Optica Applicata, Vol. XLVII, No. 1, 2017
DOI: 10.5277/oa170114

Deep data analysis in gigabit passive optical networks

TOMAS HORVATH[1*], RADKO KRKOS[2], LUBOS DUBRAVEC[3]

[1]Brno University of Technology, Faculty of Elecrical Engineering and Communication, Department of Telecommunications, Technicka 12, 616 00, Brno, Czech Republic

[2]CESNET, z. s. p. o., Zikova 4, 821 08 Prague, Czech Republic

[3]Orange Slovakia corp, Metodova 8, 821 08 Bratislava-Ružinov, Slovakia

[*]Corresponding author: horvath@feec.vutbr.cz

This paper focuses on practical aspects of gigabit passive optical networks (GPON) diagnostics during deployment, for root-cause analysis and for research purposes. While GPON signalling analysis is already quite commonly used for diagnostics, the aim of this work is a holistic approach, including both signalling and user plane (payload) analysis. User plane analysis, especially if targeted at payload Ethernet, IP and transport layers, enables detection of additional group of problems that could limit or even prevent GPON internetworking and thus degrade the user perceived service quality. Integrated signalling and payload analysis is also interesting from the research point of view, leading to the ability to study equipment idiosyncrasies that would be hard to detect otherwise and it is also one of the enablers of equipment security verification. The mentioned theories were tested during a practical diagnostic session on a real GPON network deployment and this paper presents the findings.

Keywords: GPONXpert, gigabit passive optical networks (GPON) signalling, user plane, frame structure, payload analysis.

1. Introduction

Passive optical networks (PONs) are a widely discussed topic, and many operators have come to the conclusion that they are a preferable solution for access networks due to the simplicity of their deployment, maintenance, and expansion. It has been predicted [1] that the Internet video applications will experience an annual growth rate of 47% in the next decade. Furthermore, Internet traffic is not only about direct data transfer via file transport protocol (FTP) or hyper text transfer protocol (HTTP) but in many cases peer-to-peer (P2P) (such as BitTorrent, eMule, *etc*.) transmission is used [2], with machine-to-machine type communication also steadily becoming common. From another

point of view, future cloud services and streaming will need even higher bandwidth (for example, for 4K video) [3]. PONs are the most promising solution as they are a trade-off between price and bandwidth for end users. On the other hand, the bandwidth is shared with other customers because PON solution is based on point-to-multipoint (P2MP) topology. There are many standards for PONs. In general, the differences are in data transmission protocol, such as the Ethernet frame by Institute of Electrical and Electronics Engineers (IEEE) in EPON or a proprietary International Telecommunication Union (ITU) solution in gigabit passive optical networks (GPON). In this paper we deal only with the ITU standard (GPON), because it is the most commonly used technology in Czech Republic and Slovakia.

The main contribution of this paper is the analysis of the weak and strong points of the GPONXpert equipment. The measurement was performed in a commercial optical access network of a Slovak ISP (Internet Services Provider) and the results of the analysis of the captured data are presented here to academic and industrial public for review and further study and comments.

The rest of this paper is structured as follows. Section 2 provides an analysis of related work published in the field, specifically papers aimed at practical implementation of GPON technology, diagnostic methods for GPON deployments and GPON bandwidth dimensioning. Section 3 describes the basic principles of GPON access network, the function of individual elements and frame structure. Further sections are detailing the results of a practical diagnostic session on a real GPON network deployment, with the aim on general signalling, optical network unit management and control interface (OMCI), Ethernet payload, network layer and transport layer respectively. The findings are discussed and ideas for further research are presented in Section 9.

2. Related work

In the last few years, several publications regarding PON networks have been presented. Paper [4] deals with a trade-off between PON cost and resilience and also suggests protection mechanisms for TDM, WDM, and TWDM technologies. References [5, 6] present the latest standard of passive optical networks, NG-PON2. Reference [5] introduces the physical layer and its parameters (attenuation classes, penalty, bit error rate (BER) limit, *etc*.). The second article of this series, [6], proposes system design and discusses technological feasibility. For example, tuneable laser usage in optical network unit (ONU) has to be considered, because NG-PON2 network defines many wavelengths for each ONU and a construction using multiple lasers would be inefficient, large, hard to cool and therefore too costly; on the other hand, developing multiple models, each for a different wavelength, would be inflexible and logistically complicated for the Internet services providers (ISPs). The authors of those documents consider the NG-PON2 standard as well positioned to meet the new challenges of future optical access networks [6].

SKALJO *et al*. [7] present the usage of optical power meter in passive optical networks as an improvement of previous *status quo* in GPON networks when no control

mechanism was used. This enables a rapid decrease in service outage times in case of failure. Also a method for downstream and upstream power measurements and an underlying mathematical model are presented. ŽGALJ *et al*. [8] present an alternative measurement method, known as optical time domain reflectometry (OTDR), and offers the OTDR measurement results with analysis in point-to-point (P2P) networks used for long reach optical connections. It has to be stressed that PON networks are P2MP and OTDR is not commonly used to analyse PON physical layer characteristics because of the measurement complexity due to reflections, crosstalk and attenuation on the optical splitters that make practical end-to-end measurement infeasible. This method can still be used to measure the optical fibre characteristics from the measurement point up to the splitter, if special attention is paid, but the exact methodology is not described in the original document and is beyond the scope of this paper.

MENDONÇA *et al*. [9] highlights security issues caused by reflection in the PON physical medium. The authors design a GPON model where the reflections caused by the splitter are considered. For example, an eavesdropper can receive the signal reflected from the components in the network and read data transmitted by other users. This requires the use of delicate equipment as just the splitter crosstalk attenuation is about 55 dB or more, depending on the splitter order, while the transport attenuation also applies. The main aim of [9] is to estimate the maximum BER value for the GPON network to still be able to operate. The results are compared for positive-intrinsic-negative (PIN) and avalanche photodiodes (APDs) which should be used in the ONU(s). No attempt was made to decode and verify control plane and user plane data.

References [2, 3, 10] exhibit that the PON networks are the most promising solution for the future fixed, long reach access networks. CZÉKUS *et al*. [10] perform a cost analysis of future TDM and WDM-PON access networks by Pareto distribution. According to their results, for the future networks providing up to 600 Mbps bandwidth, TDM-PON is the preferable solution but for faster networks, WDM-PON is a more suitable technology.

This paper attempts to present the measurement of GPON network as already described in [11], but more attention is paid to the activation process of the ONU units in GPON networks. In this case, the GPONXpert tool was used for capturing and processing of data but there are of course also different transmission convergence (TC) layer analysers available, such as TELNET GPON Doctor or NIVA GPON analyser, each with different set of capabilities.

3. GPON network

GPON is the most promising solution for access networks, historically mainly in European countries, nowadays all around the world. It offers many features, such as providing Triple Play services (broadband Internet access, television and telephony) on the same optical fibre, scalability, dynamic bandwidth allocation (DBA), reliable delays, and a simple management of tree topology. The previous standards only allowed transmission of asynchronous transfer mode (ATM) cells but GPON is the first standard which

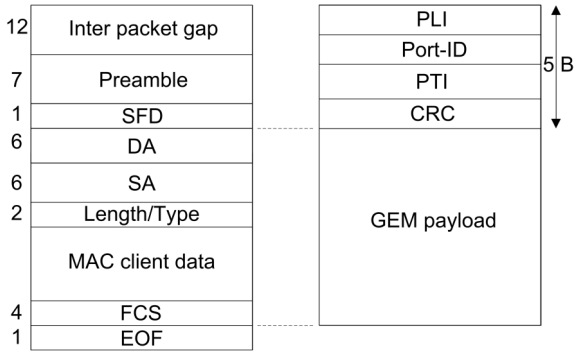

Fig. 1. Ethernet encapsulation inside the GEM frame.

allows transfer of both ATM cells and Ethernet frames. The ATM cell transport was supported until the 2004 revision of [12] but in the most current revision (2014) it was deprecated. It should be noted that the used diagnostics tool, GPONXpert, does not support ATM payload analysis. The L2 Ethernet frame is transferred inside a GPON encapsulation method (GEM) frame, no L1 Ethernet structures, such as inter-packet gap, preamble, and start of frame delimiter (SFD) are included (see Fig. 1). In general, the basic GPON topology consists of the following elements: optical line termination (OLT), optical network unit (ONU), and optical distribution network (ODN). Of the OLT elements there could be one or more, depending on the ISP's preferences but the most common variant, due to cost efficiency, is a single OLT serving many customers. Expanding on that, a single OLT is able to serve up to 128 customers on a single OLT port (OLT usually has 4 to 16 ports, depending on the chassis). Note that the OLT, as the Internet facing border element, performs encapsulation of downstream traffic and de-encapsulation of traffic targeted towards public networks. The second active device in GPON topology is the ONU which is located at the customer's premises and performs the conversion from optical domain to electrical domain. Finally, the ODN consists of everything between OLT and ONU, such as the optical fibres, splitters, connectors, *etc*.

In this paper we deal with data analysis in GPON in both downstream and upstream directions. If the basic topology as depicted in Fig. 2 is considered, data are broadcast in the downstream direction. In the beginning the ONUs look for their own parameters (serial number, ONU-ID, *etc*.) in GEM frames to identify the activation attempt. GPON frames have all exactly the same duration of 125 μs, regardless of whether they do or do not contain any data. Considering the topology shown in Fig. 2, it is of note that for each ONU the distance to OLT is different. That is the reason why it is necessary to offset various ONUs by an equalization delay parameter. This delay is assigned by the OLT during the activation process (for details refer to [11]). Next the ONU waits for a random time period before transmitting data. However, the upstream direction does not use broadcast, instead time slots which are assigned by the OLT for each and all ONUs are used. In this paper, the DBA algorithm is not considered, so the ONUs

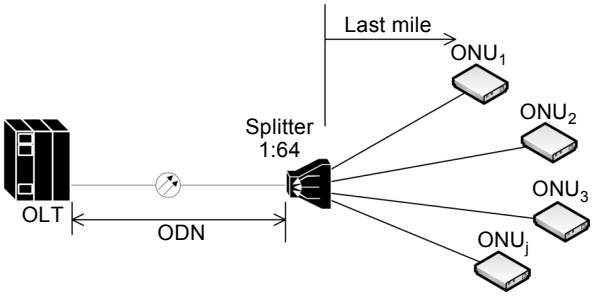

Fig. 2. The basic GPON topology.

are only expected to transfer data in time slots with pre-specified time offset and duration (start and stop time).

This paper concentrates on activation process and user data analysis. On the other hand, the activation process description is omitted because it was included in detail in our previous article [11]. Data analysis is confronted with request for comments (RFCs) and standards for various protocols.

4. Signalling

The user plane and control plane data between OLT and ONU are transferred using GEM frames. Therefore, it is not directly possible to use a common packet analyser, such as Wireshark, to read the content of each frame. In our case, we used the GPONXpert analyser in standard mode where data are saved to hard drive and post-processed for deep inspection of the transferred data (both user plane and control plane data). The GPONXpert tool has an option for continuous mode requiring additional licensing which was not available for our use. The control plane data can be divided into two parts: signalling and optical network unit management and control interface (OMCI). First of all, attention has to be paid to the signalling data with deep analysis of the frame content. Note that during the connection establishment phase the *Assign ONU-ID*, *Configure Port-ID*, *Assign Alloc-ID*, *Encrypted Port-ID*, *Encryption Key*, *Key Request* and *Key Switching Time* messages are transmitted three times what can be also seen in the tool's output. Complete GPON signalling message flow is depicted in Fig. 3.

In the analysed sample it can be seen that a PLOAM (Physical Layer Operations, Administration and Maintenance) message named *Serial Number ONU* was transferred from ONU to the OLT. Further, this message uses the ONU-ID of 255 (broadcast) and also includes the vendor serial number (in our case 0x6A4F7431, identifying the vendor as Huawei), a list of supported data profiles (GEM and/or ATM), and the value of random delay of 79 μs [12]. In other words, the mentioned values represent PLOAM broadcast and the OLT, based on this message, extracts the serial number and allocates an ONU-ID to this ONU [12]. OLT measures the time between two successive *Serial Number ONU* messages to establish unique random delay, which is used to eliminate the impact of various distances between different ONUs and the OLT. When the OLT

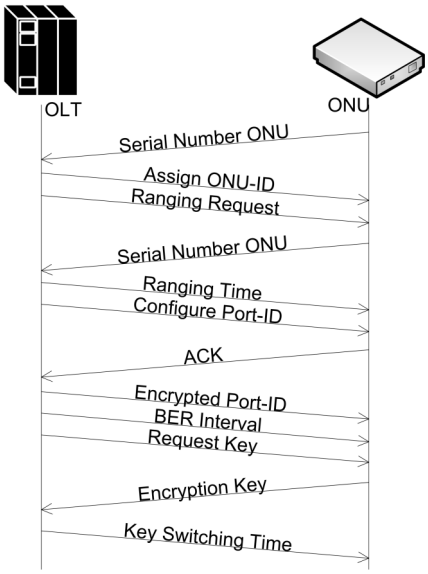

Fig. 3. GPON signalling message flow.

receives the ONU-ID, it sends the PLOAM message *Assign ONU-ID* based on the unique delay parameter. Although the OLT already knows the assigned ONU-ID, it still cannot transmit using unicast addressing based on this ONU-ID because the opposing side – the ONU still does not recognize the ONU-ID as its own, therefore the communication must be still done by broadcast, using the ONU serial number as the identifier [12]. Therefore, the OLT sends the *Assign ONU-ID* message as broadcast. Each ONU receives this message but it is processed only by the designated ONU, based on the serial number comparison. Looking at more details of the broadcast message, there can be seen a Psync portion (synchronization sequence, such as frame delimiter); forward error correction (FEC) indicator is 1 (the data are protected by FEC); ATM partition length is and has to be 0 (the ONU does not support ATM mode according to the *Serial Number ONU* message); and the BWmap portion (bandwidth allocation) is equal to 0 because the ONU cannot transfer data according to [12], as it does not yet have all the required parameters.

The very next moment the OLT sends the unicast *Ranging Request* message for the BWmap event. The ranging request is addressed to the unique ONU-ID (in our case 2) with the numerical specification of the BWmap length. In other words, our ONU is able to use a single grant to transmit data. The ONU answers by a *Serial Number ONU* message using the maximum priority transmission container (T-CONT) class, indicating urgent data. Since the ONU has sent the ranging response, the *Ranging Time* message, the OLT calculates a new value of the equalization delay. Next the OLT sends the *Configure Port-ID* message to a specific ONU (indicated by the ONU-ID identifier). This identifier is the most important from the data transmission point of view because it is used for the allocation of the selected flows into a single GEM frame

T a b l e 1. Captured GEM signalling sample from the GPON network under analysis.

Time	ONU-ID	Message type	Message source	Direction	Details
00:56.698166	Unassigned ONU ID	Serial Number ONU	PLOAM message	Upstream	Vendor ID = HWTC, Vendor SN = 0x6A4F7431, Random delay = 79 μs, ATM support = Disable, GEM Support = Enable, ONU Tx power level = Low Power
00:57.539500	Broadcast message	Assign ONU-ID	PLOAM message	Downstream	Psync = 0xB6AB31E0, Ident FEC indicator = 1, BWmap = 0, ATM partition length = 0
00:57.740125	2	Ranging Request	BWmap event	Downstream	ONU ID = 2
00:57.740161	2	Serial Number ONU	PLOAM message	Upstream	Urgent PLOAMu waiting = 1, ONU-ID = 2
00:57.741500	2	Ranging Time	PLOAM message	Downstream	Psync = 0xB6AB31E0
00:57.778000	2	Configure Port-ID	PLOAM message	Downstream	
00:57.778158	2	Acknowedge	PLOAM message	Upstream	ONU ID = 2, DM_ID = Configure port-ID
00:57.778875	2	Encrypted Port-ID/VPI	PLOAM message	Downstream	Encrypted descriptor = Not Encrypted
00:57.779750	2	BER Interval	PLOAM message	Downstream	ONU ID = 2
01:00.372250	2	Request Key	PLOAM message	Downstream	ONU ID = 2
01:00.372658	2	ENcryption Key	PLOAM message	Upstream	Key index = 7, Fragment index = 0, Key bytes = 0xCDE1D864096703CC
01:00.382500	2	Key Switching Time	PLOAM message	Downstream	Allocation ID = 258, StartTime field = 0 μs, StopTime field = 15 μs

(if possible depending upon size). The ONU has to send acknowledge (ACK) messages in exactly the same amount as the number of received messages (in our case three times). As can be seen in detail in Table 1, the downstream message identification (DM-ID) contains a field named *Configure Port-ID* containing the name of the confirmed message. Then, the OLT checks whether the port-ID is encrypted or not. In our case the Port-ID is not encrypted because the ONU is still in registration process. The ONU confirms each correctly received message by an ACK message. Further, the OLT sends a BER message, which defines the accumulation interval per ONU expressed as the number of downstream frames for the ONU considered for counting the number of downstream bit errors [12]. Now, the ONU knows only the Port-ID but for the bidirectional data communication it also requires an Alloc-ID. The allocation identifier identifies a traffic-bearing entity (can be represented by T-CONT) that is the recipient of data blocks allocated in upstream during the BWmap procedure [12]. Note that a single ONU has to have at least one Alloc-ID which is equal to the ONU-ID and this is not transmitted by OLT in the *Assign Alloc-ID* message. In our case, the OLT provides three Alloc-IDs of 258, 514, and 770 from the allocation range of 256 to 4095. As always, the ONU must acknowledge each PLOAM message by an ACK message. Then, the encryption of the Port-IDs is checked again by OLT and ONU answers with ACK messages. This part is optional because by default the data encryption is disabled. Even in commercial use, many ISPs worldwide do not enable Port-ID encryption.

In general, the communication over the optical fibres is considered secure enough, but there are means to read the content of the GEM frames and the frame structure is well-known. The encryption establishment procedure starts by the OLT sending the *Request Key* PLOAM message (transmitted only once). Initially, the ONU has its own encryption key but when OLT sends this message the ONU needs to generate a new key. The new key is calculated based on a unique parameter, for example the ONU serial number, and then it is transmitted three times in the PLOAM *Encryption Key* message. Note that the key may be divided into multiple parts based on the key length. The OLT recognizes successive key parts by the fragment index. The first fragment (0–7 bytes) of the key has fragment index of 0, for additional fragments, the fragment index gets incremented. In general, the OLT answers by the *Key Switching Time* message with the specification of the time (specified by the StartTime and StopTime parameters in BWmap field for each Alloc-ID), when the ONU is ready to use the new key. In our case it means that the new key will be used for the very next frame with the Alloc-ID of 258 since the 0th until the 15th microseconds. The ONU confirms each frame and from this point on the communication between OLT and ONU is encrypted.

5. Optical network unit management and control interface (OMCI)

The operation, administration and maintenance (OAM) communication is transferred inside the OMCI channel and is started as soon as the signalling phase is finished. In

T a b l e. 2. Captured OMCI sample from the GPON network under analysis.

Time	Transaction ID	Message type	Managed entity type	Direction
00:57.945625	10274	Get	(256) ONU G	Downstream
00:57.946908	10274	Get Response	(256) ONU G	Upstream
00:57.955500	10278	Get	(007) Software image	Downstream
00:57.956658	10278	Get Response	(007) Software image	Upstream
00:58.031500	10297	Get	(138) VOIP config data	Downstream
00:58.032658	10297	Get Response	(138) VOIP config data	Upstream

the presented case, two ONUs can be seen (in GPONXpert protocol notation – ONU and ONU2) as Table 2 illustrates. The OMCI procedures are initiated by the OLT by sending either *Get* or *Set Request* message. In general, when the OLT sends the *Get* or *Set Request* message, the ONU needs to reply by *Get/Set Response* message. The most important part of OMCI analysis here is the software image entity type because the ONU is authorized by its own serial number against the OLT database (in this particular ISP implementation). If the OLT does not have a record for the given ONU, the ONU is prevented from downloading the software image with configurations. Otherwise, the ONU downloads the software image from OLT. Note that the software images should be different for various customers because the ISP may offer different transmission speeds, functions such as TV packs, *etc*., to different customers. When the ONU has loaded the software image, it is able to transfer customer metadata and service support data, for example the request for a public IP address or higher upstream speed, *etc*. In general, the customers use multiple services in a bundle (data, video and voice). These services have different quality of service (QoS) requirements with generally the most demanding service being the voice transmission; therefore the ONU downloads another configuration data file for voice over IP (VoIP) telephony. This file includes configuration options such as the codec, constant bit rate allocation, and T-CONT priority.

Those are the most important OMCI channel procedures, but the OLT also uses this channel for synchronization verification, alarms indication (for example when the synchronization is lost), and FEC monitoring (the ONU records the BER of the received frames), see Table 2 for further details.

6. Ethernet payload analysis

Looking further at the GPON payload, an Ethernet based layer can be seen. Based on the analysis performed by the TraceSpan GPONXpert tool, several interesting parameters can be seen in the report on the Ethernet layer. The tool provides Ethernet frame listing including frame number, direction, time of the arrival on the medium, VLAN ID, source and destination MAC addresses and protocol identifier of the network layer protocol. Unfortunately, the full binary frame output is not available.

In the analysed example, all valid communication in both upstream and downstream direction is performed under the virtual LAN ID of 836; therefore all transmissions are done on the same L2 network segment. Next of note is that two distinct physical devices are the source of communication in the downstream direction. Based on the Organizationally Unique Identifier (OUI) of the MAC addresses (E0:97:96) in correlation to [13], both of these devices are manufactured by Huawei Technologies Co., Ltd., and therefore these are expected to be logical OLTs. The destination addresses are mostly either for IPv4 (01:00:5E) or IPv6 (33:33:00–33:33:FF) multicast, see [14]. The only other destination address in the downstream direction belongs again to a device manufactured by Huawei Technologies Co., Ltd., this time the ONU, communicating with one of the OLTs.

For the upstream direction, similar characteristics can be seen as the traffic follows the request-response pattern. As for the ONU identified in downstream, there are counter messages for the IPv6 multicast and responses from the OLT. In addition, there is another device, based on the OUI of the MAC address (D8:9D:67) identified in correlation with [13] as manufactured by Hewlett Packard. This device is transmitting to several IPv4 and IPv6 multicast addresses, with no responses in the opposite direction.

There is a visible phenomenon in the downstream direction, when many detected Ethernet frames are false positives. Due to their headers being filled with completely random content, these are most definitely decoding errors and not actual Ethernet frames on the medium. Because of unavailability of raw Ethernet frame data this cannot

T a b l e 3. Example of decoding errors on Ethernet layer in downstream direction.

Time (start of capture)	Destination MAC address	Source MAC address	Type	Direction
00:01:02.710125	CE:94:97:DC:C4:13	C5:70:9F:3D:1A:52	0x9C68	Downstream
00:01:04.710750	BD:D8:4F:D5:F8:CE	8C:CC:EA:6C:26:CF	0x4713	Downstream
00:01:04.711375	B0:2D:71:F9:A7:83	B3:52:D6:4D:E2:18	0x329C	Downstream
00:01:06.010875	2B:0D:D5:C4:69:90	47:B0:5F:C2:A6:33	0x4561	Downstream
00:01:06.069750	5C:58:34:AB:30:FF	9E:0F:7B:F1:C8:D5	0xF83E	Downstream
00:01:07.010750	63:27:33:B5:80:54	95:D2:E8:6A:4C:06	0xADF4	Downstream
00:01:08.011625	A9:AA:F3:FC:E1:7A	25:8D:02:BD:E3:D7	0xC314	Downstream
00:01:08.069750	57:8A:41:57:31:B4	C5:0D:F0:C7:9A:DC	0x7D56	Downstream
00:01:09.010625	05:71:06:B4:31:8D	69:EA:C5:BF:19:0C	0x9977	Downstream
00:01:10.011375	73:A6:77:CD:FC:8B	C9:EC:6B:F8:E2:D9	0x88DA	Downstream
00:01:10.069750	61:A2:09:4A:C4:D0	EA:EF:2F:70:68:79	0xB167	Downstream
00:01:11.022500	C3:06:EE:42:83:F9	D4:A5:AE:6A:37:48	0xB06B	Downstream
00:01:12.069750	94:AE:AB:BF:75:C4	19:30:11:9F:A0:C3	0x5F57	Downstream
00:01:18.043500	25:90:A0:5E:7E:04	63:D7:16:EF:E2:68	0x5925	Downstream
00:01:18.043500	1E:42:0B:69:F8:9C	68:1C:4C:2C:BE:24	0xA983	Downstream
00:01:18.043500	B5:19:E3:32:AE:84	16:02:78:74:89:D6	0xE08	Downstream

be sufficiently proven using only the output of the tool, but based on conflicting times of arrival, it seems that these frames are accidentally detected based on pattern matching in the bit stream. Of course the cyclic redundancy check (CRC) fails on such phantom Ethernet frames, so these are easily distinguishable in the tool's output, see Table 3 for illustration.

7. Network layer analysis

Next, let us have a look at the network layer analytic capabilities of the GPONXpert tool. The tool distinguishes between IPv4 and IPv6 traffic and provides information concerning these different network layer protocols separately.

For IPv4, the output includes datagram time of arrival, total length in octets, source and destination IP addresses, direction, next protocol identification and optional IPv4 header element length. The analysed example data shows 31 decoded IPv4 datagrams, two of which are in the downstream direction, matching the Ethernet layer analysis results of one of the OLTs sending two IPv4 multicast messages and receiving no response. The source IP address (192.168.1.1) is from a private, publicly unrouteable, range [15] and the destination is a multicast address (224.0.0.1) used to address all hosts in the current subnet, see [16]. The payload is identified as Internet Group Management Protocol (IGMP) [17], see Table 4. The traffic in the upstream direction is all transmitted by one different host, addressed with yet again an unrouteable public IP address (192.168.100.2) [15], which belongs to a different subnet than the downstream communication, at least if classful addressing scheme was used [18]. The destination IP addresses are, according to [16], aimed at all routers in the current subnet (224.0.0.2), indicating some sort of routeing protocol; link-local multicast name resolution [19] (224.0.0.252) and organization-local scope [20] (239.255.255.250). Again, IGMP is

T a b l e 4. GPONXpert output regarding IGMP.

Time (start of capture)	Total length	Protocol	Source address	Destination address
00:00:18.932533	32	IGMP (0x02)	192.168.100.2	224.0.0.252
00:00:20.516033	32	IGMP (0x02)	192.168.100.2	224.0.0.2
00:00:20.517662	32	IGMP (0x02)	192.168.100.2	224.0.0.252
00:00:20.549283	32	IGMP (0x02)	192.168.100.2	224.0.0.252
00:00:21.052408	32	IGMP (0x02)	192.168.100.2	224.0.0.252
00:00:27.932783	32	IGMP (0x02)	192.168.100.2	224.0.0.2
00:00:27.934783	32	IGMP (0x02)	192.168.100.2	224.0.0.252
00:00:27.939158	32	IGMP (0x02)	192.168.100.2	224.0.0.2
00:00:27.946033	32	IGMP (0x02)	192.168.100.2	224.0.0.252
00:00:28.037033	32	IGMP (0x02)	192.168.100.2	224.0.0.252
00:00:28.537283	32	IGMP (0x02)	192.168.100.2	224.0.0.252

the next protocol. All of the datagrams include the Router Alert IPv4 option [21], which indicates that routers should examine the packets more closely. The Router Alert IPv4 option is used in IntServ resource reservation along the way, see [22] for further details on this procedure.

For IPv6, the analysis output possibilities of the tool are similar to those of IPv4, except for the optional elements support, which is not present. Looking at the analysed example, most of the communication is obviously service traffic, such as address negotiations (null source address), multicast group registrations, multicast used as link local broadcast (FF02::1), refer to [23], *etc*. Also, it is of note that the analysed example shows very heavy use of IP in IP encapsulation [24], all in conjunction with the use of multicast listener discovery protocol version 2 [25], indicated by the used destination address (FF02::16) [23]. The rest of the traffic seems general, there can be seen some TCP and UDP connections over the IPv6.

8. Transport layer analysis

As for the transport layer, only user datagram protocol (UDP) decoding is supported by the tool, other transport layer protocols, such as transmission control protocol (TCP), albeit identified to be present in the traffic from the network layer analysis, have no statistics view present in the tool's output. For UDP, the output consists of datagram time of arrival, source and destination ports, payload length and direction.

The analysed example displays a few domain name server (DNS) transactions, several NAT port mapping protocol [26] transactions and one DHCPv6 [27] address negotiation in the beginning. All of these are network management procedures and show little information about the user behaviour. The observed pattern of communication is typical for user equipment early initialization.

9. Conclusion

GPONXpert is a convenient tool for GPON network diagnostics, especially for transmission convergence layer analysis because it is able to capture all communication between the OLT and ONU elements in both directions. As illustrated through the analysis of example data output from the TraceSpan GPONXpert tool, the Ethernet and higher layer analytic options of the tool are very limited in general network engineering usefulness and diagnostic potential, as opposed to detailed analysis of signalling and OMCI messages. The main problems are the requirement of manual correlation between different layers, which is unreliable anyways due to lack of matchable identifiers, and the output being seriously limited in details. Based on this trial, a better solution should be used for any serious user plane (payload) analysis of GPON traffic, preferably one that allows the export of raw packet data in some general traffic capture format, for example PCAP. Also of interest is the mechanism of resource reservation,

its use for IPv4 and IPv6 traffic, identification of the element adding this information and those consuming it, therefore this topic should be investigated further.

Acknowledgements – This work was supported by the National Sustainability Program under the grant LO1401 and the project CESNET E-infrastructure LM2010042 funded by the Ministry of Education, Youth and Sports of Czech Republic.

References

[1] RUFFINI M., MEHTA D., O'SULLIVAN B., QUESADA L., DOYLE L., PAYNE D.B., *Deployment strategies for protected long-reach PON*, Journal of Optical Communications and Networking **4**(2), 2012, pp. 118–129.

[2] FORZATI M., LARSEN C., *On the symmetry requirements for tomorrow's fibre access networks*, 11th International Conference on Transparent Optical Networks, June 28–July 2, 2009, Azores, IEEE, pp. 1–4.

[3] WEIS E., BREUER D., LANGE C., *Technologies for next generation optical access*, 14th International Conference on Transparent Optical Networks (ICTON), July 2–5, 2012, Coverty, IEEE, pp. 1–2.

[4] EFFENBERGER F.J., *PON resilience*, Journal of Optical Communications and Networking **7**(3), 2015, pp. A547–A552.

[5] JUN SHAN WEY, NESSET D., VALVO M., GROBE K., ROBERTS H., YUANQIU LUO, SMITH J., *Physical layer aspects of NG-PON2 Standards – Part 1: optical link design*, Journal of Optical Communications and Networking **8**(1), 2016, pp. 33–42.

[6] YUANQIU LUO, ROBERTS H., GROBE K., VALVO M., NESSET D., ASAKA K., ROHDE H., SMITH J., JUN SHAN WEY, EFFENBERGER F., *Physical layer aspects of NG-PON2 Standards – Part 2: system design and technology feasibility*, Journal of Optical Communications and Networking **8**(1), 2016, pp. 43–52.

[7] SKALJO E., MUJCIC A., SULJANOVIC N., *Usage of optical power meter in passive optical networks*, Fiber and Integrated Optics **30**(5), 2011, pp. 308–321.

[8] ŽGALJ A., SKALJO E., KADUŠIĆ E., *Pulse width as an influencing factor in optical time domain reflectometry measurements*, 19thTelecommunications Forum (TELFOR) Proceedings of Papers, November 22–24, 2011, Belegrad, IEEE, pp. 832–835.

[9] MENDONÇA C., LIMA M., TEIXEIRA A., *Security issues due to reflection in PON physical medium*, 14th International Conference on Transparent Optical Networks (ICTON), July 2–5, 2012, Coverty, IEEE, pp. 1–4.

[10] CZÉKUS J., MEGYESI P., MITCSENKOV A., MAZROA D., *Hardware cost and capacity analysis of future TDM- and WDM-PON access networks*, 16th International Conference on Transparent Optical Networks (ICTON), July 6–10, 2014, Graz, IEEE, pp. 1–4.

[11] HORVATH T., MUNSTER P., JURCIK J., KOCI L., FILKA M., *Timing measurement and simulation of the activation process in gigabit passive optical networks*, Optica Applicata **45**(4), 2015, pp. 459–471.

[12] *G.984.3: Gigabit-Capable Passive Optical Networks (G-PON): Transmission Convergence Layer Specification*, International Telecommunication Union, 2014, pp. 1–170.

[13] *IEEE Public Organizationally Unique Identifier List*, 2015-12, IEEE, 2015.

[14] *Ethernet Numbers: IANA MAC Address Block*, IANA, 2015.

[15] REKHTER, Y., MOSKOWITZ B., KARRENBERG D., GROOT G.J., *RFC 1918: Address Allocation for Private Internets*, February 1996.

[16] VENAAS S., *IPv4 Multicast Address Space Registry: Local Network Control Block*, 2016.

[17] FENNER W., *RFC 2236: Internet Group Management Protocol, Version 2*, 1997.

[18] FULLER, V., LI T., YU J., *RFC 1338: Supernetting: An Address Assignment and Aggregation Strategy*, 1992.

[19] ABOBA B., THALER D., ESIBOV L., *RFC 4795: Link-Local Multicast Name Resolution (LLMNR)*, 2007.
[20] MEYER D., *RFC 2365: Administratively Scoped IP Multicast*, 1998.
[21] KATZ D., *RFC 2113: IP Router Alert Option*, 1997.
[22] BRADEN B., ZHANG L., ESTRIN D., HERZOG S., JAMIN S., *RFC 3315: Resource ReSerVation Protocol (RSVP)*, 1997.
[23] VENAAS S., *IPv6 Multicast Address Space Registry: IPv6 Multicast Address Scopes*, 2015.
[24] PERKINS C., *RFC 2003: IP Encapsulation within IP*, 1996.
[25] VIDA R., COSTA L., *RFC 3810: Multicast Listener Discovery Version 2 (MLDv2) for IPv6*, 2004.
[26] CHESHIRE S., KROCHMAL L., *RFC 6886: NAT Port Mapping Protocol (NAT-PMP)*, 2013.
[27] DOMS R., BOUND J., VOLTZ B., LEMON T., PERKINS C., CARNEY M., *RFC 3315: Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*, 2003.

Received May 5, 2016
in revised form July 15, 2016