Measure and compare the convergence time of network routing protocols

Marek Bolanowski[1,*], *Tomasz* Byczek[2]

[1]Department of Complex Systems, Faculty of Electrical and Computer Engineering, Rzeszow University of Technology al. Powstańców Warszawy 12, 35-959 Rzeszów, Poland.
[2]tbyczek92@gmail.com, Poland.

Abstract. Currently, IT systems require more and more reliability. It can be guaranteed only by using redundancy both in the connectivity and network devices. The authors attempted to measure the convergence time for EIGRP and OSPF routing protocols after link or network nodes failure. Research have been conducted with the real devices and hardware traffic generator. In case of both protocols, failures have been simulated in various places in the network topology. On this basis, time in which tested protocol restored full connectivity for a specific topology with backup links have been precisely determined. Knowledge of the time required to restore the network after a failure can be useful during designing services based on networks with implemented routing. This can improve a tolerance of connectivity interruptions.

1 Introduction

Reliability is the key to proper work of modern Information and Communications Technology systems. The MTBF (Mean Time Between Failures) value for devices of critical infrastructure are getting longer and the reliability of a network devices (availability) reaches 99,999%. However this level of reliability, in some cases, is still not sufficient enough [1]. The formula of improving network availability by improving the device production process and improving the reliability parameters of network nodes seems to be reaching its limit. Another idea to improve the reliability of computer networks was the use of devices with modular structure for the construction of network nodes. Devices made with that type of architecture have duplicated management and power supply systems. Sometimes redundant switching matrix have also been used [2, 3]. Market's tendencies and customer expectations clearly indicate, the best network model is based both on redundant network devices (in single node) and redundant links[5]. Protocols which can create a single virtual device from a separate devices are used in local network (MC-LAG, Virtual Chasiss)[6]. There are also protocols which are widely used in the creation of redundant connections e.g.: RSTP, MSTP, ERP, etc. The network achieves convergence below 50 ms after a failure in the optimal scenario[7,8]. Such solutions are characteristic for campus or corporate networks with dedicated fibre optical links. As you can see, network reliability is ensured in the second layer

[*] Corresponding author: mb@prz.edu.pl

of ISO/OSI model with switching techniques. Mapping of such convergence mechanisms with layer three protocols is unimaginably expensive, and nearly impossible in some cases. However, routing protocols are widely used and the key element for the authors of this article is to measure the convergence time after a failure for selected routing protocols. In case of a node or link failure, knowledge about time required to restore network connection is essential. It allows to configure the rest of the IT system to tolerate this kind of breaks. This knowledge allows to manage computer system in a holistic way and consider it as a complex system [9,10] and use e.g. advance prediction algorithms[11].

Preliminary research of routing protocols with popular network simulators and emulation programs encountered the following problems:

- Difficulties in mapping correctly links and operating systems of network devices (e.g. small capabilities of heterogeneous environments simulation).
- Some of the advanced configurations of routing protocols algorithms (e.g. OSPF) did not work in simulators, however, worked correctly on physical devices.
- It is not possible to precisely configure all parameters of a given routing protocol available on the devices.
- The problem with the precise representation of the real environment with use of the mathematical models [12].

Therefore, the authors of this article have decided to carry out convergence tests in the real environment of network devices. The following programs were used for preliminary configuration tests: Omnet ++, Riverbed Modeler, PacketTracer. As a part of a preparatory work, the authors chose two most popular protocols for further analysis: EIGRP and OSPF[13,14]. Wider analysis, with larger amount of routing protocols is possible to perform, and such research will be conducted in the future.

2 The architecture of measuring system

A real network device environment located in the laboratory of Department of Complex Systems has been used to perform the measurements. Two groups of devices were used during this work: auxiliary and test ones. Alcatel-Lucent OmniSwitch 6850E switches were used in the first group, while Cisco 2901 and Cisco 2800 routers were used in the second group. The test traffic was generated by JDSU Testpoint TS-170. The hardware traffic generator allowed to perform the exact measurements of lost frames and the convergence time, as well as to define test stream parameters to the fourth layer (ISO/OSI). The core test network was built with Cisco routers. The entire device failure or link failure were simulated on these routers and they will be used to route traffic in the laboratory network. OS6850E switches were used as transit devices to transmit traffic between JDSU generator and routers. They were used to split the stream created by the traffic generator on a fiber optic interface, into a set of outbound streams in copper interfaces. The entire inbound and outbound streams on the switch were duplicated for its error analysis. The dedicated stations analysed them. Two of that switches were used during the tests. Their switching topology will be discussed in the next chapter. Wireshark programme was also used to analyse the traffic. First, the authors planned to use hybrid traffic generation, described in this work[15]. In this approach, the resultant test traffic is a component of the traffic coming from the hardware and software generator as well as the real part of the previously recorded network traffic. Such a network traffic has similar statistic parameters to the network flow in real environment. The initial tests shows that traffic flow which has come only from the hardware generator is sufficient to examine routing protocols convergence time. The use of more complicated flow had no impact on received results.

2.1 System topology

Two test topologies were created to perform the research, one of them to test a multiarea OSPF protocol, another one to test EIGRP protocol.

OSPF protocol. Redundant links between devices and routes were necessary for test network configuration. The network, which was using OSPF routing protocol was divided into areas. Therefore, measurements of new routes propagation and convergence time, are not limited to one area. In this case time of route propagation is related to the place where the failure occurred. Redundant links should have been provided in every place irrespective of the area.

The topology was designed to test an OSPF routes propagation time, while simulating network device's ports failure is located in a different areas. First, port on the device in area 0, which was the core area, was disabled during the tests. The next step was to measure the convergence time for area next to the backbone area. The final measurement tested the convergence time for an area which was not close to the backbone area. Fig. 1 shows the network topology, which was used to perform the measurements.

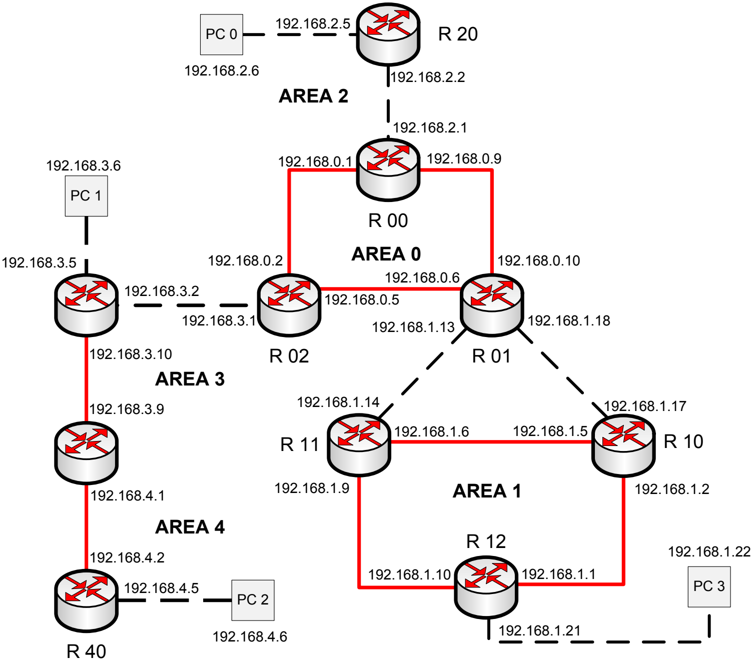

Fig. 1. OSPF protocol measurement topology.

The more complicated network was designed to avoid the need for creation of new networks for each further measurements. Changing of a network point in which frames were sent and received was sufficient to perform another tests. Cisco 2901 devices were mostly used in the design. The amount of devices which was necessary to perform the tests was larger than the held test equipment and that is why Cisco 2800 series were used as the R20 and the R40 devices. Routers with less computing power were used at the edge of the network, because in this places they had less impact on the results. The researches assumed that faults would be simulated in the zero area, the first area and the fourth area, which was set behind the virtual area. Unfortunately, the lack of additional devices forced the modification of the topology for the last measurements. The devices from the first area were used to modify the fourth area. The traffic flow would avoid the first area, so it will would not participate in the new routes propagation. It was possible to use devices with better parameters in the fourth area by eliminating one of the existing area. After performing the modification R40 was replaced with the Cisco 2800 series to 2901. Fig. 2 shows modified network topology for measurements performed for the fourth area.

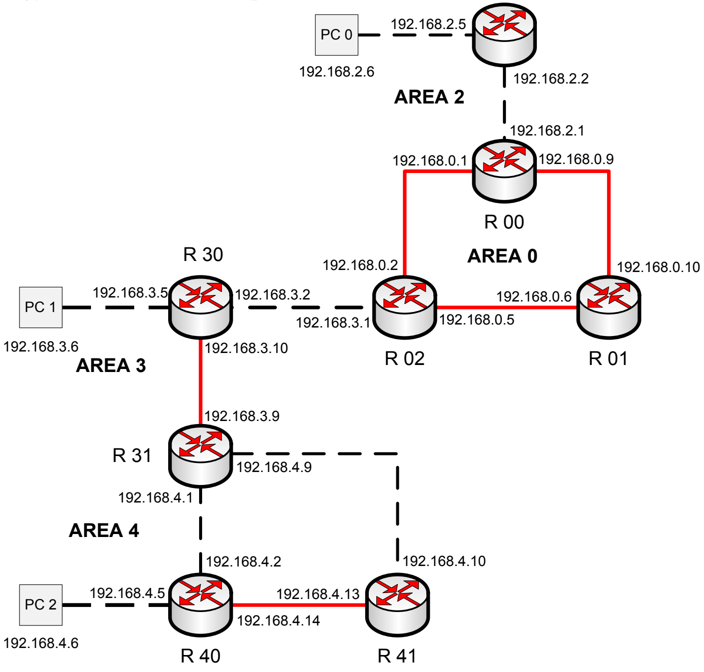

Fig. 2. AREA 4 measurement topology (OSPF protocol).

EIGRP protocol. Another protocol that was tested in this article was EIGRP. OSPF configuration is much more complex. It is not required to use functional areas with EIGRP protocol. That is why the applied topology can be much simpler. Fig. 3 shows the created topology for EIGRP, in which network convergence and routes propagation were tested.

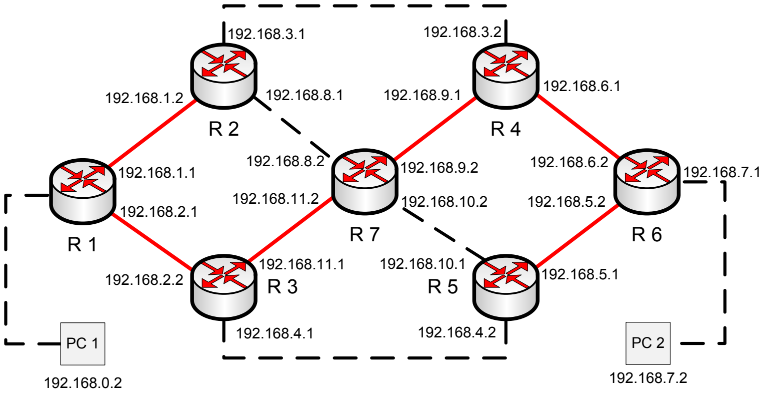

Fig. 3. EIGRP measurement topology.

Seven Cisco 2901 routers were parts of the showed topology. The end devices, which were to send and receive packets were represented by the computers.

JDSU traffic generator. Traffic flow generator was used as two end devices placed in the different endpoints of the network. Traffic was generated by Slot 1 and send to the nearest router, which route it via next nodes to the generator's Slot 2. Slot 2 was configured as the looping traffic device. Sender and recipients' addresses were reversed in every frame, then Slot 2 sent them to the nearest router which routed the frames to the Slot 1.The data were collected by the computer with packet sniffer, which was set between Slot 1 module and the nearest router. Current analysis of collected traffic allowed to determine if frames and packets was sent and received correctly. Generator and computer's connecting schema was showed in fig. 4.

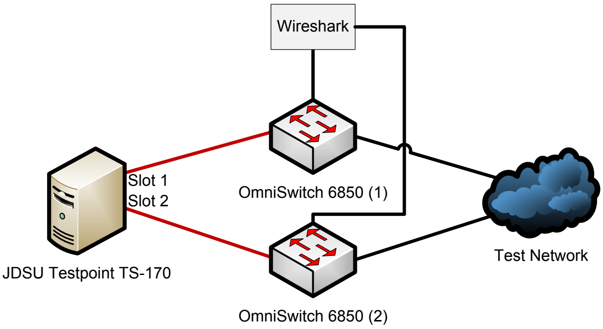

Fig. 4. Generator and computer's (frame collector) connecting schema.

3 Tests and results

The tests in case of both protocols were performed in a similar way. Packets from JDSU generator were send and received simultaneously. During the failure simulation (link disconnection or router shutdown), the routers did not know the route to a specific module (Slot 2 which reflected packets) for some time. Only outbound packets from the generator were registered by the sniffer. Every registered datagram had a time stamp. The value of a time stamp at the start of the each measurement was zero. The difference between the last packet which was returned before the breakdown and the first packet, which was registered after the failure determined the amount of time which network devices needed to learn new routes after the error occurred.

For the OSPF protocol, times were measured in four simulated network failures and then the obtained results were compared. The connection between two routers in the backbone area was dropped during the first test. It was performed by plugging out the used cable in one of the devices. A port failure or another single link connection drop was simulated in this test. The second test was performed in the same way, however, the devices between which connection was dropped were located in none backbone area. Another test was also performed in none backbone area and forcing the selection of a new route was also initiated by disconnecting two devices. However, an entry to the next node, for tested network destination, was already in the router's routing table. This simulation was possible because two interfaces had the same OSPF costs. The final test was the simulation in which the connection was dropped beyond the area adjacent to the backbone area.

Five measurements were carried out for each test. Fig. 5 shows the time needed to get a network convergence for each of the measurement for all of the performed tests.

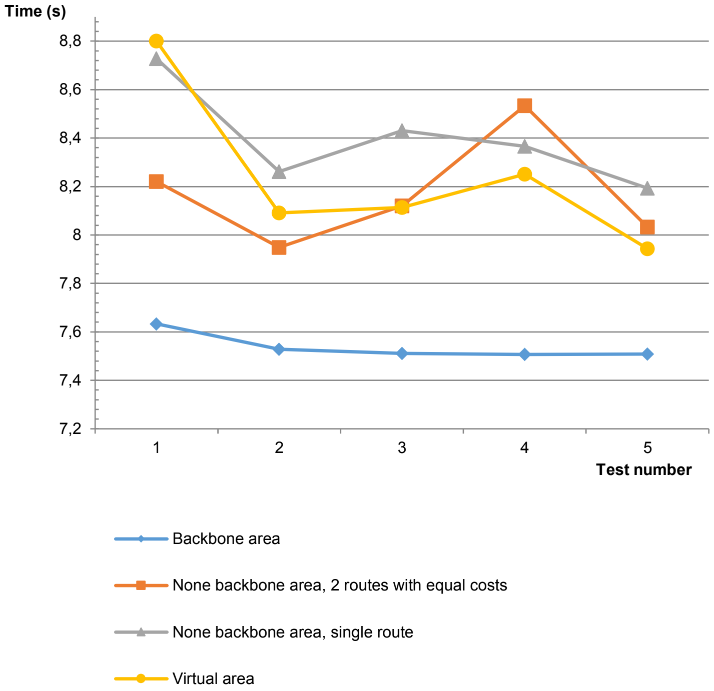

Fig. 5. Summary of measurements for each test for OSPF.

The first test in the fig. 5 which was performed in the backbone area is represented by the blue chart (marked with diamonds). Tests for none backbone area with two routes with equal cost are represented by the orange chart (marked with squares), whereas grey chart (marked with triangles) represents test for the same area, however, with a single route's entrance to the desired subnet in the routing table. The last test in the area which was not next to the backbone area is represented by the yellow chart (marked with dots).

Analysis shows that if the failure occurs in the backbone area, the OSPF protocol would learn and broadcast new route to recover a lost connection in the shortest time. From the protocol topology's point of view, backbone area is located in its centre and is the key to the entire network's proper work. Much higher convergence times can be observed for the rest of the tests, however, the differences between them are not significant. The fig. 6 shows the average convergence time for all of the configurations.

Based on the analysis, we can tell that the best convergence time for none backbone areas during the failures simulation were achieved for two equal routes to the same subnet in the routing table. The device in which the connection loss was initialized had already had an alternate route entry, thereupon switching and propagating new route information to another devices did not take as long as in the other tests. Propagating information and achieving network convergence for failure in the area which was not adjacent to the area 0 was a bit longer. The longest measurement times were achieved for a single route entry in a routing table in a device located in the first area.

EIGRP protocol could not be tested in the same conditions as the OSPF. The differences in the configurations forced changes in the network topology. The redundant network was designed for the Cisco routing protocol, in which various failures could be made. Lack of division into areas simplified the routing implementation, however, it also decreased the amount of performed measurements. The authors decided to perform tests to check whether the failure of a single link is significantly different from the failure of the entire device. In case of a device breakdown, the protocol had to choose the longer route, which could affect the measured propagation time and network convergence. To achieve more reliable results five measurements were performed for each of the EIGRP test (fig. 7.).

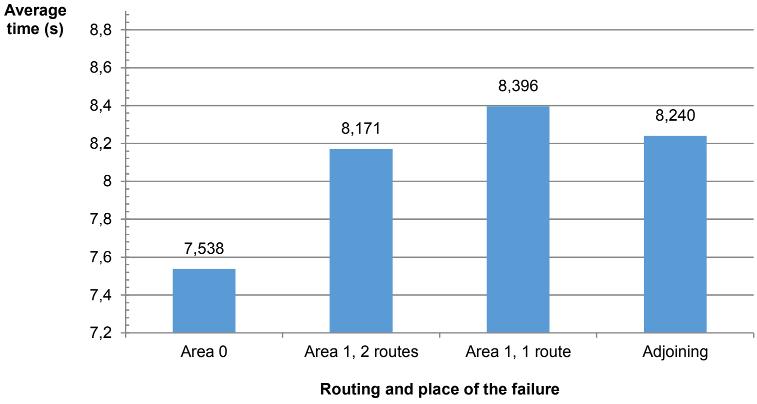

Fig. 6. Average measurements' times for OSPF protocol tests.

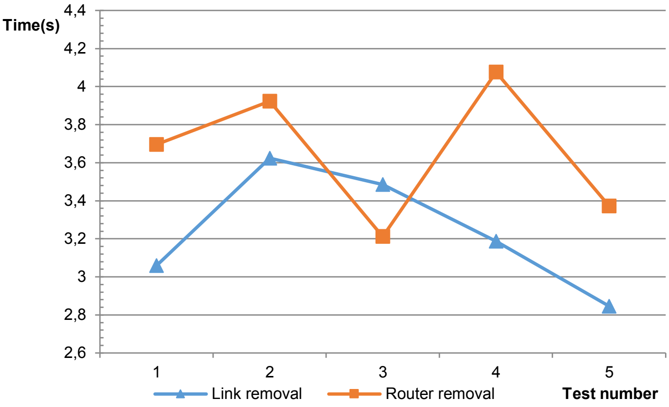

Fig. 7. Juxtaposition of each test for EIGRP protocol.

Orange data (marked with squares) show the measurements when during simulations, an entire device was broken, while blue (marked with triangles) data shows EIGRP network convergence time for a single link failure. The results were not similar to each other, so the average times of convergence were calculated for each of the tests. For measurements performed during simulation of a single link failure, the first measurement gave a value close to 3 seconds, while for the remaining three measurements longer times were recorded. Analysis of the time of the last measurement shows that the network learned the new route the fastest. For the test in which the failures of the entire device were simulated, most of the collected times were longer than in the previous test. For the third and the fifth measurements, faster route learning was noticed than for the first and the second measurement for a single link failure. To compare the performed tests, the average values were calculated and showed in fig. 8.

The presented results show the EIGRP protocol chose a new route quicker if a failure occurred only on a single link. If an entire device fail a new neighbourhood relation has to be established between routers. It means that more devices had to learn new routes. What is more, a bypass via the same device could be used for a link failure. When router stopped working, routing protocol had to find a new route without a broken equipment. It took more time, but the protocol set a new, longer route with gigabit connections instead of serial ones.

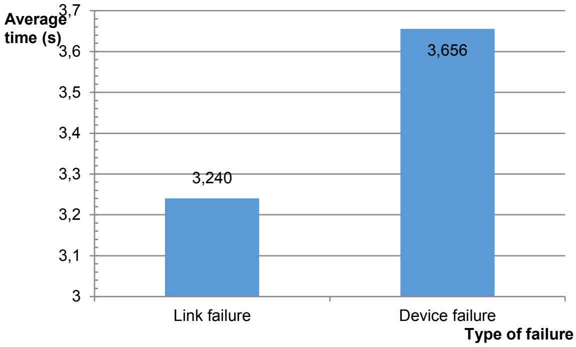

Fig. 8. Average convergence time after an interface failure and equipment for EIGRP.

Performed tests showed, that EIGRP allows for faster times of route reelection after its failure. Although EIGRP was characterized by better convergence time it is not a solution based on an open standards. This protocol can be used only with Cisco Systems devices, which limits the variety of devices in network's design. EIGRP is easier to configure and does not require as much planning as the OSPF, however, more options available in configuration can improve network's management. If one of the OSPF devices stops working, and it is not the autonomous system border router, we are certain that in the worst case scenario access to the network resources will be lost only for the devices in a specific area.

4 Summary

Methods and means for determining the times of convergence and learning alternate routes with physical laboratory's devices were presented in this paper. This type of research is often performed with simulating programs, in which consideration of the large enterprise network's specification may not be possible or leads to unreliable results. Therefore, our study focuses on the implementation of two main routing protocols in the real test network, including physical devices, to determine the amount of time needed to achieve the convergence of the network with use of redundancy mechanisms applied in the third layer. Knowledge of these times allows to modify applications, which use higher layers of ISO/OSI model (from 4 to 7) to tolerate longer breaks in the network's service, e.g. by increasing the buffering time of video streams or by enlarge session's hold time in case of virtual channel connections. Further works will be undertaken in two ways: extending the size of test networks and testing for other routing protocols; developing simulation models and their verification for known routing protocols.

References

1. M. Taifi, J. Shi, Y. Celik, *JENERGY: A Fault Tolerant Stateless Architecture for High Performance Computing*, Service-Oriented System Engineering (SOSE), 2015 IEEE Symposium on, (2015).

2. Vendor Documentation: OmniSwitch 9900 Series, Hardware Users Guide. Alcatel-Lucent Enterprise, Part No. 060409-10, Rev B, (2016).
3. Vendor Documentation: OmniSwitch 10K Hardware Users Guide. Alcatel-Lucent Enterprise, Part No. 060310-10, Rev. J, (2016).
4. F. Burda, P. Havrila, M. Knĕzek, and others, *Optimization of Network Redundant Technologies Collaboration in IMS Carrier Topology*, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, **46**, 705-712, (2011).
5. Fenge-Wang, Chang-xing-Zhu, *HSRP Protocol Based on High Reliable Redundant Campus Network Design*, Communications and Information Processing, Communications in Computer and Information Science, **289**, 107-114, (2012).
6. H. Birkholz, I. Sieverdingbeck, *Supporting Security Automation for Multi-chassis Link Aggregation Groups via the Interconnected-Asset Ontology*, Availability, Reliability and Security (ARES), 2014 Ninth International Conference on, 126-133, (2014).
7. M. Nurujjaman, S. Sebbah, C. Assi, *Design of Resilient Ethernet Ring Protection (ERP) Mesh Networks With Improved Service Availability*, Journal of Lightwave Technology, **31**(2), (2013).
8. J. Lopes, S. Sargento, A. Zúquete, *A Dependable Alternative to the Spanning Tree Protocol. Dependable Computing*, Lecture Notes in Computer Science, **7869**, 148-164, (2013).
9. M. Bolanowski, A. Paszkiewicz, *The Use of Statistical Signatures to Detect Anomalies in Computer Network*, Analysis and Simulation of Electrical and Computer Systems, Lecture Notes in Electrical Engineering, **324**, 251-260, (2015).
10. F. Grabowski, A. Paszkiewicz, M. Bolanowski, *Wireless Networks Environment and Complex Networks*, Analysis and Simulation of Electrical and Computer Systems, Lecture Notes in Electrical Engineering, **324**, 261-270, (2015).
11. J.T. Duda, T. Pełech-Pilichowski, *Enhancements of moving trend based filters aimed at time series prediction*, Advances in systems science, eds. Jerzy Świątek, Advances in Intelligent Systems and Computing **240**, 747–756, (2014).
12. B. Twaróg, R. Pękala, J. Bartman, Z. Gomółka, *The changes of air gap in inductive engines as vibration indicator aided by mathematical model and artificial neural network*, Discrete and Continous Dynamical Systems, Journal of American Institute of Mathematical Sciences, 1005-1012, AIMS (2007).
13. G. Kanti Dey, M. Ahmed, K. Tanvir Ahmmed, *Performance analysis and redistribution among RIPv2, EIGRP & OSPF Routing Protocol*, Computer and Information Engineering (ICCIE), 2015 1st International Conference on, (2015).
14. C. Wijaya, *Performance Analysis of Dynamic Routing Protocol EIGRP and OSPF in IPv4 and IPv6 Network*, First International Conference on Informatics and Computational Intelligence (2011).
15. M. Bolanowski, A. Paszkiewicz, *Performance test of network devices*, Annales UMCS Sectio AI Informatica **13**(1), 29-36 (2013).