

# Simulate and Compare Routing Protocols for Smart Green Systems

Victor Chang\*, Anusha Kamireddy, Qianwen Xu, Jie Li, Charalampos Psarros and Perk Lin Chong  
School of Computing, Engineering and Digital Technologies, Teesside University, Middlesbrough TS1  
3BX, UK

Email: V.Chang@tees.ac.uk/ic.victor.chang@gmail.com; anukamireddy1993@gmail.com;  
iamarielxu@163.com; Jie.Li@tees.ac.uk; C.Psarros@tees.ac.uk; P.Chong@tees.ac.uk

\*: corresponding author

Prof. Victor Chang is a Full Professor of Data Science and Information Systems at SCEDT, Teesside University, Middlesbrough, UK since September 2019. He has 21.5 years of experience in IT and Academia. Within four years, he completed his PhD (CS, Southampton) and PGCert (Higher Education, Fellow, Greenwich) while working full-time. He achieved 97% on average in 27 IT certifications. He won many awards and best papers including Outstanding Young Scientist 2017. He is an editor of several top journals. He founded four international conferences and gave 18 international keynotes. He is regarded as a world-leading young scientist in Data Science/IoT/AI/security/IS.

Mrs. Anusha Kamireddy is a graduate of MSc Computer Science, Teesside University, Middlesbrough, UK. She has worked under Prof. Chang's supervision and has a passion for network protocols.

Miss Qianwen Xu completed MSc Business Analytics with Distinction at University of Liverpool and Xi'an Jiaotong-Liverpool University. She has worked with Prof. Victor Chang in the last 1 year part-time. She is a capable, efficient and hardworking researcher under Prof Chang's guidance. This is related to part of her work.

Dr. Li Jie is a Lecturer in Cybersecurity, Teesside University, Middlesbrough, UK, since June 2019. He received his PhD in Computer Science from Northumbria University in September 2018. He previously worked for NHS-related projects prior joining Teesside.

Dr. Charalampos Psarros is a Research Fellow, Teesside University, Middlesbrough, UK. Charalampos' interests are wide, from VR to engineering, Design to music technology, with a current focus on immersive multi-sensory technologies including 6-Degrees-of-Freedom (6DoF) 3D-360 media. During his PhD, he specialized in touchscreen interfaces and Human Computer Interaction. Hardware and

software solutions developed during his PhD are still considered for further development and patent/IP protected work. He is also a Task Leader in a currently running Engineering-related EU H2020 project involving Demand Response, being in charge of Aerial Survey techniques combining visual/ and thermal imaging with LiDAR scans.

Dr Perk Lin Chong is a Senior Lecturer Teesside University, Middlesbrough, UK. He has 8 years of teaching experience in institutions of Higher Learning. His research interests focus on sustainable energy, geometric modelling and engineering education. He has published numerous articles in international conferences and journals. Being active in research, he has been appointed as a permanent reviewer in Journal of Engineering Science and Technology (JESTEC). In addition, he has been a technical reviewer of numerous conferences, which include ICREATE 2009, CARs&FOF 2011, and ICCHT 2014. He is a Chartered Engineer of the Institution of Mechanical Engineers (IMechE).

## ABSTRACT

---

This paper aims to investigate different routing protocols and compares network protocols, including IGRP, RIP, BGP, etc. on key metrics and identified predominant routing protocols. In order to implement the comparison of different Routing protocols for smart green systems (RPSGSs), a network has been deployed with a Cisco packet tracer. Furthermore, the commands related to respective routing protocols are selected and used in CLI mode to configure the network. Cisco packet tracer is used since it provides a user-friendly interface on which users can drag and drop many devices to connect together to perform the configuration. The comparative analysis results suggest that EIGRP is a suitable routing protocol for the network that uses Cisco devices and OSPF is the most efficient routing protocol that can be used to transfer the packet from source to destination. RPSGSs allow datagrams to travel in the shortest path throughout the network.

Keywords: Systems; network protocols; Routing protocols for smart green systems (RPSGSs); Convergence with Enhanced Interior Gateway Routing Protocol (EIGRP); Routing Information Protocol version 2 (RIPv2), Open Shortest Path First (OSPF), EIGRP with Border Gateway Protocol (BGP) .

## 1 INTRODUCTION TO RESEARCH

---

The main tenacity of routing protocols for smart green systems (RPSGSs) is to identify the number of routes which are available in-network and routing decision can be framed by considering these protocols. IP routing is termed as the procedure of transferring packets of data between the networks, but the transfer of these packets cannot be done in two different networks. Linking of routers interface with various networks can be represented by routing table, which is particularly useful for decision

making (Alweimine, Bamaarouf, Rachadi & Ez-Zahraouy, 2019). There are two primary protocols that can be used to make communication between the devices or the interconnected network. Distance vector protocol advertises the routing table to connected neighbors using bandwidth and when the route is available, all the router tables must be updated according to the new requirement. The distance vector protocol used a subnet of fixed length, which is not scalable (Chai & Zeng, 2019). Interior gateway RPSGSs are used or managing the issues related to making communication between

the networks. Interior gateway routing protocol is termed as the distance vector routing protocol that is developed by the CISCO system for routing the protocols across the medium and small-sized CISCO networks. Interior Gateway Routing Protocol (IGRP) advertise less frequently and it uses less bandwidth as compared to distance vector protocol. IGRP recognizes the assignment of a different autonomous system and it also summarizes the network class boundaries automatically (Liu et al., 2020). The load balance traffic can be accomplished by the use of this protocol. An enhanced interior gateway routing protocol is also termed as a hybrid routing protocol that is developed by the CISCO system for routing the number of protocols across an enterprise CISCO network. Convergence with Enhanced Interior Gateway Routing Protocol (EIGRP) is faster as compared to a dual update algorithm that runs when the router detects the particular route that is unavailable (Sheghdara & Hassine, 2020). In this assessment, the ethnographic analysis of various RPSGSs has been done that need to transfer the data between the networks. The optimal path can be identified by the use of a routing protocol for making the communication between the networks. The routing protocol can be used for routing the packet from one place to another place and efficient routing one place to another place is a major issue of concern for the number of network providers. A routing protocol specifies the effective communication between the nodes connected to the network and the specific characteristics of RPSGSs define the efficiency of the protocols. Finding an effective routing protocol is a challenging task, but this research is designed to identify the efficient RPSGSs for sending the packets from one place to another place. In this research, IGRP, RIP, BGP protocols have been compared and implemented by the use of CISCO packet tracer (Yang, Chen, Chen & Zhao, 2018). The comparison of various RPSGSs is usually based on several aspects; namely, cost of the hop, routing convergence and scalability. In addition to these aspects, a routing protocol's ability to manage network congestion or traffic is also important because poor congestion control or traffic control can affect the quality of the network and services provided to users (Yang, Chen, Chen & Zhao, 2018). The quality of the network or the services can be improved by the use of efficient

routing protocol. One router can interact with the other router by the use of protocols and the reachability of the network can be improved by using the efficient protocols. In this research, the evaluation of different RPSGSs has been done by performing an experimental analysis in the CISCO packet tracer. Various types of RPSGSs have been used in this approach. There are different types of metrics that can be used to define the efficiency of the RPSGSs and on the basis of these metrics, the section of best-routing protocols has been done. The comparison between the number of the protocol has been framed by the use of this comparative analysis and literature-based analysis is used in this research to validate the use of RPSGSs. The number of advantages and disadvantages has been framed or discussed in this approach in concern of various RPSGSs. The number of research articles in this research is used to validate the use of RPSGSs. With the help of this approach, the potentials of different RPSGSs can be discussed.

## 2 LITERATURE REVIEW

---

### 2.1 MULTICAST ARCHITECTURE ALONG WITH ROUTING PROTOCOL

Yang et al. (2008) studied the potentials service-centric RPSGSs by using systematic analysis. A new multicast architecture is also discussed. We defined that traditional multicast protocol constructs mainly have two types of problems. First, the lack of information since conventional protocols only have the information related to local. Second, nodes and sending of data packets consume great network bandwidth in case of traditional routing and this is the major drawback of using traditional RPSGSs. In Yang et al.'s approach, we designed a multicast architecture that can be used for multicasting the data packets or the messages from one node to another node. The information related various nodes can be multi-casted by the use of multicasting routers and there is a number of protocols that can be used for this purpose. The multicast routers handle most of the tasks related to multicasting and simultaneously, many-to-many communications can be performed by the use of architectures that are proposed in this approach in the approach. The multicasting tree can be generated by the use of multicast routers. Therefore, issues related to delay

in communication can be handled and explored by the use of this multicasting protocol. The cost of the tree is less in case of this multicasting routing protocol. The problems related to traditional casting can be resolved by using this multicasting routing protocol.

## 2.2 COMPARATIVE ANALYSIS FOR RPSGSS

Chaudhry et al. (2006) compared to the WiMob Proactive and Reactive Routing Protocol by using simulation and on-demand routing protocols are also evaluated in their approach by the use of factors that can affect the working architecture of ad-hoc networks. Ad hoc on-demand distance vector (AODV) is used in this approach for managing the issues related to traditional RPSGSSs and an optimized link-state routing protocol is also evaluated in this approach by implementing the experimental analysis. The results of the simulation performed in this analysis revealed that throughput for OLSR is 10% high as compared to the AODV. The delays in the case of optimized link-state routing protocol are less as compared to delays in ad hoc on-demand distance vector (AODV). The throughput of ad hoc on-demand distance vector (AODV) is high as compared to an optimized link-state routing protocol. Parvathi (2012) performed a comparative analysis between the Cluster Based Routing Protocol (CBRP), AODV, Destination-Sequenced Distance-Vector Routing (DSDV) RPSGSSs in a mobile ad-hoc network. Routing in MANET is a critical task because of the dynamic environment involved in the MANET. This routing protocol provides the improved RPSGSSs and the issues related to delay in the routing of packets from source to destination can be resolved by the use of CBRP, AODV, DSDV RPSGSSs in Ad-hoc mobile networks. In this paper, three routing algorithms are compared hybrid routing protocol, Cluster-Based Routing Protocol, Ad-Hoc on Demand Distance Vector Protocol (AODV) and Pro-active routing protocol. The comparison of protocols based on their characteristics, functionality, benefits and limitations has been performed by using the secondary evaluation and analysis. Masruroh et al. (2017) evaluated the performance of RPSGSSs like Routing Information Protocol version 2 (RIPv2), Open Shortest Path First (OSPF), EIGRP with Border Gateway Protocol (BGP) based on throughput, packet loss and jitter value. The

performance of the internal and external RPSGSSs has been conducted by evaluating the quality of services and throughput of the system. From their analysis, it has been summarized that OSPF-BGP has the lowest packet loss, highest throughput and smallest jitter value. Al-khdour and Baroudi (2007) analyzed the entropy-based throughput metric for wireless sensor RPSGSSs and summarized that the number of issues related to raw packets could be handled by the use of the entropy-based WSN RPSGSSs. The comparison and evaluation of the performance of well-known RPSGSSs like Low Energy Adaptive Clustering Hierarchy (LEACH) and EAD have also been performed in this analysis.

## 2.3 Q-LEACH ROUTING PROTOCOL FOR WSN

Gnanambigai et al. (2013) defined that a wireless sensor network is an efficient approach for managing congestion over the network and in their research, the sensor routing scheme has been used for the routing of packets from one network to another network. A new sensor-based routing scheme has been used by our approach to reducing the congestion over the network and the Q-DIR protocol and clustering model in corresponding LEACH protocol have been used in the observation-based analysis to manage the issues related to the location-based routing protocol. Quadrant Based Directional Routing Protocol (Q-DIR) integrates the number of dissimilar methods by considering the restricted flooding and location-based routing. The issues related to restricting flooding can be managed by the use of protocols that can be used to perform efficient routing. The location information of the destination code, current node and the source node has been used in this approach for managing the issues related to RPSGSSs and along with this, the number of clustering techniques can be used congestion control over the network. The number of observations can be derived by evaluating the efficiency of the network and protocols can be managed by considering the factors related to efficiency. The distribution of data over the network can be managed by the use of RPSGSSs and these routing protocols are evaluated on the basis of energy consumed by the protocols. The research design and RPSGSSs related to wireless sensor networks are used to consider the performance of network protocols (Guo, Wang, Huang, Tan & Zhang, 2007). According to approach, the wireless

sensor network can be efficiently used in the coal mine and this routing protocol is classified into the query-based, geographic-based and cluster-based RPSGSs. Analysis performed in this research help to define that routing protocols can provide a number of advantages to the users and multipath routing protocol is designed in this approach for the coal mining system. In this approach, the data related to coal mine can be acquired by the use of wireless sensor networks and the dependability of the coal mining system can be improved by the use of wireless sensor RPSGSs (Guo, Wang, Huang, Tan & Zhang, 2007).

#### **2.4 CHARACTERISTICS OF RPSGSs**

The analysis of different protocols has been done in Bobalo's approach by considering their characteristics and most common RPSGSs having different types of delivery as well as ways of organizing the multipath routing are also discussed in this systematic literature review (Bobalo, 2010). A comparative analysis is proposed in this approach for comparing the protocols like DVMRP, CBT, MOSPF, PIM-DM and PIM-SM. In this research, the evaluation of RPSGSs can be conducted based on the accuracy and efficiency of the network (Bobalo, 2010). This research concluded that every protocol has its benefits and drawback and can be used or a specific purpose for routing (Bobalo, 2010). Yang et al. (2008) provided an overview of the multicast architecture and routing protocol that can be used for routing the packets from one network to another network. Multicast architecture and RPSGSs that are defined in their research are very efficient and flexible as compared to the traditional approaches of multicasting and routing. The construction of multicast protocol has been done in this approach by the use of multicasting routing protocol and these protocols are called a service-centric multicast protocol. The sharing of the multicast routing protocol helps to resolve the number of issues related to the routing of packets from one network to another network. M-router referred to each group help to manage the issues related to the sending of packets from one place to another place. Delay constrained dynamic multicast algorithm can be used for managing the number of issues related to delay in the network. The cost is a factor that can be used in managing the problems associated with the use of RPSGSs and the use of

algorithms can be done by considering the efficiency and cost of the protocol. The physical construction of the multicast tree can be done by the use of the DCDM algorithm. The construction of the multicast tree over the network can be done by the use of RPSGSs and the particular type of routing packets can be used over the network for managing the issues related to multicast architecture and routing protocols. The implementation of SCMP protocols outperforms the existing protocols that can be used for routing the protocols for managing the issues related to network congestion. The promising alternative can be used for managing the issues related to RPSGSs and the flexible services can be provided to the network by the use of multicast architecture.

#### **2.5 PERFORMANCE EVALUATION OF ROUTING PROTOCOL (OSPF)**

Dey et al. (2015) provided an overview of performance analysis of different RPSGSs, including OSPF protocol. This shortest-path routing protocol has been evaluated by the use of the CISCO router simulation. The comparison between the different RPSGSs has been made. Simulations conducted in this analysis reveal that OSPF protocols can help to tackle the conflict related to congestion that exists in the network. In this research, eight CISCO routers and a switch are used to simulate the topology of the network. Four routers that work on the different RPSGSs have been simulated and the switch used in this simulation has the responsibility related to the redistribution algorithm so that the packets can be redistributed efficiently.

Jayakumar et al. (2015) provided a comparative analysis between the OSPF and RIP protocols. By use of the distance vector algorithm, the number of network problems can be investigated more effectively. In this research, literature-based analysis is used in this approach to evaluate the use of OSPF and OPNET, IGRP and RIP, EIGRP. The number of secondary resources is used in this comparative study to validate the use of different protocols. The RPSGSs that are used in the interconnection of the network is evaluated in this research by using the comparative analysis.

Krishnan and Shobha (2013) provided an overview of performance analysis in the context of EIGRP routing protocol and OSPF routing protocol. The evaluation of both the protocols has been performed based on Convergence Time, End-to-End delay, Jitter, Throughput and Packet Loss concluded that OSPF has good performance and by the use of these simulation techniques its has been concluded. The performance of the CPU has also been evaluated in this research and the issues related to poor performance RPSGSs are also evaluated in this research.

Masruroh et al. (2017) provided an overview of performance evaluation of routing protocol by considering the protocols like OSPF, EIGRP, EIPv2 and BGP. The quality of services can be provided by the use of these protocols and issues related to jitter and packet loss can be mitigated by including or using this kind of protocol. The factors like packet loss, the value of throughput, network convergence, jitter and throughput are used in this approach to evaluate the performance of the different protocols. The analysis concluded that OSPF is efficient protocols that can be used in the organization for handling the issues related to packet loss, smallest jitter value and the lowest packet has been concluded by the use of OSPF protocol.

Ming-Hao (2014) provided an overview of security analysis and the detection of attacks by the use of OSPF routing protocol. The challenges related to information security can be handled and managed by the use of the OSPF routing protocol. The routers find the best route to transfer the information from one network to another network. OSPF routing protocol works on the shortest path algorithm and the issues related to the security of the network can be managed by the use of this protocol for security purposes. The vulnerabilities related network can threaten the use of OSPF routing protocol. The detection of attacks can be proliferated by using the OSPF protocol. This research revealed that network operation could not get effected while detecting the attacks by using the OSPF routing protocol.

### 3 METHODOLOGY

---

In this approach, the experimental analysis has been proposed in order to identify and compare the number of protocols that can be used for transferring the data from one place to another. This experimental analysis has been performed in this approach by using the cisco packet tracer. This comparative analysis has been performed between the EIGRP, RIP, OSPF protocols. IGRP protocol is defined as the distance vector interior gateway protocol (IGP). This routing protocol help to manage the issues related to transfer of data one place to another place and this protocol is also termed as proprietary protocol and the limitation of RIP is its hop count because the maximum hop count that has been supported by this protocol is 15, by the use of IGRP protocol this limitation has been overcome because this protocol allows the multiple hops. The multiple metrics for each router have been supported by this protocol, such as delay, load, bandwidth, reliability and the comparison between the two routes has been done on the basis of these parameters. The protocol number for this protocol is nine and by the use of this protocol number, communication between the networks has been proliferated. This approach is used to make effective selection related to protocols in order to make effective communication. The use of RIP is defined as one of the oldest distance-vector RPSGSs that can be used to manage and transfer the data from one hop to another hop. The network size is limited in this case and RIP implements the split horizon, hold down and route poisoning mechanism for preventing the dissemination of incorrect information over the network. RIP is not the preferred choice for routing because this type of routing has poor scalability as compared to other protocols like OSPF, EIGRP and IS-IS. However, this protocol is easy to configure as compared to other protocols. In this approach, the data is evaluated on the basis of the experimental analysis and the comparison between the different protocols has been performed by considering the following steps:

#### **Step 1: Network creation (adding routers, switches, devices)**

In this step, the network in CISCO packet tracer has been designed and the number of network devices

like routers, mobile devices and switches have been arranged in this approach. The routers that are connected to the network have been used to route the information over the network and the router route the information on the basis of IP addresses and router reads the IP addresses of the network and sends the details according to the requirements. The switches are also connected to the network to broadcast the data packets over the network and routers to generate a routing table for transferring the data packets from one network to another network. The mobile devices have been connected to the network that can avail of the services that have been provided by the created network. The simulation of the network has been done by the use of CISCO packet tracer and the issues related to the routing of the data packet can be simulated by the use of CISCO packet tracer. Packet tracer is defined as the cross-platform that has been used for simulating the network and it also allows the users to simulate the CISCO routers, switches and devices. This is a drag and drop tool that has easy to use user interfaces. This software is mainly focused on evaluating the network and system that has been used to make effective communication between the networks.

### **Step 2: Connection establishment between the devices**

In this step, the connection between the nodes has been established by using the CISCO packet tracer and by assigning the IPs to the connected routers, switches and devices, the connection between the devices can be established by the use of CISCO packet tracer. The complex technologies can be visualized by the use of CISCO packet tracer and by the use of CISCO packet tracer, the issues related to simulation of network.

### **Step3: Configuration of routers (assigning the networks)**

The IP address has been assigned to the routers in order to transmit the data from one network to another network. In this approach, the different interfaces like fast Ethernet and serial cable are assigned with different network IPs in order to operate them from other networks. Furthermore, cables are connected according to the requirements of the users.

### **Step 4: Configuring the four RPSGSs**

In this step, the different types of RPSGSs have been evaluated and identified that RIP, EIGRP, OSPF are the widely used RPSGSs. As a result, we have analyzed different RPSGSs configurations procedures for the hardware devices

### **Step 5: Comparison between protocols**

On CISCO packet tracer, we have deployed a network and connected with suitable cables, executed the RPSGSs on the CISCO router. It has been analyzed that the metric of each routing protocol is different from each other. In this research, the practical implementation of the network by using RPSGSs has been done. For RIP versions one and two, we have added the directory connected networks to the interface. In EIGRP RPSGSs, the networks have been added, which are directly connected, but autonomous numbers used to be given to separate one mini-network from another mini-network similarly we have done OSPF configuration. But in this protocol area number of given to each network so that the communication can be isolated from another network.

### **Step 6: Results and analysis**

In this step, the simulation has been used to simulate the network by sending a simple PDU packet from source to destination in the entire network. They contribute to different RPSGSs because each protocol has been executed one after another. After sending the packets from one source to destination, we have executed the command to find the metrics that have been used by the packets to reach the destination in all the protocols. In the end, the formulas used for metrics evaluation have been given and analyze furthermore, it has been analyzed that the network-based up on CISCO will be suitable to have EIGRP routing protocol for the communication between the nodes because it utilizes the bandwidth to reach the destination.

## **4 IMPLEMENTATION**

In order to implement the comparison of different RPSGSs, a network has been deployed with a Cisco packet tracer. Furthermore, the commands related to respective RPSGSs are selected and used in CLI mode to configure the network. The major reason

for selecting a Cisco packet tracer is that it provides a user-friendly interface on which the user can drag and drop many devices to connect together in order to perform the configuration. In this section, we

have implemented the different RPSGSs on the network and analyses their metrics in order to find a suitable one for enabling the communication of different networks.

**Case Scenario:**

In the Cisco packet, the tracer tool workspace selected the numerous hardware devices and used a suitable cabling mechanism to connect the devices. The following diagram illustrates the interconnection of devices and addressing scheme is used for providing a unique identity to a particular PC. Selected RPSGSs to run for the comparison purposes are OSPF, RIPv1, RIPv2, and EIGRP is implemented on the same network design.

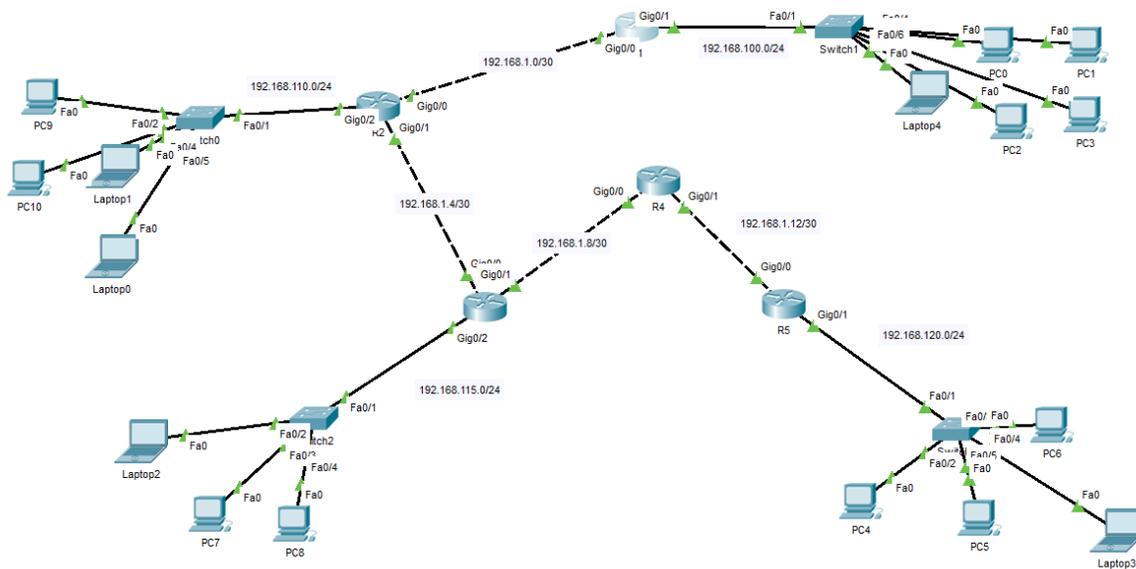
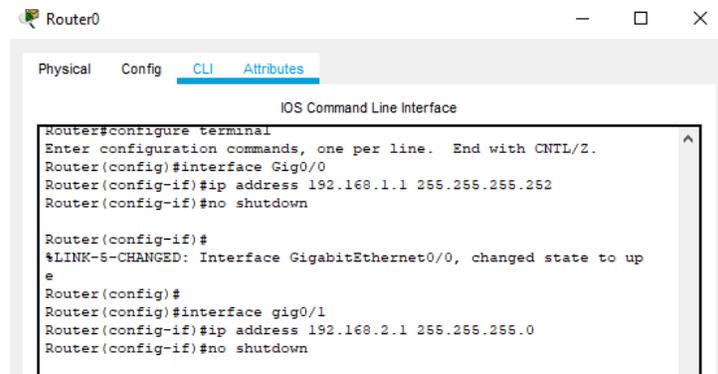


Figure 1. Interconnection of devices

**Interface addressing:**

When the router is added in the workspace, there are two ports, i.e., Fast Ethernet and Serial interface, to which the addressing is required for connecting with the other network. For the purpose of addressing, private addressing is used because a local area network is developed. The command executed for assigning addressing scheme to particular ports can be viewed in the diagram below:

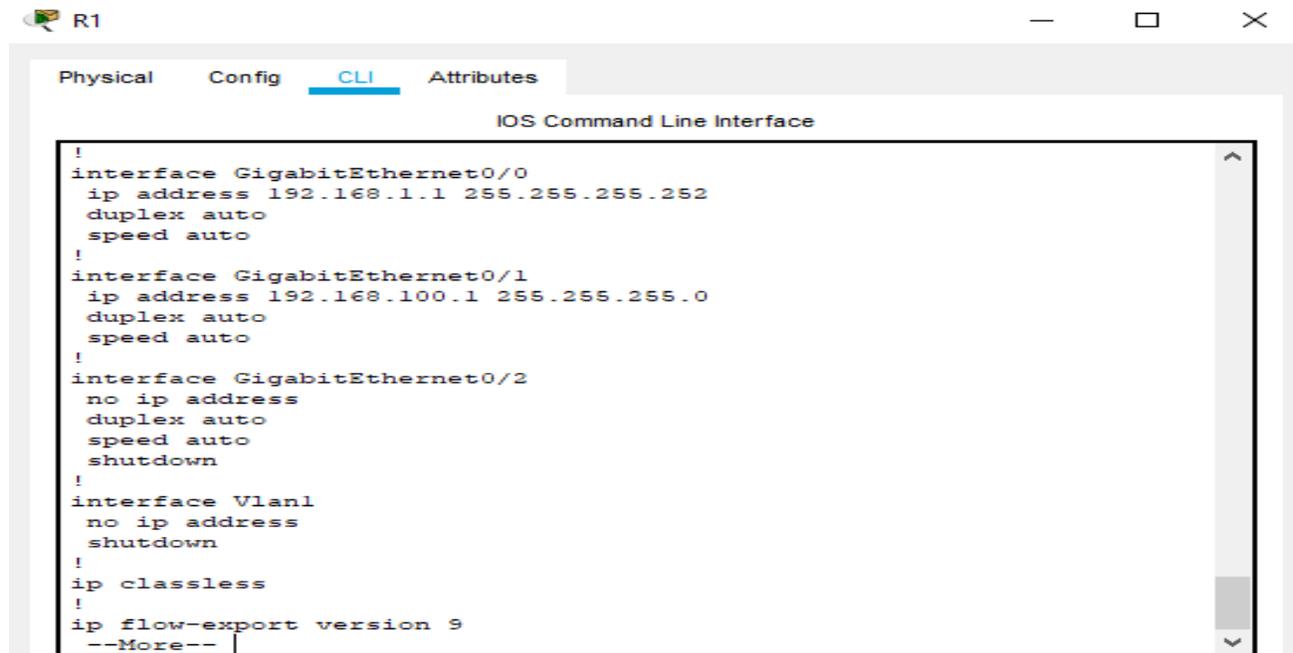


```
Router0
Physical Config CLI Attributes
IOS Command Line Interface
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface Gig0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.252
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
e
Router(config)#
Router(config)#interface gig0/1
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#no shutdown
```

Figure 2. Command executed for assigning addressing scheme

Similarly, as of router 0, the addressing scheme is assigned to the ports connected of the second network as depicted the configuration commands executed:



```
R1
Physical Config CLI Attributes
IOS Command Line Interface
!
interface GigabitEthernet0/0
ip address 192.168.1.1 255.255.255.252
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 192.168.100.1 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
shutdown
!
interface Vlan1
no ip address
shutdown
!
ip classless
!
ip flow-export version 9
--More--
```

Figure 3. Addressing scheme – R1

will depict the following configuration that has been done to differentiate with other connected networks.

To analyze addressing configuration on the R2 device, execute the "show run" command, and it

```

R2
Physical Config CLI Attributes
IOS Command Line Interface
interface GigabitEthernet0/0
ip address 192.168.1.2 255.255.255.252
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 192.168.1.5 255.255.255.252
duplex auto
speed auto
!
interface GigabitEthernet0/2
ip address 192.168.110.1 255.255.255.0
duplex auto
speed auto
!
interface Vlan1
no ip address
shutdown
!
ip classless
!
ip flow-export version 9
!
!
--More--

```

Figure 4. Addressing scheme – R2

Similarly, R3 has been assigned with different interfaces for which there is a need to configure IP addresses to designate an as unique address for transferring the information.

```

R3
Physical Config CLI Attributes
IOS Command Line Interface
interface GigabitEthernet0/0
ip address 192.168.1.6 255.255.255.252
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 192.168.1.9 255.255.255.252
duplex auto
speed auto
!
interface GigabitEthernet0/2
ip address 192.168.115.1 255.255.255.0
duplex auto
speed auto
!
interface Vlan1
no ip address
shutdown
!
ip classless
!
ip flow-export version 9
!
!
--More--

```

Figure 5. Addressing scheme – R3

**Router**

The first routing protocol selected to configure on the network is ripv1, which has the limited hop count and have a very limited area up to which the data can be sent to the destination. In the

**ripv1**

configuration commands illustrated below, the user requires to add the directly related IP networks so that the router can identify the location of devices within the network:

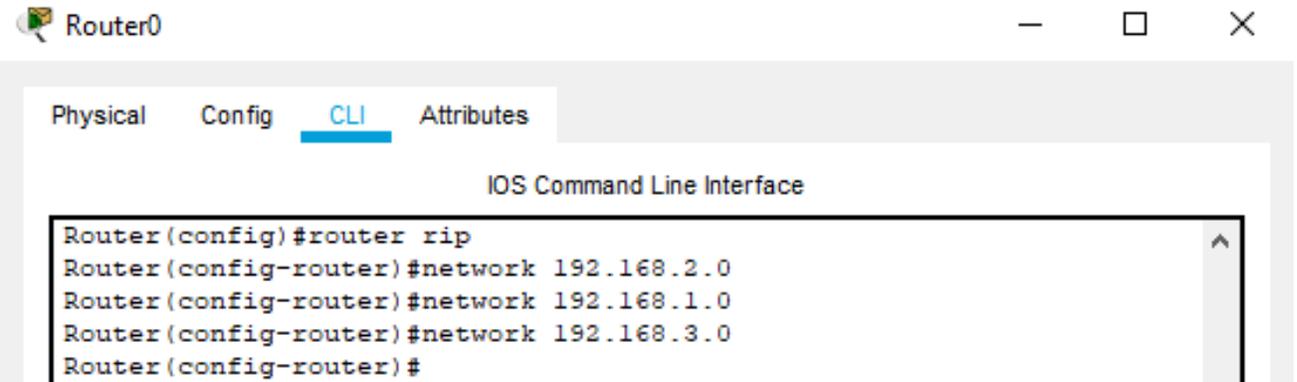


Figure 6. Router Configuration used RIPv1– Router0

The same router configuration is also performed on the router1 to enable the communication.

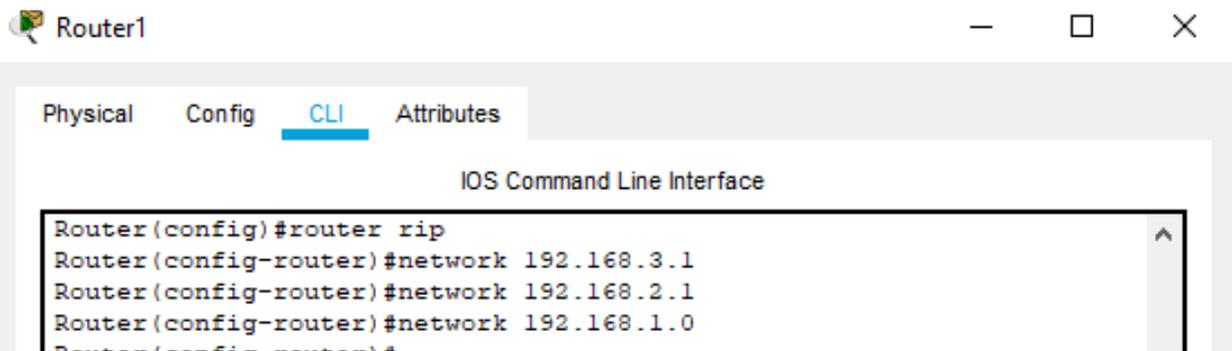


Figure 7. Router Configuration used RIPv1 – Router1

In desktop, there is a command prompt option that has been selected in order to check whether the devices are communicating with each other or not. The results below show that both the networks are communicating successfully with each other.

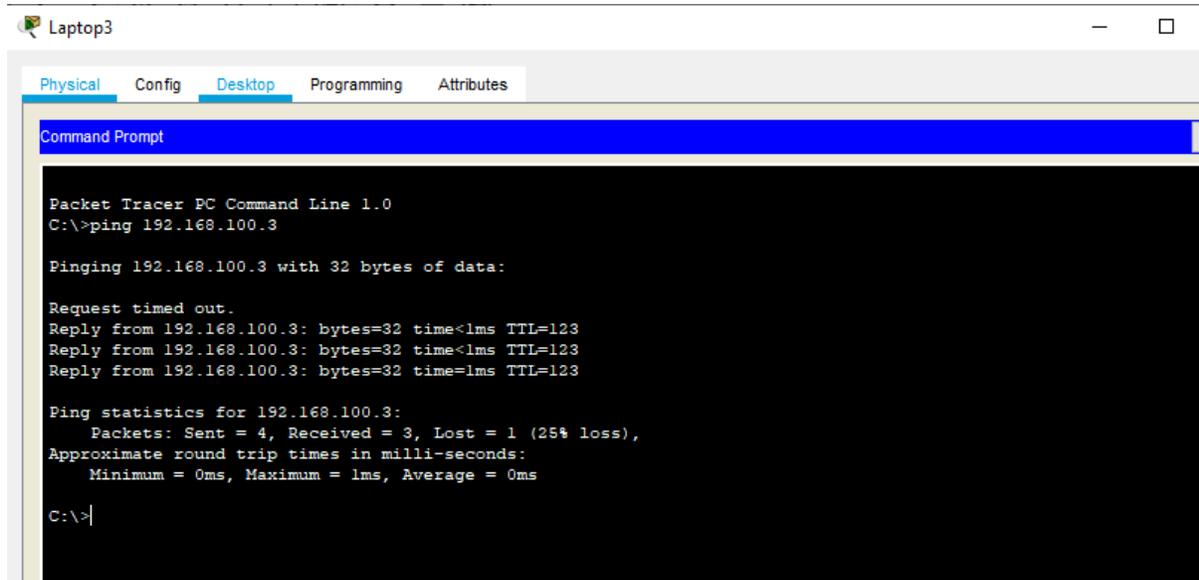


Figure 8. Communication Result

### Router RIPv2

In this section, RIP version 2 is configured, which is considered an upgraded version, and provides more hop count in order to transfer the data to the destination end. Below screenshot is used to illustrate the network configuration performed for enabling the routing ripv2 for the first network:

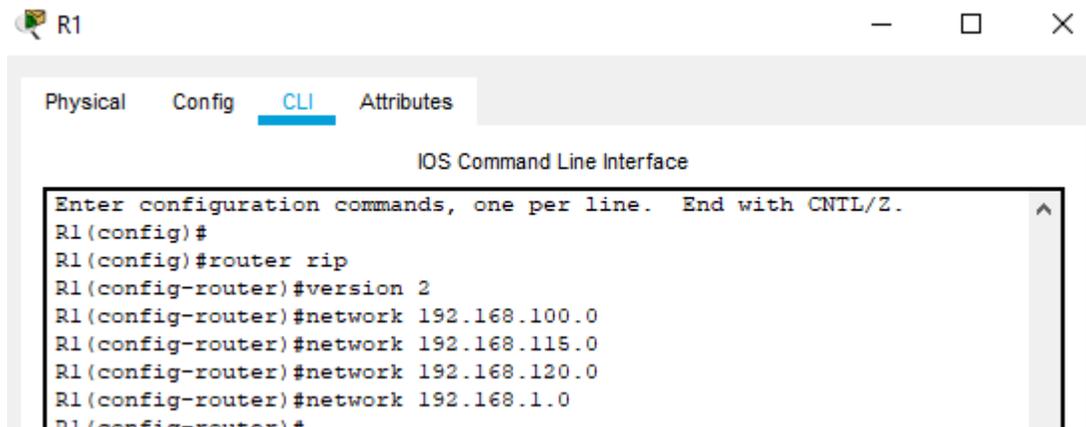
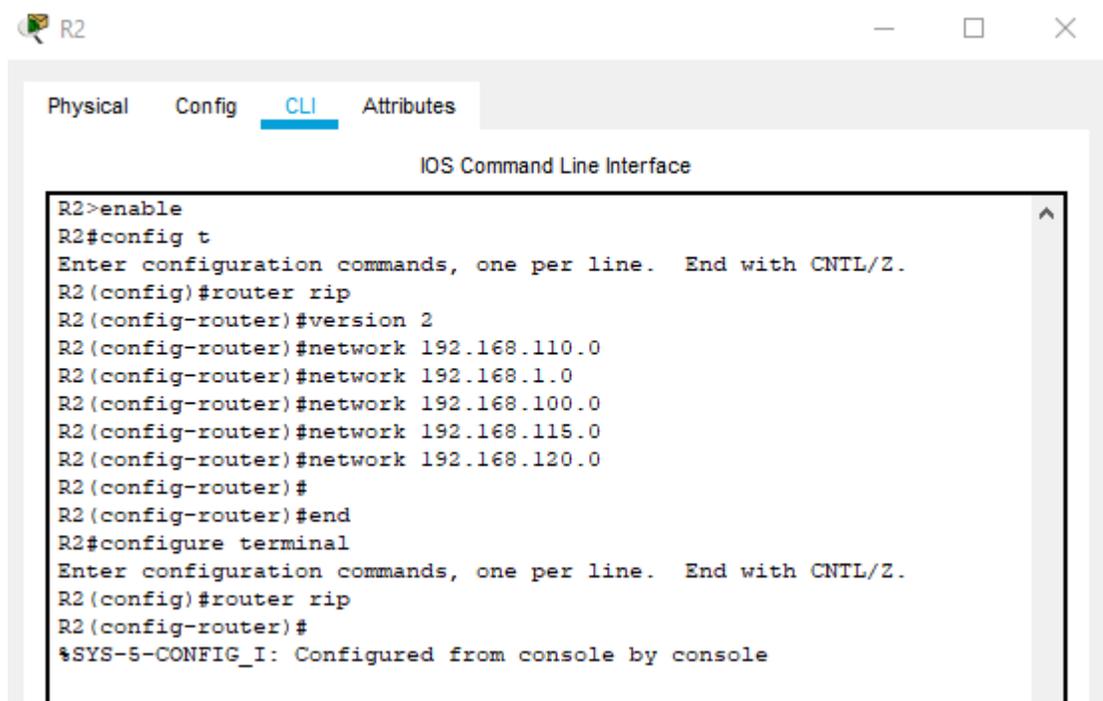


Figure 9. Router Configuration used RIPv2 – Router1

For the second network, router1 is configured that for allowing the communication. will add the networks attached directly to the router

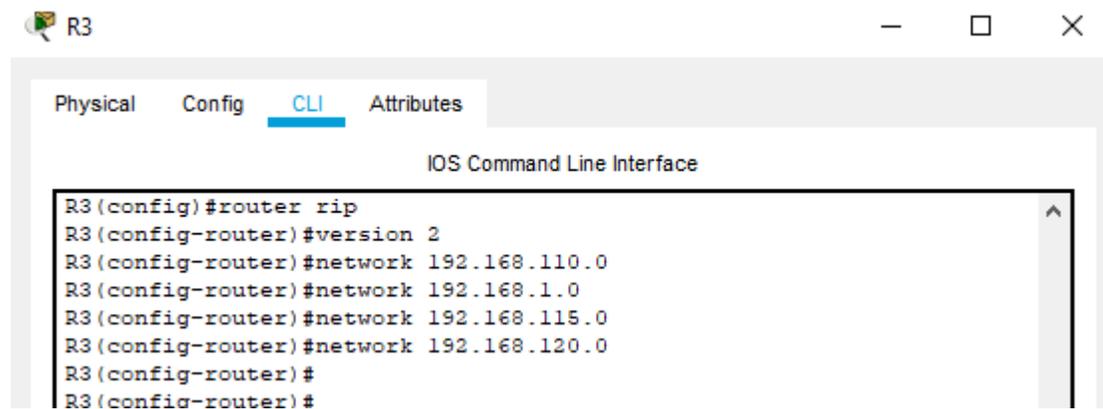


The screenshot shows the CLI interface for Router2. The window title is 'R2'. The tabs are 'Physical', 'Config', 'CLI', and 'Attributes', with 'CLI' selected. The text in the terminal window is as follows:

```
R2>enable
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#network 192.168.110.0
R2(config-router)#network 192.168.1.0
R2(config-router)#network 192.168.100.0
R2(config-router)#network 192.168.115.0
R2(config-router)#network 192.168.120.0
R2(config-router)#
R2(config-router)#end
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router rip
R2(config-router)#
%SYS-5-CONFIG_I: Configured from console by console
```

Figure 10. Router Configuration used RIPv2 – Router2

For router 3, and 4, the configuration of the router network is also performed:



The screenshot shows the CLI interface for Router3. The window title is 'R3'. The tabs are 'Physical', 'Config', 'CLI', and 'Attributes', with 'CLI' selected. The text in the terminal window is as follows:

```
R3(config)#router rip
R3(config-router)#version 2
R3(config-router)#network 192.168.110.0
R3(config-router)#network 192.168.1.0
R3(config-router)#network 192.168.115.0
R3(config-router)#network 192.168.120.0
R3(config-router)#
R3(config-router)#
```

Figure 11. Router Configuration used RIPv2 – Router3

For the R4 router, the configuration of a RIP routing protocol can be viewed, which displays that the

connected networks have been added in the devices so that the communication can be done successfully.

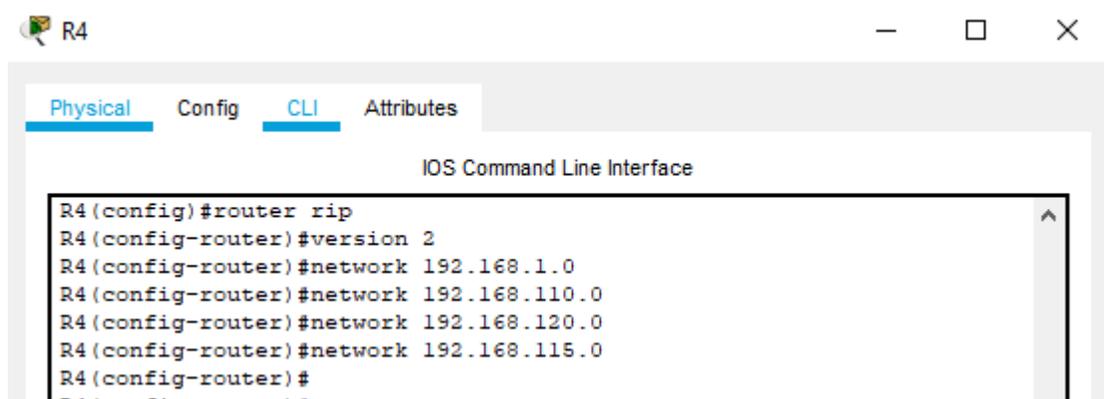


Figure 12. Router Configuration used RIPv2 – Router4

Successfully communication is necessary before evaluating the metrics for which ping command is used to view the communication of both the devices.

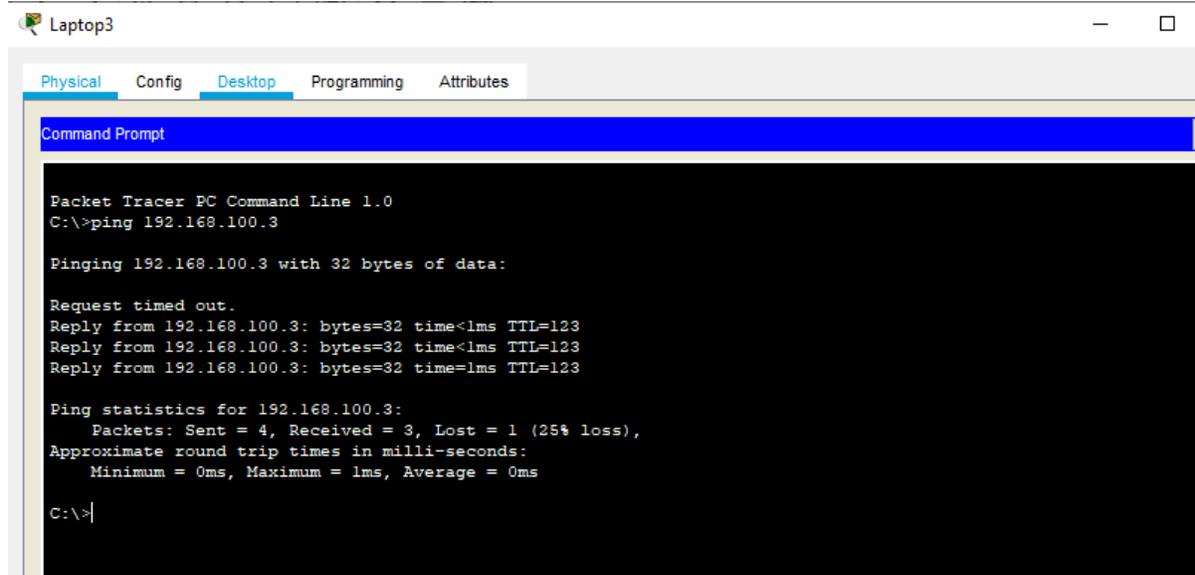


Figure 13. Communication Result

## OSPF

OSPF stands for open shortest path first protocol, which works on the basis of areas developed for respective networks. A major benefit of using OSPF routing is that areas can be developed according to

requirement, and can be further used to isolate the network for enabling the communication. The following screenshot adds the network along with area being configured for the respective configuration:

```

R1>
R1>enable
Translating "enable"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer
address

R1>enable
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router ospf 10
R1(config-router)#network 192.168.100.0 0.0.0.255 1
^
% Invalid input detected at '^' marker.

R1(config-router)#network 192.168.100.0 0.0.0.255 area 1
R1(config-router)#network 192.168.1.0 0.0.0.3 area 1
R1(config-router)#
00:11:49: %OSPF-5-ADJCHG: Process 10, Nbr 192.168.110.1 on
GigabitEthernet0/0 from LOADING to FULL, Loading Done

R1(config-router)#
R1(config-router)#exit
R1(config)#

```

Figure 14. Router Configuration used OSPF – Router1

The diagram below depicts that the configuration of the routing protocol OSPF is done for the network. because we have developed the local area network for testing purposes. The area is configured similarly to the other area

```

R2(config)#router ospf 10
R2(config-router)#network 192.168.110.0 0.0.0.255 area 1
R2(config-router)#network 192.168.1.0 0.0.0.3 area 1
R2(config-router)#network 192.168.1.4 0.0.0.3 area 1
R2(config-router)#
R2(config-router)#

```

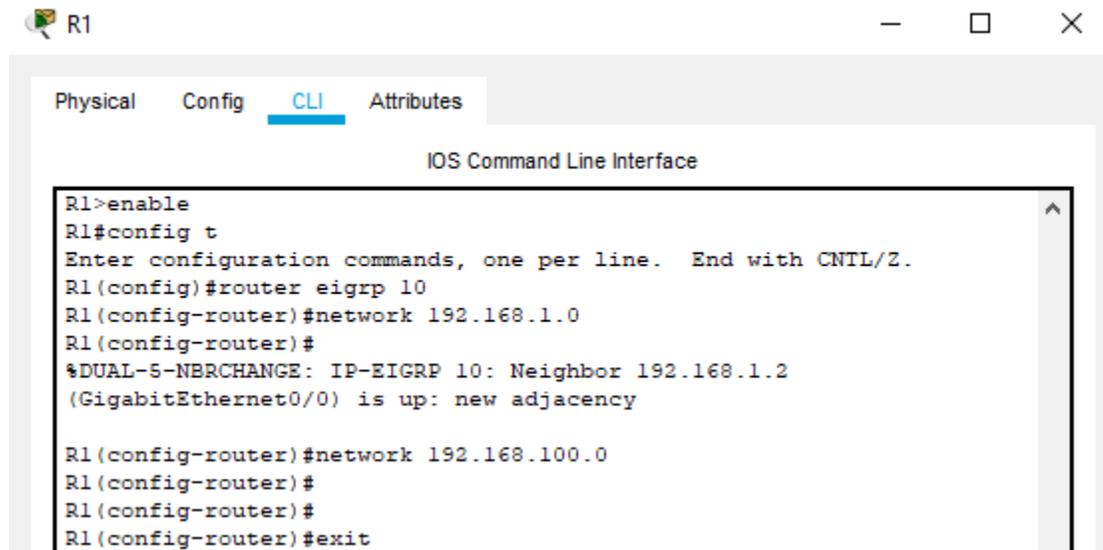
Figure 15. Router Configuration used OSPF – Router2

Communication between both the networks is tested and finds that both the network is successfully communicating with each other.

**EIGRP**

EIGRP stands for an enhanced interior gateway routing protocol, which considered to be the most suitable routing protocol if it needs to select for Cisco devices as it works only for Cisco.

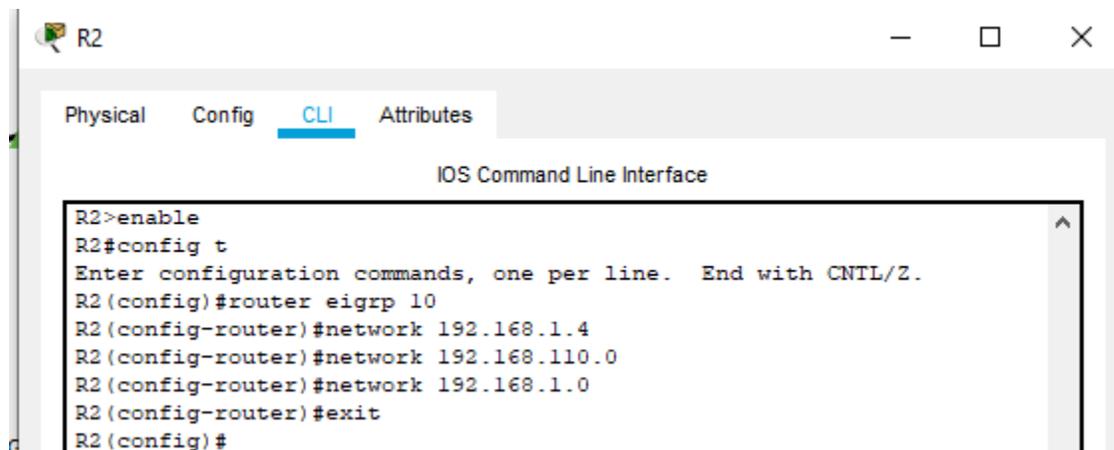
Configuration commands executed to add EIGRP routing networks to the devices can be viewed below:



```
R1
Physical Config CLI Attributes
IOS Command Line Interface
R1>enable
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router eigrp 10
R1(config-router)#network 192.168.1.0
R1(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 10: Neighbor 192.168.1.2
(GigabitEthernet0/0) is up: new adjacency
R1(config-router)#network 192.168.100.0
R1(config-router)#
R1(config-router)#
R1(config-router)#exit
```

Figure 16. Router Configuration used EIGRP – Router1

For this network, the routing networks are added so that communication can be enabled between both the devices:



```
R2
Physical Config CLI Attributes
IOS Command Line Interface
R2>enable
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router eigrp 10
R2(config-router)#network 192.168.1.4
R2(config-router)#network 192.168.110.0
R2(config-router)#network 192.168.1.0
R2(config-router)#exit
R2(config)#
```

Figure 17. Router Configuration used EIGRP – Router2

The resulted output shows that both the devices are successfully communicating with each other.

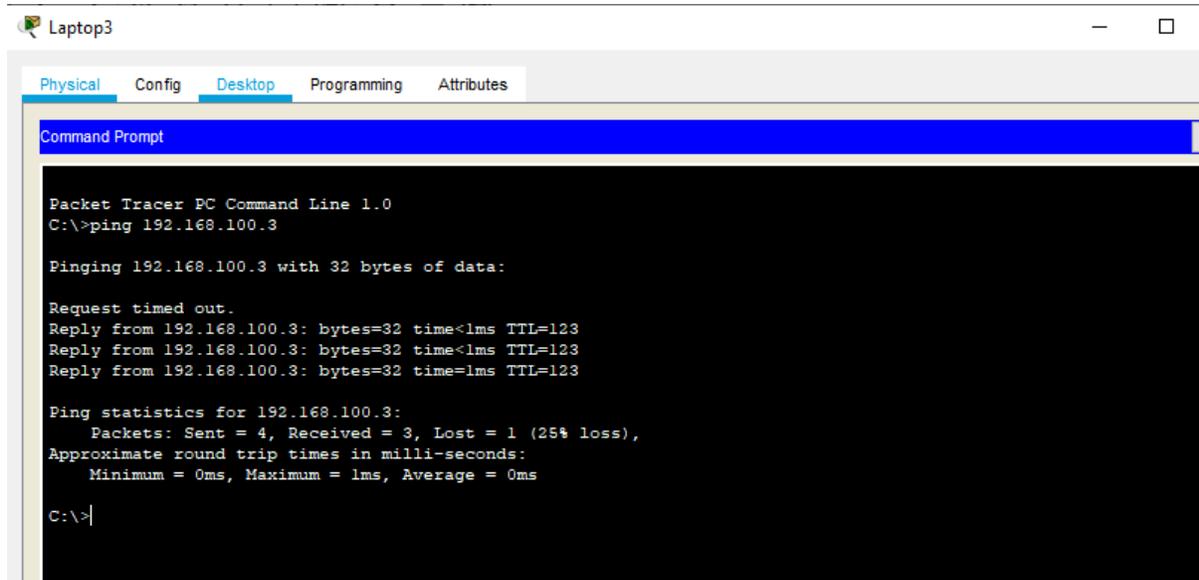


Figure 18. Communication Result

#### 4.1 RESULTS EVALUATION

The performance of the RPSGs can be compared over the metrics such as path length, reliability, routing delay, bandwidth, load, and communication cost, etc. When the network is developed, the next step was to analyze the metrics on which the data is transferred to the destination end via source device. In order to analyze the best suitable routing protocol for the network, metrics are analyzed in which there

are two parts, i.e., autonomous system/metric. In this section, all the routing tables of different RPSGs are calculated with the help of Cisco for the evaluation.

RIPv1: The diagram below is showing the routing table generated when the communication is enabled between the devices.

Routing Table for R1				
Type	Network	Port	Next Hop IP	Metric
C	192.168.1.0/30	GigabitEthernet0/0	---	0/0
L	192.168.1.1/32	GigabitEthernet0/0	---	0/0
R	192.168.1.4/30	GigabitEthernet0/0	192.168.1.2	120/1
R	192.168.1.8/30	GigabitEthernet0/0	192.168.1.2	120/2
R	192.168.1.12/30	GigabitEthernet0/0	192.168.1.2	120/3
C	192.168.100.0/24	GigabitEthernet0/1	---	0/0
L	192.168.100.1/32	GigabitEthernet0/1	---	0/0
R	192.168.110.0/24	GigabitEthernet0/0	192.168.1.2	120/1
R	192.168.115.0/24	GigabitEthernet0/0	192.168.1.2	120/2
R	192.168.120.0/24	GigabitEthernet0/0	192.168.1.2	120/4

Figure 19. RIPv1 - Routing Table for R1

For another router device R2, the metric values can be viewed that are being used by each network to

provide communication with the destination end.

Routing Table for R2

Type	Network	Port	Next Hop IP	Metric
C	192.168.1.0/30	GigabitEthernet0/0	---	0/0
L	192.168.1.2/32	GigabitEthernet0/0	---	0/0
C	192.168.1.4/30	GigabitEthernet0/1	---	0/0
L	192.168.1.5/32	GigabitEthernet0/1	---	0/0
R	192.168.1.8/30	GigabitEthernet0/1	192.168.1.6	120/1
R	192.168.1.12/30	GigabitEthernet0/1	192.168.1.6	120/2
R	192.168.100.0/24	GigabitEthernet0/0	192.168.1.1	120/1
C	192.168.110.0/24	GigabitEthernet0/2	---	0/0
L	192.168.110.1/32	GigabitEthernet0/2	---	0/0
R	192.168.115.0/24	GigabitEthernet0/1	192.168.1.6	120/1
R	192.168.120.0/24	GigabitEthernet0/1	192.168.1.6	120/3

Figure 20. RIPv1 - Routing Table for R2

Following screenshot is showing the output of metrics that being used by the directly connected networks to communicate with destination end:

Routing Table for R3

Type	Network	Port	Next Hop IP	Metric
R	192.168.1.0/30	GigabitEthernet0/0	192.168.1.5	120/1
C	192.168.1.4/30	GigabitEthernet0/0	---	0/0
L	192.168.1.6/32	GigabitEthernet0/0	---	0/0
C	192.168.1.8/30	GigabitEthernet0/1	---	0/0
L	192.168.1.9/32	GigabitEthernet0/1	---	0/0
R	192.168.1.12/30	GigabitEthernet0/1	192.168.1.10	120/1
R	192.168.100.0/24	GigabitEthernet0/0	192.168.1.5	120/2
R	192.168.110.0/24	GigabitEthernet0/0	192.168.1.5	120/1
C	192.168.115.0/24	GigabitEthernet0/2	---	0/0
L	192.168.115.1/32	GigabitEthernet0/2	---	0/0
R	192.168.120.0/24	GigabitEthernet0/1	192.168.1.10	120/2

Figure 21. RIPv1 - Routing Table for R3

For R4, metrics have been calculated by a directly connected interface can be viewed below:

Routing Table for R4

Type	Network	Port	Next Hop IP	Metric
R	192.168.1.0/30	GigabitEthernet0/0	192.168.1.9	120/2
R	192.168.1.4/30	GigabitEthernet0/0	192.168.1.9	120/1
C	192.168.1.8/30	GigabitEthernet0/0	---	0/0
L	192.168.1.10/32	GigabitEthernet0/0	---	0/0
C	192.168.1.12/30	GigabitEthernet0/1	---	0/0
L	192.168.1.13/32	GigabitEthernet0/1	---	0/0
R	192.168.100.0/24	GigabitEthernet0/0	192.168.1.9	120/3
R	192.168.110.0/24	GigabitEthernet0/0	192.168.1.9	120/2
R	192.168.115.0/24	GigabitEthernet0/0	192.168.1.9	120/1
R	192.168.120.0/24	GigabitEthernet0/1	192.168.1.14	120/1

Figure 22. RIPv1 - Routing Table for R4

Similarly, the fifth router device's routing metrics assigned to each network interface can be viewed below:

Routing Table for R5

Type	Network	Port	Next Hop IP	Metric
R	192.168.1.0/30	GigabitEthernet0/0	192.168.1.13	120/3
R	192.168.1.4/30	GigabitEthernet0/0	192.168.1.13	120/2
R	192.168.1.8/30	GigabitEthernet0/0	192.168.1.13	120/1
C	192.168.1.12/30	GigabitEthernet0/0	---	0/0
L	192.168.1.14/32	GigabitEthernet0/0	---	0/0
R	192.168.100.0/24	GigabitEthernet0/0	192.168.1.13	120/4
R	192.168.110.0/24	GigabitEthernet0/0	192.168.1.13	120/3
R	192.168.115.0/24	GigabitEthernet0/0	192.168.1.13	120/2
C	192.168.120.0/24	GigabitEthernet0/1	---	0/0
L	192.168.120.1/32	GigabitEthernet0/1	---	0/0

Figure 23. RIPv1 - Routing Table for R5

## RIPv2

The routing table is used to calculate the metric value for ripv2, which provides briefs of the information related to the maximum autonomous system for the routing protocol.

Routing Table for Router0				
Type	Network	Port	Next Hop IP	Metric
C	192.168.1.0/30	GigabitEthernet0/0	---	0/0
L	192.168.1.1/32	GigabitEthernet0/0	---	0/0
C	192.168.2.0/24	GigabitEthernet0/1	---	0/0
L	192.168.2.1/32	GigabitEthernet0/1	---	0/0
R	192.168.3.0/24	GigabitEthernet0/0	192.168.1.2	120/1

Figure 24. RIPv2 - Routing Table for R0

Similarly, the routing table is generated for the router0, as depicted below, to calculate the value of the metrics.

## OSPF

Routing Table for Router0				
Type	Network	Port	Next Hop IP	Metric
C	192.168.1.0/30	GigabitEthernet0/0	---	0/0
L	192.168.1.1/32	GigabitEthernet0/0	---	0/0
C	192.168.2.0/24	GigabitEthernet0/1	---	0/0
L	192.168.2.1/32	GigabitEthernet0/1	---	0/0
O	192.168.3.0/24	GigabitEthernet0/0	192.168.1.2	110/2

Figure 25. OSPF - Routing Table for R0

Metrics value is also calculated for the other network with the help of Cisco:

Routing Table for Router1				
Type	Network	Port	Next Hop IP	Metric
C	192.168.1.0/30	GigabitEthernet0/0	---	0/0
L	192.168.1.2/32	GigabitEthernet0/0	---	0/0
O	192.168.2.0/24	GigabitEthernet0/0	192.168.1.1	110/2
C	192.168.3.0/24	GigabitEthernet0/1	---	0/0
L	192.168.3.1/32	GigabitEthernet0/1	---	0/0

Figure 26. OSPF - Routing Table for R1

## EiGRP

The following screenshot depicts the metric values for the EIGRP routing protocol to analyze the suitable routing protocol for the usage.

Routing Table for R1

Type	Network	Port	Next Hop IP	Metric
C	192.168.1.0/30	GigabitEthernet0/0	---	0/0
L	192.168.1.1/32	GigabitEthernet0/0	---	0/0
D	192.168.1.4/30	GigabitEthernet0/0	192.168.1.2	90/3072
D	192.168.1.8/30	GigabitEthernet0/0	192.168.1.2	90/3328
D	192.168.1.12/30	GigabitEthernet0/0	192.168.1.2	90/3584
C	192.168.100.0/24	GigabitEthernet0/1	---	0/0
L	192.168.100.1/32	GigabitEthernet0/1	---	0/0
D	192.168.110.0/24	GigabitEthernet0/0	192.168.1.2	90/5376
D	192.168.115.0/24	GigabitEthernet0/0	192.168.1.2	90/5632
D	192.168.120.0/24	GigabitEthernet0/0	192.168.1.2	90/6144

Figure 27. EIGRP - Routing Table for R1

Routing table R2, the metrics being assigned to different networks can be viewed from the below screenshot:

Routing Table for R2

Type	Network	Port	Next Hop IP	Metric
C	192.168.1.0/30	GigabitEthernet0/0	---	0/0
L	192.168.1.2/32	GigabitEthernet0/0	---	0/0
C	192.168.1.4/30	GigabitEthernet0/1	---	0/0
L	192.168.1.5/32	GigabitEthernet0/1	---	0/0
D	192.168.1.8/30	GigabitEthernet0/1	192.168.1.6	90/3072
D	192.168.1.12/30	GigabitEthernet0/1	192.168.1.6	90/3328
D	192.168.100.0/24	GigabitEthernet0/0	192.168.1.1	90/5376
C	192.168.110.0/24	GigabitEthernet0/2	---	0/0
L	192.168.110.1/32	GigabitEthernet0/2	---	0/0
D	192.168.115.0/24	GigabitEthernet0/1	192.168.1.6	90/5376
D	192.168.120.0/24	GigabitEthernet0/1	192.168.1.6	90/5888

Figure 28. EIGRP - Routing Table for R2

Metrics of the R3 router device can be viewed by the screenshot and illustrated interface's networks being used for sending the information to the destination end.

Routing Table for R3

Type	Network	Port	Next Hop IP	Metric
D	192.168.1.0/30	GigabitEthernet0/0	192.168.1.5	90/3072
C	192.168.1.4/30	GigabitEthernet0/0	---	0/0
L	192.168.1.6/32	GigabitEthernet0/0	---	0/0
C	192.168.1.8/30	GigabitEthernet0/1	---	0/0
L	192.168.1.9/32	GigabitEthernet0/1	---	0/0
D	192.168.1.12/30	GigabitEthernet0/1	192.168.1.10	90/3072
D	192.168.100.0/24	GigabitEthernet0/0	192.168.1.5	90/5632
D	192.168.110.0/24	GigabitEthernet0/0	192.168.1.5	90/5376
C	192.168.115.0/24	GigabitEthernet0/2	---	0/0
L	192.168.115.1/32	GigabitEthernet0/2	---	0/0
D	192.168.120.0/24	GigabitEthernet0/1	192.168.1.10	90/5632

Figure 29. EIGRP - Routing Table for R3

For R4, the value of the metrics being used by each interface in this router is extracted by executing the command.

Routing Table for R4

Type	Network	Port	Next Hop IP	Metric
D	192.168.1.0/30	GigabitEthernet0/0	192.168.1.9	90/3328
D	192.168.1.4/30	GigabitEthernet0/0	192.168.1.9	90/3072
C	192.168.1.8/30	GigabitEthernet0/0	---	0/0
L	192.168.1.10/32	GigabitEthernet0/0	---	0/0
C	192.168.1.12/30	GigabitEthernet0/1	---	0/0
L	192.168.1.13/32	GigabitEthernet0/1	---	0/0
D	192.168.100.0/24	GigabitEthernet0/0	192.168.1.9	90/5688
D	192.168.110.0/24	GigabitEthernet0/0	192.168.1.9	90/5632
D	192.168.115.0/24	GigabitEthernet0/0	192.168.1.9	90/5376
D	192.168.120.0/24	GigabitEthernet0/1	192.168.1.14	90/5376

Figure 30. EIGRP - Routing Table for R4

Metrics being used by each network interface can be viewed from the given screenshot. This screenshot includes network address, interface, next HOP address and its metric.

Routing Table for R5

Type	Network	Port	Next Hop IP	Metric
D	192.168.1.0/30	GigabitEthernet0/0	192.168.1.13	90/3584
D	192.168.1.4/30	GigabitEthernet0/0	192.168.1.13	90/3328
D	192.168.1.8/30	GigabitEthernet0/0	192.168.1.13	90/3072
C	192.168.1.12/30	GigabitEthernet0/0	---	0/0
L	192.168.1.14/32	GigabitEthernet0/0	---	0/0
D	192.168.100.0/24	GigabitEthernet0/0	192.168.1.13	90/6144
D	192.168.110.0/24	GigabitEthernet0/0	192.168.1.13	90/5888
D	192.168.115.0/24	GigabitEthernet0/0	192.168.1.13	90/5632
C	192.168.120.0/24	GigabitEthernet0/1	---	0/0
L	192.168.120.1/32	GigabitEthernet0/1	---	0/0

Figure 31. EIGRP - Routing Table for R5

## 5 COMPARISON RESULTS:

In the Cisco packet tracer, the different RPSGS configurations are performed on the same network and analyzed the metric. To find the best suitable routing protocol, one needs to view the highest prefix value has with the routing protocol. The following table depicts that EIGRP has the highest

prefix value due to which routing protocol EIGRP is considered to be best. One of the main reasons for obtaining the highest prefix value for EIGRP is that this protocol is mostly used for Cisco-based devices because it does not provide any support to other vendor-devices.

Routing protocols under RPSGSs	Metric Values
RIPv1	120/1
RIPv2	120/1
EIGRP	90/5376
OSPF	110/2

Different metrics are used by each routing protocol of RPSGSs to establish communications with their target destinations. All the listed metrics have been used by each routing protocol in the same network to have communication with the destination end. Metric value varies according to network and transfers information to destination whenever needed for the communication with destination end.

Calculation of metrics:

Routing Protocol	Metric	Description / Formulas
RIP	Hop count	It represents a number of router devices that occur in between the packet transmission to reach the destination. There is no formula to calculate metrics because hop count is utilized to find an optimized path to reach the destination.
EIGRP	Bandwidth, delay	Delay and bandwidth are two major metrics considered while calculating the administrative distance to reach the destination. <b>Formula:</b>  <b><math>256 * (\text{Bandwidth} + \text{Delay})</math></b>
OSPF	Cost	OSPF uses cost metrics to optimize the path to reach the destination. <b>Formula:</b>  <b><math>10^8 / \text{bandwidth}</math></b>

## 6 DISCUSSION

---

OSPF is defined as an interior Gateway routing protocol used for distributing the routing information within an autonomous system. OSPF is the most widely used routing protocol in the network of large enterprises and OSPF is based on link-state technology by making the use of the SPF algorithm on the basis of which the shortest path can be identified. OSPF works on the SPF algorithm and in this algorithm, Dijkstra Shortest Path First approach has been to identify the shortest path from source to destination (Yee, 2006). The algorithm helps to identify the edge having the smallest distance and the packets must be sent to the identified distance. The cost of OSPF has been calculated by sending the packets across a specific interface and formula for calculating the cost is  $100000000/\text{band width in bps}$  and this formula defined that if the bandwidth is wider, the cost would be lower. This metric can be used to define the efficiency of the proposed approach and based on this metric, the selection of OSPF has been made. OSPF protocol is defined as the autonomous system that can be divided into the number of sections (Yee, 2006). The calculation of the shortest path has been done by using the Dijkstra Shortest Path First approach and by doing this, an effective solution can be provided for the number of issues related to congestion control. As compared to RIP, OSPF, the number of hops can be connected because, in RIP, only the 15 hops can be connected. OSPF handles the network of any length along with Variable Length Subnet Masks (VLSM), but RIP cannot. The most important feature of this protocol that it converges as much faster rate as compared to the other protocols. The most important feature of OSPF is its convergence at a faster rate as compared to RIP protocol, but this feature cannot be effective in the case of small enterprises, but it is very effective in case large networks for a large enterprise. RIP is defined as the standardized vector distance routing protocol that uses the form of distance as the hop count metric. It is also defined as the distance vector that has a very limiting number of hops from the source to destination (Yee, 2006). RIP prevents the number of routing loops and a maximum number of loops that are present in this network is 15 and this can restrict the size of the network. When this protocol was designed, it sends

the full updates every 30 seconds. Routing information protocol can be used for managing the issues related to the delivery of packets from source to destination. RIP has four timers Update Timer, Invalid Timer, Hold-down Timer and Flush Timer. Update timer can define how often the router can send out the routing table. The invalid timer is defined as a timer that indicates how long a router will exist in the corresponding routing table before it has been marked as an invalid router (Yee, 2006). A hold-down timer is defined as a timer that specifies how long the router will route from the receiving updates when the corresponding router is in hold downstate and the default seconds for this approach is 180 seconds. The hold-down timer has the default timer of 180 seconds and the router will go into the hold-down state by the number of reasons like the expiration of an invalid timer, when the update has been received from another router and route went into 16 metrics, which could be unreachable. An update has been received from any other router and the route will go into the higher metric that is currently in use. (Yee, 2006).

In the network, there are different RPSGSs that can be used to enable communication between the devices. EIGRP is a routing protocol that configures the router when Cisco-based devices are configured on the network. The major advantage of being having EIGRP routing protocol is that it is flexible with Cisco based devices and utilized as per the need. This section has discussed the analysis of both the RPSGSs and the reasons to select the EIGRP routing protocol to enable the communication between two ends. For the analysis, Cisco packet tracer software 6.0.1 is used on which the case scenario is developed for the purpose of implementing the different RPSGSs on the network. The analyses of all the RPSGSs have been completed based on metrics that are used for sending the information to the destination. The comparison results show that all the RPSGSs have different metrics and select a path to destination end on the basis of parameters like bandwidth, delay, hop count, etc.

The analyses of all the RPSGSs have been completed based on the metrics used to reach the destination by all the packets. In the RIP routing protocol, 120 network unit is a default administrative distance used by the routing protocol

to reach the destination end. When the metric value in this routing protocol is analyzed, it can be viewed that it has a syntax of 120/A. D used. Hence, the routing interface has different administrative distances and requires to reach the destination by sending the data. Furthermore, the discussion of routing protocol analysis for other networks has been done and evaluated the administrative distance being used by each interface to reach the destination end. OSPF is also a suitable routing protocol used for providing the communication process to transfer information to the destination. In this routing protocol, the communication is enabled within the network depends upon areas and the total number of networks available for connectivity. Configuration of OSPF routing protocol on router provides a deterministic path to data packets to travel from its source address to destination address. In case of congestion, an alternate path is chosen by the data packets automatically. Additionally, three tables are created by this routing protocol in order to store all information regarding neighbors, topology used and routing table. In addition, this routing protocol majorly focuses on its area that helps to divide router in an appropriate manner. Area ID used by this routing protocol is similar to the numbers assigned to devices internally. OSPF uses routers such as ABR, ASBR, DR and BDR for segmenting the network. The administrative distance of this routing the protocol is fixed 110, and the output results display the total number of distances that have been covered by the packets to reach the destination end. In the last, routing protocol EIGRP is discussed that provides the communication between two ends based upon the autonomous system. The default autonomous system of this routing protocol is 90. The hop count of this protocol is also evaluated as 3328 and it varies according to the interface being used for transferring the information to the destination. Based on our analysis, EIGRP is a suitable routing protocol for the network that uses Cisco devices because it is based upon this routing protocol. According to the analysis, it can be said that this routing protocol is reliable with the Cisco device, and increases the lifetime of devices. There are more advantages of being using the EIGRP routing protocol for providing the communication of two end networks. A reliable connection is formed, which means the connection can not be denied access to the

destination, which resulted in being successful communication of two end devices. On the comparison of all the RPSGSs, the administrative distance is considered as the common parameter being used for the communication stability testing.

## **7 CRITICAL REFLECTION ON THE RESEARCH PROCESS UNDERTAKEN.**

---

In this approach, we compared the number of protocols in order to identify the best-suited protocol for managing the issues related to congestion control. The shortest path between the source and the destination was identified by the protocol to send the packet from the source to the destination. In this approach, we used comparative analysis, which was performed on the basis of various metrics of the protocols. The issues related to poor quality of network can be handled by implementing the efficient routing protocol. OSPF is the most efficient routing protocol that can be used to transfer the packet from source to destination.

### **7.1 CONTRIBUTION**

The major contribution of this research was its practical implementations. In this research, logical analysis and software simulations were used to analyze RPSGSs. We presented the literature, research methodology, routing set up and architecture. We demonstrated that RPSGSs could be set up in real scenarios and could be effective for smart systems. The live scenario related to any organization could be simulated and results could be useful to let decision-makers know the benefits of such deployment and understand. The implementations of protocols in a live scenario could be done in order to understand performance evaluation and identify potential drawbacks. The literature of this research could represent the current state of the art related to the RPSGSs, which could be used to route the information from one network to another. This simulation-based analysis used in this research helped to evaluate network performance for smart green systems. Despite there were a number of protocols that could use to handle the congestion over the network, OSPF was the most frequently used protocol. By using this protocol, the more efficient quality of services could be provided to the users of the network.

## 7.2 FUTURE WORK

The future plans of this research will include using the effective tools to perform large-scale simulations, and a number of protocols can be compared to justify the better performance outputs of our research. In addition, these protocols can be implemented in the life scenario so that the real-life threats can be evaluated. The reliability of the research can be increased by including the real-time scenario and the use of this approach help to enhance the knowledge related to the best protocol that can be used for making the communication between the mobile nodes.

## Acknowledgment

This work is partly supported by VC Research (VCR 0000047).

## 8 REFERENCES

1. Al-khdour, T., & Baroudi, U. (2007). An Entropy-Based Throughput Metric for Fairly Evaluating WSN Routing Protocols. *2007 IEEE International Conference On Network Protocols*. DOI: 10.1109/icnp.2007.4375872
2. Chaudhry, S., Al-Khwildi, A., Casey, Y., Aldelou, H., & Al-Raweshidy, H. WiMob Proactive and Reactive Routing Protocol Simulation Comparison. *2006 2Nd International Conference On Information & Communication Technologies*. DOI: 10.1109/ictta.2006.1684843
3. Masruroh, S., Fiade, A., Iman, M., & Amelia. (2017). Performance evaluation of routing protocol RIPv2, OSPF, EIGRP with BGP. *2017 International Conference On Innovative And Creative Information Technology (Icitech)*. DOI: 10.1109/innocit.2017.8319134
4. Parvathi, P. (2012). Comparative analysis of CBRP, AODV, DSDV routing protocols in mobile Ad-hoc networks. *2012 International Conference On Computing, Communication And Applications*. DOI: 10.1109/iccca.2012.6179145
5. Yuanyuan Yang, Jianchao Wang, & Min Yang. (2008). A Service-Centric Multicast Architecture and Routing Protocol. *IEEE Transactions On Parallel And Distributed Systems, 19(1)*, 35-51. DOI: 10.1109/tpds.2007.70711
6. YUANYUAN YANG, JIANCHAO WANG, & MIN YANG. (2008). A SERVICE-CENTRIC MULTICAST ARCHITECTURE AND ROUTING PROTOCOL. *IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, 19(1)*, 35-51. DOI: 10.1109/TPDS.2007.70711
7. Parvathi, P. (2012). Comparative analysis of CBRP, AODV, DSDV routing protocols in mobile Ad-hoc networks. *2012 International Conference On Computing, Communication And Applications*. DOI: 10.1109/iccca.2012.6179145
8. Gnanambigai, J., Rengarajan, N., & Anbukkarasi, K. (2013). Q-Leach: An energy efficient cluster based routing protocol for Wireless Sensor Networks. *2013 7Th International Conference On Intelligent Systems And Control (ISCO)*. doi: 10.1109/isco.2013.6481179
9. Bobalo, J. *International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET), 2010* (2nd ed.).
10. Guo, Y., Wang, Q., Huang, H., Tan, W., & Zhang, G. (2007). The Research and Design of Routing Protocols of Wireless Sensor Network in Coal Mine Data Acquisition. *2007 International Conference On Information Acquisition*. doi: 10.1109/icia.2007.4295690

11. Dey, G., Ahmed, M., & Ahmmed, K. (2015). Performance analysis and redistribution among RIPv2, EIGRP & OSPF Routing Protocol. *2015 International Conference On Computer And Information Engineering (ICCIE)*. doi: 10.1109/ccie.2015.7399308
12. Jayakumar, M., Ramya Shanthi Rekha, N., & Bharathi, B. (2015). A comparative study on RIP and OSPF protocols. *2015 International Conference On Innovations In Information, Embedded And Communication Systems (ICIIECS)*. DOI: 10.1109/iciiecs.2015.7193275
13. Krishnan, Y., & Shobha, G. (2013). Performance analysis of OSPF and EIGRP routing protocols for greener internetworking. *2013 International Conference On Green High Performance Computing (ICGHPC)*. DOI: 10.1109/icghpc.2013.6533929
14. Masruroh, S., Fiade, A., Iman, M., & Amelia. (2017). Performance evaluation of routing protocol RIPv2, OSPF, EIGRP with BGP. *2017 International Conference On Innovative And Creative Information Technology (Icitech)*. DOI: 10.1109/innocit.2017.8319134
15. Ming-Hao, W. (2014). The Security Analysis and Attacks Detection of OSPF Routing Protocol. *2014 7Th International Conference On Intelligent Computation Technology And Automation*. DOI: 10.1109/icit.2014.200
16. Yee, J. (2006). On the Internet routing protocol Enhanced Interior Gateway Routing Protocol: is it optimal?. *International Transactions In Operational Research*, 13(3), 177-194. DOI: 10.1111/j.1475-3995.2006.00543.x
17. Alweimine, A., Bamaarouf, O., Rachadi, A., & Ez-Zahraouy, H. (2019). Local routing protocols performance for computer virus elimination in complex networks. *Physica A: Statistical Mechanics And Its Applications*, 536, 120984. DOI: 10.1016/j.physa.2019.04.220
18. Chai, Y., & Zeng, X. (2019). Regional condition-aware hybrid routing protocol for hybrid wireless mesh network. *Computer Networks*, 148, 120-128. DOI: 10.1016/j.comnet.2018.11.008
19. Liu, J., Wang, Q., He, C., Jaffrès-Runser, K., Xu, Y., Li, Z., & Xu, Y. (2020). QMR: Q-learning based Multi-objective optimization Routing protocol for Flying Ad Hoc Networks. *Computer Communications*, 150, 304-316. DOI: 10.1016/j.comcom.2019.11.011
20. Sheghdara, M., & Hassine, J. (2020). Automatic retrieval and analysis of high availability scenarios from system execution traces: A case study on hot standby router protocol. *Journal Of Systems And Software*, 161, 110490. DOI: 10.1016/j.jss.2019.110490
21. Yang, X., Chen, Q., Chen, C., & Zhao, J. (2018). Improved ZRP Routing Protocol Based on Clustering. *Procedia Computer Science*, 131, 992-1000. DOI: 10.1016/j.procs.2018.04.242
22. Zemrane, H., Baddi, Y., & Hasbi, A. (2019). Mobile AdHoc networks for Intelligent Transportation System: Comparative Analysis of the Routing protocols. *Procedia Computer Science*, 160, 758-765. DOI: 10.1016/j.procs.2019.11.014

