Performance Evaluation of The QUAGGA Router

Vincent Omollo, Dr. K. Langat, Dr. S. Musyoki, P. Nyakomita, P. Otieno

Department of Telecommunication and Information Engineering, Jomo Kenyatta University of Agriculture and Technology.

Abstract

Quagga router is an open source routing software. It implements routing protocols such as routing Information Protocol (RIP) and Open Shortest Path First (OSPF). Unlike the traditional router design where all the configuration data of the router were found on a single file, this router maintains crucial information in different configuration files. In this paper, we investigate the performance of this router in a conventional real network. Our approach included installing this router in Linux, configure it and finally connect it to a real network using switches. Then performance parameters such as throughput, average delay and jitter were determined. Its resistance against common router attacks such as HTTP Configuration Arbitrary Administrative Access Vulnerability was also investigated. It was observed that Quagga's performance in terms of the identified parameters was better compared to the conventional routers such as Cisco and Juniper tested under similar conditions. This can be attributed to the ease with which the router can be customized to support various protocols and services. The router resisted the above attack and can therefore be regarded as being more secure compared to its counterparts such as Cisco. It is therefore suggested as the most appropriate mechanism of selecting the best routes from the source to the destination.

Key words: *Routing, protocols, open source throughput, average delay, jitter.*

I. INTRODUCTION

Complex and redundant networks such as the internet require different routing policies from those typically found on local area networks (LAN). The routers will know all the paths that lead to the target [1]. It provides implementations of Open Shortest Path First version 2 (OSPFv2), Open Shortest Path First version 3 (OSPFv3), Routing Information Protocol version 1 and 2 (RIP v1/v2), and Border Gateway Protocol (BGP) [2]. It is normally implemented in UNIX platforms such as FreeBSD, Linux, Solaris and NetBSD. Configuring routers manually is confusing and often leads to mistakes. On the internet, the situation if even worse. The remedy for this is to distribute dynamically changing route information automatically. The web world community has developed special routing protocols for this purpose. These routing protocols are normally found on router such as Cisco and Juniper. Quagga router on the other hand gives information technology (IT) administrators the opportunity of taking part in the world's largest group of routers, with a Linux computer [1]. The Quagga project originated with the Zebra routing daemon by Kunihiro Ishiguro.

A computer that has Quagga installed in it acts as a dedicated router. However, the Quagga software does not handle the routing as this is still under the control of the underlying operating system (OS) kernel. With this router, the computer exchanges routing information with other network devices using routing protocols [3]. It then uses this information to update the kernel routing table so that data gets to the required destination.

The internet is made up of many connected subnets. The packets transmitted in these networks need to find the best path between source and destination. A network of routers that are managed by a team of system administrators is known as an autonomous system (AS). The routing protocols are categorized into protocols which distribute the routes within an autonomous system. These systems can also be subdivided which means that many routers can manage many routes. There are also protocols that distribute the routes between these autonomous systems. The protocols within an AS are known as Interior Gateway Protocols (IGP), while those outside an AS are referred to as Exterior Gateway Protocols (EGPS). Examples of IGPs are RIP, OSPF and Intermediate System to Intermediate System (IS-IS). The only IGP that is in existence is the BGP. Within a given organization, an IGP will be used for routing while the BGP will be used to handle routing between providers or between providers and institutions [1]. RIP was developed in 1988 and is considered outdated hence not frequently used in the internet. OSPF introduces a hierarchy of areas to partition the network. It is also possible for one area to have multiple networks. The single stage hierarchy begins at area 0, which is the backbone area. Each further area must be connected through a router although it need not exist physically in a production environment.

Routers utilize multicasts to exchange data through the local area networks. This multicast IP address is 224.0.0.5 [1]. This address can be authenticated using message digest version 5 (MD5) for security reasons. The routers normally send the HELLO messages to enable them discover their neighbours. After sending these messages, they then send Link State Announcements (LSAs). The LSAs normally contain such information as the routers' routing table, areas and interface bandwidths. All the network routers then employ this piece of data to update their respective routing table. When two links lead to a similar network, the path that has higher data rates will be the one to be used. When two paths have equal network access speeds, then it is the responsibility of the network administrator to manually add a weighting value to the configuration. This is then reflected in the LSA data. If a given link fails, then the router on the alternative path handles network traffic for that link.

In this paper, the Quagga was investigated against network performance parameters. These parameters include throughput, average delay and delay. We also analyzed this router against some of the common router vulnerabilities such as HTTP Configuration Arbitrary Administrative Access Vulnerability (HCAAAV) attacks. A comparison is then made against the values obtained in [5] to determine how well the Quagga router performs.

II. METHODOLOGY

To analyze the Quagga router against the parameters mentioned above, a series of experiments were performed. The router was configured as explained in [4]. Figures 1, 2 and 3 show these configurations.

```
!
 hostname Zebra
password omollo
enable password omollo
!
interface eth0
description LINK TO ETH0
link-detect
ip address 192.168.1.1/24
ipv6 nd suppress-ra
!
 interface lo
description LINK TO LO
 link-detect
ip address 192.168.10.1/24
!
interface wlan0
 description LINK TO WLAN
link-detect
ip address 192.168.20.1/24
ipv6 nd suppress-ra
!
line vty
!
 end
```

Figure 1: Configuration of the Zebra daemon

In addition to these configurations, the daemons configuration file and the debian files were also configures as shown in Figures 4 and 5. The daemon configuration controls the active routing protocol [4]. The debian configuration file on the other hand controls the interfaces through which the device will be remotely accessed. For security reasons, it is a good idea to change the default local host address as the interface through which the various daemons could be accessed. This has been implemented in Figure 5 for daemons bgd, zebra, ripd and ospfd. These are the daemons that were used.

```
!
 hostname protocol_rip
 password omollo
 enable password omollo
 !
router rip
network 192.168.1.0/24
network 192.168.10.0/24
network 192.168.20.0/24
!
line vty
!
end
```

Figure 2: Configuration of the RIP daemon

```
!
hostname protocol_ospf
password omollo
 enable password omollo
!
 interface eth0 ! interface lo
 !
interface wlan0
!
router ospf
network 192.168.1.0/24 area 0.0.0.5
network 192.168.10.0/24 area 0.0.0.5
 network 192.168.20.0/24 area 0.0.0.5

 !
 line vty
 !
end
```

Figure 3: Configuration of the OSPF daemon

```
!
zebra=yes
bgpd=yes
ospfd=yes
ospf6d=yes
ripd=yes
ripngd=yes
isisd=yes
babeld=yes
!
```

Figure 4: Configuration of the Daemons file

```
vtysh_enable=yes
zebra_options=" --daemon -A 192.168.1.1 -P 2601 -u quagga -g quagga --keep_kernel --retain"
bgpd_options=" --daemon -A 192.168.10.1 -P 2605 -u quagga -g quagga --retain -p 179"
ospfd_options=" --daemon -A 192.168.20.1 -P 2604 -u quagga -g quagga"
ospf6d_options=" --daemon -A ::1 -P 2606 -u quagga -g quagga"
ripd_options=" --daemon -A 192.168.30.1 -P 2602 -u quagga -g quagga --retain"
ripngd_options=" --daemon -A ::1 -P 2603 -u quagga -g quagga --retain"
isisd_options=" --daemon -A 127.0.0.1 -P 2608 -u quagga -g quagga"
babeld_options=" --daemon -A 127.0.0.1 -P 2609 -u quagga -g quagga"
```

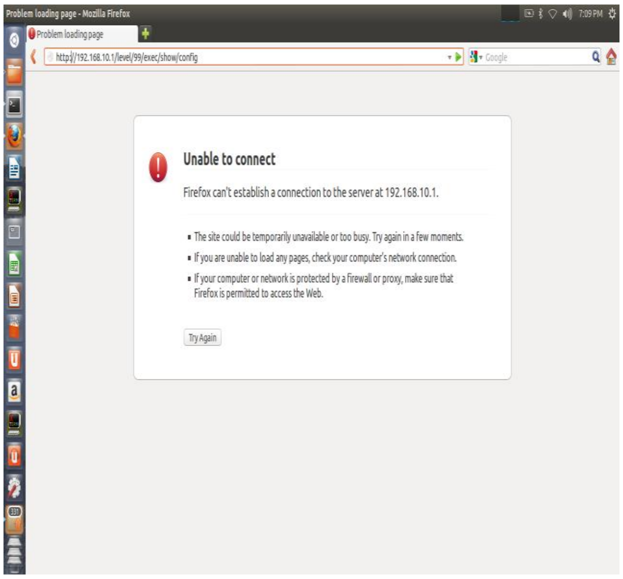
Figure 5: Configuration of the Debian file

III. RESULTS AND DISCUSSIONS

In this section, we examine and explain on some of the results obtained by adopting the above experiments.

HCAAAV Evaluation

This is one of the vulnerabilities that affect most of the Cisco routers. It is easily found by most network scanners and is very easy to exploit. In most cases, it results into full remote administrative control of the affected router. A web browser is used and one only needs to point at the vulnerable router in the uniform resource locator (URL) [4]. As shown in Figure 6 below, the response was a connection problem. Therefore the famous intrusion mechanism that works for Cisco routers is not generic, and cannot apply to other network routers or devices.


Problem loading page - Mozilla Firefox
7:09 PM
Problem loading page
http://192.168.10.1/level/99/exec/show/config
Google
Try Again

Unable to connect

Firefox can't establish a connection to the server at 192.168.10.1.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

Figure 6: Evaluation of Quagga against HCAAAV attack

Throughput

This is the number of packets effectively transferred in a computer network. It is measured in terms of packets per second or per time slot [4]. Figure 7 below the measured throughput values. As can seen, the throughput values oscillated between 2 Mbps and 2.5 Mbps.

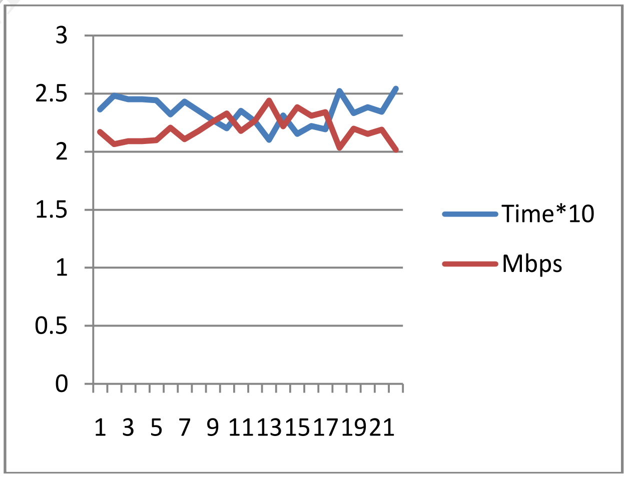


Figure 7: Evaluation of Quagga throughput

Average delay

This is also known as latency. It represents the time taken by a bit of data to travel form the source to the destination. The main sources of delay can be grouped into propagation delay, source processing delay, queuing delay, transmission delay and destination processing delay. Figure 8 below shows the average delay values obtained. It can be observed that this value lies between 0.236 and 0.254 milliseconds.

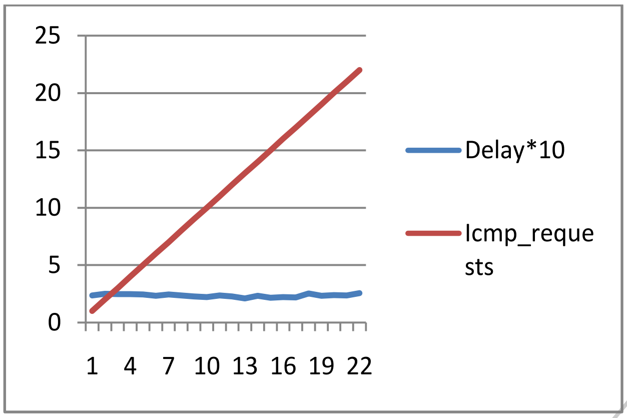


Figure 8: Evaluation of Quagga Average delay

Jitter or delay variation

This can be regarded as the end-to-end delay variation between consecutive packets. Its value is calculated from the end to end delay. Jitter reveals such information as latency in the computer network which is in most cases caused by congestion, route changes and queuing. It determines the performance of the network and indicates how consistent and stable the network is. The values obtained are shown in Figure 9. From the figure, the jitter was found to oscillate between 0.019 and 0.033 milliseconds.

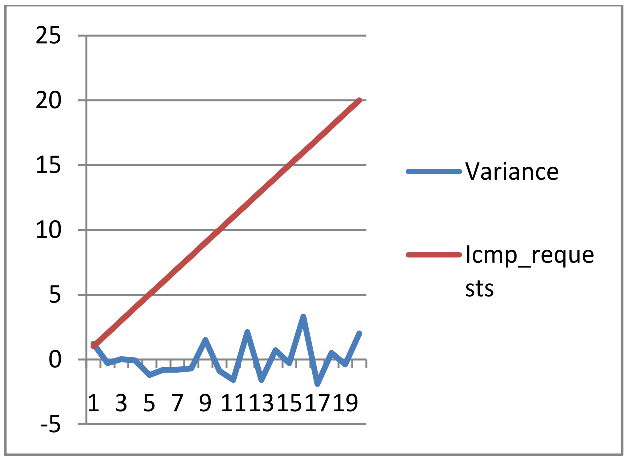


Figure 9: Evaluation of Quagga Jitter

Comparing the results we obtained and the ones obtained in [5], we can see that the Quagga router's performance is well over the other commercially available routers such as Cisco and Juniper.

IV. CONCLUSION

From the results obtained above, it is clear that Quagga is a good option when a network administrator is faced with the decision of selecting the kind of router to implement in a given network. To start with, the router is immune towards the HCAAAV attack, a serious attack that can lead to full control of a Cisco router. Its throughput values were also high and its implementation introduced very minimal network delays. All these coupled with the fact that Quagga router does not need hardware device for its application makes it a nice choice for most network administrators.

References

[1] Konstantin Agouros, “Dynamic Routing in Linux with Quagga ”, Linux New Media USA, LLC, 2013.

[2] Dayphin, Lexort, “Quagga Routing Suite”, 2010.

[3] Kunihiro Ishiguro, “Quagga, A routing software package for TCP/IP networks”, 2013

[4] Vincent Omollo, Dr. Langat, Dr. Musyoki, “Secure LAN Architecture by using routing stack transformation”, 2013.

[5] Zuoning Yin and Matthew Caesar, “ Towards nderstanding Bugs in Open Source Router software”, 2011.