VOL. 17, NO. 6, MARCH 2022 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

COMPARATIVE ANALYSIS OF IGP PROTOCOLS OF AN ENTERPRISE NETWORK

Gowtham Sri Vishwesh, Rithvik S, Likhitha Reddy K and Ravikumar CV
Vellore Institute of Technology, SENSE, India
E-Mail: ravikumar.cv@vit.ac.in

ABSTRACT

This paper shows an usage of IPV4 & IPV6 logical addressing for an Enterprise Network Various configuration's done in this network are Access Control Lists (ACL's) on Edge Router of an Organization Network connected to ISP router to block some services from our Network to outside internet. NAT is done in edge router of an organization to secure organizations private IP addresses. Virtual LAN's (VLAN's) is done in each switch of an organization which provides layer2 security. The best interior gateway protocol can be found in an Enterprise network by comparative analysis.

Keywords: IPV4, IPV6, access control lists, Virtual LAN, network address translation, OSPF, EIGRP.

1. INTRODUCTION

In our daily life large-scale networks plays a very crucial role. Many of these networks runs through a complex routing protocol. The task of a routing protocol is to determine the communication channels that can pass messages from source to the destination node in a network. The objective of an efficient routing protocol is to determine the best path between source and destination node, and also cost effective plays an important role [1]. With a routing protocol, communication between nodes can be performed on several different networks.

Along with the increasingly rapid development of technology, the growth of communication networks is also getting larger. In modern communication networks such as the Internet network, a dynamic routing protocol, Open Short Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP) can be used in a network organisation. These two Routing Protocols has their merits and demerits. The determination and selection of routing protocols depends on several parameters such as how quickly the protocol adapts to changes in the network and convergence time. There are two factors that determine convergence time. The time it takes to recognize a failure and the time that it takes to select a new route. There may or may not be differences between OSPF and EIGRP in detection and as mentioned there are things like BFD(Bi-directional forwarding detection) that can help improve time to recognize the failure. In terms of time to select a new route, if there is a feasible successor then EIGRP is faster than OSPF, if there is no feasible successor then it is hard to know which is faster and it may very well depend on the topology of the network. The administrative distance for OSPF is lesser than EIGRP. OSPF is the best choice for larger networks and RIP can be limited to small networks [2].The packets sent by EIGRP are smaller than that sent by OSPF because the data transmission process performed by the OSPF is more often than EIGRP [3].

2. INTERIOR GATEWAY PROTOCOL

An Interior Gateway Protocol (IGP) is a type of protocol used for exchanging routing information between gateways with in an autonomous system.

2.1 Enhanced Interior Gateway Protocol (EIGRP)

Enhanced interior gateway routing protocol belongs to advanced distance vector routing protocol. It uses distance vector and link state algorithm to find the best path. It is easy to design and configure. It uses delay, bandwidth, load and reliability as metric. At whatever point new router is included into the system EIGRP takes order of three stages neighbour disclosure, topology trade and choosing router. EIGRP routers sent a hello packet in order to evaluate the router parameter to determine whether the router should become neighbour. In topology exchange the routers broadcasts the topology information's regularly so that the changes in the topology can be updated automatically. Each router analyses the topology table for choosing the route based on the cost metric. The route with lowest cost value is selected as a best route. EIGRP is beneficial for large enterprise networks because it consumes fewer resources compared to that of link-state IGPs. It is the one of the best distance-vector IGPs available [4]. EIGRP uses RTP (Reliable Transport Protocol) to update the topology information's. It sends back the information which is not received by the neighbours. The EIGRP metric has two inputs, bandwidth and delay. EIGRP avoids congested links as the metric takes into account least bandwidth. The delay part in the metric the makes sure that the routing is done through a route with a less connection. If the router receives multiple paths with the *same* administrative distance and *cost*, load-*balancing* can occur which is known as Equal-metric load balancing in EIGRP [5].

2.3. Open Shortest Path First protocol (OSPF)

Open Shortest Path First Protocol is a link state routingprotocol. It is an open standard protocol. Metric used is cost value. Lower the cost, higher will be the speed. By default cost value is 10^ (8)/bandwidth in bits/second. In OSPF name it-self represents that low cost

path is selected. In OSPF configuration, to identify the neighbour's, the routers send and receive OSPF Hello packets. The router checks for its neighbour and if found, it will check for its neighbour's parameters and they will exchange their Link state algorithms, thus they will complete their link state database. The best path to forward the data is estimated by the shortest path algorithm.

Each router consists of a unique identifier. When a router sends Hello packet, it will send as "Hello, my Router-ID is xxx." Router-ID is used to identify the router inside OSPF database. Thus neighbours are identified by their Router-ID.

The SPF algorithm finds all possible paths from the router to the destination. In a network there may be more than one router and decision has to be taken about through. Which router the data has to be sent. Here, the router checks the metric for the briefest way and the first-class path is found. This process is complex [6]. The metric for the router is calculated from the network diagram, router status information.

Cost is the metric used in instance of OSPF protocol. It can be set directly with an interface subcommand or by using the formula, the IOS choose default costs. In this method interface bandwidth is in denominator and reference bandwidth is in numerator. When the interface bandwidth is higher, the calculated OSPF cost will emerge aslower [7].

At the point when the interface cost is lower, there is more possibility for choosing that interface by SPF. The least OSPF cost permitted is 1.

OSPF supports load balancing. A router could load balance the packets on a per-packet basis. The packets are sent in a sequential order. For example, if the router has three OSPF paths of equal-cost, the router will sent one packet through the first route, the next packet through the second route and the next through the third route.

Table-1. Important parameters of OSPF and EIGRP Protocols.

Protocol	OSPF	EIGRP
Convergence time	Fast	Fast
VLSM	Yes	Yes
Bandwidth usage	Low	Low
Resource usage	High	Low
Multiple path Support	Yes	Yes
Scalability	Yes	Yes
Non-IP Protocol	No	No

3. SECURITY

ACL's and NAT configurations are implemented which provides security to organisation.

3.1 Access Control Lists (ACL's):

ACL is a set of rules which allow or deny specific traffic moving through router controls flow of traffic from one network to other via router. Two steps should be followed while applying ACL's implementation of ACL rules to desired transit router and applying set of rules to desired interface may be inbound or outbound traffic [8]. Total of four rules are implemented in edge router i.e. is R3 of organisation.

a) Permit tcp any host 209.165.201.65 eq www: This Acl rule says that web service is allowed from internet devices to webserver inside organisation.
b) Permit icmp any any echo-reply: Only echo reply is possible and not echo-request for internet devices when ping from our network.
c) Permit tcp any eq www any established: any source to any destination access possible until it is web page access. established keyword above provides extra security from hackers like when they to try to connect to our network by knowing our allowed ports service at firewall
d) permit UDP any host 192.168.35.253 eq domain: permit any host from internet until it is DNS service request

3.2 Network Address Translation (NAT):

Method of translating private IP address to public IP address in order to communicate with internet we must have registered public IP addresses. Nat can be configured on routers, fire walls, and servers. Two types of Nat implemented in paper on edge router i.e. R3 of organisation [9].

a) Static Nat: OnetoOnemappingdonemanually. Every privateaddressneedsoneregisteredpublicIPaddress. IP Nat inside source static 192.168.35.252 209.165.201.65: This command tells web server is known as 209.165.201.65 public IP for internet

b) Dynamic Nat: Oneto Onemappingdoneautomaticallyby Natdevice. Forevery privateI Poneregistered IP. Portaddress translation (dynamic Nat overload): Thousands of privateusers uses ingle public address. Uses port address to differentiate between different Users.

```
ipnatpool r2natpool 209.165.201.66 209.165.201.69 netmask 255.255.255.248
ipnat inside source list 15 pool r2natpool overload
ipnat inside source list 25 pool r2natpool overload
```

The above commands are used to use public IP addresses of range 209.165.201.66-69 when hosts in our network when goes to internet.

4. PROPOSED WORK

The proposed work i.e. network topology of an enterprise network is created in cisco packet tracer software for comparison of which IGP protocol OSPF or EIGRP is best suited for implemented topology. Topology consists of total five routers r1,r2,r3,r4,r5.all inter-vlan routing configurations using sub interface is done in r1

Gig0/0 interface which is connected to lan switch of an organisation for VLAN's communication within LAN network redundancy vlan configurations are also done in r3 if in case r2 link fails or r1 goes down. DHCP is configured in r1 for configuration of hosts in vlan's 15,25 so hosts gets IP address ,default-gateway, DNS server etc. and also redundancy DHCP configurations done in r3.

Total of four VLAN's are created in LAN network i.e. research vlan (vlan15), development vlan (vlan25), management vlan(vlan88) used for administration purpose to make any changes in topology host pc admin is used for administration purpose servers vlan (vlan35) to which webserver and DNS server are connected. Total of 6 servers are used namely DNS server-1 to resolve r2, r3ip address for internet devices and dnsserver-2 for resolving IP address for devices inside lan network and webservers inside lan and on internet are used for web access of devices inside lan and devices on internet.ipv6server used for testing and web access of ipv6 host on a lan network to which r3 is connected.

Dynamic routing protocols OSPF and EIGRP are implemented in r1,r2,r3,r5 routers.ipv4 routing OSPFv2 implemented on r1,r2,r3,r5 and ipv6 routing OSPFv3 implemented on r2,r3.between r2 and r4 i.e. edge router of an organisation and isp router default routing is done for communication purpose and in r2 passive interface is done so that OSPF advertisements are not send to isp router. Security is provided for organisation using access control lists and network address translation.

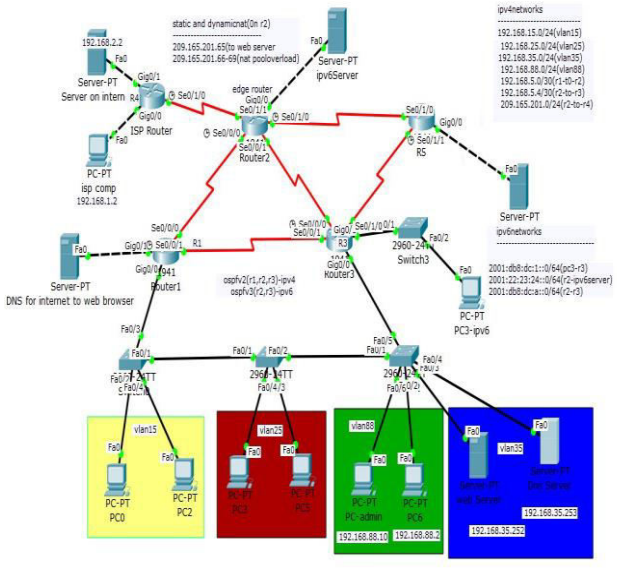

Figure-1. Design topology for analysis.

Table-2. Topology IP addresses (VLAN's).

Node	Interface	IP Address
Vlan15 Hosts	Fa0/2, Fa0/4	Dynamic DHCP
Vlan25 Hosts	Fa0/3,Fa0/4	Dynamic DHCP
Vlan88 Hosts	Fa0/2	192.168.88.10
	Fa0/6	192.168.88.2
Vlan35 Hosts	Fa0/3	192.168.35.252
	Fa0/4	192.168.35.253

Table-3. Topology IP addresses (router r1, r3).

Node	Interface	IP Address
Router r1	g0/0.15	192.168.15.1
	g0/0.25	192.168.25.1
	g0/0.88	192.168.88.1
	g0/0.35	192.168.35.1
	g0/1	192.168.3.1
	s0/0/1	17.1.1.1
	s0/0/0	192.168.5.1
Router r3	g0/0.15	192.168.15.3
	g0/0.25	192.168.25.3
	g0/0.88	192.168.88.3
	g0/0.35	192.168.35.3
	g0/1	2001:DB8:DC:A::2
	s0/0/0	192.168.5.6
	s0/1/0	11.1.1.1
	S0/0/1	17.1.1.2

Table-4. Topology IP addresses (router r2, r4, r5).

Node	Interface	IP Address
Router r2	s0/0/0	192.168.5.2
	s0/1/1	209.165.201.66
	s0/0/1	192.168.5.5
	s0/1/0	10.1.1.1
	g0/0	2001:22:23:24::2
Router r4	g0/0	192.168.1.1
	g0/1	192.168.2.1
	s0/1/0	209.165.201.1
Router r5	s0/1/0	10.1.1.2
	s0/1/1	11.1.1.2
	g0/0	12.1.1.1

5. EXAMING THE SECURITY CONFIGURATION

5.1 Verification of ACL Configurations

```
Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time=61ms TTL=125
Request timed out.
Reply from 192.168.2.2: bytes=32 time=14ms TTL=125
Reply from 192.168.2.2: bytes=32 time=16ms TTL=125
```

Figure-2. Ping from our network to internet.

```
C:\>ping 209.165.201.65

Pinging 209.165.201.65 with 32 bytes of data:

Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.
```

Figure-3. Ping from internet to our network.

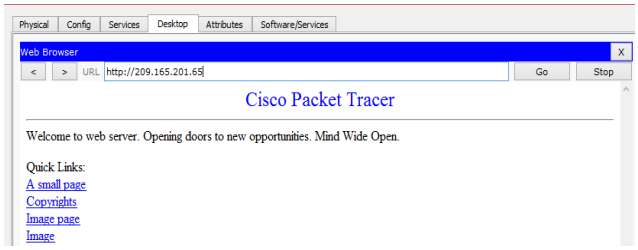

Figure-4. Web service request from internet to our Web server:

5.2 Verification of NAT Configurations:

5.2.1 Static NAT

Resolves 209.165.201.65 to 192.168.35.252

```
r1#sh ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  209.165.201.65    192.168.35.252     ---                ---
tcp 209.165.201.65:80  192.168.35.252:80  192.168.2.2:1025   192.168.2.2:1025
tcp 209.165.201.65:80  192.168.35.252:80  192.168.2.2:1026   192.168.2.2:1026
```

5.2.2 Port address translations

Resolves our network pc's IP address to 209.165.201.66-209.165.201.69 and pings outside internet

```
r1#sh ip nat translations
Pro  Inside global     Inside local       Outside local
Outside global
icmp 209.165.201.66:5  192.168.15.7:5     192.168.2.2:5
192.168.2.2:5
icmp 209.165.201.66:6  192.168.15.7:6     192.168.2.2:6
192.168.2.2:6
icmp 209.165.201.66:7  192.168.15.7:7     192.168.2.2:7
192.168.2.2:7
icmp 209.165.201.66:8  192.168.15.7:8     192.168.2.2:8
192.168.2.2:8
---  209.165.201.65    192.168.35.252     ---
tcp 209.165.201.65:80  192.168.35.252:80  192.168.2.2:1025
192.168.2.2:1025
tcp 209.165.201.65:80  192.168.35.252:80  192.168.2.2:1026
192.168.2.2:1026
```

6. ANALYSIS

6.1 End to End delay

End to end delay is time taken to sent packets from source to destination. Packets are sent from source to destination, the average time taken for transmission in each protocol is calculated and is mentioned in Table-7 and Table-8.

Table-7. average end to end delay for OSPF.

S. No	Source	Destination	Average end to end delay time(ms)
1.	pc0	FTP server	77,288.00
		DNS server for intenet devices	0
		DNS server for internal devices	1.00
		Inernet Web server	3.00
		Inernal Web server	0
2.	pc3	FTP server	73,562.00
2.	pc3	DNS server for internet devices	4.00
		DNS server for internal devices	0
		Internet Web server	4.00
		Internal Web server	0

Table-8. Average end to end delay for EIGRP.

S. No	Source	Destination	Average end to end delay time (ms)
1.	pc0	FTP server	80,400.00
		DNS server for internet devices	0
		DNS server for internal devices	0
		Internet Web server	3.00
		Internal Web server	2.00
2.	pc3	FTP server	75,288.00
		DNS server for internet devices	1.00
		DNS server for internal devices	5.00
		Internet Web server	11.00
		Internal Web server	2.00

By comparing two Tables 7, 8 of OSPF and EIGRP for average end to end delay calculation OSPF has less end to end delay from source to destination for maximum of services like ftp for file download, web server for web page access for both internal and internet devices, DNS service for resolving IP address for both internal and internet devices so OSPF is best suited for best end to end time delay results for the implemented network topology.

6.2 Convergence Time

A source sends packets whose datagram size is 50 and 100. During the dispatch of a sequence of packets, a path gets failed leading to packets dropping, and ends only when a new update converges to all routers. Average Convergence time is calculated by multiplying packet loss with each average end to end delay and heavily depends on protocol's reaction speed to a network change. Comparison is made when OSPF and EIGRP redundancy is created in the topology at the edge router of the organisation which is connected to internet total of three links are created from our routers to Three ports of our edge router are s0/0/0,s0/1/0,s0/0/1.when no port is blocked analysis done which link is best out of three for both EIGRP and OSPF. Best port is s0/0/1 EIGRP and s0/0/0 for OSPF when s0/0/1 is blocked. EIGRP uses s0/0/0 and OSPF uses s0/0/1 when s0/0/0 is blocked. Convergence time for OSPF is better because EIGRP has no feasible successor so it has to send query to each path to find new route if link fails which is proved from below tables 9, 10, 11 results.

Table-9. Convergence time for OSPF and EIGRP with ACL's and NAT when no port is blocked.

S. No	protocol	No. of packets sent	Packet loss	Average convergence time(ms)
1.	OSPF	50	9	54.0
		100	10	40.0
2.	EIGRP	50	8	56.0
		100	10	80.0

Table-10. Convergence time for OSPF and EIGRP with ACL's and NAT when port S0/0/0 in OSPF and s0/0/1 in EIGRP is blocked.

S. No	protocol	No. of packets sent	Packet loss	Average convergence time(ms)
1.	OSPF	50	6	30.0
		100	8	48.0
2.	EIGRP	50	9	36.0
		100	8	56.0

Table-11. Convergence time for OSPF and EIGRP without ACL's and NAT when port S0/0/0 in OSPF and s0/0/1 in EIGRP is blocked.

S. No	protocol	No. of packets sent	Packet loss	Average convergence time(ms)
1.	OSPF	50	4	12.0
		100	5	20.0
2.	EIGRP	50	2	12.0
		100	7	42.0

From above Tables 9, 10, 11 packet loss and convergence time is more when acls and nat are implemented and also convergence time is least for OSPF when compared to EIGRP for the implemented topology.

7. CONCLUSIONS

From above results we can say that all above configurations are verified successfully .acls used in above network act as firewall between our network and internet Nat is used to translate private IP to public address when connected to internet .vlanprovide layer 2 security and it does not allow vlan's to communicate until specific configurations are done. All comparisons are done between OSPF and EIGRP protocols and redundancy links are also created for our network to ensure proper communication with internet.

REFERENCES

[1] Ioan Fitigau Gavril Toderean. 2013. Network performance evaluation for RIP, OSPF, EIGRP protocols. 2013 International Conference on electronics, Computers and Artificial Intelligence (ECAI). June, 1-4

[2] L.D. Circiumarescu, G. Predusca, N. Angelescu, D. Puchianu. 2015. Comparativ analysis of protocol RIP, OSPF, EIGRP and IGRP for service Video conferencing, E-mail, FTP, HTTP. CSC20, CSCS20, The 20th International Conference on Control Systems and Computer Science 27-29 May 2015, Faculty of Automatic Control and Computers, University Politehnica of Bucharest, Romania. pp. 584-589.

[3] Y. Navaneeth Krishna, G Shobha. 2013. Performance analysis of OSPF and EIGRP routing protocols for greener internetworking.2013 IEEE International Conference on Green High Performance Computing (ICGHPC). March, 1-4.

[4] Wijaya C. 2011. Performance analysis of dynamic routing protocol EIGRP and OSPF in IP v4 and IPv6 network. 2011 First International Conferenceon Informatics and Computational Intelligence. 355-360.

[5] Ravi Kumar, C. V. and Kalapraveen B. 2017. MC-CDMA Receiver Design Using Recurrent Neural Networks for Eliminating Multiple Access Interference and Non–linear Distortion. International Journal of Communication systems, Wiley. 30(16).

[6] Vladimir Vesely, Jan Bloudicek; Ondrej Ryšavý. 2014. Enhanced Interior Gateway routing protocol for OMNET++. International Conference on Simulation and modelling.

[7] Uyless Black. 2000. IP routing protocols: RIP, OSPF, BGP, PNNI and Cisco routing protocols, Prentice Hall Professional, New Jersey, USA.

[8] Ravi Kumar, C. V. and Kalapraveen B. 2017. Receiver design using Artificial Neural Networks for signal detection in MC-CDMA System. International Journal of Intelligent Engineering & Systems, 10(3), pp. 66–74.

[9] Baker F. 1994. OSPF Fundamentals. LAN Magazine. 9(13): 71-78

[10] DJ. Garcia-Alfaro, N. Boulahia-Cuppens, and F. Cuppens. 2008. Complete analysis of configuration rules to guarantee reliable network security policies. International Journal of Information Security. 7(2): 103-122.

[11] D. Miles and M. Townsley eds. 2009. Layer2- Aware NAT. IETF Internet draft, work in progress.

[12] Ravikumar CV Kalapraveen B. 2016. Performance analysis of HSRP in layer3 for corporate networks. Indian Journal of Science and Technology. 9(20).

[13] Yash, Ravi Kumar, C.V. Venugopal P. 2020. A smart wheelchair for healthcare monitoring system. 11(4): 22-29. International Journal of Electrical Engineering and Technology

[14] Md. Imaudin, Ravi Kumar C.V. and Kalapraveen B. 2020. Signal detection in MC-CDMA system using

ELM receiver to mitigate MAI and non-linear distrortion. Asian Research Publishing Network (ARPN)

[15] Jitish Ravi Kumar, C. V. Kalapraveeen B. 2020. LPWAN technologies for IoT deployment. 11(3): 285-296. International Journal of Electrical Engineering and Technology

[16] Jayaprabath Ravi Kumar C. V. and Rahul Varma C. 2019. Performance analysis of interior and exterior routing protocols. Asian Research Publishing Network (ARPN).

[17] Ravikumar C. V. and Kalapraveen B. 2019. Design of Multilayer Perceptron Receiver for MC-CDMA system to Mitigate Multiple Access Interference and Non-linear Distortion. Neural Computing & Applications. 31(S-2):1263-1273.

[18] Ravikumar C. V. Saranya K.C. 2016. Improoving Interference alignment of Gaussian MIMO x channel and Gaussian MIMO z channel. International Journal of Applied Engineering and Research. 11(9).

[19] Ravikumar C. V. 2016. Kalapraveenbagadi.-Robust Neural Network based multiuser detector in MC-CDMA for multiple access mitigation. Indian Journal of Science & Technology. 9(30).

[20] Ravikumar C. V., Saranya K.C. 2016. Implementing Mobile ad-hoc networks with AODV Protocol. International Journal of Applied Engineering and Research. 11(9).

[21] Dhanamjayulu and Ravikumar CV. 2019. Real-Time Implementation of a 31 level Asymmetrical cascaded multilevel inverter for dynamic loads, DOI 10.1109/ACCESS.2019.2909831