2: bytes=32 time=12ms TTL=125
Reply from 20.0.0.2: bytes=32 time=13ms TTL=125
Reply from 20.0.0.2: bytes=32 time=10ms TTL=125

Ping statistics for 20.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 13ms, Average = 8ms
```

Figure 26. End devices communication, see communications timing

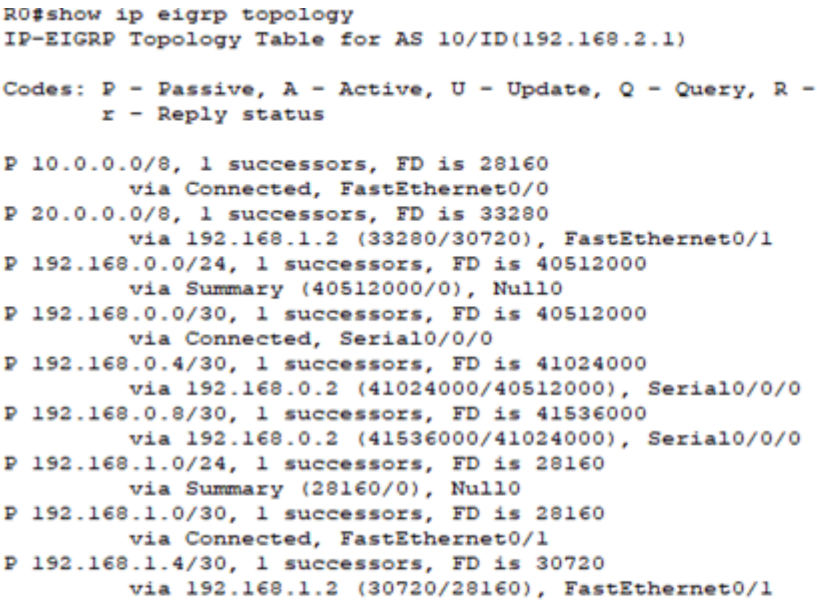
These are all the routes EIGRP uses to reach to the destination:



```
R0#show ip route eigrp
D    20.0.0.0/8 [90/33280] via 192.168.1.2, 00:27:25, FastEthernet0/1
     192.168.0.0/24 is variably subnetted, 4 subnets, 2 masks
D       192.168.0.0/24 is a summary, 00:27:26, Null0
D       192.168.0.4/30 [90/41024000] via 192.168.0.2, 00:27:17,
Serial0/0/0
D       192.168.0.8/30 [90/41536000] via 192.168.0.2, 00:27:17,
Serial0/0/0
     192.168.1.0/24 is variably subnetted, 3 subnets, 2 masks
D       192.168.1.0/24 is a summary, 00:27:26, Null0
D       192.168.1.4/30 [90/30720] via 192.168.1.2, 00:27:25,
FastEthernet0/1
     192.168.2.0/24 is variably subnetted, 4 subnets, 2 masks
D       192.168.2.0/24 is a summary, 00:27:17, Null0
D       192.168.2.4/30 [90/2681856] via 192.168.2.2, 00:27:17,
Serial0/0/1
D       192.168.2.8/30 [90/3193856] via 192.168.2.2, 00:27:17,
Serial0/0/1
```

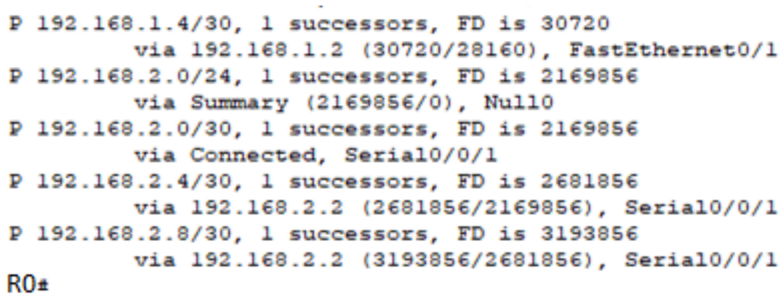
Figure 27. Routes the EIGRP follows

Here are all the devices connected with each other:



```
R0#show ip eigrp topology
IP-EIGRP Topology Table for AS 10/ID(192.168.2.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 10.0.0.0/8, 1 successors, FD is 28160
         via Connected, FastEthernet0/0
P 20.0.0.0/8, 1 successors, FD is 33280
         via 192.168.1.2 (33280/30720), FastEthernet0/1
P 192.168.0.0/24, 1 successors, FD is 40512000
         via Summary (40512000/0), Null0
P 192.168.0.0/30, 1 successors, FD is 40512000
         via Connected, Serial0/0/0
P 192.168.0.4/30, 1 successors, FD is 41024000
         via 192.168.0.2 (41024000/40512000), Serial0/0/0
P 192.168.0.8/30, 1 successors, FD is 41536000
         via 192.168.0.2 (41536000/41024000), Serial0/0/0
P 192.168.1.0/24, 1 successors, FD is 28160
         via Summary (28160/0), Null0
P 192.168.1.0/30, 1 successors, FD is 28160
         via Connected, FastEthernet0/1
P 192.168.1.4/30, 1 successors, FD is 30720
         via 192.168.1.2 (30720/28160), FastEthernet0/1
```

p 192. 168. 2. 0 /24 , 1 successors, FD is 2169856



```
P 192.168.1.4/30, 1 successors, FD is 30720
         via 192.168.1.2 (30720/28160), FastEthernet0/1
P 192.168.2.0/24, 1 successors, FD is 2169856
         via Summary (2169856/0), Null0
P 192.168.2.0/30, 1 successors, FD is 2169856
         via Connected, Serial0/0/1
P 192.168.2.4/30, 1 successors, FD is 2681856
         via 192.168.2.2 (2681856/2169856), Serial0/0/1
P 192.168.2.8/30, 1 successors, FD is 3193856
         via 192.168.2.2 (3193856/2681856), Serial0/0/1
R0#
```

Figure 28. Devices connected with EIGRP

CONCLUSIONS AND PROSPECTS

OSPF and EIGRP are two of the most comprehensive and pervasive protocols in the network architecture. Through this paper, a comparison analysis was conducted to determine which procedure dominated given a certain typology and a set of measurements. After doing a comprehensive literature study to determine the characteristics of the two protocols as well as their implementation, this research effort evaluates the acquired data and simulation results to determine which methodology has the best performance. The majority of researchers in this field assert that the EIGRP protocol offers superior performance, particularly in terms of network convergence time and CPU consumption. Such results are herein confirmed, but in more detail, based on the presented case studies. However, the, major goal of this paper has been to present in a tutorial fashion the whole analysis in order to be reproducible by other researchers too. However, more complex networking topologies should be investigated and more complex scenarios should be analysed in the near future.

CONFLICT OF INTERESTS

The authors confirm that there is no conflict of interests associated with this publication.

REFERENCES

[1] M. e. a. Goyal, "Improving Convergence Speed and Scalability in OSPF: A Survey, *Communications Surveys & Tutorials, IEEE*, 14 (2), pp. 443-463," 2012.

[2] Cisco., "Enhanced Interior Gateway Routing Protocol.," 2015.

[3] K. A. T. H. M. &. S. M. Al-Saud, "Impact of MD5 Authentication on Routing Traffic for the Case of: EIGRP, RIPv2 and OSPF, *Journal of Computer Science*," p. 4, 2008.

[4] C. Wijaya, "Performance Analysis of Dynamic Routing Protocol EIGRP and OSPF in IPv4 and IPv6 Network. Informatics and Computational Intelligence (ICI)," Indonesia, 2011.

[5] B. Wu, "Simulation Based Performance Analyses on RIPv2, EIGRP, and OSPF Using OPNET, Math and Computer Science Working Papers," p. 23, 2011.

[6] K. &. S. P. Ittiphon, "Link Recovery Comparison between OSPF & EIGRP,*International Conference on Information and Computer Networks (ICICN)*, 27," p. 192, 2012.

[7] e. a. Shafiul H., "Performance Evaluation of Dynamic Routing Protocols on Video Streaming Applications, *Current Trends in Technology and Science*, 2 (1)," p. 4, 2013.

[8] T. S. G, “Dynamic routing protocol implementation decision betweenEIGRP, OSPF and RIP based on technical background using OPNET modeler, *Computer and Network Technology (ICCNT)*,” Bangkok, 2010.

[9] X. L. &. J. W. Jun B, “OSPF performance measurements and scalability study, *Wireless and Optical Communications Networks*.,” Bangalore, Beijing.

[10] X. &. C. L. J. Che, “VoIP Performance over Different Interior Gateway Protocols, International *Journal of Communication Networks and Information Security (IJCNIS)*,” pp. 34-41, 2009.

[11] G. &. P. D. Kalyan, “Optimal selection of Dynamic Routing Protocol with real time case studies, *Recent Advances in Computing and Software Systems (RACSS)*. Chennai, 25-27 April 2012. India: IEEE.,” 2011.

[12] S. e. a. Sendra, “Dynamic Routing Protocols, In: Doyle, J. Routing TCP/IP (CCIE Professional Development), A detailed examination of interior routing protocols. U.S.A.:Cisco Press, 1.,” 2001.

[13] D. &. R. K. Medhi, “Network Routing: Algorithms, Protocols, and Architectures. Oxford, U.K.: Elsevier Inc,” 2007.

[14] J. F. &. R. K. W. Kurose, “Computer Networking. 3rd edn. Pearson Education.,” 2004.

[15] S. &. G.-L.-A. J. J. Vutukury, “MDVA: A Distance-Vector Multipath Routing Protocol, INFOCOM 2001, *Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies, IEEE*, (1),” pp. pp. 557-564, 2001.

[16] P. e. a. Rakheja, “Performance Analysis of RIP, OSPF, IGRP and EIGRP Routing Protocols in a Network. *International Journal of Computer Applications,* 48 (18),” pp. 6-11, 2012.

[17] Y. &. R. A. N. Liu, “A fast rerouting scheme for OSPF/IS-IS networks. *13th International Conference on Computer Communications and Networks (ICCCN)*,” USA, 11-13 October 2004, .

[18] Z. J. &. P. M. R. Haas, “The Performance of Query Control Schemes for the Zone Routing Protocol. *IEEE/ACM Transactions on Networking (TON)*, 9 (4),,” pp. 427-438.

[19] A. A. A. &. Z. S. Y. Hinds, “Evaluation of OSPF and EIGRP Routing Protocols for IPv6. *International Journal of Future Computer and Communication*, 2 (4),” pp.287-291.

[20] G. R. &. Jonson, “Routing Protocols and Concepts, CCNA Exploration Companion Guide. London: Pearson Education. Companion Guide series.,” 2008.

[21] J. Ferguson D. & Moy, “OSPF Version 3, RFC 5340. Sycamore Networks, Inc.,” 2008.

[22] Cisco., “OSPF Design Guide. [Online]. Available at:http://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/7039-1.html#t6,” 2005.

[23] F. e. a. Shamim, “Troubleshooting IP Routing Protocols. London: Cisco Press,,” 2002.

[24] E. Leahy, “EIGRP – Packets & Neighborships. [Online]. Available at:http://ericleahy.com/index.php/eigrp-packets-neighborships,” 2015.

[25] J. Moy, “OSPF Version 2, RFC 2328. Ascend Communications Inc.,” 1998.

[26] B. G.-L.-A. J. J. &. B. J. Albrightson, “EIGRP – A fast routing Protocol Based on Distance Vectors.,” pp. 1-13, 2011.

[27] Cisco., “Introduction to EIGRP.,” 2005.

[28] “https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/enhanced-interiorgateway-routing-protocol-eigrp/whitepaper_C11-720525.pdf,” [Online].

[29] B. R. J. &. T. M. (. Fortz, “Traffic engineering with traditional IP routing protocols, *Communications Magazine, IEEE*, 40 (10), pp. 118-124”.

[30] I. &. S. M. Kaur, Kaur, I. & Sharma, M. (2011) Performance evaluation of hybrid network using EIGRP & OSPF for different applications, *International Journal of Engineering Science and Technology (IJEST)*, 3 (5), pp. 3950-3960., pp. 3950-3960.