Network Monitoring of the MHT Company Using the DUDe

FATIMA SAPUNDZHI
Department of Communication and Computer Engineering and Technologies
South-West University "Neofit Rilski"
66 Ivan Mihaylov Str., Blagoevgrad 2700
BULGARIA

KRASIMIR YORDANOV
Department of Communication and Computer Engineering and Technologies
South-West University "Neofit Rilski"
66 Ivan Mihaylov Str., Blagoevgrad 2700
BULGARIA

Abstract: - In the current study we present a monitoring of the MHT network system by using the DUDe. It is an effective monitoring system for administrators covering services to every client. The administrators are constantly striving to maintain smooth operation of their networks. The system enables to monitor the status changes particularly outside the monitoring area. In the observed system, we use the Open Shortest Path First protocol, which is based on the link state routing protocol concept and uses Dijkstra's shortest path first routing algorithm. An alert system is built to the MHT network. It can be used to supervise the network and can report the state of the network by using an alert system in the monitoring area.

1 Introduction

Nowadays the computer networks are connecting millions of computers, and devices such as smartphones, tablets, Internet of Things (IoT) devices in throughout the world. They have become an infrastructure for many applications in our lives and therefore it is important for the networks to properly manage. For network management it requires continuous monitoring in real time.

The monitoring of network represents mechanisms that allows network administrators to know instantaneous state and trends of a complex computer network.

In supporting a network, the alert systems and monitoring are needed for the network control and also a system that can monitor network condition by using alarm system or others for alert in monitoring area.

For effectively monitoring of the system the administrators need alert systems that can report on network status when they are not in the monitoring area.

In the present investigation we look the downlink/uplink decoupling (DUDe) [1]-[3]. The aim of the current research is to present a monitoring system using the DUDe with e-mail as alert system notification (ASL). The DUDe is a powerful and flexible network monitoring system (NMS) by MikroTik [4]-[7]. The NMS in our investigation is situated in Petrich town, South-West Bulgaria. The name of the system is MHT company [8]-[15].

2 Materials and Methods

The algorithms of shortest-path routing have been widely used in computer networks and Internet Protocol (IP) networks. A communication network (CN) is made up of *nodes* and *links*. The nodes have different names that depend on the type of CN. In an IP network a node is called a *router*. A link connects 2 routers in an IP network is called an *IP link* (IP trunk) and the end of a link outgoing from a router is called an *interface*. A CN carries traffic that flows from a start node to an end node.

Fatima Sapundzhi, Krasimir Yordanov

For a CN is important to route traffic from a source node to a destination node. For this objective we need to determine a route, which is a path from the start node to an end node.

The algorithm of Dijkstra computes shortest paths to all destinations from a source, which is very useful, especially in a communication network, since a node wants to compute the shortest path to all destinations.

In general, in graph theory $G = (V, E)$ denote a directed graph with non-negative integral edge lengths $c: E \rightarrow Z_{\geq 0}$.

Let vertices $u, v \in V$ and we denote $dist(u, v)$ as the minimal total length of a path in G from u to v, or ∞ if v is not reachable from u.

For a given source set S which is non-empty and vertexes $s \in S, v \in V$ we define a function

$$d: V \rightarrow Z_{\geq 0} \cup \{\infty\}:$$

$$d(v) = min\{dist(s, v) | s \in S, v \in V\}.$$

For a given target $T \subseteq V$ and vertex $t \in T$ we can compute the distance:

$$d(t) = min\{(d, t) | t \in T\}.$$

In computer networks theory we consider a generic node i in a network of N nodes from where we want to compute shortest paths to all other nodes in $L = \{1, 2, \ldots, N\}$. A generic destination node will be denoted by j $(j \neq i)$. We will use the following two terms:

d_{ij} - link cost between node i and node j.

$dist(d_{ij})$ -cost of the minimum path between i and j.

The algorithm divides the sets of nodes L into 2 sets: it starts with permanent set L_1, which represents nodes already considered, and tentative set L_2, for nodes not considered yet.

As the progress of the algorithm, set L_1 expands with new nodes included while set L_2 compressions when nodes newly included in L are deleted from this set. It stops when set N_2 becomes empty.

At first $L_1 = \{i\}$ and $L_2 = L \setminus \{i\}$ (i.e., all nodes in L except node i).

ALGORITHM: Dijkstra's shortest path algorithm

Step 1: Start with source node i in the permanent set of nodes considered, i.e., $L_1 = \{i\}$; all the rest of the nodes are put in the tentative set labeled as L_2.

$$dist(d_{ij}) = d_{ij}, \text{ for all } j \in L_2.$$

Step 2: Identify a neighbouring node (intermediary) k not in the current list L with the minimum cost path from node i, i.e., find $k \in L_2$ such that

$$dist(d_{ik}) = min_{m \in L_2} . dist(d_{im}) \qquad (1)$$

Add k to the permanent set L_1, i.e., $L_1 = L_1 \cup \{k\}$.
Drop k from the tentative set L_2, i.e., $L_2 = L_2 \setminus \{k\}$.
If L_2 is empty, stop.

Step 3: Consider the list of neighbouring nodes, L_k, of the intermediary k (but do not consider nodes already in L) to check for improvement in the minimum cost path, i.e., for $j \in L_k \cap L_2$

$$dist(d_{ij}) = min\{dist(d_{ij}), dist(d_{ik}) + d_{kj}\} \quad (2)$$

Go to Step 2.

3 Results and Discussion

In the current study we present a monitoring of a network system with multiple devices and users. For proper maintenance of the network it is necessary to know the status of all devices in real time.

For a complete Network Monitoring Solution (NMS) we were used the DUDe of the Microtik- a free application that can improve the way the managing of the network. For check the availability of hosts on the network, the Netwatch service was used. The registered hosts of the devices were monitored by the Mikrotik RouterOS Network. The observed system, named MHT consists of:

1 router - MikroTik RouterOS. Its functions are: routing, customer service priority, customer priority, firewall, NAT, load balancing, VPN server, etc;

Fatima Sapundzhi, Krasimir Yordanov

1 Smart router HP ProCurve Switch 2848, 24-Port Gigabit PoE with 4 SFP Slots. Key features are: access layer switch, enterprise-class features, Layer 2 and Layer 3 lite feature set, scalable 10/100/1000 connectivity, gigabit fibber uplinks. It is used to connect to servers and a net control connection device that monitor real-time temperature, humidity, flood, power and more with instant alerting and historical reporting;

1 OLT (Optical Line Termination) device- V-solution EPON V1600D4. It acts as the endpoint hardware device in a Passive Optical Network (PON) [4];

13 Routers ONU (Optical Network Unit) - converts optical signals transmitted via fiber to electrical signals. These electrical signals are then sent to individual subscribers. It designed for fulfilling FTTH ultra-broadband access request of home and SOHO (Small Office/Home Office) users. IT supports NAT/firewall and so on functions. OLT supports bandwidth allocation that allows to make smooth delivery of data float to the OLT, that usually arrives in bursts from customer;

37 TP-LINK TL-SF1008D *switches* - provide 810/ 100 Mbps Auto-Negotiation RJ45 ports, support auto MDI/MDIX and this eliminates the need for crossover cables. The TL-SF1008D Fast Ethernet Switch is designed for SOHO or workgroup users;

1 NetControl 4RU1SH2S device including a set of different inputs and outputs: relays, temperature sensor, humidity sensor, voltage/ current measurement, energy measurement etc. It has integrated WEB server, accessible from any standard browser, allowing users to control and monitor any input or output. 200 pcs. active devices, access points, client routers, cameras, and more [5];

The MHT system also consists of 400 pcs. client devices, such as desktops, laptops, tablets, mobile phones, TVs, multimedia systems, etc.

In the observed system, we use the Open Shortest Path First (OSPF) protocol, which is based on the link state routing protocol concept and uses Dijkstra's shortest path first routing algorithm presented above. In the MikroTik RouterOS implements OSPF Version 2 (RFC 2328). It is on the link-state protocol that takes care of the routes in the dynamic network structure that can employ different paths to its subnetworks. It always chooses the shortest path algorithm to the subnetwork first. OSPF is defined directly on top of IP by being assigned a protocol-type field at the IP level. Once the path is computed, the next hop is also extracted from the shortest path computation to update the routing table, and subsequently, the forwarding table. The routing table entries are for destinations identified through hosts or subnets or simply IP prefixes, not in terms of end routers [5]-[7]. OSPF uses protocol l89 to communicate with the neighbours.

OSPF protocol is one of the most widely used protocols in existence today because of being able to implement it cross multivendor platforms. In the observed system it was used for: automatic distribution of routing information instead of using static routes; making fail-over connections; load balancing.

The Mikrotik device use the Netwatch service then send Internet Control Message Protocol (ICMP) packets to them. When a host does not respond, it is considered to be down and the system administrator should act on this situation. The actions can be performed through Mikrotik scripts - writing to the system log, sending an alert e-mail or a SMS message. Simple monitoring with Mikrotik RouterOS Netwatch is shown in the Fig. 1.

For each device there is:
- *host* (IP address) - timeout during which time to send ping to monitored devices;
- *timeout* - the time when the device does not return the request states it is down - no connection;
- *status* - shows the status with up - there is a connection with the device, down - no connection;
- *since* - the time and date of the last recorded change in the table.

There is also a launch console scripts: status up, and status down, with which certain actions can happen dynamically.

Fig.1. Monitoring by Mikrotik RouterOS
Netwatch of the MHT network.

A monitoring by the DUDe is shown in the Figure 2. The system automatically creates a map with information about the devices - type, colour, icon, and others. Different settings per device can be made. The map can be scaled up for faster and more convenient work on large networks as well as to see in detail the connections between the devices and to track the traffic between them.

Fig.2. Monitoring by the DUDe of the MHT network.

In the Figure 2 is shown the basic configuration of the MHT system. Depending on our needs we can scale-up and make very versatile and effective monitoring solution.

A simple example of the network monitoring along with the interface traffic and outage alerts is presented in the Figure 3. The chart shows a network map and data in the DUDe for investigated MHT system. The devices are monitored by RouterOS or Simple Network Management Protocol (SNMP). The SNMP service includes agents that monitor the activity of network devices and report to the network workstation.

All devices that are in a lit condition on the subnet are opened by the DUDe and automatically is formed a network map of all the found devices. From the Figure 3 can be known condition of each device, can also be known transfer rate between device (router).

The status of equipment whether its network up, down or any service that timed out can be seen as: *green colour* - the network and equipment ok (up) or the service is running well; *red colour* - there is a network or equipment

interruption (down) or the services are off; *orange colour* - there are services that are timed out, or in certain intervals occasionally timed out, or some services are not running well.
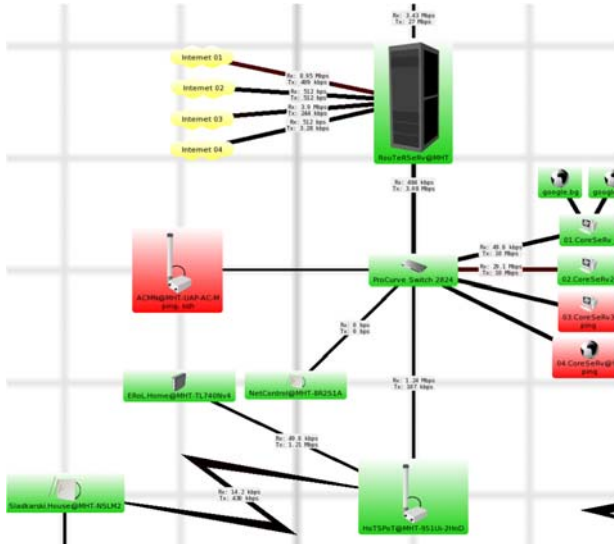
Fig.3. Monitoring of the server connections and Internet connection of the MHT network.

In the Figure 4 are displayed all the devices, sorted by name, address, MAC address, Device type, or Map they are on. It also displays which services are currently down for each device, and their notes

Fig. 4. The device list that the server has knowledge about.

In the Figure 5 are shown devices that have been marked as RouterOS in the device settings. The present table includes additional information, authentication status, version, architecture, system hardware type, upgrade

status and packages. Here R_X means received traffic and T_X means transmitted traffic, these directions are based on the interface they are being read from. The panel is optimized for upgrading of RouterOS devices.

A wireless base station that is controlled and monitored by the DUDe is presented in Figure 6. As can be seen from the chart all devices are light up in green, which means that they have an Internet connection. Through the system can specify the type of connection, maximum bandwidth, colour, thickness, shape, and so on.

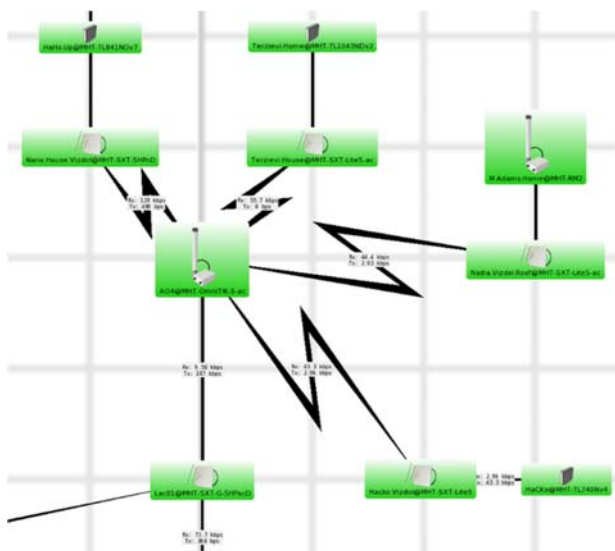**Fig. 5.** List of RouterOS devices of the MHT network.

Fig.6. Wireless base station of the MHT network.

In managing and monitoring the network we are interested to keep an eye on the latency of the network links, which are connected with a dedicated Internet connection and an IPSec VPN tunnel to the datacentre.

The network latency refers to any of several kinds of delays typically incurred in processing of network data. It describes a delay that takes place during communication over an Internet network. It is a time interval between the stimulation and response of some physical change in the monitoring of the system [3]-[10]. The low latency network connection is one that generally experiences small delay times, while a high latency connection generally suffers from long delays.
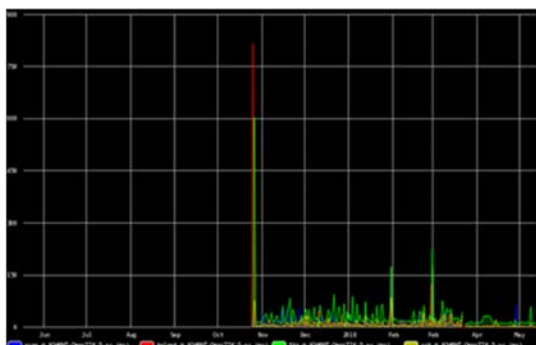
Fig.7. Graphical lag and the stability of the connection between the main router and the PON terminal.

In the Figure 7 is shown the graphical lag and the stability of the connection between the main router and the PON terminal. This Internet connection was changed at the end of February 2018, as shown on the chart.
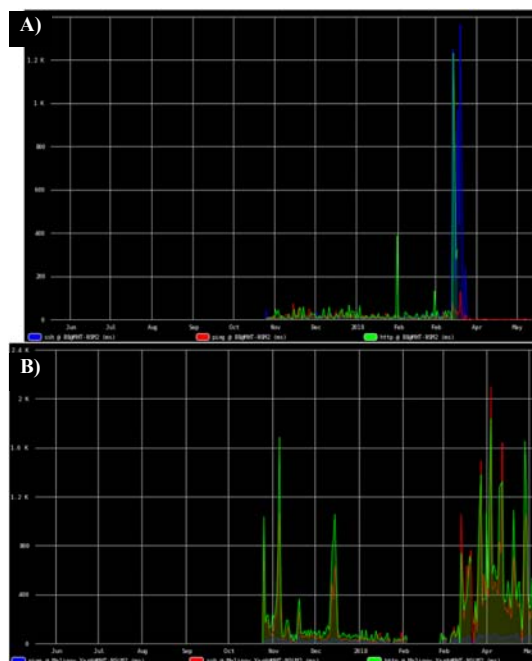
Fig.8. A base station at a 2.4GHz frequency band connected to the PON since the end of April 2018. A) There is an increase in lag. B) Transfer high definition video signals with about 12-17 Mbit/s.

When the administrators troubleshoot in a network they complain that they frequently lost connectivity with multiple local server's and also sometimes with the Internet. Sometimes pings replies works fine but latency gets high or timeout/breaks occurs (see Figure 8) [8]-[16].

The generated graphics shown on Fig.8 can reveal the quality (packet loss and latency variability) and reachability of the IP address from several distributed locations. There is an increase in the lag and therefore the stability of the connection, the reason is the transmission of high-quality video signals with about 12-17 Mbit/s.

In red is displayed the optimal sinus-curve thru the points of one week. Light-green is the "can-be-range" of the traffic that was not alarmed. Yellow is the "warning-range" of the curve and every other point cause a CRITICAL-Warning in our monitoring. So, we bring the

statistics-calculations into the monitoring [14]-[20].

In the Figure 9 is presented the average speed of two of the Internet connections to the main router. The monitoring was carried out through RuterOS. The charts show empty spaces that indicate that there were no connection and no values were recorded, statistics, packet flow and graphs in real time. Those graphs show the traffic of a network interface and the incoming and outgoing transfer rate of the interface.

Fig. 9. Graphics of the average speed of two of the Internet connections to the main router: A)10WAN1-B1-M, B) 12WAN3-B3-M.
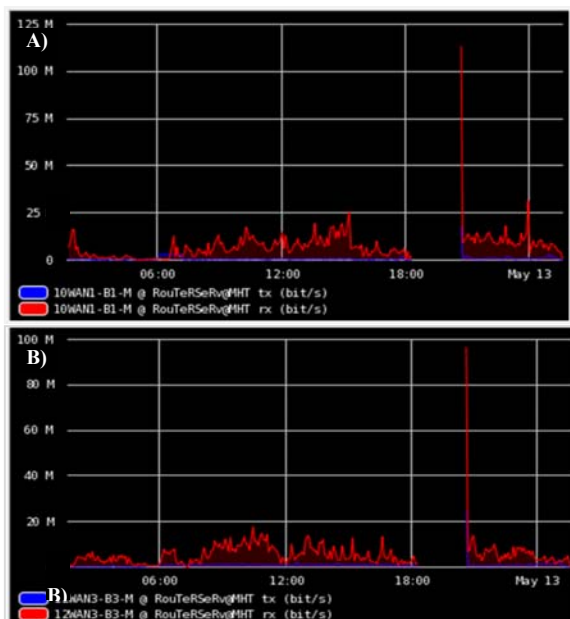
In the Mikrotik system can monitor the traffic of every interface, queue or firewall rule in real-time. In the Figure 10 is shown the ethernet traffic monitoring graphs. This diagram is observed if at least one of the devices supports RouterOS or SNMP and is selected the network interface to be monitored.
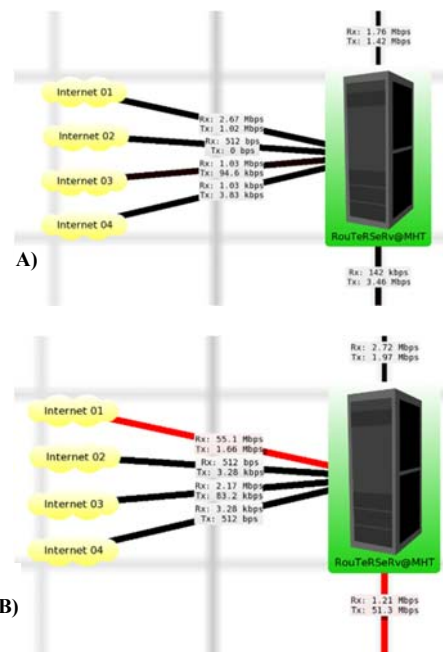
Fig. 10. Monitoring of the Internet connections, input and output connections from the router to the PON and servers. In red is shown overloading an Internet connection to set the maximum bandwidth of the network.

Monitoring of the MHT system for two months is presented in Figure 11.

The DUDe is one of the most powerful free network monitors. An alert system is built to the observed MHT network. The system is used to supervise and report for the network state. The administrator receives SMS from Windows base DUDe by using Mikrotik attached GSM modem. A GSM device is connected with Mikrotik for send/receive purposes and a SMS base HTTP gateway. The user is received the DUDe notification via SMS using Mikrotik GSM/Mobile device, in case any critical device/server goes down. The system sends email to the specified recipient. Since the DUDe can execute commands with arguments locally on an operating system where the client is installed, this option can be used to create a custom notification method like Facebook messenger (©MAGIC HackeR Team®).

Fig.11. Monitoring of the MHT system: A) May 2018; B) June 2018 after a thunderstorm.

4 Conclusion

The research methodology in the present study is based on the increasing size and the number of network devices in the MHT network. This network need for continuous monitor.
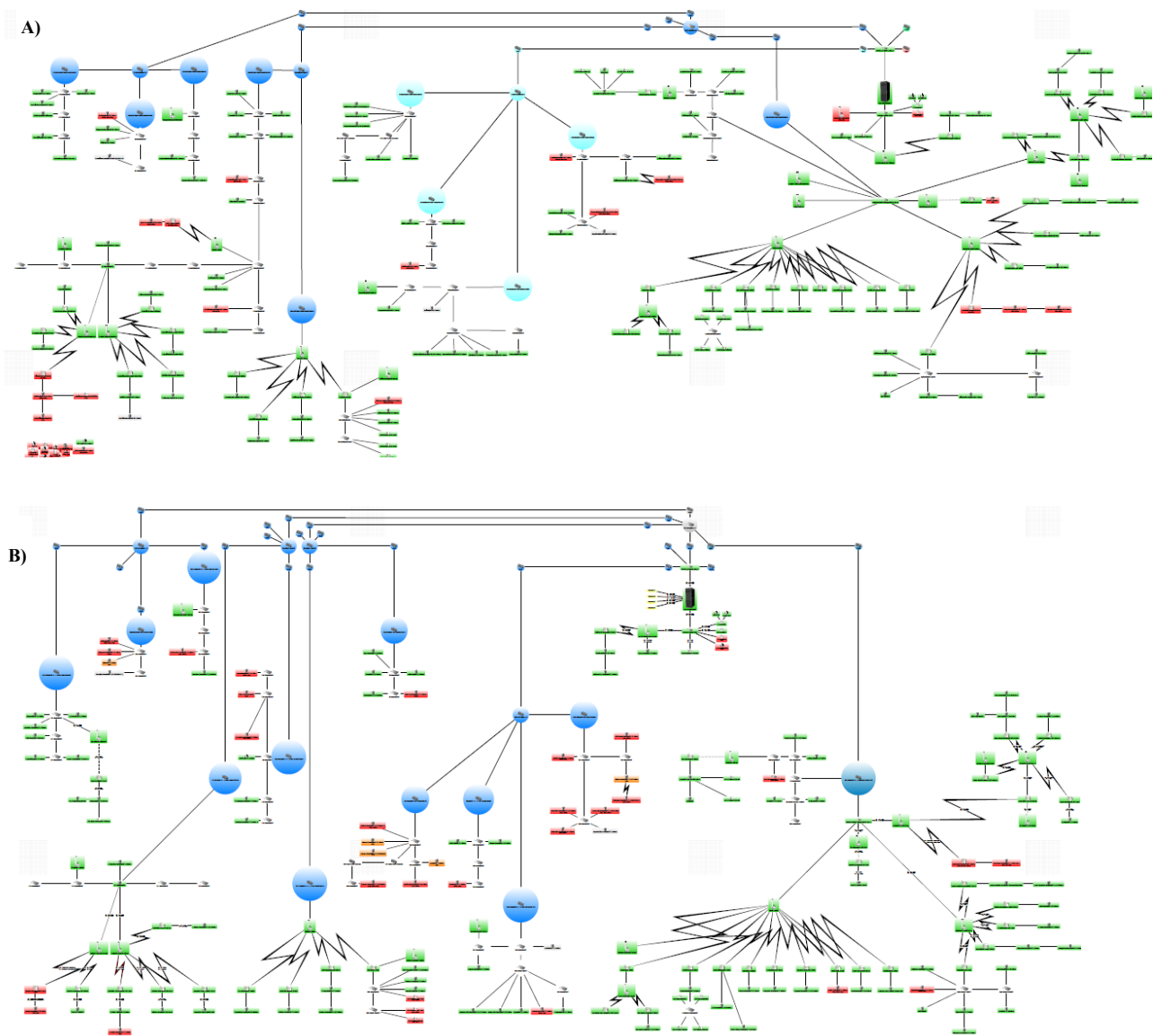
We have presented a monitoring of the MHT network by using the Open Shortest Path First protocol, which is based on the link state routing protocol concept and uses Dijkstra's shortest path first routing algorithm.

References:

[1] Author, Title of the Paper, *International Journal of Science and Technology*, Vol.X, No.X, 200X, pp. XXX-XXX.

[2] Author, *Title of the Book*, Publishing House, 200X.

[3] H. Elshaer, F. Boccardi, M. Dohler, and R. Irmer, Downlink and Uplink Decoupling: A Disruptive Architectural Design for 5G networks, *Proceeding of IEEE Global Communications Conference (IEEE GLOBECOM'14)*, 2014, pp.1798–1803.

[4] F. Boccardi et al., Why to Decouple the Uplink and Downlink in Cellular Networks and How To Do It, *IEEE Communications Magazine*, Vol.54, No.3, 2016, pp.110–117.

[5] https://mikrotik.com/thedudeTerm

[6] https://techterms.com/definition/latency

[7] https://v-solution.en.alibaba.com/product/ 60373103585-212077032/ V1600D4_ GEPON_4_PON_OLT_Fiber_ Optical_Line_

[8] J. Moy, "OSPF version 2," *IETF RFC 2328*, April 1998. http://www.rfc-editor.org/rfc/rfc2328.txt

[9] P.Tadimety, "OSPF: A Network Routing Protocol", 1st ed., Apress, 2015.

[10] A.Tabona, 2015. "The top 20 free Network Monitoring and Analysis Tools for sysadmins. [Online]. Available: https://techtalk.gfi.com/the-top-20-free-network-monitoring-and-analysis-tools-for-sys-admins/ comment-page-1/

[11] R.Khan, S. Khan, R.Zaheer, and M.Babar, "An efficient network monitoring and management system" *International Journal of Information and Electronics Engineering*, vol. 3 (1), 122-126, 2013.

[12] S. Lee, K.Levanti, and H. Kim, "Network monitoring: Present and future", *Computer Networks,* vol.65, pp. 84-98, 2014.

[13] J.Cheng, L.Hu, J.Liu, Q.Zhang, and Ch.Yan, "A New Mechanism for Network Monitoring and Shielding in Wireless LAN", *Mathematical Problems in Engineering*, vol. 2014, pp.1- 8, 2014.

[14] M.Smitha, R. Liub, and R. Mounce, "Traffic Control and Route Choice; Capacity Maximization and Stability". *Transportation Research Procedia*, vol.7, pp. 556-577, 2015.

[15] N.Dhillon, and U. Ansari, "Enterprise Network Traffic Monitoring, Analysis, and Reporting Using WINPCAP Tool with JPCAP API". *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 2, 2012.

[16] D. Prangchumpol, "A Network Traffic Prediction Algorithm Based on Data Mining Technique". *International Journal of Computer, Electrical, Automation, Control and Information Engineering*, vol. 7, 999-1002, 2013.

[17] Z. Wang, and J. Crowcroft, "Analysis of Shortest-Path Routing Algorithms in a Dynamic Network Environment", *Computer Communication Review*, 63-71, 1992.

[18] D. Medhi, and K. Ramasamy, "Network Routing: Algorithms, Protocols, and Architectures", 2nd ed., Morgan Kaufmann Publishers Elsevier, 2017.

[19] V. Vladimirov, F. Sapundzhi, R. Kraleva, and V. Kralev, "Modified Genetic Algorithm to Traveling Salesman Problem for Large Input Datasets". *Biomath Communications*, vol. 3 (1), P71, 2016.

[20] V. Kralev, "Different Applications of the Genetic Mutation Operator for Symetric Travelling Salesman Problem", IJASEIT, 7 (5), 762 -770, 2017.

[21] V. Kralev, R. Kraleva, "A local search algorithm based on chromatic classes for university course timetabling problem", International Journal of Advanced Computer Research, 7 (28), pp. 1-7, 2017.

[22] V. Kralev, "A genetic and memetic algorithm for solving the university course timetabling problem," *International Journal "Information Theories & Applications*, vol. 16(3), pp. 291-299, 2009.

[23] F.Sapundzhi, and M. Popstoilov. "Optimization algorithms for finding the shortest paths". *Bulgarian Chemical Communications*, vol.50, Special Issue B, 2018.