VOL. 14, NO. 17, SEPTEMBER 2019 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

PERFOMANCE ANALYSIS OF INTERIOR AND EXTERIOR ROUTING PROTOCOLS

Jayaprabhath M. V. G., Sridhar Kartheek M., Rahul Varma C., and Ravikumar C. V.
School of Electronics Engineering, Vellore Institute of Technology, Vellore, India
E-Mail: ravikumar.cv@vit.ac.in

ABSTRACT

Dynamic routing protocols play an important role in enterprise networks. For example, if there are two universities and they use different protocols. Then, to establish a connection or communication between them we need to use exterior gateway protocols. If we use redistribution technique, the safety is very less and all the routes get redistributed. So in this paper we are implementing border gateway protocol (both IBGP and EBGP) between the interior gateway protocols. There are several different protocols available, with each having its own advantages and limitations. Protocols can be described and compared on the basis of where they operate and how they operate. Routing protocols play an important role in the field of networks today. There are two types of dynamic routing protocols. Interior Gateway Protocols (IGPs) and Exterior Gateway Protocols (EGPs). IGPs such as RIP (Routing Information Protocol) and OSPF (Open Shortest Path First) are used for routing within an Autonomous system (AS) whereas EGP is used to exchange the routing information between the autonomous systems. In this paper we have implemented and connected different protocols using BGP (IBGP and EBGP) without using redistribution technique by using GNS3 Software.

Keywords: IGPs, EGPs, RIP, OSPF, BGPs, IBGP, EBGP, AS.

INTRODUCTION

Before you analyze the behavior of individual routing protocols, you can group similar protocols together. You can group them in several different ways. One option is to group them based on whether protocols operate within or between AS. An AS represents a collection of network devices under a common administrator. Typical examples of an AS are an internal network of an enterprise or a network infrastructure of an internet service provider. You can divide routing protocols based on whether they exchange routes within an AS or between different AS.

Interior gateway protocols: These are used within the organization, and exchange routes within an AS. They can support small, medium-sized, and large organizations, but their scalability has its limits. The protocols can offer very fast convergence, and basic functionality is easy to configure. The most commonly used IGPs in enterprises are EIGRP, OSPF, and RIP (rarely used). IS-IS is commonly found within the service provider internal network.

Exterior gateway protocols: These take care of exchanging routes between different AS, BGP is the only EGP that is used today. The main capability of BGP is to exchange a huge number of routes between different AS that are part of the Internet.

ROUTING INFORMATION PROTOCOL

RIP is an interior gateway protocol that is used in smaller networks. It is a distance vector routing protocol that uses hop count as a routing metric. There are three versions of RIP: RIPv1, RIPv2, and RIPng. RIPv1 and RIPv2 route in IPv4 networks. RIPng routes in IPv6 networks. RIP is standardized IGP routing protocol that works in a mixed-vendor router environment. It is one of the easiest routing protocols to configure, making it a good choice for small networks.

- Distance vector protocol
- Metric is hop count

RIP is a distance vector protocol that uses hop count as the metric. If a device has two paths to the destination network, the path with fewer hops will be chosen as the path to forward traffic. If a network is 16 or more hops away, the router considers it unreachable. RIP exists in three versions: RIPv1, RIPv2, and RIPng. RIPv1 is a classful routing protocol that was replaced by RIPv2, which is a classless routing protocol. Classless routing protocols can be considered second generation because they are designed to address some of the limitations of the earlier classful routing protocols. A serious limitation in a classful network environment is that the subnet mask is not exchanged during the routing update process, thus requiring that the same subnet mask be used on all subnetworks within the same major network. RIPv1 is considered a legacy, obsolete protocol. RIPng operates much like RIPv2. Both protocols use UDP as the transport layer protocol and both use a multicast addressto exchange updates (RIPv1 uses broadcast). Because both protocols are classless, it means that they support VLSM. Both protocols use hop count as the metric. The administrative distance (trustworthiness of the routing source) is 120 in both cases. With both protocols, updates are being propagated throughout the network every 30 seconds to make sure that a change occurs in the network. Also, both protocols support authentication. There are two major differences between RIPv2 and RIPng. RIPv2 advertises routes for IPv4 and uses IPv4 for transport. RIPng advertises routes for IPv6 and uses IPv6 for transport. Also, the configuration of RIPng is quite different when compared to RIPv2 configuration.

ENHANCED INTERIOR GATEWAY ROUTING PROTOCOL

EIGRP is an advanced distance vector routing protocol, designed by Cisco. Basic configuration is simple and easy to understand, so it is commonly used in smaller networks. Its advanced features are it provides rapid convergence, higher scalability and supports for multiple routed protocols, fulfills requirements in complex network environments. EIGRP supports IPv4 and IPv6. Although standard EIGRP configuration between IPv4 and IPv6 differs, it can be unified using the newly introduced EIGRP configuration mode. EIGRP was developed as an enhanced version of the older IGRP and has many characteristics of the advanced interior gateway protocols, such as high-speed convergence, partial updates and the ability to have multiple network layer protocols. The first step in configuring EIGRP is to establish EIGRP neighbor relationships over the various interface types. To know how these relationships have been properly formed and how parameters like hello and hold timers, different Wide Area Network technologies influence on the session establishment. EIGRP uses a composite metric to calculate the best path to the destination. Metric weights or K-values determine which components are to be used for the metric calculation. Bandwidth and delay are used by default. Reliability and load can optionally be used but are not recommended. MTU (maximum transmission unit) is included in the update but is not used for the metric calculation.

EIGRP uses a composite metric to determine the best path to the destination. To find metric we need below parameters

Bandwidth: The least value of the bandwidth for all links between the router, which computes the metric, and the destination.

Delay: The cumulative delay is obtained as the sum of values of all delays for all links between the source and destination.

Reliability: The worst reliability between source and destination, which is based on keepalives (this message is delivered every 60 seconds by default to check that connection is stable or not).

Load: The worst load on the link between the source and the destination, load is selected based on the packet rate and the bandwidth of the interface.

Metric = [(KI * bandwidth + [(K2 * bandwidth) / (256 load)] + K3 * delay) * K5 / (K4 + reliability)] * 256

If K4 and K5 values are set to the default values, which are 0, the quotient K5 / (K4 + reliability) is not used i.e. it is set to 1.

The formula thus effectively reduces to:

Metric = (Kl * bandwidth + [(K2 * bandwidth) / (256 load)] + K3 * delay) 256.If you take into account the default Kl to K3 values, Kl = K3 = 1, and K2 - 0, the formula reduces to

Metric=(bandwidth+delay)*256

Note that changing the K values is not recommended.

EIGRP uses hello, update, query, reply, and acknowledgment packets. EIGRP uses a composite metric, which is, by default, based on bandwidth and delay. The Reported distance (RD) is a metric value reported by the neighboring router. The Feasible distance (FD) is the lowest distance to a destination from the perspective of the local router. An alternative path must satisfy the feasibility condition to become a feasible successor. The RD of an alternative path must be less than the FD.

OPEN SHORTEST PATH FIRST

OSPF, it is one of the most commonly used interior gateway protocols in IP networking. OSPF has two layer area hierarchy: Backbone area or transit area (area O): Two principal requirements for the backbone area are that it must connect to all other non-backbone areas, and it must be always contiguous it is not allowed to be split. Generally, end users are not found within a backbone area. Non-backbone area: The primary function of this area is to connect end users and resources. Non-backbone areas are usually set up according to functional or geographical groupings. Traffic between different non-backbone areas must always pass through the backbone area. At a high level, OSPF operation can be divided into three distinct steps. In the first step, the OSPF router must discover all OSPF-speaking neighbor routers on directly connected interfaces. To establish neighbor relationships, OSPF uses small hello packets, similar to EIGRP. Before two routers on directly connected links become OSPF neighbors, they must agree on certain parameters specified in the hello packet. Once two OSPF routers establish neighbor adjacency, the second step can begin. In the second step of the OSPF operation, the router exchanges link-state information that describes the topology of the network within an OSPF area. Link-state information, conveyed in the form of LSAs, is flooded through an OSPF area until all routers have identical entries stored in their link state database. LSAs received from the neighbor are used in the local router to build the picture of the network topology from the perspective of the local router. Information communicated in LSAs includes each router's identifier (router ID), interface, IP address, mask, subnet, and a list of all routers reachable on each interface. Once the link state database on all routers within an area are synchronized and have identical database entries, the last step can begin best path calculation. To calculate the best path to a given destination, OSPF uses SPF(short path first) or Dijkstra's algorithm. The SPF algorithm analyzes and compares all possible paths to the destination from the local router's perspective and selects the one with the smallest metric (cost). This path, together with the next hop and the outgoing interface to the destination, is then a candidate to be placed in the routing table. OSPF has some restrictions when multiple areas are configured in an OSPF AS. If more than one area is configured, one of these areas has to be area 0.It is called the backbone area. When designing networks, it is good practice to start with the first layer as 0 or core layer which becomes area 0 and then expand into other areas later. So, while configuring ospf we have chosen ospf area as a 0.The backbone has to be at the center of all other areas, and other areas have to be connected to the backbone. The main reason for that is

ospf expects all areas to inject routing information into the backbone area which distributes that particular information to other areas. The important requirement for the backbone area is that it must be contiguous i.e, splitting up area 0 is not allowed. ospf routers progress through seven states

Down: No active neighbor is detected
INIT: Hello packet is received
2-WAY: Own router ID is received hello
Exstart: Master and slave roles to be determined
Exchange: Database description packets are sent
Loading: Exchange of Link state request
Full: Neighbors are fully adjacent

BORDER GATEWAY PROTOCOL

Border Gateway Protocol (BGP) is a standard exterior gateway protocol designed to exchange routing and sending information among the autonomous systems (AS) on the Internet. The protocol is often classified as a path vector protocol but is sometimes also called as distance vector routing protocol. The Border Gateway Protocol (BGP) is the routing protocol of the Internet, used to route traffic across the Internet. For this reason it is a very important protocol. Border Gateway Protocol (BGP) is an inter domain routing protocol which uses path vector routing. Path vector routing proved to be useful for inter domain routing. In path vector routing we also assume that there is one node in each autonomous system that acts on behalf of the entire autonomous system.

The speaker node in an autonomous system creates a routing

Table and advertises it to speaker node in the neighboring AS. Only speaker node can communicate with each other which is not possible in distance vector routing.

BGP SESSIONS: The exchange of the routing information between two routers by using BGP take place in a session. BGP

Sessions are also known as semi-permanent connection as whenever a TCP connection is created for BGP it lasts for a long time until something unusual happens. BGP utilizes TCP for reliable transfer of its packets, on port 179.

Use BGP in these cases:

An AS is multihomed. An AS is a transit AS.

Inter-AS routing policy must be manipulated.

Do not use BGP in these cases:

The AS is single-homed. Memory and processor resources are insufficient. There is insufficient understanding of BGP route filtering and unavailable path selection. When there is no need to manipulate your routing policy.

TYPES OF BGP

EBGP (External Border Gateway Protocol): Betweenthe autonomous systems. It has hop restriction by default it assumes 1.

When BGP is running between the routers in different autonomous systems, it is called EBGP. By default, routers that are running EBGP must be directly connected to each other. Session between BGP peers with different AS numbers by default and must be directly connected. Peer receives and advertises prefixes to and from remote AS. An EBGP neighbor is a router outside a home AS. An enterprise network can have a connection to one or several ISPs, and the ISPs themselves might be connected to several other ISPs, as well. For each such connection between different autonomous systems, there is an EBGP session that is required between EBGP neighboring routers. EBGP neighbors are directly connected and they establish a TCP session before exchanging BGP updates. When multiple different autonomous systems are connected to each other and an enterprise network is connected to multiple ISPs, BGP runs between the ISPs and the enterprise network. Requirements for establishing an EBGP neighbor relationship include the following:

DifferentAS number: EBGP neighbors must reside in different autonomous systems to be able to form an EBGP relationship.

Defined neighbors: A TCP session must be established before starting BGP routing update exchanges.

Reachability: EBGP neighbors must be directly connected, by default and IP addresses on that link must be reachable inside each AS.

IBGP (Interior Border Gateway Protocol): Within theAutonomous system there is no hop restriction. BGP between routers within the same AS is called IBGP.IBGP runs within an AS to exchange BGP information so that all BGP speakers have the same BGP routing information about outside autonomous systems. BGP session operates between peers in the same AS. Neighbor must be defined on both sides. Neighbors must be able to reach each other.

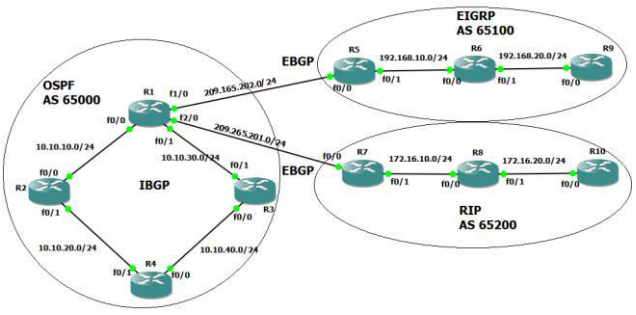
Requirements for establishing an IBGP neighbor relationship include the following:

Same AS number: IBGP neighbors must reside in the same AS to be able to form an IBGP relationship.

Defined neighbors: A TCP session must be established between neighbors before exchanging BGP routing updates.

Reachability: IBGP neighbors must be reachable. Therefore, IGP typically runs inside an AS.

IMPLEMENTATION OF VARIOUS PROTOCOLS



The scenario covers the implementation of OSPF, RIP, EIGRP, EBGP and IBGP. Our whole network is

divided into 3 autonomous systems (AS). AS 65000 is having four set routers R1, R2, R3 and R4. AS 65100 is having set of three routers R5, R6 and R9.The another is AS 65200 having set of three routers R7, R8 and R10. Every router has loopback IP address for example router R1 has id of 1.1.1.1, similarly for router R2 has 2.2.2.2 but expect R10. Router (R10) loopback IP address is 20.20.20.20.

CONFIGURATIONS

CONFIGURATION AT R1:

```
R1 # configure terminal
R1 (config)#interface Loopback0
R1(config-if)# ip address 1.1.1.1 255.255.255.255
R1 (config) # interface FastEthernet0/0
R1 (config-if) # ip address 10.10.10.2  255.255.255.0
R1 (config-if) # no shutdown
R1 (config-if) # exit
R1 (config) # interface FastEthernet1/0
R1 (config-if) # ip address 209.165.202.129 255.255.255.0
R1 (config-if) # no shutdown
R1 (config-if) # exit
R1 (config) # interface FastEthernet0/1
R1 (config-if) # ip address 10.10.30.1  255.255.255.0
R1 (config-if) # no shutdown
R1 (config-if) # exit
R1 (config) # interface FastEthernet2/0
R1(conig-if)# ip address 209.165.201.29 255.255.255.0
R1(config-if)# no shutdown
R1 (config-if) #exit
```

Similarly configure for R2, R3, R4,R5,R6,R7,R8,R9,R10.

Now Configuring RIP on R7,R8,R10:

```
R7(config)#router
R7(config-router)#network 172.16.10.0
R7(config-router)#network 7.0.0.0
R8(config)#router RIP
R8(config-router)#network 172.16.10.0
R8(config-router)#network 172.16.20.0
R8(config-router)#network 8.0.0.0
R10 config)#router RIP
R10(config-router)#network 172.16.20.0
R10(config-router)#network 20.0.0.0
```

Now Configuring OSPF on R1,R2,R3,R4

```
R1(config)#router OSPF 1
R1(config-router)#network 10.10.10.0 0.0.0.255 area 0
R1(config-router)#network 10.10.20.0 0.0.0.255 area 0
R1(config-router)#network 10.10.30.0 0.0.0.255 area 0
R1(config-router)#network 10.10.40.0 0.0.0.255 area 0
R1(config-router)#network 1.1.1.1 0.0.0.0 area 0
```

Similarly configure router R2,R3,R4

Now Configuring EIGRP on R5,R6,R9

```
R5(config)#router EIGRP 1
R5(config-router)#network 5.0.0.0
R5(config_router)#network 192.168.10.0
```

Similarly configure router R6 and R9 according to their networks.

RIP, OSPF and EIGRP work on intra-domain so to connect through different autonomous system we require Exterior Broader Gateway Routing (E-BGP) because an EBGP neighbor relationship is established between the routers in different AS. Without using redistribution technique we have to use IBGP protocol because an IBGP neighbor relationship is established between routers in the same AS.

CONFIGURING BGP ON R1:

```
R1(config)#router bgp 65000
R1(config-router)#network 1.1.1.1 mask 255.255.255.255
R1(config-router)#network 10.10.10.0 mask
255.255.255.0
R1(config-router)#network 10.10.30.0 mask
255.255.255.0
R1(config-router)#network 209.165.201.0
R1(config-router)#network 209.165.202.0
R1(config-router)#neighbor 2.2.2.2 remote-as 65000
R1(config-router)#neighbor 2.2.2.2 update-source
Loopback0
R1(config-router)#neighbor 2.2.2.2 next-hop-self
R1(config-router)#neighbor 3.3.3.3 remote-as 65000
R1(config-router)#neighbor 3.3.3.3 update-source
Loopback0
R1(config-router)#neighbor 3.3.3.3 next-hop-self
R1(config-router)#neighbor 4.4.4.4 remote-as 65000
R1(config-router)#neighbor 4.4.4.4 update-source
Loopback0
R1(config-router)#neighbor 4.4.4.4 next-hop-self
R1(config-router)#neighbor 5.5.5.5 remote-as 65100
R1(config-router)#neighbor 5.5.5.5 ebgp-multihop 255
R1(config-router)#neighbor 5.5.5.5 update-source
Loopback0
R1(config-router)#neighbor 7.7.7.7 remote-as 65200
R1(config-router)#neighbor 7.7.7.7 ebgp-multihop 255
R1(config-router)#neighbor 7.7.7.7 update-source
Loopback0
R1(config-router)#exit
R1(config)#
R1(config)#ip route 5.5.5.5 255.255.255.255
209.165.202.130
R1(config)#ip route 7.7.7.7 255.255.255.255
209.165.201.30
R1(config)#exit
```

CONFIGURATION OF BGP ON R7:

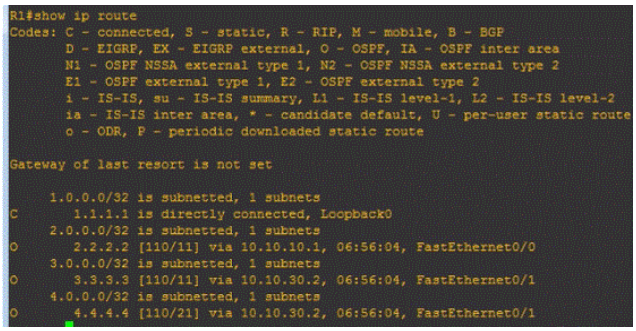
```
R7(config)#router bgp 65200
R7(config-router)#network 7.7.7.7 mask 255.255.255.255
R7(config-router)#network 172.16.10.0 mask
255.255.255.0
R7(config-router)#network 209.165.201.0
R7(config-router)#network209.165.20 mask
255.255.255.255
R7(config-router)#neighbor 1.1.1.1 remote-as 65000
R7(config-router)#neighbor 1.1.1.1 ebgp-multihop 255
R7(config-router)#neighbor 1.1.1.1 update-source
Loopback0
R7(config-router)#neighbor 8.8.8.8 remote-as 65200
R7(config-router)#neighbor 8.8.8.8 update-source
Loopback0
R7(config-router)#neighbor 8.8.8.8 next-hop-self
```

R7(config-router)#neighbor 20.20.20.20 remote-as 65200
R7(config-router)#neighbor 20.20.20.20 remote-as 65200
R7(config-router)#neighbor20.20.20.20update-source Loopback0
R7(config-router)#neighbor 20.20.20.20 next-hop-self
R7(config-router)#exit
R7(config)#ip route 1.1.1.1 255.255.255.255 209.165.201.29 2 R7(config)#exit

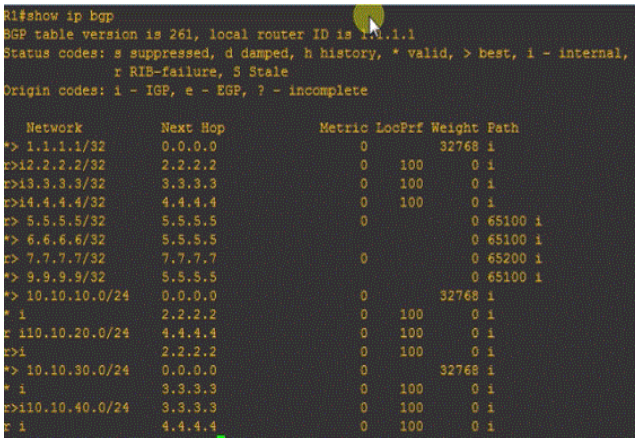
CONFIGURATION BGP ON R5:

R5(config)#router bgp 65100
R5(config-router)#network 5.5.5.5 mask 255.255.255.255
R5(config-router)#network 192.168.10.0
R5(config-router)#network 209.165.202.0
R5(config-router)#neighbor 1.1.1.1 remote-as 65000
R5(config-router)#neighbor 1.1.1.1 ebgp-multihop 255
R5(config-router)#neighbor 1.1.1.1 update-source Loopback0
R5(config-router)#neighbor 6.6.6.6 remote-as 65100
R5(config-router)#neighbor 6.6.6.6 update-source Loopback0
R5(config-router)#neighbor 6.6.6.6 next-hop-self
R5(config-router)#neighbor 9.9.9.9 remote-as 65100
R5(config-router)#neighbor 9.9.9.9 update-source Loopback0
R5(config-router)#neighbor 9.9.9.9 next-hop-self
R5(config-router)#exit
R5(config)#ip route1.1.1.1 255.255.255.255 209.165.202.129
R5(config)#exit

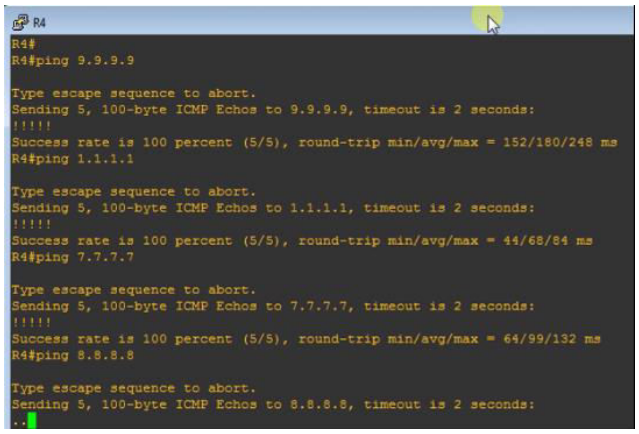
OUTPUT:



Show ip route - It displays the routing table; it gives complete information about the routes in the router.



The above picture gives the information of border gateway protocol in router (R1) “show ip bgp” shows which route is the valid route or best route for sending information.



The above picture is an example of ping from router (R4) to the other routers and time taken for sending and receiving the acknowledgement. For an example in the picture “ping 9.9.9.9” is the loopback ip address of router (R9). We got 100% success rate.

Time taken is min/avg/max = 152ms/180ms/248/ms.

CONCLUSIONS

By using the redistribution technique every route gets redistributed. It is not safe, when we want only particular routes to communicate between BGP and IGP using IBGP technique. To form IBGP we require IGP protocol to run TCP session. Here we implemented RIP, OSPF and EIGRP in different autonomous system. To get communicated with this protocol we should use Exterior border gateway protocol and Interior border gateway protocol. BGP uses TCP as the transport mechanism, which provides reliable connection oriented delivery. The output (pictures) shows that how the router R1 is connected to different routers by means of RIP, OSPF, EIGRP and BGP.

REFERENCES

[1] http://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/8606-redist.html

[2] http://computernetworkingnotes.com/routing-static-dynamics-rip-ospf-igrp-eigrp/basic-router-configurations.html

[3] Implementation and Comparison of Performance of Various EGPs and IGPs with Traffic Management.

[4] B. A. Forouzan. 2007. Data Communications and Networking, 4thEdition, McGraw Hill.

[5] C. V. Ravikumar, Kala Praveen Bagadi. 2016. Performance analysis of HSRP in provisioning Layer-3 Gateway Redundancy for Corporate Networks. Indian Journalof Science and Technology. 9(20): 89851.

[6] C. V. Ravi kumar, Kala Praveen Bagadi. 2016. Performance analysis of IPv4 to IPv6 Transition Methods. Indian Journal of Science and Technology. 9(20): 90005.

[7] Kanaparthy Rama Bramham & Ravi Kumar C. V. 2015. Comparison and Optimization of Layer2 and Multilayer switch protocols to implement converged and reliable network. International Journal of Applied Engineering and Research. 10(8): 20139-20154.

[8] C. V. Ravikumar, Kala Praveen Bagadi. 2016. Robust Neural network based multiuser detector in MC-CDMA mMAI mitigation. Indian Journalof Science and Technology. 9(30): 95994.

[9] C. V. Ravikumar, Kala Praveen Bagadi. 2017. Receiver design using artificial Neural Network for signal detection in MC-CDMA system. International Journal of Intelligent Engineering & Systems.

[10] C. V. Ravikumar, Saranya K. C. 2016. Implementing Mobile adhoc Networks with improved AODV protocol. International Journal of Applied Engineering and Research. 11(9): 6284-6289.