*Bulgarian Chemical Communications, Volume 52, Issue A (pp. 203-211) 2020 DOI: 10.34049/bcc.52.A.242*

# Network monitoring of the MHT company using the DUDe

F. Sapundzhi*, K. Yordanov

*South-West University Neofit Rilski, 2700 Blagoevgrad, Bulgaria*

Received August 01, 2019, 2019; Accepted October 29, 2019

In the current study we present a monitoring of the MHT network system by DUDe. The administrators are constantly striving to maintain smooth operation of their networks. The system enables monitoring of 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.

**Keywords:** computational models, network algorithms, network monitoring, shortest path problem, LAN, DUDe

## INTRODUCTION

Nowadays the computer networks are connecting millions of computers, and devices such as smartphones, tablets, Internet of Things (IoT) devices 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. Network management requires continuous monitoring in real time. The monitoring of network represents mechanisms that allow network administrators to know the instantaneous state and trends of a complex computer network.

In supporting a network, 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 [8-12].

## 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* [13-15]. The nodes have different names that depend on the type of CN. In an IP network a node is called a *router*. A link connecting 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.

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 the 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 $c: E \to \mathrm{Z}_{\geq 0}$.

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 $\infty$ 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:

$$d: V \to \mathrm{Z}_{\geq 0} \cup \{\infty\}:$$

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

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 the 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 the permanent set $L_1$ which represents nodes already considered, and the

* To whom all correspondence should be sent.
E-mail: sapundzhi@swu.bg

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 $L_2$ compresses 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 $L_2 = L\backslash\{i\}$ (i.e., all nodes in $L$ except node $i$).

**ALGORITHM:** Dijkstra's shortest path algorithm

**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 $L_2$.

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

**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

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

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., $L_2 = L_2\backslash\{k\}$. If $L_2$ is empty, stop.

**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 $j \in L_k \cap L_2$

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

Else. Back to Step 2.

## RESULTS AND DISCUSSION

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 needs continuous monitoring.

We present 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.

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

*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 fiber 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)* - convert optical signals transmitted *via* fiber to electrical signals. These electrical signals are then sent to individual subscribers. It is 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 an integrated WEB server accessible from any standard browser, allowing users to control and monitor any input or output, 200 pcs. of active devices, access points, client routers, cameras, and more [5].

The MHT system also consists of 400 pcs. of 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. 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 uses the Netwatch service, then sends 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 an SMS message. Simple monitoring with Mikrotik RouterOS Netwatch is shown in Figure 1.

| Host | Timeout (ms) | Status | Since |
|---|---|---|---|
| ;;; XoLanDeCa@MHT-NSLM2 | | | |
| 1.1.1.40 | 1000 | down | May/12/2018 |
| ;;; Belasica@MHT-TL941NDv4 | | | |
| 1.1.1.78 | 1000 | down | May/12/2018 |
| ;;; Rangers.Home@MHT-TL740Nv6 | | | |
| 1.1.1.167 | 1000 | down | May/12/2018 |
| ;;; Martina.Home@MHT-TL-WR740Nv4 | | | |
| 1.1.1.195 | 1000 | down | May/12/2018 |
| ;;; 100.Hijata.Cam.00@MHT-HikVision | | | |
| 192.168.111.100 | 1000 | down | May/12/2018 |
| ;;; Emil.Vangelov@MHT-NSLM2 | | | |
| 1.1.1.42 | 1000 | up | May/12/2018 |
| ;;; B13B@MHT-NSLM2 | | | |
| 1.1.1.96 | 1000 | up | May/12/2018 |
| ;;; RockFeller@MHT | | | |
| 1.1.1.54 | 1000 | down | May/12/2018 |
| ;;; Milushevi.Home@MHT-WR740Nv4 | | | |
| 1.1.1.64 | 1000 | down | May/12/2018 |
| ;;; M.Adams.Home@MHT-RM2 | | | |
| 1.1.1.157 | 1000 | down | May/12/2018 |
| ;;; E.Vangelov@MHT-TL740Nv4 | | | |
| 1.1.1.113 | 1000 | up | May/12/2018 |
| ;;; XoLanDeCa.Home@MHT-WR840Nv2 | | | |
| 1.1.1.163 | 1000 | up | May/12/2018 |
| ;;; Trampata@MHT-TL740Nv4 | | | |
| 1.1.1.87 | 1000 | down | May/12/2018 |
| ;;; B.Mitev.Home@MHT-TL740Nv6 | | | |
| 1.1.1.144 | 1000 | up | May/12/2018 |
| ;;; Shtangata.Home@MHT-TL-WA901NDv2.3 | | | |
| 1.1.1.191 | 1000 | down | May/12/2018 |
| ;;; Gosho.K.Home@MHT-WR841Nv11 | | | |
| 1.1.1.194 | 1000 | down | May/12/2018 |
| ;;; Angelovi.AP@MHT-TL740Nv4 | | | |
| 1.1.1.24 | 1000 | down | May/12/2018 |
| ;;; Malinov.Home@MHT-TL-WR740Nv4 | | | |
| 1.1.1.47 | 1000 | down | May/12/2018 |
| ;;; Hija.Belasica@MHT-SXT-5HacD-2n-r2 | | | |
| 1.1.1.164 | 1000 | down | May/12/2018 |
| ;;; Besedkinsk@MHT | | | |
| 1.1.1.103 | 1000 | down | May/12/2018 |
| ;;; Trendafilov@MHT-TL740Nv4 | | | |
| 1.1.1.27 | 1000 | down | May/12/2018 |
| ;;; KIKO@MHT | | | |
| 1.1.1.80 | 1000 | down | May/12/2018 |
| ;;; Malinov.Yard@MHT-NSLM2 | | | |
| 1.1.1.19 | 1000 | down | May/12/2018 |
| ;;; Machkoniz.Home@MHT-TL841NDv5 | | | |
| 1.1.1.20 | 1000 | down | May/12/2018 |
| ;;; Sarikovi.Home@MHT-TL-WR940Nv1.6 | | | |
| 1.1.1.92 | 1000 | down | May/12/2018 |
| ;;; Niki.B13@MHT-TL740Nv4 | | | |
| 1.1.1.99 | 1000 | down | May/12/2018 |
| ;;; Atanas.B28.Home@MHT-WR740Nv6 | | | |
| 1.1.1.63 | 1000 | down | May/12/2018 |
| ;;; Cent@MHT-TL841Nv9.1 | | | |
| 1.1.1.105 | 1000 | down | May/12/2018 |
| ;;; Atanas.N.Home@MHT-TL740Nv5 | | | |

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

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 are also launch console scripts: status up, and status down, with which certain actions can happen dynamically. A monitoring by the DUDe is shown in Figure 2. The system automatically creates a map with information about the devices - type, color, 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. On 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 solutions.

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

A simple example of the network monitoring along with the interface traffic and outage alerts is presented in Figure 3. The chart shows a network map and data in the DUDe for the 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.

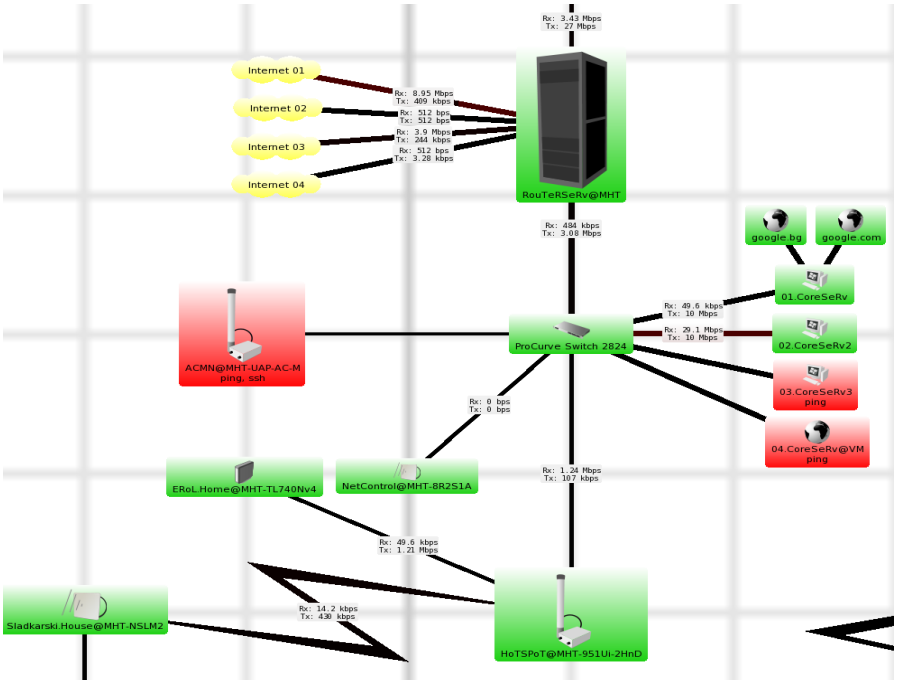


**Fig. 3.** Diagram of server connection and Internet connection of the MHT network.

**Table 1.** Monitored devices of the MHT network.

| Name | Addresses | MAC | Type |
|---|---|---|---|
| RouTeRSeRv@... | 1.1.1.0.192.168.0.1 | E4:8D:8C:3E:68.01 | Mikro Tik Device |
| Device 1 | 1.1.1.2 | UbiqitiNe:FC:D4:C4 | AP |
| Device 2 | 1.1.1.3 | UbiqitiNe:FC:d4:A1 | AP |
| Device 3 | 1.1.1.4 | UbiqitiNe:F2:18:A9 | AP |
| Device 4 | 1.1.1.5 | D8:5D;4C:D8;53:0D | Router |
| Device 5 | 1.1.1.6 | 00:27:22:12:96:4C | Client-Bridge |
| Device 6 | 1.1.1.7 | 90:F6:52:C3:ED:25 | Web Server |
| Device 7 | 1.1.1.8 | F8:1A:67:E5:B4:91 | Router |
| Device 8 | 1.1.1.9 | A0:F3:C1:88:90:00 | Router |
| Device 9 | 1.1.1.10 | 10:FE:ED:2E:C4:23 | Router |
| Device 10 | 1.1.1.11 | 00:27:19:CC:73:83 | Router |
| Device 11 | 1.1.1.12 | D8;5D;4C:EA:25:75 | Router |
| Device 12 | 1.1.1.15 | 00:23:CD:17:73:35 | Router |
| Device 13 | 1.1.1.17 | 24:A4:3C:E2:88:92 | Client-Bridge |
| Device 14 | 1.1.1.19 | 00:27::22:4E:74:4C.0 | AP |
| Device 15 | 1.1.1.20 | D8:5D:4C:E1:4D:68 | Router |
| Device 16 | 1.1.1.21 | D8:5D:4C:D8:6A:81 | Router |
| Device 17 | 1.1.1.22 | 64:70:02:45:93:F1 | Router |
| Device 18 | 1.1.1.24 | E8:DE:27:DE:85:C1 | Router |
| Device 19 | 1.1.1.25 | A0:F3:C1:79:E4:A5. | Router |
| Device 20 | 1.1.1.26 | D8:5D:4C:EA:42:4D | Router |
| Device 21 | 1.1.1.27 | 10:FE:ED:D3:64:2D | Router |
| Device 22 | 1.1.1.28 | F8:D1:11:A8:47:DF | Router |
| Device 23 | 1.1.1.29 | 64:66:B3:F8:A3:FB | Router |
| Device 24 | 1.1.1.30 | 54:E6:FC:C8:55:61 | Router |
| Device 25 | 1.1.1.32 | 74:EA:3A:EA:B1:BB | Router |
| Device 26 | 1.1.1.34 | 00:27:22:12:FF:C6 | Client-Bridge |
| Device 27 | 1.1.1.35 | 00:27:22:7C:47:B9 | Client-Bridge |
| Device 28 | 1.1.1.36 | G4:70:02:83:E8:4D | Router |
| Device 29 | 1.1.1.37 | 00:27:22:2E:40:39 | AP |
| Device 30 | 1.1.1.38 | 00:27:22:2E:40:1D | Client-Bridge |

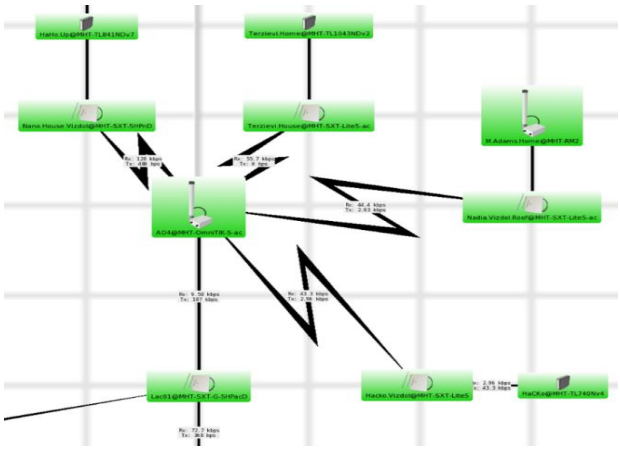

**Fig. 4.** Wireless base station of the MHT network.

**Table 2.** List of RouterOS devices of the MHT network.

| Router Device | Rx Bytes | Tx Bytes | Rx Packets | Tx Packets | Rx Rate |
|---|---|---|---|---|---|
| 1 | 3606.3kB | 3649.8kB | 63902 | 64540 | 112 bps |
| 2 | 3461.3 kB | 3950.9kB | 61256 | 69538 | 112 bps |
| 3 | 3362.8 kB | 3804.4kB | 60824 | 69039 | 112 bps |
| 4 | 3472.5 kB | 3966.1kB | 61479 | 69892 | 112 bps |
| 5 | 3536.8 kB | 4020.6 kB | 64249 | 73100 | 112 bps |
| 6 | 3312.7 kB | 3564.2 kB | 60020 | 63853 | 112 bps |
| 7 | 3475.7 kB | 3986.7 kB | 61478 | 70071 | 112 bps |
| 8 | 3369.8 kB | 3453.5 kB | 61047 | 61795 | 112 bps |
| 9 | 3240.0 kB | 3740.3 kB | 58650 | 66999 | 112 bps |
| 10 | 2612.3 kB | 4736.1 kB | 47414 | 86262 | 112 bps |
| 11 | 3273.5 kB | 3894.6 kB | 59437 | 70787 | 112 bps |
| 12 | 3434.8 kB | 3577.2 kB | 62802 | 65416 | 112 bps |
| 13 | 3246.9 kB | 3746.0 kB | 58790 | 67200 | 112 bps |
| 14 | 3306.2 kB | 3394.6 kB | 60016 | 61626 | 112 bps |
| 15 | 3164.3 kB | 3690.8 kB | 57449 | 67056 | 112 bps |
| 16 | 3182.0 kB | 3690.8 kB | 57449 | 67056 | 112 bps |
| 17 | 3549.0 kB | 4020.9 kB | 64468 | 73073 | 112 bps |
| 18 | 3647.3 kb | 3677.3 kB | 64653 | 65141 | 112 bps |
| 19 | 3297.9 kB | 3410.5 kB | 59847 | 61918 | 112 bps |
| 20 | 3340.1 kB | 3833.7 kB | 59790 | 68350 | 112 bps |
| 21 | 3487.1 kB | 3965.0 kB | 61770 | 70073 | 112 bps |
| 22 | 3644.8 kB | 4170.3 kB | 64700 | 74167 | 112 bps |
| 23 | 3876.1 kB | 3970.5 kB | 68848 | 70369 | 112 bps |
| 24 | 3488.6 kB | 3993.6 kB | 61754 | 70275 | 112 bps |
| 25 | 4627.2 kB | 3995.4 kB | 75681 | 70329 | 112 bps |
| 26 | 3652.3 kB | 3752.1 kB | 66332 | 68169 | 112 bps |
| 27 | 3500.7 kB | 3992.1 kB | 62009 | 70451 | 112 bps |
| 28 | 3248.8 kB | 3713.7 kB | 58986 | 67471 | 112 bps |
| 29 | 3828.7 kB | 4443.1 kB | 68429 | 78439 | 112 bps |
| 30 | 5.6 MB | 6.6 MB | 86888 | 78801 | 112 bps |

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 apparatus. From Figure 3 can be known the condition of each device and also the transfer rate between devices (router).

The status of equipment whether its network is up, down or any service that timed out can be seen as: *green color* - the network and equipment ok (up) or the service is running well; *red color*- there is a network or equipment interruption (down) or the services are off; *orange color* - there are services that are timed out, or in certain intervals occasionally timed out, or some services are not running well. In Table 1 are displayed all devices, sorted by name, address, MAC address and type.

Table 2 shows devices that have been marked as RouterOS in the device settings. This 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 4. 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 the type of connection, maximum bandwidth, color, thickness, shape, and so on can be specified. 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 datacenter. 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 the response of some physical change in the monitoring of the system [3-6]. The low latency network connection is one that generally experiences small delay times, while a high latency connection generally suffers from long delays.

Figure 4 show 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.

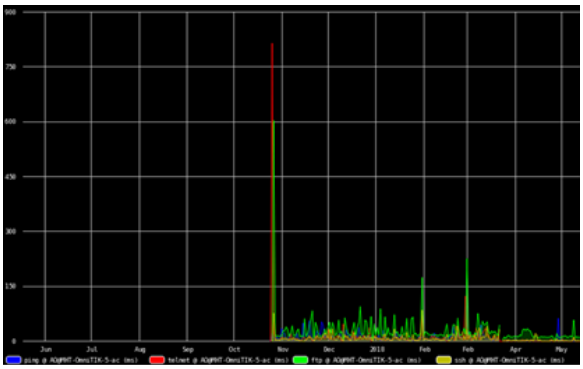

**Fig.4.** Graphical lag and stability of the connection between the main router and the PON terminal.

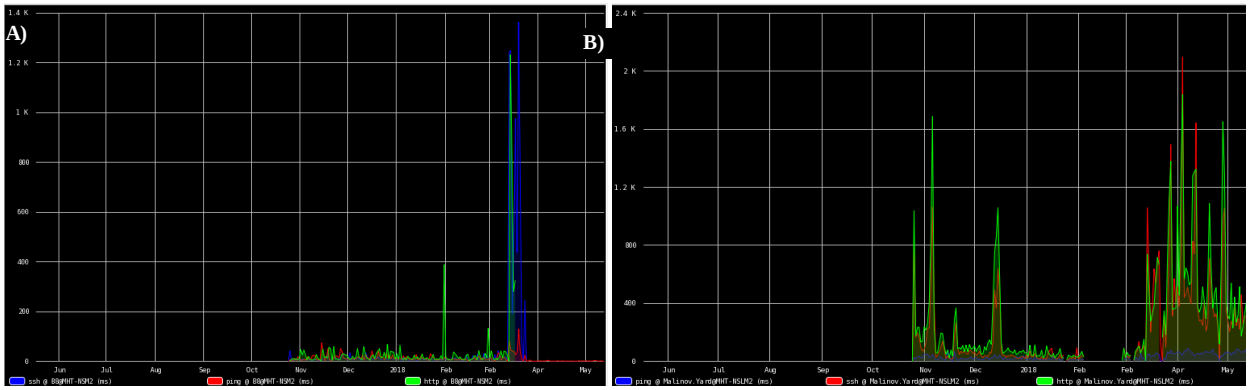


**Fig. 5.** A base station at a 2.4GHz frequency band connected to the PON since the end of April 2018. A) There is an increase in lag. B) Transfer high definition video signals with about 12-17 Mbit/s.

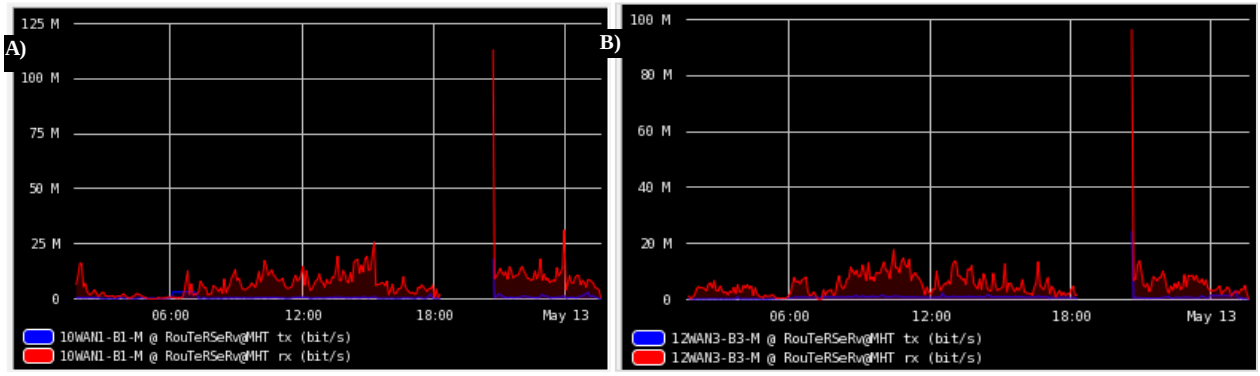


**Fig. 6.** Graphics of the average speed of two of the Internet connections to the main router: A)10WAN1-B1-M, B) 12WAN3-B3-M.

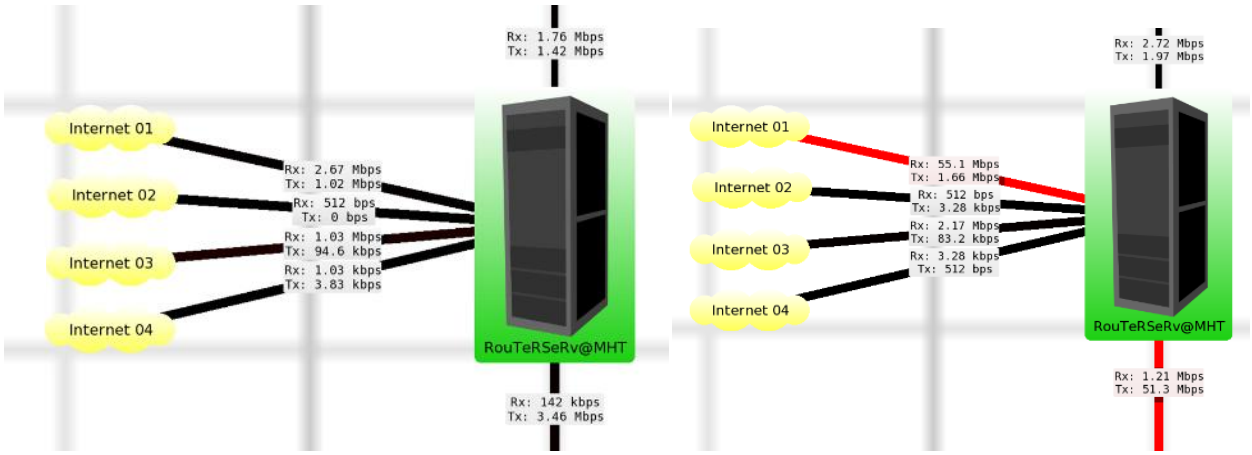


**Fig. 7.** Monitoring of the Internet connections, input and output connections from the router to the PON and servers. In red is shown the overloading of an Internet connection to set the maximum bandwidth of the network.

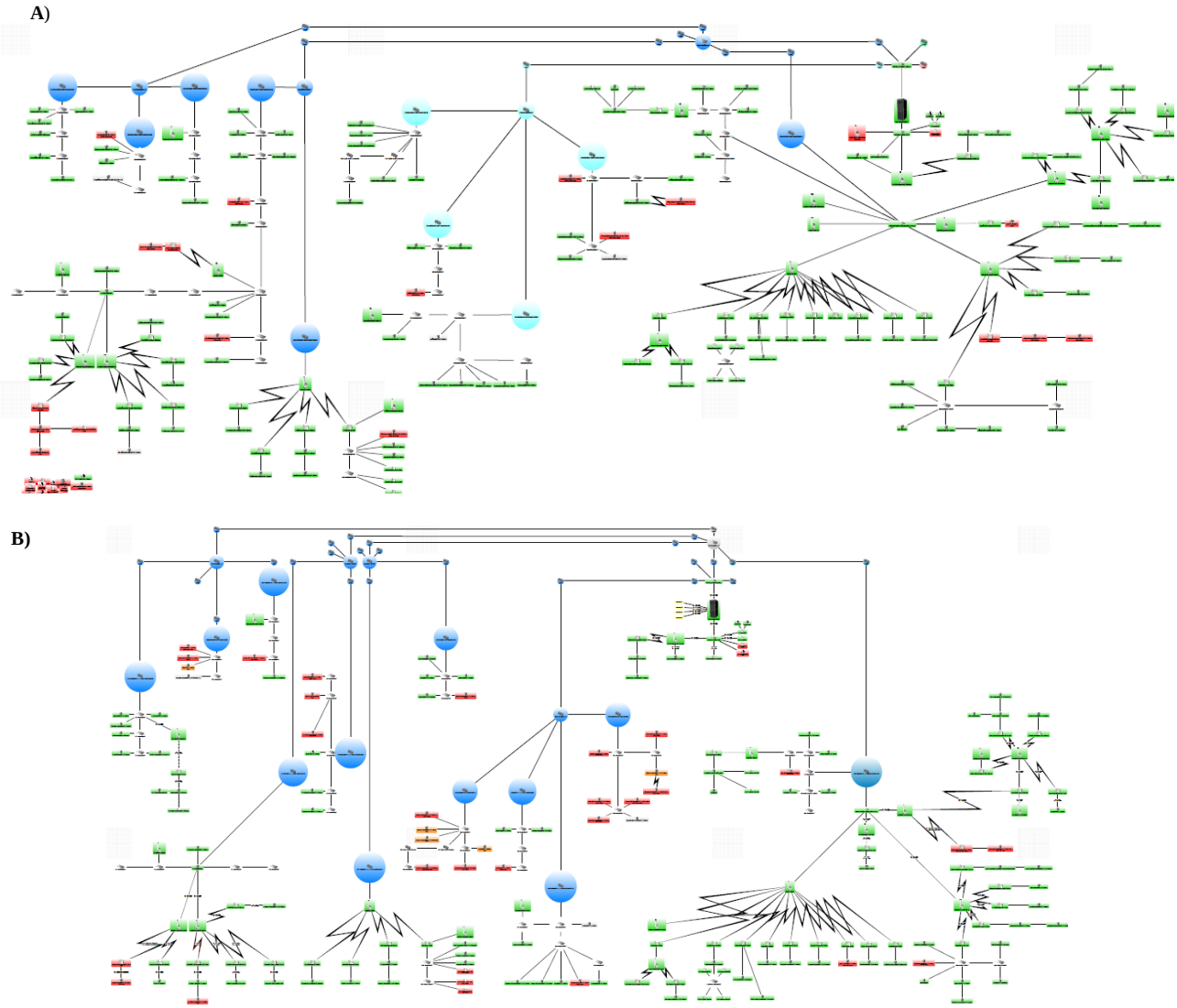


**Fig. 8.** Monitoring of the MHT system: A) May 2018; B) June 2018 after a thunderstorm

When the administrators troubleshoot in a network they complain that they frequently lost connectivity with multiple local servers and also sometimes with the Internet. Sometimes pings replies work fine but latency gets high or timeout/breaks occur (Figure 5) [8-10].

The generated graphics shown on Figure 6 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 in 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 through 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 causes a CRITICAL-Warning in our monitoring. So, we bring the statistics-calculations into the monitoring [14-20].

In Figure 6 is presented the average speed of two of the Internet connections to the main router. The monitoring was carried out through RouterOS. The charts show empty spaces that indicate that there was 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. In the Mikrotik system the traffic of every interface can be monitored, queued or firewall ruled in real-time. In Figure 7 are shown the Ethernet traffic monitoring graphs. This diagram is observed if at least one of the devices supports RouterOS or SNMP and the network interface to be monitored is selected [21, 28].

Monitoring of the MHT system for two months is presented in Figure 8. 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 [29, 30]. The administrator receives SMS from Windows base DUDe by using Mikrotik attached GSM modem. A GSM device is connected with Mikrotik to send/receive purposes and a SMS base HTTP gateway. The user receives the DUDe notification *via* SMS using Mikrotik GSM/Mobile device, in case any critical device/server goes down. The system sends an 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®).

## CONCLUSION

The advantages of the system used for monitoring devices are: the status of various devices can be monitored and controlled from anywhere; the operation of the system is very simple and can be used by anyone with a basic knowledge of operating mobile phones; easy to upgrade as per the user requirement.

***Acknowledgement:*** *This paper is partially supported by National Scientific Program "Information and Communication Technologies for a Single Digital Market in Science, Education and Security (ICTinSES)", financed by the Ministry of Education and Science.*

## REFERENCES

1. H. Elshaer, F. Boccardi, M. Dohler, R. Irmer, *Proceedings of IEEE Global Communications Conference* (IEEE GLOBECOM'14), 1798 (2014).
2. F. Boccardi, J. Andrews, H. Elshaer, M. Dohler, S. Parkvall, P. Popovski, S. Singh, *IEEE Communications Magazine*, **54** (3), 110 (2016).
3. https://mikrotik.com/thedudeTerm.
4. https://techterms.com/definition/latency.
5. https://v-solution.en.alibaba.com/product
6. J. Moy OSPF version 2, *IETF RFC 2328*, (1998).
7. P. Tadimety, OSPF: A Network Routing Protocol, 1st edn., *Apress*, 2015.
8. A. Tabona, The top 20 free network monitoring and analysis tools for sysadmins, 2015.
9. R. Khan, S. Khan, R. Zaheer, M. Babar, *IJIEE*, **3**(1), 122 (2013).
10. S. Lee, K. Levanti, H. Kim, *Computer Networks*, **65**, 84 (2014).
11. J. Cheng, L. Hu, J. Liu, Q. Zhang, Ch. Yan, *Mathematical Problems in Engineering*, **1** (2014).
12. M. Smitha, R. Liub, R. Mounce, *Transportation Research Procedia*, **7**, 556 (2015).
13. F. Sapundzhi, M. Popstoilov, *Bulg. Chem. Commun.*, **50**, Special Issue B, 115 (2018).
14. D. Prangchumpol, *IJCEACIE*, **7**, 999 (2013).
15. Z. Wang, J. Crowcroft, *CCR*, **22**, 63 (1992).
16. D. Medhi, K. Ramasamy, Network Routing: Algorithms, Protocols, and Architectures, Morgan Kaufmann Publishers, Elsevier, 2017.
17. F. Sapundzhi, T. Dzimbova, P. Milanov, N. Pencheva, *International Journal Bioautomation*, **17 (1)**, 5 (2013).
18. F. Sapundzhi, T. Dzimbova, N. Pencheva, P. Milanov, *Der Pharma Chemica*, **8**, 118 (2016).
19. F. Sapundzhi, T. Dzimbova, N. Pencheva, P. Milanov, *Bulg. Chem. Commun.*, **50**, Special Issue B, 44 (2018).
20. F. Sapundzhi, T. Dzimbova, *Bulg. Chem. Commun.*, **50**, Special Issue B, 15 (2018).
21. F. Sapundzhi, K. Prodanova, M. Lazarova *AIP Conference Proceedings*, **2172**, 100008 1-6 (2019)
22. F. Sapundzhi, *International Journal of Online and Biomedical Engineering*, **15 (11),** 139 (2019).
23. F. Sapundzhi, T. Dzimbova, *International Journal of Online and Biomedical Engineering*, **15 (15)**, 39 (2019).
24. V. Kralev, R. Kraleva, IJACR, **7** (28), 1 (2017).
25. F. Sapundzhi, *International Journal of Online and Biomedical Engineering*, **15 (12)**, 88 (2019).
26. Sn. Andonova, *Tekstil i Obleklo*, **8**, 65 (2004).
27. Sn. Andonova, *Tekstil i Obleklo*, **6**, 144 (2017).

28. F. Sapundzhi, *Bulg. Chem. Commun.*, **51 (**4), 569 (2019).
29. G. Cherneva, *International Scientific Journal Trans. Motauto World*, **2 (4)**, 147 (2017).
30. I. Nedyalkov, A. Stefanov, G. Georgiev, *International Conference on High Technology for Sustainable Development, HiTech 2018 – Proceedings*, 1 (2018).