UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CHARTER COMMUNICATIONS, INC.,
PETITIONER,

v.

IARNACH TECHNOLOGIES, INC.,
PATENT OWNER.

CASE IPR2024-01286
PATENT 8,942,378

DECLARATION OF DR. KERRY I. LITVIN

TABLE OF CONTENTS

CURRENT EXHIBIT LIST iii
I. INTRODUCTION 1
II. PROFESSIONAL BACKGROUND AND QUALIFICATIONS 1
III. RELEVANT TIME 6
IV. LEVEL OF ORDINARY SKILL IN THE ART 7
V. MATERIALS CONSIDERED 9
VI. OVERVIEW OF THE PATENTED INVENTION 10
VII. RELEVANT PROSECUTION HISTORY 20
VIII. OVERVIEW OF THE CITED REFERENCES 26

A. RFC 1112 (Aug. 1989) ("IGMPv1") 26
B. Overview of Japanese Patent Publication No. JP2004-343243A ("Murakami") 29

1. Nomenclature and Topology 29
2. Functionality 33

C. RFC 4601 ("PIM-SM") 40
D. CITED REFERENCES DEAL WITH "LOW LEVEL" FUNCTIONALITY 44

IX. CLAIM CONSTRUCTION 49

A. "Services" 49
B. "Common Key" 53
C. "Bearer Channel" 53

X. PETITIONER'S PRIOR ART REFERENCES FAIL TO RENDER OBVIOUS ANY CHALLENGED CLAIM 54

A. All Challenged Claims (Claims 1–13): Murakami in View of IGMPv1, PIM-SM, and the Knowledge of Persons of Skill, Alone or in Combination, Do Not Teach Limitations 1b/c and

9c, Found in Every Claim, or Show That These Limitations Would Be Obvious 54

[1b/c] . . . using **the common key** to encrypt multicast service data of **all different multicast services** in a **same bearer channel** and then sending encrypted data; wherein the multicast service data of **all different multicast services** in the **same one bearer channel use a same common key** to carry out encryption; 54

[9b] said encryption unit is configured to: encrypt multicast service data of **all different multicast services born in a same one bearer channel with a same common key**; 54

XI. DECLARATION 87

APPENDIX A (RESUME) 88

CURRENT EXHIBIT LIST

No.	Brief Description
1001	U.S. Patent No. 8,942,378 ("'378 Patent" or "Patent-at-Issue")
1002	'378 Patent Prosecution History
1003	Declaration of Dr. George Rouskas
1004	JP2004-343243A (Published Dec. 2, 2004) ("Murakami")
1005	Corrected Certified English Translation of Murakami
1006	RFC 1112 (Aug. 1989) ("IGMPv1")
1007	RFC 4601 (Aug. 2006) Protocol Independent Multicast—Sparse Mode ("PIM-SM")
1008	U.S. Patent Application 20020150097 A1 ("Yen")
1009	Complaint, *Iarnach Techs. Ltd. v Charter Comms., Inc.*, 2:24-cv-00230 (E.D. Tex. filed Apr. 5, 2024) (Doc. 1)
1010	RFC 2362
1011	Docket Control Order, *Iarnach Techs. Ltd. v Charter Comms., Inc.*, No. 2:24-cv-00230 (E.D. Tex. filed Aug. 7, 2024) (Doc. 55)
2001	Intentional Left Blank
2002	Intentional Left Blank
2003	Jiang *et al.*, Multicast Broadcast Services Support in OFDMA-Based WiMAX Systems, IEEE COMMUNICATIONS MAGAZINE (Aug. 2007) ("Jiang2007")
2004	Excerpts from U.S. Patent No. 7,194,090 (Issued Mar. 20, 2007)
2005	ITU-T Rec. G.984.1 (03/2003) Gigabit-capable Passive Optical Networks (GPON): General characteristics, *available at* https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-G.984.1-200303-S!!PDF-E&type=items
2006	Service, Microsoft Computer Dictionary (2002 5th Ed.)
2007	Excerpt from Raiz, Capstone Project Report for Multicast in MPLS based Networks and VPNs (Apr. 28, 2015), *available at*, https://era.library.ualberta.ca/items/0b81726d-9494-4a67-9498-0e462de8190e/view/3eee32bb-cabd-417f-b45d-0fac28d90014/Riaz_H.pdf

No.	Brief Description
2008	Excerpt from Source Specific Multicast (SSM) Mapping, Cisco (May 26, 2011), *available at* https://www.cisco.com/en/US/docs/ios-xml/ios/ipmulti_igmp/configuration/15-1s/SSM_Mapping.html
2009	Carmoody, Netflix Opens Up Streaming-Only for US Customers, DVD Plans Get Price Bump (Nov. 22, 2010)
2010	Source, Webopedia, (May 2021), *available at* https://www.webopedia.com/definitions/source/
2011	Excerpt from HILL, The Canadian Journal of Economics, Vol. 32, No. 2, pp. 426–46 (Apr. 1999), *available at* https://www.jstor.org/stable/136430
2012	Internet Group Management Protocol, Version 3 (Oct. 2002), *available at* https://datatracker.ietf.org/doc/html/rfc3376 ("IGMPv3")
2013	3 Reasons Why a Cloud Hosting Datacenter Provided with Multiple Datacenters Should Be in Your Firm's Future, Network Specialists, *available at* https://www.networkspecialists.com/3-reasons-why-a-cloud-hosting-datacenter-provider-with-multiple-datacenters-should-be-in-your-firms-future/
2014	Diot *et al.*, Deployment Issues for the IP Multicast Service and Architecture, IEEE Network, Vol. 14 Issue 1, pp. 78–88 (Feb. 29, 2000), *available at* https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=a434d6cbf08297f284440fc0d07f7707fe8311a7
2015	Service Provider, National Institute of Standards and Technology, U.S. Department of Commerce (last visited October 30, 2024), *available at* https://csrc.nist.gov/glossary/term/service_provider (citing NISTIR 4734 (1992) *available at* https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir4734.pdf)
2016	Intentional Left Blank
2017	Intentional Left Blank
2018	Intentional Left Blank

I. INTRODUCTION[1]

¶1. My name is Dr. Kerry I. Litvin. I have been retained by Iarnach Technologies, Inc. ("Patent Owner") to provide my expert assessment and technical opinions in connection with the above captioned inter partes review ("IPR") of U.S. Patent No. 8,942,378 ("'378 Patent" or "Patent-at-Issue"), Ex. 1001.

¶2. Patent Owner is compensating me for my study and testimony in this case. This compensation is not contingent upon my performance, the outcome of this IPR, or any issues involved in or related to this IPR.

¶3. This declaration is based on information currently available to me. I reserve the right to expand, modify, or supplement my opinions if I become aware of evidence or information that was not available for review at the time I drafted this declaration.

II. PROFESSIONAL BACKGROUND AND QUALIFICATIONS

¶4. I have attached my resume as Appendix A to this declaration. The resume includes a list of my qualifications and publications. Nonetheless, I now summarize my background related to the field of encrypting multicast service data in passive optical network ("PON") systems.

[1] All emphasis is added in this report unless otherwise noted.

¶5. I am currently the President and Founder of H-Bar Omega, LLC, a high-technology consultancy with expertise in fiber optic telecommunications technologies, which serves the needs of clients in the legal and investment professions who have interests in this field of technology. I founded the H-Bar Omega, LLC consultancy in the spring of 2014.

¶6. Prior to this, from June 2011 through December 2013, I was a Principal Research and Development Engineer at Futurewei Technologies (also known as Huawei Technologies). I served directly under the company's Vice President for Access Optical Network Research and Development. My focus was the development of new technologies for passive optical (unrepeated) access networks.

¶7. Prior to joining Futurewei, I was a Principal Staff Engineer at the Motorola Broadband Communications Sector (now part of CommScope, Inc.) from February 2000 through October 2010 and worked in the Advanced Optical Communications Technology Applied Research and Development Group. My focus there was the development of state-of-the-art fiber optic communications technologies for applications in both hybrid-fiber-coaxial access network infrastructure and passive optical networks.

¶8. I previously had served as a Staff Engineer working for the Lockheed Martin Missiles and Space Company from 1995 through 2000, developing cutting-edge microwave and millimeter-wave communications components and systems and also

fiber optic signal distribution technologies all for applications onboard space-based platforms. This included acting as a principal engineer conducting the development of the first 60 GHz space-qualified power amplifier utilizing monolithic millimeter-wave integrated circuits.

¶9. I received my Ph.D. in Electrical Engineering (minor in Applied Physics) from Cornell University, Ithaca, NY in 1994. I was awarded an Arco Company Fellowship to support my first year of studies at Cornell. During my second year at Cornell University, I was named a Howard Hughes Doctoral Fellow, and the Hughes Aircraft Company then supported me during all subsequent years of study and research through to my graduation. My dissertation was entitled "Metal-Semiconductor-Metal Photodiodes with applications in Monolithic Optical Receiver Circuits Capable of Detecting and Amplifying a Millimeter-Wave Modulation Signal Being Transmitted Via an Optical Carrier."

¶10. I received my M.S. degree in Electrical Engineering from the California Institute of Technology (Caltech), Pasadena, CA in 1986. While at Caltech I was an Institute Fellow. My research was supervised by Professor David Rutledge and focused on microwave power combining in a quasi-optical free-space cavity.

¶11. In 1985, I received a B.S. degree in Electrical Engineering from Drexel University, Philadelphia, PA and graduated with high honors, in the top 2% of my

class. My senior research project at Drexel concerned the optical control of a microwave oscillator.

¶12. Through education and work, I have gained extensive experience in all aspects of the design and implementation of fiber optic communications networks, subsystems, and components. This includes advanced research and development efforts in systems, components, and physical phenomena occurring within the fiber insofar as they impact the quality of the communications signals being transmitted. I have extensive hands-on laboratory experiment construction and test and measurement experience and have also developed various theoretical mathematical models to accurately predict the performance of optical communication systems using computer simulations. I have dealt directly with some of the largest telecommunications service providers in designing optical networks and troubleshooting optical communications issues occurring in field-deployed in-service systems.

¶13. I have presented my research findings over the years at professional conferences such as the Optical Fiber Communications Conference ("OFC") and the International Microwave Symposium ("IMS"), as well as in refereed professional journals. In total, I have presented or published 13 such articles. Additionally, I have written many technically-extensive white papers on several topics directly

related to fiber optic communications for the internal consumption of my colleagues on behalf of my former employers.

¶14. I am a member of both Tau Beta Pi (National Engineering Honor Society) and Eta Kappa Nu (National Electrical Engineering Honor Society).

¶15. I am listed as an inventor/co-inventor on many patents and patent applications, including the following issued patents related to the field of fiber optic communications technology:

Number	Title	Issued
EP 2,837,114	Raman Crosstalk Mitigation in a Multi-Wavelength System Utilizing an Optical Equalizing Signal Modulated with Composite Bandwidth-Limited Data Sources	July 27, 2016
9,118,388	Raman Crosstalk Mitigation in a Multi-Wavelength System Utilizing an Optical Equalizing Signal Modulated with Composite Bandwidth-Limited Data Sources	Aug. 25, 2015
8,666,260	Burst Mode Laser Transmitter having an Extremely Fast Response Time when Triggered from a Totally Off State	Mar. 4, 2014
8,391,723	Raman Back-Pumped Near Zero Dispersion CWDM System and Method	Mar. 5, 2013
CA 258,9851	Method and Apparatus for Reducing Crosstalk and Nonlinear Distortions Induced By Raman Interactions in a Wavelength Division Multiplexed (WDM) Optical Communication System	June 6, 2012
8,155,524	Method and Apparatus for Transmitting Multiple Channels in a Wavelength Division Multiplexed (WDM) Optical Communication System with Reduced Raman Crosstalk and Nonlinear Distortions	Apr. 10, 2012

Number	Title	Issued
7,920,795	Method and Apparatus for Transmitting Multiple Channels in a Wavelength Division Multiplexed (WDM) Optical Communication System with Reduced Raman Crosstalk and Nonlinear Distortions	Apr. 5, 2011
7,783,197	Method and Apparatus for Reducing Crosstalk in a DWDM Transmission System	Aug. 24, 2010
7,693,366	Aligned Narrowband Optical Filters having Flat Passbands and Comprising of Offset Cascaded Broadband Optical Filters	Apr. 6, 2010
7,418,205	Method and Apparatus for Controlling a Frequency Hopping Laser	Aug. 26, 2008
7,271,948	Method and Apparatus for Reducing Crosstalk and Nonlinear Distortions Induced By Raman Interactions in a Wavelength Division Multiplexed (WDM) Optical Communication System	Sept. 18, 2007
6,788,839	Time Slot Tunable All-Optical Packet Data Routing Switch	Sept. 7, 2004
6,671,426	Monolithic Integrated Terahertz Optical Asymmetric Demultiplexer	Dec. 30, 2003
6,650,800	Time Slot Tunable All-Optical Packet Data Demultiplexer	Nov. 18, 2003

III. RELEVANT TIME

¶16. I have been asked to assume that the Patent-at-Issue has an effective priority date of January 25, 2010 ("Effective Priority Date").

¶17. To the extent that I cite to exhibits created or published after the Effective Priority Date, I consider that the reference is still relevant to what a POSITA would have understood the point for which I cite the reference at or around the time of the invention.

IV. LEVEL OF ORDINARY SKILL IN THE ART

¶18. I understand that Petitioners have proposed that a person of ordinary skill in the art ("POSITA") at the time of Effective Priority Date for the '378 Patent "would have at least a bachelor's degree in electrical engineering, computer science or comparable degree or 2–3 years industry experience designing and/or maintaining back-end networking equipment." Pet. 13.

¶19. I understand that Patent Owner believes that this level of skill—which literally could be as little as 2 years' industry experience of simply "maintaining" back-end networking equipment—is too low.

¶20. I further understand that Patent Owner has proposed a POSITA would, at or around the Effective Priority Date, have a bachelor's degree in electrical engineering or comparable degree and 2 or more years' experience designing encryption, multicast service data, and passive optical networks ('PON') and that more experience would make up for less education, and *vice versa*.

¶21. Based on my review of the '378 Patent, the technology, the educational level and experience of active workers in the field, the types of problems faced by workers in the field, the solutions found to those problems, the sophistication of the technology in the field, and drawing on my own experience, I concur with Patent Owner that Petitioner's proposal of a POSITA is too low and a POSITA should be defined in accord with Patent Owner's proposal.

¶22. Under Petitioner's proposal, the POSITA doing "maintenance" of "back-end network equipment" with no educational minimum would include a high school student working part time in a back office doing tasks such as repowering "hung" devices, re-routing cables, etc. for equipment that has nothing to do with the PON for which the Patent-at-Issue concerns. It would be hard to imagine that such a "POSITA" would be capable of understanding the technology and prior art at issue, or be capable of making a reasoned and principled determination as to obviousness. In fact, a POSITA for the case-at-hand would require extensive knowledge of the complex signaling protocols utilized in passive optical networks and how this technology is utilized to efficiently and securely distribute multicast services to the ONUs connected on a PON. A POSITA for this case would also have a degree of familiarity with the relevant PON standards for such systems, as adopted by the ITU and IEEE. As such, a POSITA would require a higher level of skill, education, and experience than what the Petitioner has proposed. For example, a person involved with the direct research and engineering development of such communications systems and/or a contributor to the relevant PON standards committees of the industry organizations would presumably have such in-depth knowledge, as opposed to a person tasked only with "maintaining" such devices in the back-office of a service provider's field offices or headend locations.

¶23. Given that I have been deeply involved with advanced research and engineering development of PON technology dating back to the early 2000's (starting with B-PON) and have also contributed inputs to the ITU PON standards committee, it is my opinion that I do qualify as a person of ordinary skill in the art at the relevant time under either of the above descriptions. In fact, I exceed this level of knowledge, experience, and education. So I am qualified to provide an expert opinion in this proceeding.

¶24. I have approached my analysis from the perspective of a POSITA as set forth by Patent Owner as of the Effective Priority Date. I do this to err on the side of caution, as my use of Patent Owner's higher level of education and experience should be a *lower* hurdle for finding obviousness than if I used Petitioner's much lower level of education and experience. Hence, if there is no obviousness with Patent Owner's definition of a POSITA, I would have even more conviction that this is the case if the Prior Art was considered from the point of view of Petitioner's proposed POSITA.

V. MATERIALS CONSIDERED

¶25. In forming my opinions expressed herein, I have considered the exhibits listed in the Current Exhibit List beginning on page iii, as well as the Petition.

VI. OVERVIEW OF THE PATENTED INVENTION

¶26. The Patent-at-Issue concerns the "passive optical network" ("PON") environment. Ex. 1001 at 1:7–10. It is "passive" because there are no powered components, such as amplifiers or repeaters, between the operator's headend (or OLT site) and the end-user's (subscriber) ONU. There is only, for example, inert fiber and splitters allowing for the transport of the data-carrying optical signals to and from the OLT site and the ONUs on a given PON. The PON network generally has an Optical Line Terminal ("OLT") at the "office side" that sends data to multiple Optical Network Units ("ONUs") at the "customer side." *Id.* 1:14–19. A PON is an access network connecting end users (customers/subscribers) to all the various data services that a service provider supplies. A single PON is more or less a localized neighborhood network and seldom reaches much beyond a 20 km distance, as measured between the OLT site and the farthest ONU connected on a particular PON. A typical PON will have about 2^n ONUs connected to it, where 2^n often falls between 32 and 128. A single ONU may service any number of user devices (connected to the ONU via some type of customer premise equipment ("CPE")) via a local router connected to it (TV STBs, computers, VOIP phones, smart phones, tablets, smart devices, IOT devices, etc.). A single ONU may connect all the users' connected devices in a single household, or an entire office complex, or an entire apartment complex, or other MDU to the network.

¶27. Because of the PON physical architecture, every ONU connected on a PON will receive every data frame transmitted downstream by the PON's OLT transceiver. So there is the potential for anyone or anything connected to a PON ONU to maliciously receive/pirate any data being transmitted to any of the ONUs without regard for its intended recipient. This prompts the need for the encryption technology implementations used specifically in PONs so that an ONU cannot intercept and process data that was not intended for it or for the users connected to that ONU. The signaling protocols, including assigned LLIDs, mLLIDs, and encryption technology, determine whether a given compliant ONU can or will process the information contained in a particular data frame. The access network encryption that a PON utilizes is a layer of security that is in addition to any applied encryption that may have been utilized upstream from the PON by the source supplier of any services being provided to the subscribers, such as SSL (secure socket layer) or TLS (transport layer security) technologies, or DRM (digital rights management) encryption technology.

¶28. Before being activated, for example during the discovery and activation cycle, an ONU may "receive various plaintext data packets"—i.e., unencrypted packets—"sent from the OLT PON port." *Id.* 1:31–32. Plaintext packets may correspond to broadcast messages (broadcast Alloc-IDs), such as serial number grants in the

GPON to which ONUs that request activation respond by transmitting serial number IDs to the OLT for initial authentication and ranging purposes.

¶29. The ’378 Patent distinguishes “legal users” whose ONU has registered with the OLT from “malicious users” who have physically connected an ONU to the OLT but “neglects the registration request sent from the OLT.” *Id.* 1:20–28 (describing a serial number grant allocation in GPON). A POSITA understood that the ’378 Patent’s reference to “neglect” meant intentional failure to register, as opposed to a rogue (malfunctioning) ONU that is defective in some way but would have otherwise been compliant with the PON operating standards. It is also worthwhile to note that a malicious eavesdropping ONU would have no reason to register on the PON as it need only synchronize its optical receiver with the downstream data bursts transmitted by the OLT. This is because it will, regardless of registration status, in any case, receive every downstream data frame transmitted by the PON’s OLT. To intercept downstream data, there is no need for a malicious eavesdropper to transmit upstream. The malicious eavesdropper can remain silent, potentially going undetected (though OTDR and other measurements may still reveal its presence on the PON). In fact, transmitting a malicious signal upstream would potentially reveal the presence of the malicious ONU to the system operator, which would then necessitate enacting overt security actions to protect the PON. Indeed, an

unregistered ONU transmitting data to an OLT in the upstream direction may disrupt the operation of the entire PON.

¶30. The users connected to an ONU (via local routers or other CPE) may make various requests for services, such as VOIP services and IPTV or conference/group calling, etc. Such requests are generally communicated upstream to the OLT via the ONU and then passed onto the core internet—ultimately reaching any of the multiple physical sources of these various services for the requests to be completed and the services then provided to the user. Such services may entail the transmission of sensitive data both in the upstream and downstream directions. Again, this prompts the need for encryption technology to be employed internally within PONs to protect the data in transit between the OLT and an ONU to guard against unauthorized access of downstream data, which could also include information such as data traffic patterns, specific website access information, end user identity, etc., in addition to the primary payload data.

¶31. Within a PON itself, downstream data may be intended for the reception of all the ONUs (broadcast), a subset of all ONUs (multicast), or for a single ONU (unicast). The ’378 Patent is primarily concerned with encrypting multicast data whereby the OLT uses a common key to encrypt multicast service data of all different multicast services in a same bearer channel (for example, mLLID) and then sending encrypted data, wherein the multicast service data of all different multicast

services in the same one bearer channel use a same common key to carry out encryption. *See id.* 1:39–42 (explaining that with multicast data, "only one service data is sent from the OLT PON port, and all users or part of users who meet the requirements receive and use the service data."). Unicast data is generally encrypted utilizing a unique encryption key for the data sent to the intended ONU (addressed to its LLID for example) that is not shared with the other ONUs. An unauthorized, malicious ONU generally would not be able to communicate with the OLT, and thus cannot make requests of it; hence, the ONU will not be given encryption/decryption keys to unlock protected data being transmitted by the OLT.

¶32. The '378 Patent further explains that, at the time of the invention, there was effective PON encryption for "*unicast* encryption mechanisms." *Id.* 1:33–39 (emphasis added). But for multicast data, the practice at the time was for operators to "duplicate the multicast service data packets to each PON port [on] the unicast channel of the ONU" and use the unicast "encryption so as to protect the multicast service data from being stolen by malicious users." *Id.* 1:49–53. Additionally, "operators set a universal key in the overall network range to encrypt the services" that had the "disadvantage . . . that once the key [was] acquired by a malicious user, all service content in the overall network [could] be decrypted and stolen." *Id.* 1:43–47.

¶33. Therefore, a key aspect of the ’378 Patent was “to provide a method and device for encrypting multicast service in a passive optical network (PON) system to increase the security and reduce the complexity of [the] OLT encryption mechanism and the burden of the OLT.” *Id.* 1:59–62. Specifically, the ’378 Patent teaches to encrypt an entire multicast “bearer channel” from the OLT to ONUs (i.e., “multicast service data of all different multicast services . . . us[ing] a same common key”), *see, e.g.*, *id.* 1:66–2:3, 3:9–14, 7:64–65, with keys that the OLT provides to the ONUs via a “separate management control channel” only after the ONU is successfully activated, *see, e.g.*, *id.* 2:4–7, 2:33–34, 8:3–5. That is, a subset of all the ONUs, on a particular single PON, that have permission to access the same multicast bearer channel will all use the same key for that multicast bearer channel.

¶34. To explain further, while multicast services may be first encrypted at their respective sources upstream from the PON OLT, this is a different level of encryption from that referred to in the ’378 Patent. The ’378 Patent is referring to multicast encryption done by the PON itself. Multicast encryption is done/needed on one particular PON so that other users on that PON who are not registered to receive a group of multicast services assigned to a multicast bearer channel, on that PON, cannot receive and use such services without authorization. This is needed because every ONU on a given PON will receive every data frame transmitted by the PON’s OLT and could therefore potentially utilize a group of services it is not

authorized to use. The multicast encryption of all multicast services on the one bearer channel protects against this.

¶35. What combination of all different services are grouped together for transmission on a particular multicast bearer channel (mLLID) may be (but is not required to be) a function of the network operator, as opposed to the multicast services' various data providers.

¶36. A different grouping of multicast services traversing the OLT to the ONUs may be assigned to a different multicast bearer channel from the first one and may also, therefore, utilize a different common encryption key for that second multicast bearer channel from the key used for the first multicast bearer channel. *See, e.g., id*. claim 7. That is, different subsets of ONUs (that could overlap one another) may have access permission for different multicast bearer channels that may or may not utilize the same encryption key. *See, e.g.*, Ex. 1002 at 384.

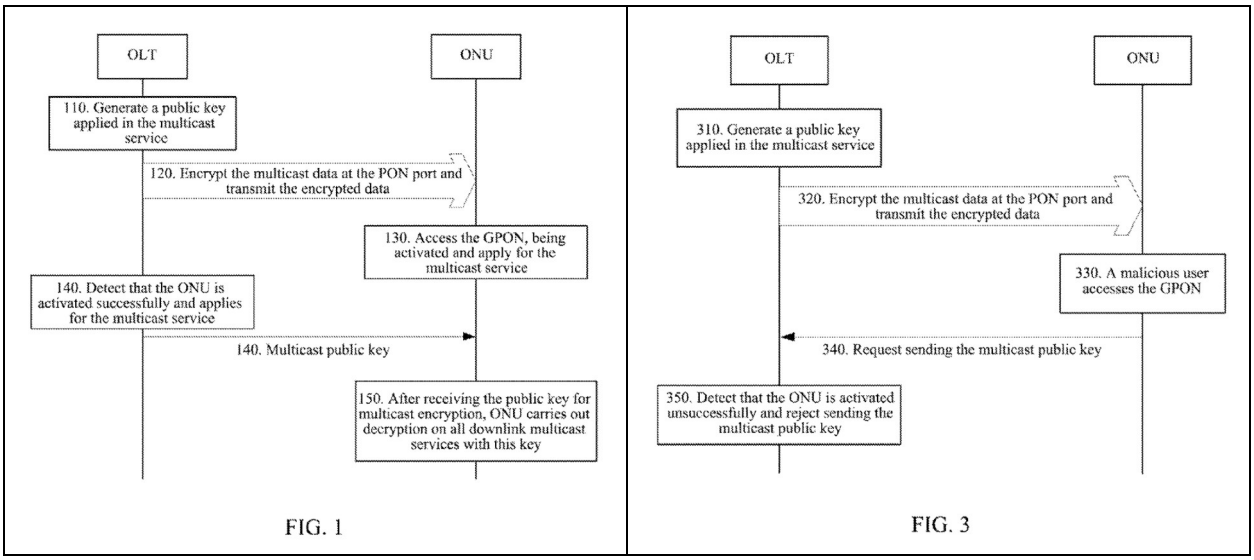
¶37. In one embodiment, the "bearer channel is a logical channel of the PON, and it can be the general encapsulation model (GEM) channel born by the GPON[2] port or the logical link identification (LLID) channel of the EPON[3] port." Ex. 1001 4:4–8. The "management control channel might also be a logical channel of the PON, such as a physical layer operation administration maintenance (PLOAM) channel or

[2] Gigabit-Capable Passive Optical Network. *Id.* 1:34–35.

[3] Ethernet Passive Optical Network. *Id.* 1:37.

an OMCI[4] channel in the GPON system, . . . an extended OAM channel in the EPON system [or] a digital channel." *Id.* 4:9–15.

¶38. The '378 Patent illustrates how the multicast encryption channel protects from malicious users through embodiments shown in Figures 1 and 3 below.



In these embodiments, the first two steps are the same. At steps 110 and 310, the OLT generates a key for encrypting multicast services. And in steps 120 and 320, the encrypted multicast service data is sent to the ONU. *Id.* 4:44–47. In the first embodiment, at step 130, a legal user accesses the GPON and applies for the multicast service. *Id.* 4:48–50. In step 140, the OLT detects that the ONU has successfully activated and therefore sends the multicast channel key. *Id.* 4:54–56. Therefore, at step 150, the legal user may decrypt all downlink multicast services on this bearer channel with this key. *Id.* 5:1–3. In contrast, in the third embodiment,

[4] ONU Management and Control Interface. *Id.* 3:55–56.

the malicious user is unable to use the data in the encrypted multicast channel, and if the malicious user requests the key for the bearer channel as shown in step 330, at step 350 the OLT rejects the request as it detects that this ONU has not successfully registered yet. *Id.* 5:54–67.

¶39. Moreover, the '378 Patent's invention contemplates that the OLT may set an "aging time" for the keys it sent to the ONUs. *See, e.g.*, *id.* 2:14–19, 5:36–40, claims 3 and 5, & Fig. 2. When the aging time arrives, the OLT will generate a new encryption key that the OLT will use going forward. *Id.* NIST refers to these key aging times as "cryptoperiods" (see NIST Special Publication 800-57 Part 1 Revision 4 *Recommendation for Key Management* Part 1: General 5.3 page 33 https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-57pt1r4.pdf). "A cryptoperiod is the time span during which a specific key is authorized for use by legitimate entities, or the keys for a given system will remain in effect." The OLT will provide the new key to previously activated ONUs and to newly activated ONUs that apply for multicast service data. *Id.* The '378 Patent's second embodiment in Figure 2 shows this aging time variation.

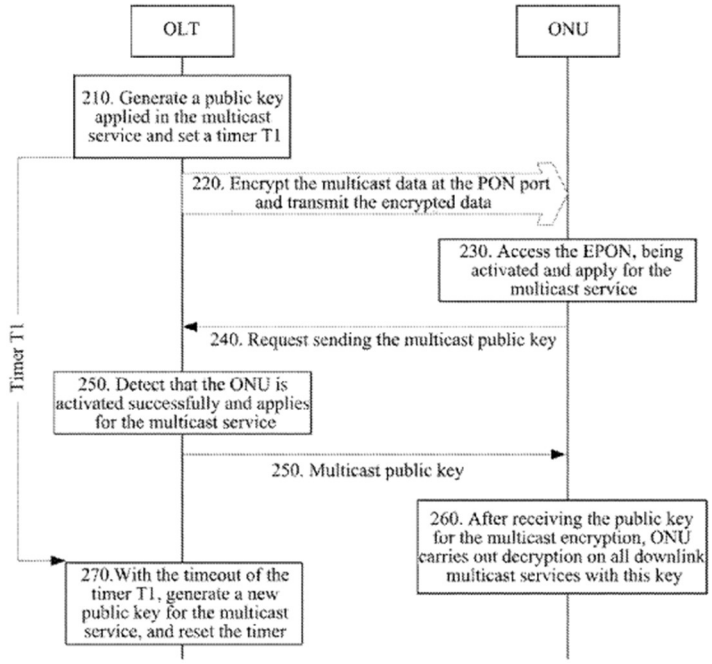


FIG. 2

As seen, steps 210–260 are similar to the embodiment in Figure 1; however, in step 210 the OLT sets a timer, T1, and the ONU requests the multicast channel key in step 240. *Id.* 5:9–11, 20–21. When the timer T1 times out, the OLT will generate a new key for the service and reset the timer in step 270. *Id.* 5:33–35.

¶40. The fourth and last embodiment in the ’378 Patent is shown in Figure 4, and contemplates that there may be more than one encrypted multicast bearer channel, each having a bearer channel identification, and that the OLT may generate different keys for different multicast bearer channels. *See, e.g.*, *id.* 6:9–20, 6:41–47, & claim 4.

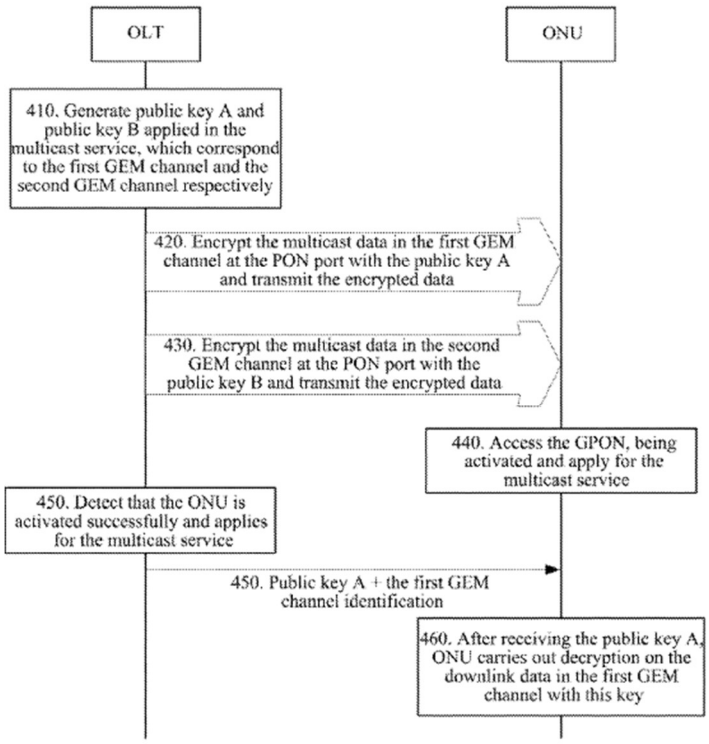


FIG. 4

As seen, in step 450, after the OLT detects the ONU is successfully activated and has applied for a multicast service, the OLT provides the ONU with both the bearer channel identification and the key that applies to the bearer channel. *Id.* 6:26–30.

VII. RELEVANT PROSECUTION HISTORY

¶41. On June 14, 2013, the Examiner rejected the original claims as being anticipated by CN1855834 to He (Nov. 1, 2006, translation by Dialog) [hereinafter He].[5] *See, e.g.*, Ex. 1002 at 328–29. In response, on August 12, 2013, the Applicant amended the claims. Claim 1 is an example:

[5] He's Dialog translation does not appear to be in the prosecution history. *See* Ex. 1002.

> an optical line terminal (OLT) generating a common key, and using the common key to encrypt multicast service data of all multicast services in a bearer channel and then sending encrypted data, wherein the multicast service data of all multicast services in ~~a~~ the same one bearer channel ~~using~~ use a same common key to carry out encryption; and

Id. 341. The Applicant clarified that the amendments were made to capture that one bearer channel includes a plurality of service channels to bear different multicast services. *Id.* 352. This was in contrast to He that only "discloses to encrypt the multicast data stream in one service channel" and "does not disclose any information about more than one service channel and further does not disclose any information about the bear[er] channel at all." *Id.* (emphasis removed). In this context, "the multicast data stream" implies the continuum of data being transmitted in order to provide a singular multicast service from any physical source providing this multicast service. Hence, a POSITA understood that the Applicant was arguing that only one multicast service is to be encrypted per multicast channel according to (or is implied by) He which is distinctly different from what is claimed by the '378 Patent.

¶42. On May 21, 2014, the Examiner presented a different reference, Jiang *et al.*, Multicast Broadcast Services Support in OFDMA-Based WiMAX Systems, IEEE COMMUNICATIONS MAGAZINE (Aug. 2007) ("Jiang2007"). *See* Ex. 2003. The Examiner admitted that "He does not teach all multicast services" (i.e., "using the common key to encrypt multicast service data of all multicast services in a bearer

channel"), Ex. 1002 at 374 (emphasis removed), but nonetheless relied upon Jiang2007 for this limitation.

¶43. Specifically, Jiang2007 teaches:

> The [multicast and broadcast service controller] delivers an [multicast and broadcast service ("MBS")] program to one or more MBS zones, each of which consists of multiple [base stations ("BS")] of a WiMAX network. [Mobile stations/subscriber stations] that access the same MBS channel in the same zone share a single 802.16 [WiMAX standard] multicast connection. *Note that all BS in the same MBS zone use the same key for encrypting the same MBS program. This reduces substantially the handoff delay between BS in the same MBS zone*.

Ex. 2003 at PDF 5 (original page 82) (emphasis added); *see also* Ex. 1002 at 374 (citing Jiang2007 at 82).

¶44. On August 1, 2014, the Applicant traversed the rejection and explained that:

> [O]ne bearer channel can include a plurality of service channels to bear different multicast services for different terminals, i.e., one bearer channel may include 3 service channels A, B and C, for example, the service channel A can bear multicast service 1 to terminal a, b and c, the service channel B can bear multicast service

> 2 to terminal a and c, and the service channel C can bear multicast service 3 to terminal b and c.
>
> In the amended claim 1, the OLT uses only one common key to encrypt multicast service data of all multicast services which are born in different service channels in the same one bearer channel, so that, different ONUs which are legal for the OLT can decrypt the multicast services using the same common key.

Id. 384 (emphasis removed). So, the Applicant made it clear that ***the amendments meant one bearer channel carries a plurality of service channels encrypted by the same key***. That is, the single multicast bearer channel that is carrying the plurality of multicast service channels is what is encrypted by the same common key. The individual multicast service channels will, in all likelihood, have additional encryption layers as explained above.

¶45. The Applicant further explained that Jiang2007 does not meet the "using the common key to encrypt multicast service data of all multicast services in a bearer channel" limitation, for two reasons. First, Jiang2007 only discloses using the same key on "the same MBS program of ONE MBS zone," which is only using a key on a single (not plural) multicast service. *Id.* 385 (emphasis removed). Second, Jiang2007 uses the same key so that "when the handoff occurs between different [base stations] in the ONE MBS zone, the delay due to the different keys handoff

can be avoided." *Id.* Since those "skilled in the art would know that the handoff between the different BSs and one MS should be on different bearer channels," thus Jiang2007's key was also used on different bearer channels. *Id.* (emphasis removed). While cellular phone technology that uses wireless communication with different encoding is largely unrelated to the PON technology at issue, a POSITA in this the relevant field still understood that this was so, because it is basic knowledge among technologists that cellular systems networks are designed such that neighboring base stations operate at different frequencies to minimize signaling interference. As the Applicant succinctly summed up the difference: "Jiang2007 is not for 'the multicast service data of all different multicast services in the same one bearer channel,' but is used in the ***same*** MBS program [i.e., ***one*** multicast service] on ***different*** bearer channels between the different [base stations] and the one [mobile subscriber]." *Id.* (different emphasis).

¶46. On September 16, 2014, the Examiner issued a final rejection noting that, while Applicant's arguments were "not persuasive," *id.* 393, 399, the "Applicant made a valid argument that Jiang2007 teaches the common key for all BS encrypting the same MBS program." *Id.* 401. But the Examiner explained that Jiang2007 met the limitation because "although the key is common for all BS[,] it may be different for [a] different time when another MBS program is delivered." *Id.*

¶47. On November 11, 2014, the Applicant amended the claims such that they took their final form, as seen in Claim 1, for example:

> an optical line terminal (OLT) generating a common key, and using the common key to encrypt multicast service data of all <u>different</u> multicast services in a <u>same</u> bearer channel and then sending encrypted data, wherein the multicast service data of all multicast services in the same one bearer channel use a same common key to carry out encryption; and

Id. 416. With this change, the Applicant again argued that Jiang2007 only disclosed "encrypting the ***same*** MBS program in the ***different*** bearer channels, which is totally contrary to the feature using the common key to encrypt multicast service data of all ***different*** multicast services in a ***same*** bearer channel' defined in the amended claim 1." *Id.* 413 (some emphasis removed).

¶48. After doing an additional search, *see id.* 426–28, on November 17, 2014, the Examiner issued a Notice of Allowance, *id.* 432. The Examiner said that "Applicant's arguments regarding the amendment submitted on 11/11/2014 have been considered and are persuasive." *Id.* 437. The Examiner explained his Reason for Allowance as "none of the prior art of record alone or in combination teaches ***using the common key to encrypt multicast service data of all different multicast services in a same bearer channel and then sending encrypted data***, wherein the multicast service data of all different multicast services in the same one bearer channel use a same common key to carry out encryption." *Id.* 438–39 (emphasis

added). That is, neither He nor Jiang2007 taught encrypting and sending ***plural*** multicast services in a ***single*** bearer channel using the same common key.

VIII. OVERVIEW OF THE CITED REFERENCES

A. RFC 1112 (Aug. 1989) ("IGMPv1")

¶49. RFC 1112 (Aug. 1989) ("IGMPv1") concerns extensions of the Internet Protocol ("IP") to support multicasting. Ex. 1006 at 1. As set forth therein, a "host group" is "a set of zero or more hosts identified by a single IP destination address." *Id.* A "host" is "any internet host or gateway other than those acting as multicast routers." *Id.* at 2. "A multicast datagram [addressed to this single IP destination address] is delivered to all members of its destination host group." *Id.* at 1. "A host may be a member of more than one group at a time." *Id.*

¶50. When a "host transmits an IP multicast datagram . . . [it] reaches all immediately-neighboring members of the destination host group [and] [i]f the datagram has an IP time-to-live greater than 1, the multicast router(s) attached to the local network take[s] responsibility for forwarding it towards all other networks that have members of the destination group." *Id.*

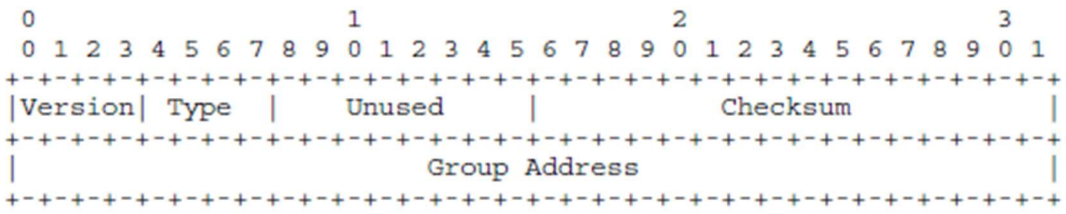
¶51. "Host groups are identified by class D IP addresses ['IPAs'], i.e., those with '1110' [0x0E] as their high-order four bits." *Id.* at 3. That is, multicast IPAs have values in the range of E0.00.00.00 to EF.FF.FF.FF hexadecimal or "from 224.0.0.0 to 239.255.255.255" decimal. *Id.* "The address . . . 224.0.0.1 is assigned to the

permanent group of all IP hosts (including gateways)." *Id.* "An IP host group address is mapped to an Ethernet multicast address by placing the low-order 23-bits of the IP address into the low-order 23 bits of the Ethernet multicast address 01-00-5E-00-00-00 (hex)." *Id.* at 6.

¶52. "Multicast IP datagrams are sent using the same 'Send IP' operation used to send unicast IP datagrams [where] an upper-layer protocol module merely specifies an IP host group address, rather than an individual IP address, as the destination." *Id.* at 5.

¶53. IGMPv1 also specifies that "IGMP is used to keep neighboring multicast routers informed of the host group memberships present on a particular local network" and "[t]o support IGMP, every level 2 host must join the 'all-hosts' group (address 224.0.0.1)." *Id.* at 8.

¶54. "IGMP messages are encapsulated in IP datagrams" as shown. *Id.* at 11.



Id. Type 1 indicates a message is a "Host Membership Query" or just "Query," while Type 2 indicates a message is a "Host Membership Report" or just "Report." *Id.* 11–12. A Query is sent by a multicast router and asks: "what groups is everyone in?" *Id.* at 12. "Queries are addressed to the all-hosts group

(address 224.0.0.1)." *Id.* "In a Host Membership Query message, the group address field is zeroed when sent, ignored when received." *Id.* at 11–12. A member responds to a Query, letting the multicast router know what groups the member is a part of, by sending a Report message. *Id.* at 12. "In a Host Membership Report message, the group address field holds the IP host group address of the group being reported." *Id.*

¶55. "Multicast routers send Queries periodically to refresh their knowledge of memberships present on a particular network. If no Reports are received for a particular group after some number of Queries, the routers assume that the group has no local members and that they need not forward remotely-originated multicasts for that group onto the local network." *Id.* at 13.

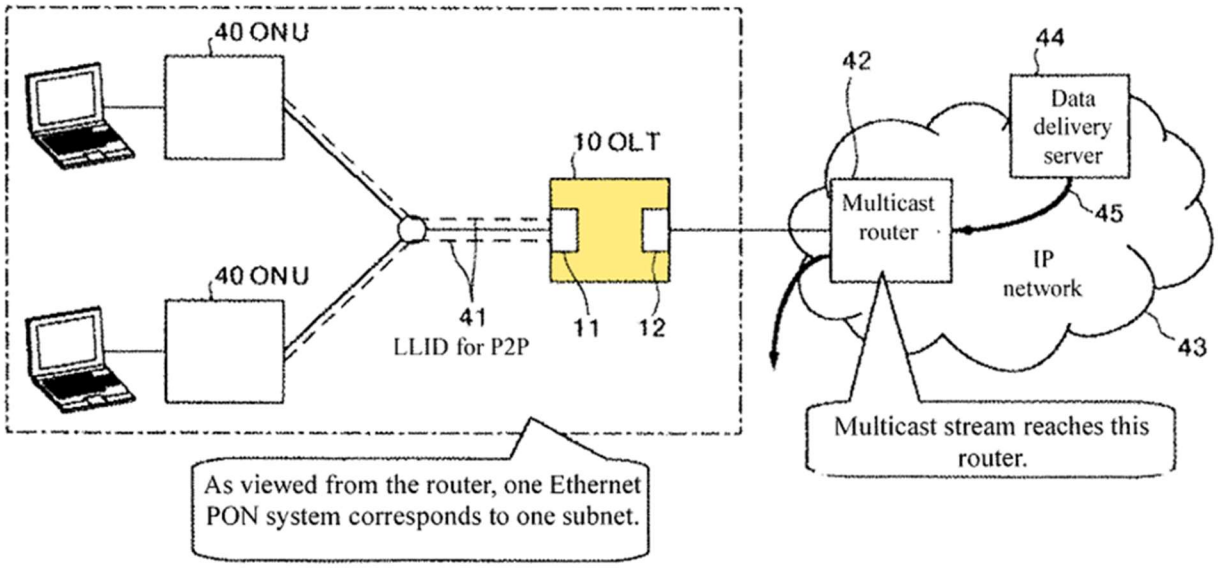
¶56. IGMPv1 specifies the basic functionality and protocols of IP multicast group management insofar as requests by host devices to join multicast groups are concerned (multicast group join requests). IGMP allows a host device to communicate upstream, to the edge router, that it wants to receive data (a service) and hence join the group associated with this multicast service.

¶57. As now described below, Murakami describes identifying which hosts using a PON (via their respective ONUs) want to join (or already are members of) specific multicast groups using IGMP snooping.

B. Overview of Japanese Patent Publication No. JP2004-343243A ("Murakami")

1. Nomenclature and Topology

¶58. Murakami is concerned with a central office with OLTs acting as a transparent bridge between (1) an Ethernet network using Media Access Control ("MAC") frames and the Internet Group Management Protocol ("IGMP") on one side to (2) multiple subscriber-side units ONUs on the other.[6] Ex. 1005 [0001–03]. This is illustrated below.



[6] With IGMP, a multicast router identifies its members by periodically multicasting "query messages." *Id.* [0004]; *see also* IGMPv1, § VIII.A *supra*. The router detects a member when the member "replies with a report message." *Id.* The router determines a member is no longer part of the group when a previously detected member "does not transmit a report message back" in IGMPv1 or, in IGMPv2, a member "provides a notification in the form of a leave message." *Id.*

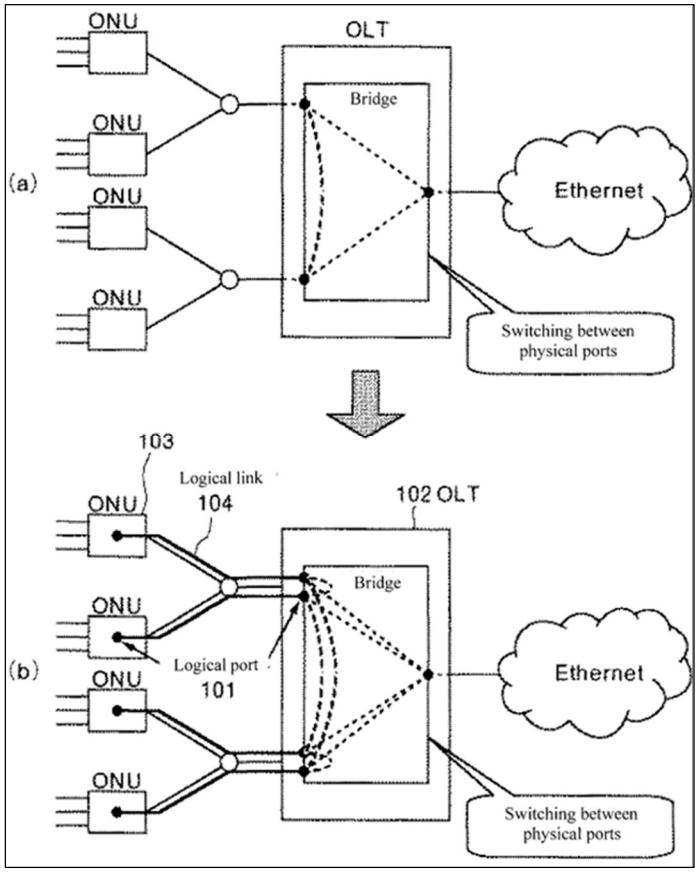
Id. Fig. 4 (highlighting added). As seen, "[t]he PON system comprises one OLT 10 and multiple ONUs 40" connected via a splitter. *Id.* [0026].

¶59. A POSITA understood that Murakami's OLT 10 would represent a single OLT transceiver servicing a single PON consisting of multiple ONUs (typically between 32 and 128). Several such OLT transceivers may be plugged into an OLT chassis, with each one servicing a separate PON. A POSITA would also have understood that there is clearly one direct hop between the PON OLT and any of the ONUs connected to this PON. Hence, a POSITA understood that, within a PON, due to its physical architecture, there are no signal routes that need to be determined. The directionality of the passive optical splitter will also preclude any possibility of direct communications between any ONUs on this PON. All upstream signaling passes through the OLT's optical receiver. However, all downstream signals transmitted by the OLT will reach, with one direct hop, every ONU on the PON. Hence, there must be a means by which each ONU may determine whether particular data contained within a downstream data frame is meant to be processed by it. The logical link identifiers provide this mechanism and the PON encryption technology provides the data security for signals in transit that are internal to a PON (i.e. between a PON's OLT and the one-hop to any of its ONUs).

¶60. In Murakami, there may be one physical OLT port or PON interface carrying two logical links. That is, a "point-to-point logical link 41 is set for each ONU 40."

Id. The point-to-point logical link "frames are encrypted during the data transmission in the downstream (OLT ➔ ONU) direction."[7] *Id.* A POSITA would have understood that the point-to-point logical link also corresponds to a single physical direct hop between the OLT and the ONU and that no physical routes or paths need to be determined for data traffic internal to the PON itself.

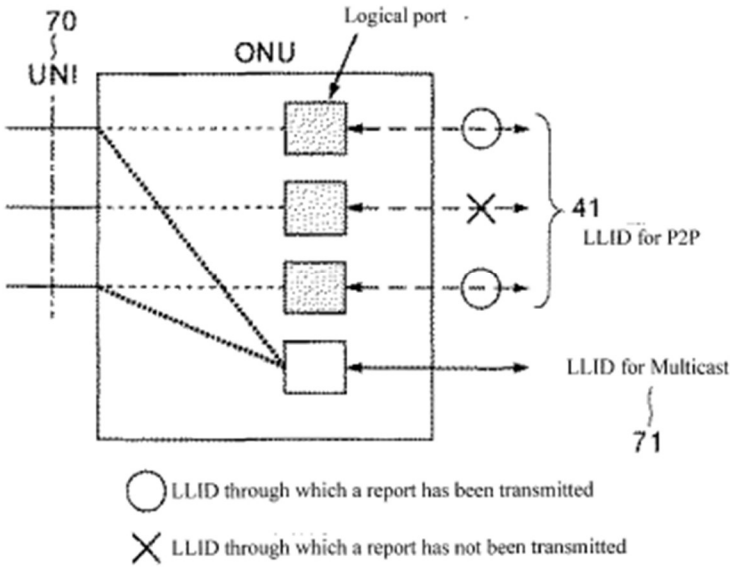
¶61. Murakami contrasts (1) its logical port switching shown in Figure 4 and Figure 8(b) with (2) the conventional OLT physical PON interface switching shown in Figure 8(a), where the OLT "switches on a per physical-port basis." *Id.* [0016].



[7] The encryption is discussed in more detail below in this section on page 38.

Id. Fig. 8. As seen in Figure 8(b), each ONU has one logical port and the OLT has two corresponding logical ports identified as 101.

¶62. Figure 7 more clearly shows that the lines extending to the left of each ONU in Figure 8 are multiple User Network Interfaces ("UNIs"). *Id.*



Id. Fig. 7. As indicated by the arrow and described in the specification, a logical port may also correspond to a UNI of an ONU. *Id.* [0016].

¶63. Murakami teaches that "[l]ogical *ports* 101 . . . are connected through logical *links* 104." *Id.* [0016] (emphasis added). The OLT assigns each logical link a Logical Link Identifier ("LLID") that is unique in the PON. *Id.* [0017–18].

¶64. The CPE is typically what is connected to the UNI. The UNI is the point of demarcation between the service provider's network equipment and the user's network connection equipment. The CPE may be in-home network (wireless) routers or home network switches or TV set-top boxes or network adapter cards, etc.

The CPE is typically owned (or leased) by the subscriber. As such, depending upon the design of an ONU, a UNI may be nothing more than a connection port located on the ONU. Customer devices such as computers, smart phones (using the home network), tablets, televisions, etc. will connect to the CPE in order to gain access to the service provider's PON and beyond.

2. Functionality

¶65. Murakami discloses realizing multicast communication security using logical links without requiring routing functions on the subscriber (ONU) side. *Id.* at Abstract and [0011]. A POSITA understood that this makes sense for a single PON architecture, because in this scenario every ONU will receive every frame that the OLT for that PON transmits, so there is no need for physical routing and only logical routing is needed.

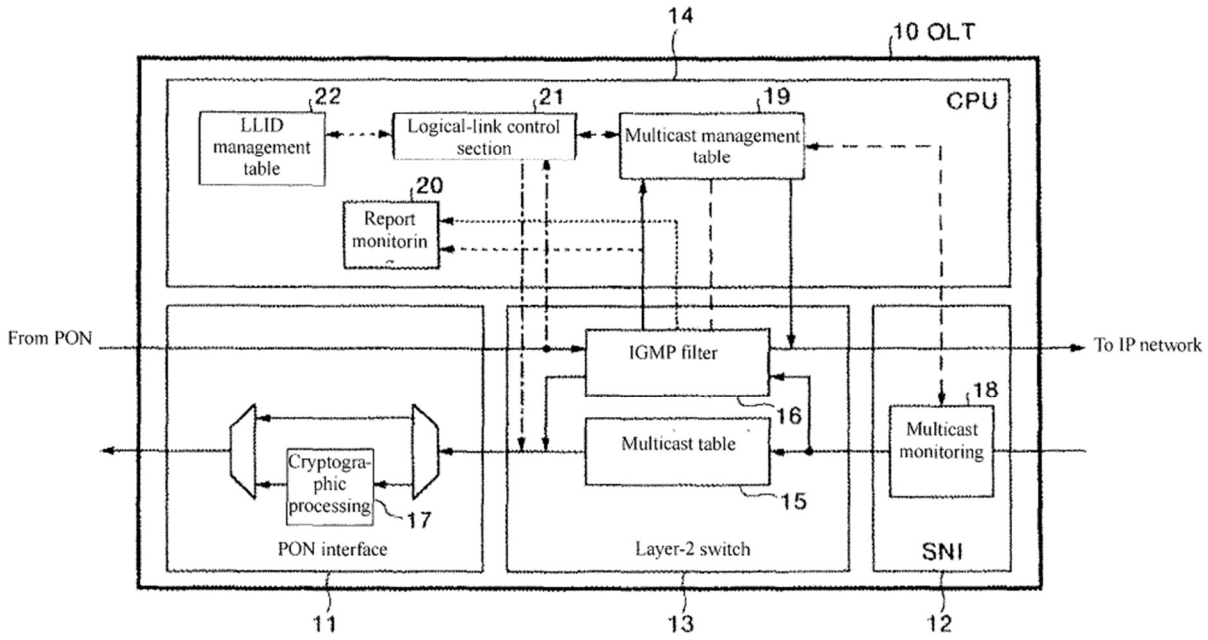
¶66. Specifically, Murakami's "invention is configured to snoop IGMP messages in the central office unit of a PON system, interlock the result of the snooping with the logical-link control, and further process the multicast data through a cryptographic step." *Id.* [0013].

¶67. Note that the multicast join requests for a particular service originate from the customer devices connected to the CPE via the UNI connected to a particular ONU. For example, join requests could come from equipment such as computers, tablets, smart phones, STBs/smart TVs, IOT devices, IP telephones, or any other device that

needs to join a multicast group to utilize a requested service. The ONU is simply the means of passing this information upstream on a PON to the OLT system. As such, a POSITA understood that Murakami's PON ONUs or the OLT would not be considered to be a host, nor would they be considered to be a multicast group member.

¶68. A block diagram of an OLT in Murakami is shown in Figure 1.

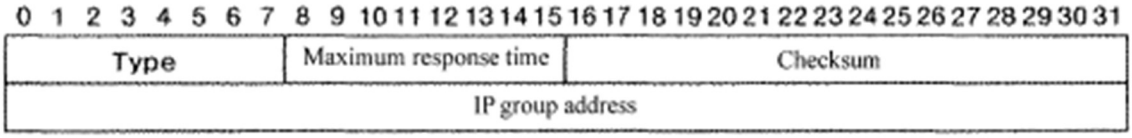
Figure 1



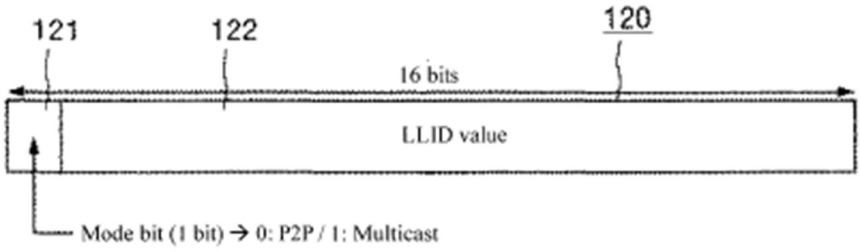
Id. Fig. 1. The PON interface to ONUs is shown on the left and the interface to the IP network is shown on the right. *Id.* [0019].

¶69. Murakami explains its operation with practical examples. First, Murakami describes its operation when a "report message[] [is] received from [a] PON

interface." *Id.* [0027]. Murakami indicates that it will be "snooping" IP datagrams having the following format.



Id. Fig. 5. Murakami also notes that it will be looking at the MAC preambles having a format as shown below. *Id.* [0018].



Id. Fig. 10. Murakami recognizes Report messages as having a "IP group address" in the multicast address range[8] and a "Type" of Type 2.[9] *Id.* [0027].

¶70. When the OLT finds a Report message, it searches through the Multicast Management Table ("MMT") shown below "using the IP group address as the key."[10] *Id.* [0029].

---

[8] A Multicast IP address is in the range of 224.0.0.0 to 239.255.255.255. *See* IGMPv1, § VIII.A *supra.*

[9] The Type field would have value 0x12 or 0x16 for IGMPv1 and IGMPv2 respectively. *Id.* [0027].

[10] The use of the word "key" here can be confusing. The "key" here refers to a unique index into the MMT, not a cryptographic key.

Multicast Management Table 19

Multicast Address (IP Group Address)	Access Port	ONU (LLID for P2P)	LLID for multicasting	Encryption key
yyy.yyy.yyy.yyy	2	1 3	100	#1
	4	2 5	110	#3
⋮	⋮	⋮	⋮	⋮

Id. Fig. 3. If the multicast address from the IP datagram is not in the table, the OLT creates a new entry in the MMT for the multicast address, populates the physical access port (aka PON interface) at which the Report arrived, and fills in the P2P LLID (found in the MAC preamble) for the ONU that sent the Report. *Id.* [0029]. The OLT may also forward the Report message to the IP network. *Id.* [0030].

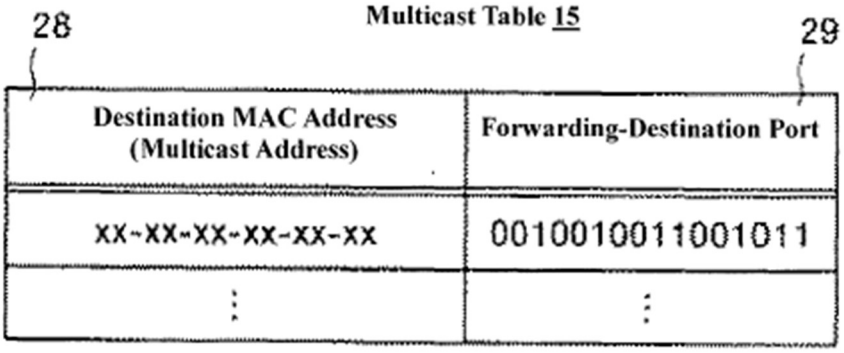
¶71. After the OLT creates a new entry in the MMT for the multicast address, the OLT "generates a new encryption key used [for] multicast communication" and selects an unused LLID that will be used as "a multicast logical link for the ONU." *Id.* [0030–31]. The OLT informs the ONU of the assigned multicast LLID and multicast key by sending a Register message addressed to the ONU via the "LLID to point-to-point logical link 41 of the ONU." *Id.* [0031–32]. The Register message is encrypted with the encryption used for OLT-to-ONU P2P transmissions, thereby

"preventing the stored encryption key from being eavesdropped by another ONU." *Id.* [0032].

¶72. A POSITA understood that the initiating cause of the key generation was ultimately the fact that a user or device connected to the ONU receiving the Register message subscribed to a multicast service via an IGMP join request. And the P2P encryption is used to ensure that other ONUs cannot receive multicast traffic by intercepting (stealing) the information needed to receive and decrypt the multicast service corresponding to a group for which a user did not properly subscribe to and request. Without knowledge of the multicast encryption key, an ONU cannot decipher the multicast service. It is worth emphasizing that the multicast encryption provided by the PON in Murakami provides an additional layer of data security for information specifically traveling only inside of a PON between an OLT transceiver and the ONUs, a direct one-hop journey.

¶73. The multicast LLID and multicast key are stored in the MMT for the multicast address after the ONU "transmits REGISTER_ACK message 111 to the point-to-point logical link 41" for the OLT. *Id.* [0031–32].

¶74. Additionally, as this is the first Report message for this IP multicast address, the Layer-2 ("L2") switch of the OLT will add an entry in Multicast Table 15 shown below.



Id. Fig. 2. This Multicast Table allows the L2 switch to quickly forward incoming frames with multicast destination MAC addresses to the appropriate ports.[11] The table index is a unique Multicast MAC Address, and the Forwarding-Destination Port column is a bitmap where a "1" indicates that the data is to be forwarded to a port. *Id.* This example looks to be a 16-port switch, and the multicast group MAC address xx-xx-xx-xx-xx-xx is mapped to ports 1–2, 4, 7–8, 11 and 14 indicated by the 1s. As indicated by the ":", every different multicast MAC address has its own forwarding-destination port mapping via a corresponding bitmap. So, for example, two multicast services might be mapped in the Multicast Table as follows.

Destination MAC Address (Multicast Address)	Forwarding-Destination Port(s)
01-00-5E-00-00-03	0000000100000000
01-00-5E-00-00-04	0100000000001000

[11] A Multicast MAC address starts with 01-00-5E and "lower 23 bits of the IP multicast address and the MAC address are the same." *Id.* [0033]; *see also* IGMPv1, § VIII.A *supra.*

¶75. When multicast data corresponding to the Multicast MAC Address/IP Multicast Address arrives from the IP network, the data is "encrypted with the encryption key corresponding to . . . the encryption key . . . whose destination IP address matches the IP multicast address in the multicast management table" and "forwarded to the access port according to the contents of multicast table 15." *Id.* [0034]. That is, for security purposes, as explained above, the OLT uses a separate encryption key per multicast group for multicast data than the encryption the OLT uses for P2P communication between an OLT to ONU.

¶76. If the OLT snoops a Report message having an IP multicast address that is already in the table from an ONU not already associated with the IP multicast address, "a new ONU (LLID) is remembered in the matching entry in multicast management table 19." *Id.* [0036]. As seen from Table 19 in Figure 3 above, if the ONU sending the Report message is on a physical access port not already associated with the IP multicast address, the OLT uses a different multicast LLID and multicast key (i.e., the OLT uses a different multicast LLID and multicast key per access port). *Id.* [0037–39].

¶77. The OLT also snoops Query messages coming from the Ethernet Network, and "[s]ubscribers who do not transmit a report message by the time the next query message is received are deemed to have left the multicast communication so that the multicast logical links set for their areas are released, and their access ports are

removed from multicast table 15 and multicast management table 19." *Id.* [0048]. Similarly, the OLT can snoop when a subscriber explicitly transmits an IGMPv2 Leave message and such subscribers "are [also] deemed to have left the multicast communication." *Id.* [0054]. In either case, the OLT also sends a Register message with the "Flags field [set] to Deregister" so that the "ONU, upon receipt of the message, releases the . . . multicast logical link." *Id.* [0049], [0055]. "In the case in which all ONUs leave the multicast communication, the entry for the multicast communication is deleted from multicast table 15 and multicast management table 19." *Id.* [0050], [0056].

C. RFC 4601 ("PIM-SM")

¶78. RFC 4601 specifies the Protocol Independent Multicast—Sparse Mode ("PIM-SM") protocol. Ex. 1007 at 1. Its purpose is to specify a protocol for efficiently routing data to multicast groups. *Id.* at 4. The protocol is for "unidirectional shared trees rooted at a single Rendezvous Point (RP) per group. *Id.* at 1.

¶79. Most of PIM-SM is irrelevant to Murakami, because PIM-SM tree-building and data-routing occurs upstream from the PON OLT. Once multicast data reaches the OLT, there is no need to determine PIM-SM paths or routes because all ONUs on the PON will receive every data frame transmitted downstream by the PON's

OLT simply due to the architecture of the PON. Nonetheless, I present a short summary of how PIM-SM works.

¶80. The trees are built using "PIM Join/Prune message[s]" that are sent in the opposite direction from the direction data flows. *Id.* at 5. Specifically, when a receiver expresses an interest in joining a group, the appropriate designated router ("DR") "sends a PIM Join message towards the RP for that multicast group" referred to as a "(* ,G) Join because it joins group G for all sources to that group." *Id.* at 6. The specification explains how the join messages end up adding a branch to the RP tree as so:

> The (* ,G) Join travels hop-by-hop towards the RP for the group, and in each router it passes through, multicast tree state for group G is instantiated. Eventually, the (*,G) Join either reaches the RP or reaches a router that already has (*,G) Join state for that group. When many receivers join the group, their Join messages converge on the RP and form a distribution tree for group G that is rooted at the RP. This is known as the RP Tree (RPT), and is also known as the shared tree because it is shared by all sources sending to that group.

Id.

¶81. With an RPT tree in place, a "multicast data sender" may "just start[] sending data destined for a multicast group," the RP then "forwards them onto the shared

tree." *Id.* The data follows that route set up via the join messages in the reverse direction, and routers "replicate[] wherever the RP Tree branches" such that the data "eventually reach[es] all the receivers for that multicast group." *Id.*

¶82. "[W]hen the RP receives a register encapsulated data packet from source S on group G," the RP will usually then build another "source-specific tree for S" from the source to the RP. *Id.* 7. The RP does this by "initiat[ing] an (S,G) source-specific Join towards S." *Id.* 6. While there is some transition from encapsulated to native data transmission, eventually traffic ends up "flowing natively from S along a source-specific tree to the RP, and from there along the shared tree to the receivers." *Id.* 7. But "[w]here the two trees intersect, traffic may transfer from the source-specific tree to the RP tree and thus avoid taking a long detour via the RP." *Id.*

¶83. After the initial creation of the RPT with the (*,G) join messages and creation of the source-specific tree from the RP to the source with the (S,G) messages, "[f]or many receivers, the route via the RP may involve a significant detour when compared with the shortest path from the source to the receiver." *Id.* As such, a router for a host in the group may, similar to the way the RP did, also "issue[] an (S,G) Join towards S," rather than towards RP. *Id.* "This instantiates state in the routers along the path to S" and "either reaches S's subnet or reaches a router that already has (S,G) state." *Id.* At this point, data packets flow from S to the router along the "shortest-path tree (SPT)" following the (S,G) path. *Id.* The router then

"sends an (S,G) Prune message towards the RP," which is "propagated until it reaches the RP or a router that still needs the traffic from S for other receivers," i.e., removing unneeded branches on the RPT in view of the new SPT. *Id.*

¶84. When a receiver knows a particular source address from which it wishes to receive data, "and no other receiver on the LAN requires all the traffic for the group," then the process of setting up the RPT may be skipped, and the DR may set up the SPT immediately by issuing the source-specific (S, G) join towards the source. *Id.* 7–8.

¶85. In sum, PIM-SM specifies the basic functionality/router-control protocol for IP multicasting. PIM-SM is used to convey group and source join requests starting from the edge router and propagating up stream to all relevant routers located between it and the multicast source site to establish efficient (i.e. shortest path tree) non-flooding multi-hop routing of multicast IP data for purposes of ultimately delivering said multicast service *only to those* hosts that have requested it (via IGMP).

¶86. Said routers *are not part of the PON* and are located upstream from the OLT. For example, PIM-SM is concerned with the routers located farther upstream in the metro and core networks that are positioned between the multicast data source(s) that are providing the requested service. The routers may be located anywhere in

the world. The routers include the edge router that is connected to the specific OLT of the PON through which the requesting host device is connected via its ONU.

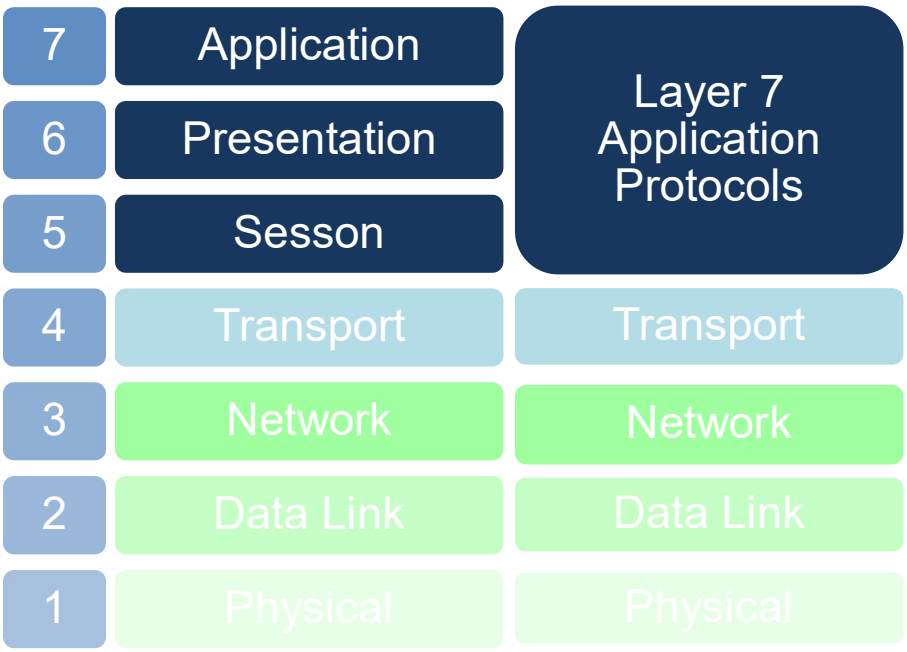
¶87. PIM-SM defines the control protocols for IP routers, upstream from the PON OLT, to set up IP multi-hop routing paths that ultimately deliver the host-requested multicast service. The multicast service data arrives at the edge router, which passes this data to the PON OLT, where it will then be processed and transmitted onto the PON's one-hop ODN for reception by the requesting host's ONU and finally to the host device itself via the CPE connecting it to the local ONU.

¶88. Hence, PIM-SM is concerned with communicating router management messages/instructions between said routers that reach far outside the PON access network's simple "direct one-hop" OLT-ONU connection (the OLT-ONU one direct hop is typically not more than a 20 km long route). *There are no routers between a PON's OLT and its ONUs* and, as such, PIM-SM is concerned with complexities that are completely external to the PON itself and of no direct consequence to the operation of a PON beyond efficiently directing requested multicast traffic loads to the PON's OLT.

D. CITED REFERENCES DEAL WITH "LOW LEVEL" FUNCTIONALITY

¶89. The references that Petitioner cites—Murakami, IGMPv1, and PIM-SM—concern lower-level operations dealing with physical and logical routing of IP datagrams, as well as inclusion of hosts in IP multicast groups, while the concept of

a service is only understood and specified at a higher level with which the references are only minimally concerned. Communications over networks may be modeled with the Open Systems Interconnection ("OSI") conceptual framework that sets forth seven layers as shown.



¶90. In theory, as shown in the middle column, it is the top layer, 7, that provides the claimed ***services*** to the end user. Layer 6 is supposed to perform the task of syntax processing, or formatting data such as translating data from one format to another. At the Session Layer, or Layer 5, construction, direction, and conclusion of connections between devices is supposed to occur. In practice, however, these layers are too fine-grained, and the three layers may practically be collapsed into a single layer referred to as the "Layer 7 Application protocols," as shown in the column on the right.

¶91. It is this upper layer (or these upper layers, as the case may be) where the claimed service—with which a user of the network interacts—resides. Examples of a service with Layer 7 application protocols might be a video or audio streaming service.

¶92. Layer 4 is responsible for transmission of data across network connections. This layer coordinates amount, speed, numbering, error checking, etc. of data between two nodes. For instance, a transport layer may be handled by the well-known internet Transport Control Protocol ("TCP") or User Datagram Protocol ("UDP").

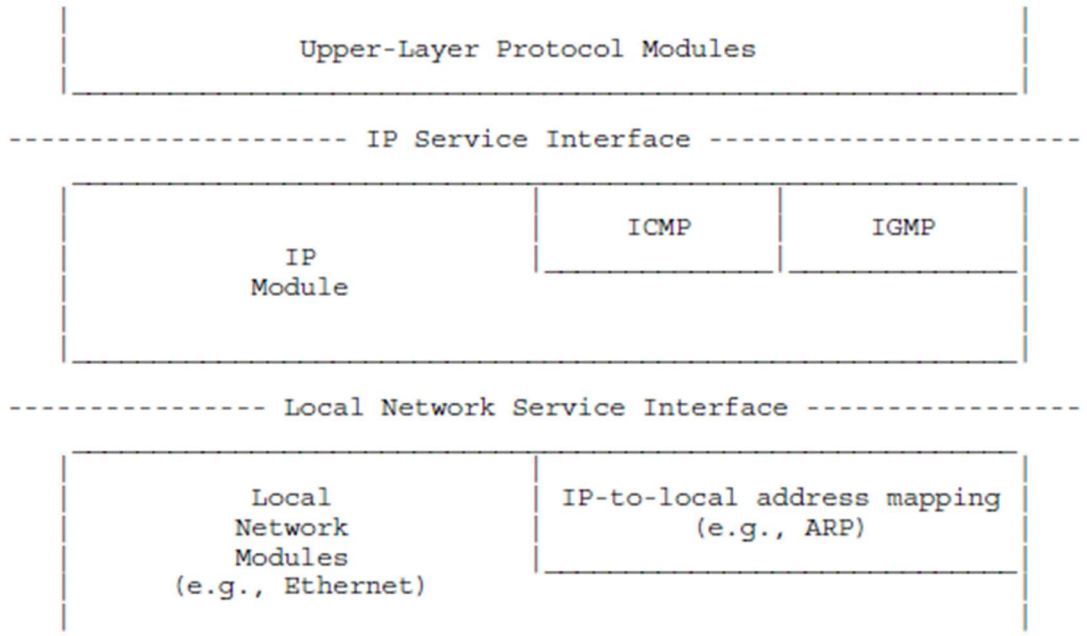
¶93. Layer 3, or the Network layer, handles the routing of the data, including mapping of logical addresses to physical addresses. The Internet Protocol ("IP") is perhaps the best-known Layer 3 protocol. ICMP (internet control message protocol) and IGMP (internet group management protocol) also fall into Layer 3.

¶94. The Data Link Layer, or Layer 2, is generally further subdivided into Media Access Control ("MAC") and Logical Link Control ("LLC") layers. This layer sets up links across the network, puts data into frames, ensures data reaches its destination, etc. Ethernet is a well-known Layer 2 protocol.

¶95. The last layer, Layer 1 or physical layer, encompasses specifying the electrical transmissions, including the cabling, pinouts, voltages, switch and transceiver functionality, etc. At this layer, raw bits are sent over the transport media.

¶96. Petitioner's references are concerned with Layer 3 and below. For instance, Murakami discusses how OLTs are connected to ONUs "via an optical transport medium" (Layer 1) and transmit data by "means of MAC frames . . . through communication that uses logical links" (Layer 2). Ex. 1005 [0012]. Murakami's invention further concerns snooping IGMP which "is a protocol used to manage IP multicast groups" (Layer 3). *Id.* [0002], [0012]. Indeed, the heart of Murakami, its MMT, is provided to a ***Layer-2*** switch—referring to Layer 2 of the OSI model—"used for the switching of multicast frames as well as unicast frames . . . [via] sets of destination MAC address," *id.* [0021] (emphasis added), as well as snooping from "the PON that uses the IGMP as the IP protocol for multicasting" (Level 3), *id.* [0022]. Murakami is concerned with routing multicast data arriving from an "IP network" via the functionality of OSI Layers 1–3. *See, e.g.*, *id.* [0026].

¶97. Likewise, IGMPv1 is a paradigmatic Level 3 protocol that "specifies the extensions required of a host implementation of the Internet Protocol (IP) to support multicasting." Ex. 1006 at 1. Indeed, IGMPv1 notes that it is "considered to be implemented within the IP module" of the layered model illustrated below showing it underlying the "Upper-Layer Protocol Modules." Ex. 1006 at 4.



Id. And while IGMPv1 discusses how upper-layer protocol modules send and receive IP datagrams to/from multicast groups, *see id.* §§ 6–7 at pp. 5–7, IGMPv1 does not otherwise specify how Level 7 services would or should make use of IGMP multicasting.

¶98. A POSITA would also know that Murakami's IGMP snooping is implemented on layer 2 (i.e. by the PON OLT) in order to acquire needed information about the multicast group memberships of the host devices connected to it (via CPE and ONUs). A POSITA would consider PIM-SM as a Level 3 specification, because it is dealing with setting up links across the network and ensuring that data reaches its destination. PIM-SM impacts components that are completely external to a PON.

¶99. While the majority of PIM-SM lies completely outside the scope of PON technology, PIM-SM does discuss how "sources" may address a group. *See, e.g.*, Ex. 1007 at 6. However, "sources" are not "services." As PIM-SM specifies, a source "S" is determined by its IP address. *See, e.g.*, Ex. 1007 at 18 ("S is the source address of the packet."), 82 ("[T]he source address used for multicast messages is the link-local address of the interface on which the message is being sent."). PIM-SM does not address how multiple plural services would or could use a single RPT (Rendezvous Point Tree).

IX. CLAIM CONSTRUCTION

A. "Services"

¶100. Although the '378 Patent specifically addresses PONs, a POSITA would understand that the "services" spoken of in the '378 Patent are the data-centric products the consumer/subscriber is paying to receive and interact with—regardless of the specific hardware type, connection mechanism, or the media transporting and communicating the data to provide these products.

¶101. Indeed, the '378 Patent refers to the GPON specification, *see* Ex. 1001 1:34–35, and GPON makes clear that services are "described by the name that is clearly recognized by everyone." Ex. 2005 at 8. GPON further gives examples of types of "services," including "digital broadcast services, VOD ['video on demand'], file download, content broadcast, e-mail, file exchange, distance learning, telemedicine,

online-gam[ing],” “group software,” “private line services,” etc. *Id.* at 10–11. The entity providing the service is generally referred to as a “service provider.” *See* Ex. 2015.

¶102. In the relevant field, these are more generally regarded as what a consumer views as the “service” he/she is receiving. For example, a computer dictionary from the time defines “service” as “[a] customer-based or user-oriented function.” Ex. 2006.

¶103. I further note that, while “services” can also refer to additional fees for service levels for things such as differing degrees of Quality of Service (“QoS”) or data rates, a POSITA would understand that the ’378 Patent is not concerned with these performance features or SLAs (service level agreements), and is instead referring to the customer-focused “services,” for example, bandwidth demanding services such as audio or video focused streaming applications that a subscriber wishes to listen to or view (or both).

¶104. The “sources” from PIM-SM and IGMPv1 are not the same as the “services” used in the Patent-at-Issue. A POSITA reading these PIM-SM and IGMPv1 specifications understood that “sources” in the context of those documents means the IP address from which a low-level data packet is sent. *See, e.g.*, Ex. 1006 at 6 (“The IP ***source*** address of the outgoing datagram must be one of the individual addresses corresponding to the outgoing interface.”) (emphasis added); Ex. 1007 at

18 ("***S is the source address*** of the packet.") (emphasis added). This is in-line with the general meaning of "source" in the computer world as "[a] place from which data is taken," *see, e.g.*, Ex. 2010, a definition that has not changed from the Effective Priority Date until today.

¶105. Indeed, in the context of multicast, a source sends data to a group of host receivers. Different multicast sources, located in different parts of the world, may send the exact same data to different groups of host receivers, thereby implementing exactly the same multicast service to different multicast groups, however, originating from different sources (i.e., different source IP addresses).

¶106. As further examples to emphasize the difference between a service and its source, "a video-conferencing ***service***" may have "many ***sources*** come and go." Ex. 2007 at 2 (emphasis added). Or a TV broadcasting ***service*** may provide "two video ***sources*** simultaneously for the same TV channel" for redundancy in case there is a "***source*** failure," and, in this failure scenario, the receiver can switch to receiving the redundant TV channel ***source***. Ex. 2008 at 2 (emphasis added). Source redundancy obviously will protect against a localized system failure by providing backup mechanisms to ensure data delivery (and protect against data loss). Source redundancy also improves the performance of the multicast service delivery by reducing latency (sourcing the multicast data from the location closest to the requesting host group members) or by balancing traffic loads amongst available

sources and networking resources (routers switches, etc.) during periods of heavy data demand.

¶107. Petitioner points to the Applicant's argument during prosecution to justify its erroneous position that a "source" is equivalent to a "service." Pet. 32 (referencing the Aug. 12, 2013, Applicant Arguments/Remarks Made in an Amendment, Ex. 1002 at 352). However, the Applicant did not discuss a "source." Rather, the Applicant referred to a "***data stream*** in one ***service channel***," Ex. 1002 at 352, which parallels the claim language "multicast ***service data*** of all ***multicast services***" and indicates that the referred to "data stream" of the "service channel" is the claimed "service data" of the "service," respectively.

¶108. Indeed, a POSITA at the time generally understood that "data stream" has equivalency to multicast service data (the digital bits from which the multicast services is fundamentally built upon). Whereas "service channel" has equivalency to a multicast bearer channel.

¶109. In my opinion, it is likely that the Applicant did not use the word "source" because the '378 Patent is concerned with encrypting all different multicast ***services*** in a same one bearer channel with a same common key, regardless of where the data for the services came from (i.e., their source(s)).

B. "Common Key"

¶110. I agree with both Parties that a "common key" is used in symmetric encryption to refer to the case where the same key is used for both encryption and decryption. I additionally note that, in the context of the '378 Patent, the "common key" is also "common" because the same encryption key is used to encrypt all different multicast services on a multicast bearer channel.

C. "Bearer Channel"

¶111. A POSITA at the Effective Priority Date reading this claim term in the context of the claim limitation and in light of the specification would have understood that the plain and ordinary meaning of "bearer channel" is the channel that bears (transports) the "multicast service data" for the "different multicast services" referenced in the claim.

X. PETITIONER'S PRIOR ART REFERENCES FAIL TO RENDER OBVIOUS ANY CHALLENGED CLAIM

A. All Challenged Claims (Claims 1–13): Murakami in View of IGMPv1, PIM-SM, and the Knowledge of Persons of Skill, Alone or in Combination, Do Not Teach Limitations 1b/c and 9c, Found in Every Claim, or Show That These Limitations Would Be Obvious

> **[1b/c]** . . . using **the common key** to encrypt multicast service data of **all different multicast services** in a **same bearer channel** and then sending encrypted data; wherein the multicast service data of **all different multicast services** in the **same one bearer channel use a same common key** to carry out encryption;
>
> **[9b]** said encryption unit is configured to: encrypt multicast service data of **all different multicast services born in a same one bearer channel with a same common key**;

¶112. I have considered the '378 Patent in light of Murakami, IGMPv1, PIM-SM, and the knowledge of a POSITA, and it is my opinion that none of the cited references, alone or in combination, would have rendered the Challenged Claims obvious. Specifically, it is my expert opinion that Murakami does not teach that all the different services sent in the same bearer channel are encrypted with a common key, as required by Limitations 1b/c and 9c. Further, neither (1) IGMPv1's disclosure that a host that is not part of a multicast group may address a group, nor (2) PIM-SM's disclosure that multiple "sources" may address a Rendezvous Point Tree ("RPT") lead me to conclude that it would be obvious to modify Murakami to arrive at the claimed invention.

¶113. In fact, it is my opinion that the ’378 Patent and Murakami teach divergent means of delivering multicast content to the ONUs on a PON. In the case of the ’378 Patent, groupings of different multicast services are transmitted to the ONUs on a single bearer channel that has been encrypted with one common encryption key for this bearer channel. Only those ONUs that have been successfully activated on the PON and have also applied to receive (one or more) said multicast services that are carried by this bearer channel will have been supplied with the OLT-assigned multicast bearer channel logical link identification and the corresponding encryption key for the multicast data being transmitted on it. Indeed, in this ’378 Patent scenario, it is up to the ONU or downstream devices such as the CPE, after reception and decryption of the multicast bearer channel content data, to process the multiple services carried on the bearer channel.

¶114. *By contrast*, Murakami places the burden of determining which multicast service corresponding to a multicast group needs to be delivered to which subset of ONUs onto the OLT. In the Murakami multicast delivery scheme, individual multicast service content is placed on its own singular multicast bearer channel with its own OLT-assigned logical link identification and its own particular encryption key. Only those ONUs which have hosts subscribed to the said multicast service connected to the ONUs will have been provided with the multicast LLID and the encryption key for this multicast singular-service bearer channel, as only these

ONUs will have passed on the IGMP join requests of their respective host devices to the OLT for this multicast service. Therefore, again, only those ONUs that have been given this information (mLLID and multicast encryption key via an encrypted P2P management channel) will then have the ability to receive, decrypt, and further process the multicast service content being carried on the multicast single-service bearer channels.

¶115. A POSITA in 2010, having understood the Murakami multicast service delivery framework, would not have been led to then reformulate Murakami into the '378 Patent's multicast service delivery scheme. Indeed, Murakami teaches simplification of ONU operations and more data security isolation by placing more "intelligence" in the OLT, *see, e.g.*, Ex. 1005 [0011], while the '378 Patent proceeded in the opposite direction with a solution that requires *more* processing functionality of the ONU and *less* service isolation among ONUs.

¶116. To put a finer point on the issue, an ONU within the '378 Patent's framework would be able to process (decrypt) all the multicast services carried by the bearer channel and may, as a result, receive additional multicast services for which no attached host receiver device has explicitly subscribed. In contrast, Murakami is designed to carry one service per multicast bearer channel, whereby Murakami provides a unique multicast encryption key for each individual multicast service

thereby providing per service encryption isolation. Thus, a POSITA would have been led away from the ’378 Patent invention by the teachings of Murakami.

¶117. The table below compares and contrasts the salient aspects of each patent.

Murakami	’378 Patent
one multicast service per logical multicast bearer channel	multiple multicast services per logical multicast bearer channel
one multicast encryption key per multicast service	one common multicast encryption key used for all the services carried on this one bearer channel
burden of determining which specific *singular* multicast service needs to be delivered to which subset of ONUs is on the OLT once an ONU requests the multicast service on behalf of connected receiver host device(s). The OLT sets up the mLLID bearer channel carrying this one service to those ONUs.	After determining which ONUs have applied to receive a multicast service (or services) carried by a particular multicast bearer channel on behalf of connected receiver host device(s), the OLT delivers all services (requested or not) to the ONUs that have applied for at least one multicast service on this bearer channel. The individual ONUs then have the burden of filtering out and delivering only those multicast services its connected hosts have requested.
only those ONUs which have host devices subscribed to the single multicast service carried by the bearer channel will be able to receive and process the multicast service data stream (these ONUs will have the mLLID and encryption key)	all ONUs which have host devices subscribed to any one or more of the multiple multicast services carried by the bearer channel will be able to receive and process the entirety of the multiple multicast services data streams (these ONUs will have the mLLID and the common encryption key)

¶118. The above differentiation can be seen in the design of Murakami's MMT. As previously discussed, Murakami indexes its MMT by "Multicast Address (IP Group Address)," as shown below in the highlighted first column.

Multicast Management Table 19

Multicast Address (IP Group Address)	Access Port	ONU (LLID for P2P)	LLID for multicasting	Encryption key
yyy.yyy.yyy.yyy	2	1 3	100	#1
	4	2 5	110	#3
⋮	⋮	⋮	⋮	⋮

Id. Fig. 3 (highlighting added).

¶119. A POSITA understood that, with Murakami, an "IP multicast group" refers to the grouping of all the host receiver devices that are receiving a particular multicast service. This is because some members of an IP multicast group may be on the same PON, while others may be spread over multiple different PONs. While still others may not be using a PON at all, but rather connecting by means of a different type of access network technology. The IP multicast group is constructed upstream of the PON and is agnostic to the type of access network technology the receiving host members are utilizing. Indeed, a POSITA understood there may be multiple such multicast groups, wherein generally each such IP multicast group corresponds to a

different (single) multicast service or a different grouping of receiving hosts (i.e. a group of hosts in Texas receiving the same multicast service as a different group of hosts located in Pennsylvania, likely from a different source as well) or a different source of a multicast service.

¶120. Further, the end-user host devices that are members of an IP multicast group—i.e., the IP multicast group members that requested to join the group using IGMP—need not be on the same PON because the IP multicast group is an entity that is constructed upstream of a PON OLT and has no geographical boundaries (unlike a PON). The IP multicast group is assigned a common, but network unique, IP multicast group address. Indeed, "content providers will expect that their assigned multicast addresses are unique (minimally, for the duration of their session)." Ex. 2014 at 5.

¶121. A session refers to the (usually transitory) connection between devices such as the multicast source and its multicast group host members. In this case, a specific multicast session is associated with a particular timeframe, a particular service, the specific source sending this service, and the multicast group member hosts receiving this service. With respect to the same group of receiving hosts, two different multicast sessions could then refer to two different connection time periods, or two different services, or two different sources of the service, or any combination

thereof. Different groupings of multicast receiving hosts would constitute different sessions as well.

¶122. Service providers will expect that their assigned multicast addresses are unique for several reasons:

> First, applications will not expect data from separate sessions to arrive on the same multicast address. Second, separate sessions may have different bandwidth requirements, and if they are on the same multicast–tree, a high-bandwidth session will drown out a low-bandwidth session unnecessarily. Finally, placing separate sessions on separate multicast addresses makes network management easier (for tracking of problems). Other reasons can be found.

Id. In fact, if two content provider services did accidentally send content to user applications on the same multicast group address (an address collision), the result would be "angry customers," as the services would, at best, become unacceptably slow "because packets from other sessions would need to be processed and dropped," and—more likely—both services would not work at all. *Id.* at 11.

¶123. Given Murakami's MMT structure refers only to intra-PON operations (the OLT transceiver and the finite number of ONUs connected to it), a POSITA understood that IP group address "yyy.yyy.yyy.yyy" corresponds to one service

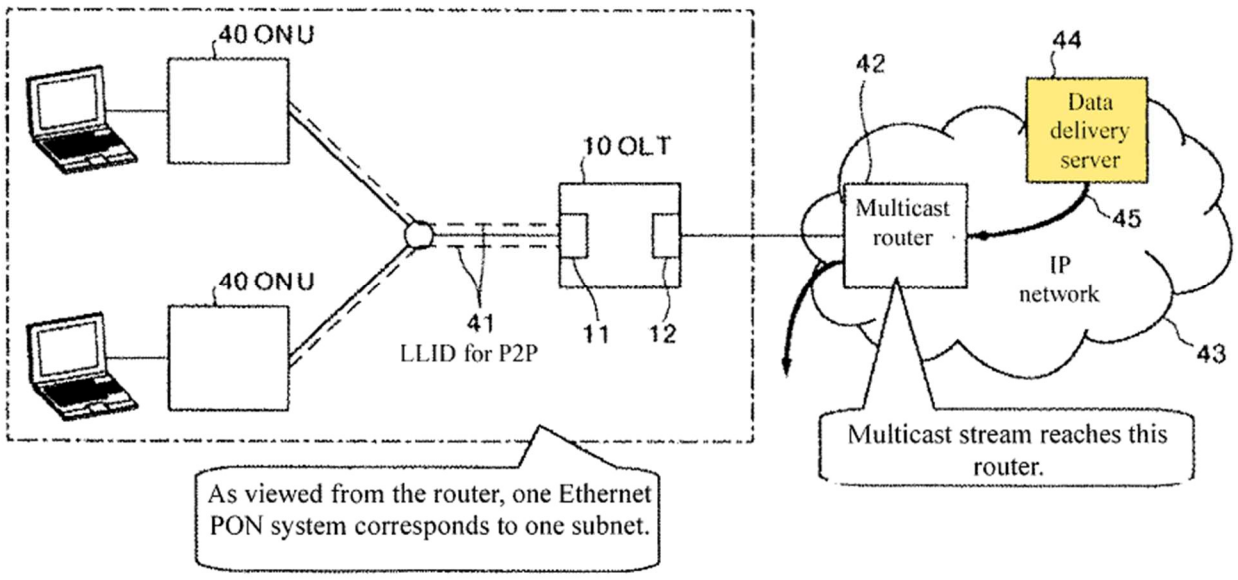
("YYY Service") , and the next row would correspond to another multicast group address for a different service, for instance "zzz.zzz.zzz.zzz" ("ZZZ Service"). Indeed, given the fairly localized nature of a PON, a POSITA would expect the same service would be sourced from the same sending sites; hence, the IP addresses in the MMT correspond to different services.

¶124. Murakami explicitly discloses that it assigns unique LLIDs and encryption keys for each multicast group in the MMT. Ex. 1005 [0030–31]. Therefore, the OLT will use a different multicast LLID that Petitioner identifies as a "bearer channel," and a different encryption key for the YYY Service than the OLT will use for the ZZZ Service sent to the same ONU.

¶125. In fact, Murakami explicitly explains its rationale for using separate LLIDs and separate encryption keys for each group/service, saying that encrypting the Register message with OLT-to-ONU P2P encryption key "prevent[s] the stored multicast encryption key from being eavesdropped by another ONU." *Id.* [0032]. Therefore, Murakami only uses the same key for different ONUs for the same service on the same physical port, because these ONUs will get the same data in any case since downstream devices on the ONUs had subscribed to the same service. This is now explained through a real-world illustration.

¶126. Consider a service from an internet service provider ("ISP") that may be multicasting a basic video package, such as live Internet Protocol Television

("IPTV") to subscribers that have paid for this service. As an OLT concerned with routing Layer 2 communications and snooping the higher-level IGMP Queries and Reports, from Murakami's view this is simply a data stream coming from a "Data delivery server," as shown below:



Ex. 1005, Fig. 4 (highlighting added). The multicast IP group addresses correspond to the "service channels" by which different multicast services are sent.

¶127. For instance, an ONU on Access Port 2 of an OLT assigned P2P LLID 1—call it "ONU A"—may send an IGMP Report (originating from one of the end-user host devices connected via CPE to this ONU) to request joining the IP multicast group with IP address 224.0.0.4 that corresponds to the IPTV multicast group address. And, as a reminder, Murakami's OLT detects member's groups by snooping IGMP Report messages where "the group address field holds the IP host

group address of the group being reported." Ex. 1005 [0004], Ex. 1006 at 12. Therefore, after ONU A subscribes to the basic video package, Murakami's MMT may look as follows:

Multicast Address (IP Group Address)	Access Port	ONU (LLID for P2P)	LLID for multicasting	Encryption key
224.0.0.4 **(IPTV)**	2	1	**100**	**#1**

Murakami uses this MMT entry and the related L2 Switch to route and encode the IPTV service communications sent over service channel 224.0.0.4 to ONU A.

¶128. And because (1) no other ONUs on Access Port 2 have subscribed to this service, and (2) the OLT transmitted the multicast encryption key value for this service in a P2P encrypted message to ONU A using the unique P2P encryption for which only ONU A can decrypt, *see id.* [0032], no other ONU may decrypt this multicast service.

¶129. Now, if the same ONU A also subscribed to an intraoffice video conferencing ("VC") service provided by the ISP, ONU A would send another IGMP Report message indicating its desire to join the VC multicast IP group address, say 224.0.0.5. Because the second address is different, "no matching IP multicast address is found" in the MMT, and the OLT "recognize[s] [the Report] as the first access" for this service. So the OLT creates a new row, and "the [second] IP

multicast address, the access port, and the ONU (LLID) are remembered in an unused entry in multicast management table 19." Ex. 1005 [0029]. That is, the OLT will set up another entry in the MMT because the table is indexed by the Multicast Address (IP Group Address). *Id.*

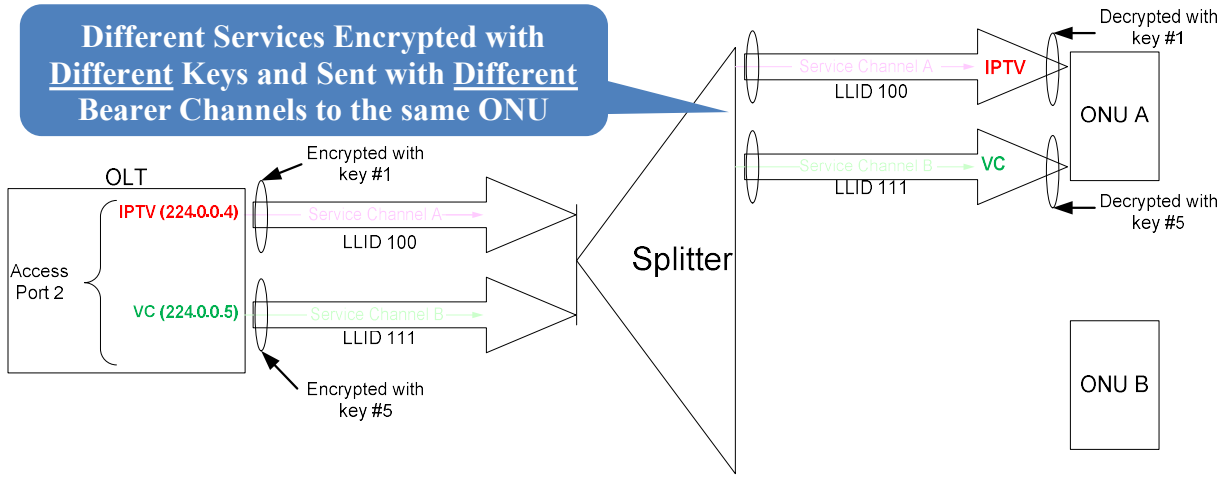
¶130. With Murakami, when no matching IP multicast address from the Report message is found (as would be the case with the second Report message), the OLT (1) "sets up a multicast logical link for the ONU that has made access[;] [s]pecifically, logical-link control section 21 refers to LLID management table 22, selects one of the unused LLIDs at the access port," *id.* [0030]; and (2) "generates a new encryption key used in this multicast communication and transmits it to the point-to-point logical link 41," *id.* [0031]. Therefore, the MMT may look as follows after the OLT snoops the two Report messages from ONU A subscribing to the different services:

Multicast Address (IP Group Address)	Access Port	ONU (LLID for P2P)	LLID for multicasting	Encryption key
224.0.0.4 **(IPTV)**	2	1	**100**	**#1**
224.0.0.5 **(VC)**	2	1	**111**	**#5**

Murakami then uses this second MMT entry and the related L2 Switch to route and encode the VC service communications sent over service channel 224.0.0.5 to ONU A, and no other ONUs on Access Port 2 may decrypt (i.e., "eavesdrop

on") the VC service.

¶131. In short, for subsequent data sent in these service channels, i.e., addressed to these two multicast groups, Murakami's OLT would use (1) bearer channel LLID 100 and encryption key #1 for the IPTV service and (2) bearer channel LLID 111 and encryption key #5 for the VC service. I illustrate this below[12]:



These are ***different*** keys for the different service channels (i.e., multicast IP group addresses) used by the different multicast services, on ***different*** bearer channels—that Petitioner identifies as the LLIDs—not the claimed "using the

[12] As a side note, given the physical architecture of a PON, ONU B would have also received the exact same frames containing the multicast service streams transmitted downstream by the OLT, but since it is not in possession of the LLIDs nor the corresponding encryption keys for the respective multicast bearer channels, it is unable to process the multicast service content contained in these bearer channels. For simplicity, this unencryptable data to ONU B is not illustrated in the diagram below.

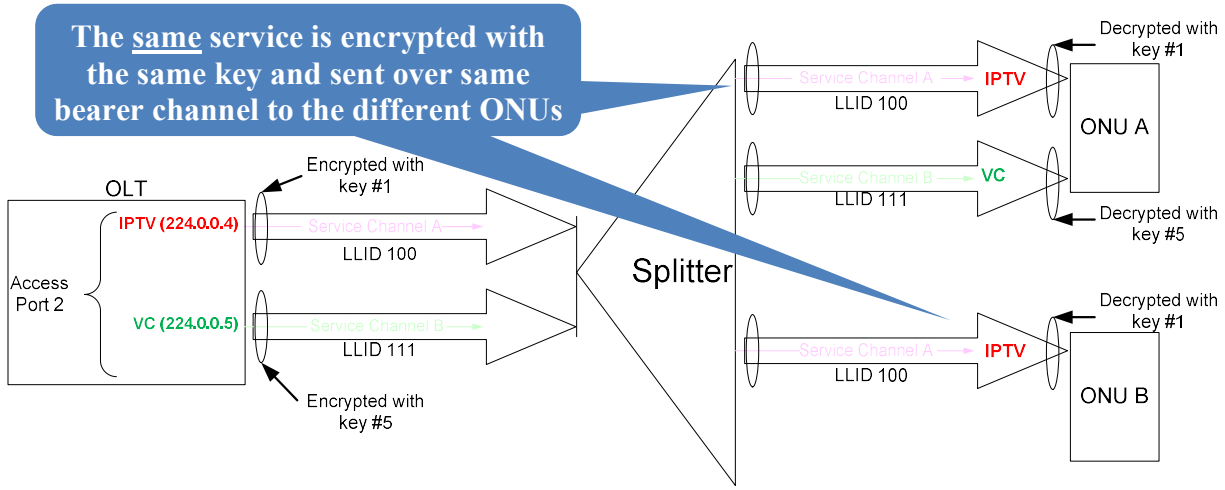
common key to encrypt multicast service data of all different multicast services in a same bearer channel." So, Murakami's architecture is different from the claims of the '378 Patent because Murakami does not route all the different services on the same bearer channel using the same common key.

¶132. Therefore, Petitioner focuses on the case where two ONUs are attached to the same PON serviced by the same OLT transceiver. *See, e.g.*, Pet. 22 (discussing "two ONUs belonging to a multicast group, each connected to the OLT's physical port 2, receiving multicast data communications via a downstream logical link having LLID 100"). However, as discussed above, a POSITA understood that if the two ONUs belonged to the same ***group***, this would be the same ***service***—not the claimed ***different-- service***. Continuing the example, if another ONU, "ONU B," on Access Port 2 that had P2P LLID 3 sent a Report to also join the IPTV service, Murakami would give the IPTV encryption key to ONU B and Murakami would further build the MMT that might now look as follows:

Multicast Address (IP Group Address)	Access Port	ONU (LLID for P2P)	LLID for multicasting	Encryption key
224.0.0.4 **(IPTV)**	2	1	**100**	**#1**
		3		
224.0.0.5 **(VC)**	2	1	**111**	**#5**

That is, while different ***ONUs***—listed in the third column of the first row—will

receive the encrypted data, this is data from the ***same*** multicast service—specified by the multicast IP group address and listed in the first column—on LLID 100. There is no concern for "eavesdropping" in this case because the ONUs have legitimately subscribed to the same multicast service on behalf of their respective connected receiver host devices. This situation is illustrated below.



Given that the MMT is indexed by multicast group address and these addresses correspond to a multicast service, a POSITA would understand that keys and bearer channels are assigned ***per service***. In contrast, the Patent-at-Issue claims using the same key for "data of all ***different*** multicast services." Petitioner admits that this is so. Pet. 19 ("Murakami explicitly discloses all but one element of independent Claim 1 (i.e., 'all **different** multicast services')."").

¶133. So, Petitioner turns to IMPGv1 and PIM-SM for the proposition that "the encryption and transmission of different multicast ***service*** data in the same bearer

channel would have been obvious, in view of RFCs 1112 and 4601," because "RFCs 1112 and 4601 teach that . . . the content of communications to each such multicast group can be drawn from different ***services***." Pet. 28 (emphasis added). But the evidence that Petitioner cites does not support this proposition. PIM-SM teaches that communications to a multicast group can be drawn from different ***sources***, not ***services***. And the cite to IPMGv1 section says nothing concerning multiple services (***or*** sources for that matter).

¶134. Specifically, for IPMGv1, Petitioner simply points to IPMGv1's disclosure that "IP datagrams can be sent by ***sources*** other than those constituting hosts." *Id.* 31 (citing Rouskas Dec'l, Ex 1003 ¶89 (in turn citing Ex. 1006 at 1)). And this is true; IPMGv1 says that "[a] host need not be a member of a group to send datagrams to it." Ex. 1006 at 1. But IGMPv1 is simply clarifying that a source need not be part of the group; this says nothing about ***how many sources***—whether part of the group or not—can send data to a group, much less the relationship of a service to a source or that multiple services can or should address a group. A POSITA understood that the text the Petitioner cites is simply saying that the IP multicast group members are all receiver hosts which are to be distinguished from a sending host (the source), which is not required to be a member of the group. And IGMPv1 certainly does not address encrypting, much less encrypting all different multicast services on the same bearer channel with the same common key.

¶135. For PIM-SM, the specification does say that "sources"—plural—may send data destined for a group to a Rendezvous Point, *see, e.g.*, Ex. 1007 at 4; *see also id.* at 5 ("The root of [a] tree may be either the ***source*** or the RP, depending on the context.") (emphasis added). However, PIM-SM's disclosure of multiple ***sources*** also falls short of teaching multiple ***services*** would or should share a single group multicast destination address. Like IGMPv1, PIM-SM does not discuss the relationship between a source and a service.

¶136. A POSITA understood that a "source" is not the same as a "service." To understand why, some background regarding multicasting in general is useful. An IP multicast group is an arbitrary number of host receivers that join said group in order to receive a particular data stream (i.e. a singular multicast service). The multicast IP address associated with this IP multicast group identifies the bearer channel in this case. As such, only one service can be communicated over the IP multicast bearer channel.

¶137. And the multicast group has no physical or geographical boundaries. That is, the receiving group member hosts can be located anywhere on the internet. This is unlike a PON, which is typically limited to just 20 km (~ 12.4 mile) fiber runs from the OLT transceiver site to the ONUs that it serves. Furthermore, the ONUs of a PON are positioned one hop away from the OLT site. There are no routers located between the ONUs and the OLT transceiver servicing the PON. As such, there is a

clear distinction between the membership of an IP multicast group and the PON itself.

¶138. A single PON, with typically 16 to 128 ONUs attached to it, is a fairly localized single-hop access network which may, for example, only service the residences (or businesses) located on one or two street blocks in a typical American (sub)urban neighborhood. With so few ONUs connected to a single OLT transceiver, it should be clear that the number of host devices utilizing a single PON that are also members of a particular IP multicast group will probably comprise only a very small percentage of the total membership in this IP multicast group. Furthermore, these host devices will be concentrated in a very localized geographical region—perhaps all within just a few hundred meters of the PON splitter. Therefore, insofar as the PON is concerned, all the host devices on this PON that are members of an IP multicast group likely are being served by a single common source for this service.

¶139. By simple extension, the combined IP multicast group member hosts from all the PONs (access ports) connected via a single OLT chassis will likely have their multicast service for this particular group provided by a single source of this service since the multicast service data sent by the source must pass through the same OLT site and all of the ONUs will be located within about a 20 km fiber run of the OLT chassis location.

¶140. By contrast, different geographically-dispersed IP multicast group host members will utilize correspondingly disbursed PON OLT sites (or even entirely different access network technologies). This is so because the IP multicast group is not tied to the access network technology, but is only tied to the multicast service being provided. Thus, a reason for allowing/needing multiple sources to provide the multicast data/service to an IP multicast group is simply the fact that the entirety of the IP multicast group membership may be located over vast geographical locations.

¶141. And a POSITA understood that PIM-SM contemplates that different sources of the same service may provide more optimal delivery (such as reduced latency, fewer hops, fewer needed network resources, etc.). Optimal routing from a source of the multicast service to a (collection of) receiving host member(s) is provided for in protocols such as PIM-SM. Other reasons that multiple sources of a service are implemented are discussed below.

¶142. Furthermore, the protocols defined by PIM-SM are applicable upstream from the PON and don't apply to the PON itself as there are not any routers located inside of a PON between the OLT transceiver and its ONUs. There are no routes to be determined nor trees (or routes) to be optimized inside of a PON. As such, a POSITA would not have been inclined to consult PIM-SM for the application at-hand: intra-PON multicast service delivery.

¶143. In truth, a "service" is distinctly different from a "source" (of the service). A "source" is the physical location (with granularity potentially down to a particular component, for example, a specific server located within a data center building) where a specific service's data or remote applications are stored and/or where the specific service data are transmitted from (i.e. the sending host) when requested by a subscriber using that particular service. The terms "sending host" and "source" may at times be used interchangeably. Data centers are an example of sources where services emanate from. *See, e.g.*, Ex. 2013. All different (multicast) services may be delivered to the consumer from different sources or potentially the same source location. Data centers are typically distributed across a region or country; hence, the same service may emanate from different source locations depending upon where the end-user of the service is located and which specific service is being used.

¶144. There are many reasons why a service may have multiple sources. For instance, group members may be sources that come and go, for instance in a video chat. *See, e.g.,* Ex. 2007 at 2.

¶145. Or a service may use one source for one type of content, such as video, and another source for different but corresponding content, such as audio, and the receiver applications may be designed to recombine the two source streams.

¶146. Or sources may correspond to different "channels," for instance in an IPTV service. That is, one source may carry C-SPAN content and another source of providing PBS content.

¶147. Other reasons for utilizing multiple sources of the multicast service would be to allow for load balancing during periods of very high demand for the service.

¶148. Yet another reason for having multiple sources for a service is to help ensure service availability should some sort of system failure occur. *See, e.g.,* Ex. 2008 at 5. Typically, in the case of some sort of source or network failure, the system operator would perform the redundancy switchover from one service's source to another (most likely automated and ideally within a very short period of time so as not to adversely interrupt the subscriber's experience) in order to continue providing the multicast service to the receiving host devices, now sourced from an alternative sending host, thereby keeping the service operative and available.

¶149. Indeed, the authors of PIM-SM and IGMPv1 were aware that their target audience were highly technical individuals within the relevant industry and that the specifications were ultimately meant to be the standard by which different companies would agree to conform their products. As such, a POSITA understood that the authors would be very precise in the language that they used to minimize any potential misunderstanding. Therefore, when the specifications use the term "sources," a POSITA would know exactly what the authors meant, and this word

choice was not "fuzzy" or unconsidered language. As such, a POSITA would not equate "sources" with "services," because the two terms mean different things to an artisan in the field.

¶150. Petitioner argues that a POSITA would design a system in light of the prior art whereby "data from more than one different multicast service" is sent to "a particular multicast group." Pet. 34. However, Petitioner's suggested modification is misaligned with Murakami's teachings. As a reminder, IGMPv1 reserves "Class D" IP addresses from 224.0.0.0 to 239.255.255.255 for multicast groups, Ex. 1006 at 3, and Murakami indexes its MMT by these addresses. As such, Murakami's MMT theoretically can have approximately ***268 million*** Multicast Address IP Group rows with the same number of multicasting LLIDs and encryption keys for a single ONU. Nonetheless, Petitioner argues that, despite Murakami having hundreds of millions of multicast group addresses available and a ready system that handles different services by assigning different LLIDs and encryption keys for each group, a POSITA would analyze Murakami, IGMPv1, and PM-SIM and conclude different services should be routed to the same multicast group address. The following table illustrates that the Petitioner is making a post hoc suggestion in an attempt to meet the claim limitations requiring "all different multicast services in the same one bearer channel use a same common key."

Multicast Address (IP Group Address)	Access Port	ONU (LLID for P2P)	LLID for multicasting	Encryption key
224.0.0.4 **(IPTV, VC, online-gaming, file distribution, content broadcast, e-mail, file exchange, distance learning, telemedicine, group software, private line services, etc.)**	2	1	**100**	**#1**
		3		
224.0.0.5	2	1	**Unused**	**Unused**
		3		
⋮	2	1	**Unused**	**Unused**
		3		
239.255.255.255	2	1	**Unused**	**Unused**
		3		

Up to ≈268 Million Unused Multicast IP Group Addresses

¶151. Additionally, with Petitioner's proposal to force multiple services on the same group, Murakami is no longer able to prevent the stored encryption key for a service "from being eavesdropped by another ONU," *see* Ex. 1005 [0032], because any ONU that subscribed to any service in this group must necessarily be given the LLID multicasting key, and so one ONU may decrypt services that only another ONU has subscribed. That is to say, Murakami, as is, provides for individual service level

security as discussed earlier in this document, and Petitioner's proposal would vitiate Murakami's designed security. This is clearly a disincentive to try and somehow morph the teachings of Murakami into the multicast delivery scheme taught by the '378 Patent.

¶152. Moreover, I find Petitioner's rationalizations for disregarding Murakami's fundamental design—whereby the MMT assigns different keys/channels per multicast group, a natural division for different services—undeveloped and unsound. *See* Pet. 34–38.

¶153. For instance, Petitioner argues that a POSITA would arrive at a system in light of Murakami/IGMPv1/PIM-SM whereby different multicast services are sent to a single multicast group "to provide subscribers registered with a particular multicast group with data from more than one different multicast service to enhance the services offered to such subscribers." Pet. 34. (citing Ex. 1003 ¶93). However, a subscriber may register with many multicast services, each multicast service having their own assigned multicast group, *see* Ex. 1006 at 1 ("A host may be a member of more than one group at a time."), so subscribers may get "data from more than one different multicast service" without forcing different multicast services to share a single multicast group.

¶154. Indeed, delivering multiple service data streams to the same IP multicast group where there is no indication that ONUs/CPE are designed to handle multiple

streams is a recipe for data collision errors that would crash the multicast delivery of all services to this one group of hosts that are members of said IP multicast group. *See, e.g.*, Ex. 2014 at 5, 11. To understand why this is so, recall that a multicast receiver host equates directly to an end-user device. It is these receiver hosts (the devices that the subscribers directly interact with such as computers, smart phones, tablets, smart TVs or STBs, smart appliances, etc.) that are the actual members of the IP multicast group which are receiving and using, in some way, the multicast service sent from a source. The IP multicast address for a given IP multicast group essentially designates the bearer channel for a singular service being delivered to said IP multicast group members. It is then the function of the IP routers operating in conjunction with protocols such as IGMPv1 and PIM-SM to route the data of the multicast service from a source towards the receiving host devices that are members of the corresponding IP multicast group.

¶155. In the case of receiving host devices that are accessing the internet by way of a PON, the requested multicast data stream will be routed, typically over many multiple hops, to the edge router that is connected to the PON's OLT and then to the OLT itself. Once the multicast data for the service reaches the edge router, the job of PIM-SM is done—it has no role to play within the PON itself. At the OLT, the IP multicast data will be processed and configured to conform with the standards of the PON technology employed, such as the transmission-convergence layer of an

ITU type PON (GPON, XGSPON, etc.) or an IEEE type PON (EPON 10GEPON, etc.) in preparation for transmission downstream into the PON. Here it will be inserted onto another multicast bearer channel specifically for intra-PON transmission from the OLT transceiver to the ONUs connected on the PON. It is the purpose of the intra-PON multicast bearer channel to securely deliver the multicast data only ***to those ONUs*** on a given PON which have subscribing receiver host devices, to said multicast service, connected to them (via CPE). This, of course, is implemented using mLLIDs and encryption.

¶156. It is very important to understand the distinction between the PON multicast bearer channel and the IP multicast bearer channel. The IP multicast bearer channel carries, starting from the source, the singular multicast service expected by the receiver host devices that are members of the corresponding IP multicast group. The multicast service data, sent by the multicast source via the IP multicast bearer channel designated by the IP multicast group address, is ultimately destined to be delivered to each receiver host (i.e. each end-user device) that is a member of the IP multicast group. ***By distinction,*** *it is the sole purpose of the intra-PON multicast bearer channel to assist in this delivery process* ***by securely ferrying*** *the IP multicast service data, carried by the IP multicast bearer channel, from the OLT downstream to the ONUs on the PON (a one hop "ride").* Only those ONUs with IP multicast group member hosts attached to them will then be able to further process the intra-

PON multicast bearer channel payload and thereby deliver the requested IP multicast service to the subscribing end-user devices that are connected to it via CPE.

¶157. So, the IP multicast service, delivered via the IP multicast group designated by its multicast group IP address (effectively an IP multicast bearer channel), after departing the source, is sent on a journey to reach the end-user host devices that are members of the multicast group associated with this service. In order to reach host devices that are connected to the internet using a PON access network, the IP multicast data must be placed onto *an intra-PON multicast bearer channel which will take the IP multicast data part of the way "home" and deliver it to the ONUs.* All of the ONUs will, in turn, receive the PON multicast bearer channel and, only if subscribing hosts devices are connected to it, will an ONU then be able to process the information carried by it and finally deliver the requested IP multicast service data to the subscribing end-user receiving host devices via CPE.

¶158. Now, an ONU located at a residence, business, campus, or MDU will almost certainly have multiple end-user devices connected to it. Any combination of these receiver host devices may be members of any number of IP multicast groups receiving a corresponding assortment of different services (with each service being sent from their respective multicast source). The PON must then deliver these all-different multicast services first to the ONUs which have end-user devices connected to them that are members of any of the corresponding IP multicast groups, and then

deliver the specific multicast service requested to the respective multicast group member host devices themselves.

¶159. For reasons already discussed, a source for an IP multicast group delivers only a single service to the receiving host devices that are the members of the multicast group associated with the service. Murakami straightforwardly extends this singular IP multicast service delivery framework in a one-to-one fashion to a corresponding multicast service delivery scheme suitable for the PON whereby each individual intra-PON multicast bearer channel ferries only a single IP multicast service from an OLT to the ONUs on its PON. There must be one multicast bearer channel designated for each different multicast service requested by the host devices connected to the PON's ONUs. Each multicast bearer channel is also individually encrypted with its own key; hence each multicast service is also individually protected during its transport within a PON.

¶160. Divergent from the Murakami teachings, the '378 Patent recognizes that since an ONU can be made to determine the proper destination host devices for all the different services it receives, delivered to it by an intra-PON multicast bearer channel, it is perfectly plausible that a single intra-PON multicast bearer channel would then be able to deliver multiple such IP multicast services to the ONU. Whereby, an ONU, with subscriber host device(s) connected, would process (for example, decrypt all the different multicast services) and then may, for example,

properly deliver each one of the respective all different multicast services only to those corresponding host devices that are members of the respective IP multicast group of each one of the different multicast services. The ONU would have been provided the mLLID and same common encryption key after successfully applying to receive said multicast services. The '378 Patent teaches to implement a bearer channel-level encryption—opposed to Murakami's service-level encryption. That is, with the '378 Patent, all-different multicast services being transported by a singular intra-PON multicast bearer channel are encrypted with the same common key (as opposed to one key per service, as they are in Murakami).

¶161. Moreover, the '378 Patent's claimed invention also simplifies the encryption of the multicast services, which is beneficial to the PON operation and is perfectly feasible given that, in all likelihood, each one of the all-different multicast services were also transmitted in an encrypted format by their respective sending sources (e.g., using SSL, TLS, DRM, etc.), as described in the overview of the Patent-at-Issue. *See* Section VI. Thus, a POSITA understood that the PON is adding another layer of encryption, during the transport between the OLT and the ONUs.

¶162. Thus, given that Murakami teaches (1) only a single IP multicast service carried by each multicast bearer channel with each channel individually encrypted using a unique key, and (2) that the IP multicast source delivers only a singular service to host devices that have joined the corresponding multicast group

(designated by its multicast IP address, essentially the bearer channel for delivering the singular multicast service sent by the multicast source), and (3) that neither IGMPv1 nor PIM-SM discuss sending multiple multicast services over a singular multicast bearer channel (that is to an IP multicast group), and (4) that furthermore PIM-SM plays no role in the "router-less" ***passive optical network*** architecture, a POSITA would not have been led to the teachings of the '378 Patent via any obvious deductive route utilizing, as per the Petitioner's assertions.

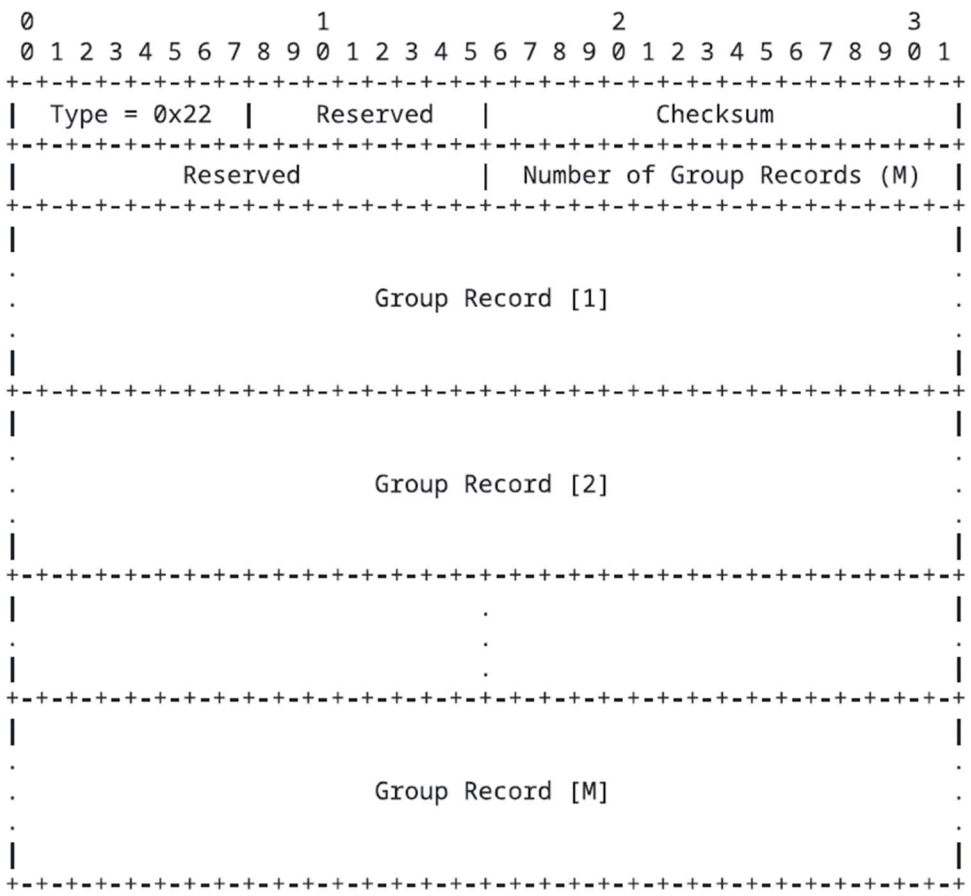
¶163. Petitioner also argued, relying solely on Dr. Rouskas' declaration, that having different services address a single IGMP multicast group would "deliver that data to a subscriber in a single bearer channel more efficiently." Pet. 34. (citing Ex. 1003 ¶93). However, I have reviewed the cited section, and I find no explanation as to why this should be so. In any case, I disagree. As explained above, multicast services expect to have a unique IGMP multicast group reserved for the service, and generally bad results occur when two services inadvertently use the same IGMP multicast group.

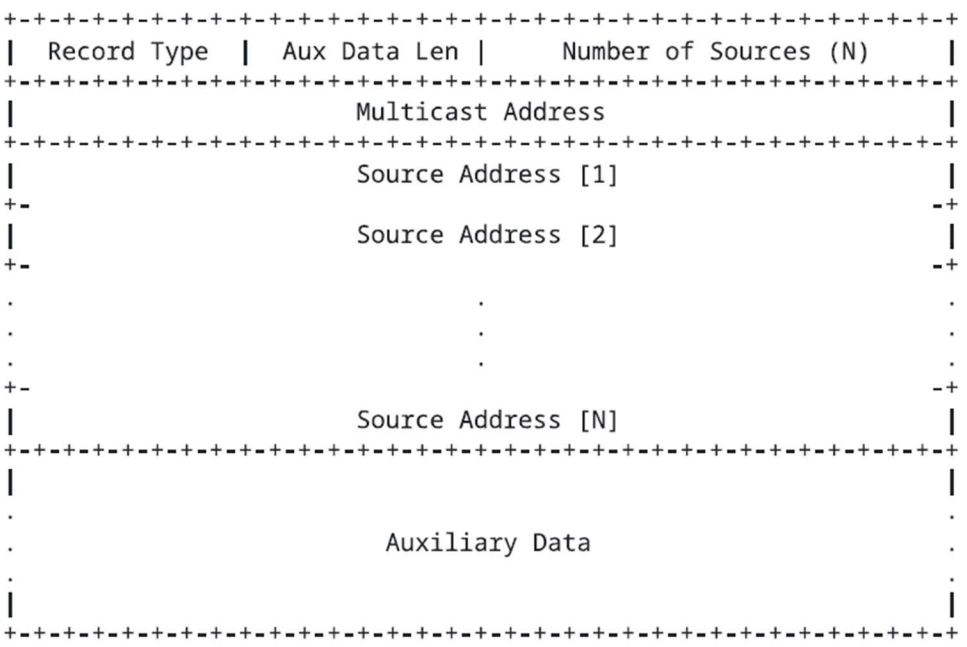
¶164. Petitioner further says that a POSITA would design a system whereby different multicast services would be sent to a single multicast group to "ensure compatibility with published standards protocols, such as RFC 4601," "so that it could enjoy the benefits of the advances in IGMP standards (*i.e.* IGMPv3)," "the advances provided by RFC 4601 also enabled more selection of more selective data

sources," and "Murakami's system and methods are compatible with multicast data consisting of different multicast services and are employable with more recent IGMP standards." Pet. 34. It appears that not only is Petitioner suggesting that a POSITA would abandon Murakami's different key/channel per multicast group design and have all services use only a single IGMP multicast group, but that the Petitioner's suggested redesign would have all the different services correspond to different sources and rely upon the customer side devices to issue "source-specific joins" to set which multicast service data the joining device would like to receive.

¶165. But Petitioner immediately undercuts its proffered design by saying "a POSA would not have undertaken to differentiate multicast data composed of data from a plurality of sources based upon its source," Pet. 34–35, because, to implement IGMPv3 and Petitioner's plan to use a single group and IGMPv3's source filtering, ***that is exactly what is required***. Under Petitioner's scheme, the OLT can no longer merely snoop for IP datagrams and "us[e] the IP group address as the [MMT] key," Ex. 1005 [0027–29] & Fig. 5, and start delivering "upon receipt of a report message from a subscriber terminal" and "stop[] the delivery of multicast data upon receipt of a leave message from the subscriber terminal," *id.* [0005]. Because with IGMPv3, the IP multicast group destination address is no longer sufficient to know whether multicast data should be forwarded to an ONU.

¶166. With IGMPv3, Report messages have the following format (shown on the top), and each group record in the Report message has the format (shown on the bottom):





Ex. 2012 at 13–14. Using these new Report formats, receivers may now specify that they want to receive "packets *only* from specific source addresses" and "from *all but* specific source addresses." *Id.* 2. As such, for Murakami to do routing by snooping IGMPv3 packets, Murakami must keep track of what multicast address and source address combinations ONUs have included and excluded and coordinate across ONUs sharing a physical access port. *See, e.g.*, *id.* 5–7 (explaining rules for when different receivers make overlapping include/exclude requests); *see also* Ex. 1007 at 7 (explaining that a prune message is only propagated if there is no other receiver on the router "that still needs the traffic from S").

¶167. I additionally note that PIM-SM has been public for close to two decades, and yet Petitioner has not put forth a single example of multiple services sharing a

multicast group and relying upon subscribers to perform source-specific group joins to filter data only from the services the subscriber desires.

¶168. Moreover, Petitioner's requirement—that the subscribers ***must*** use source specific joins—would render Murakami unusable with IGMPv1 and IGMPv2, which do not support source specific joins. If a host did a general group join—the only option under IGMPv1 and IGMPv2—with Petitioner's system that had all services send data to the same group, the receiving host would now get and be unable to process unexpected data from multiple services. That is, Petitioner's suggested system-wide restriction would render Murakami unsuitable for use with IGMPv1 and IGMPv2.

¶169. I ultimately conclude that Murakami's design that allows for millions of different bearer channels using different keys for different services is the opposite of the '378 Patent's goal to reduce encryption complexity by having an OLT designate and encrypt a bearer channel for sending encrypted data using a common key for all the different multicast services on that bearer channel. And IMPGv1's teaching that a ***source*** outside a multicast group can address a multicast group, or PIM-SM's teachings that multiple ***sources*** that can come from a ***single*** service, may address a multicast group does not change Murakami's fundamental design. Therefore, the limitation "using the common key to encrypt multicast service data of all different multicast services in a same bearer channel and then sending

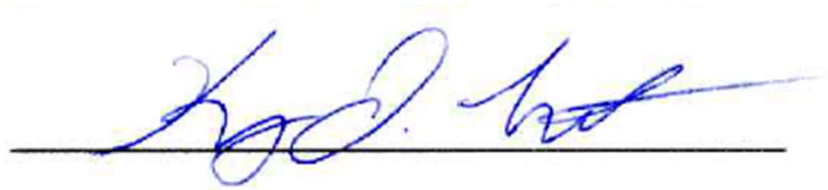
encrypted data" is not taught, and is not rendered obvious, by Murakami, IGMPv1, or PIM-SM, either individually or collectively.

XI. DECLARATION

¶170. I recognize that this declaration will be filed as evidence in a contested case before the Patent Trial and Appeal Board ("PTAB") of the United States Patent and Trademark Office. I also recognize that I may be subject to cross examination on the subject matter of this declaration. If cross examination is required of me, I will appear for cross examination within the United States during the time allotted under the rules and as specified by the PTAB.

¶171. I declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true. Further, these statements are made with the knowledge that willful false statements are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Executed on November 21, 2024 at Huntingdon Valley, Montgomery County, PA.



Dr. Kerry I. Litvin

APPENDIX A (RESUME)

KERRY I. LITVIN, PH.D.

1874 PINE ROAD, HUNTINGDON VALLEY, PA 19006-7940

+1.267.625.6478 Kerry@HBarOmegaLLC.com www.HBarOmegaLLC.com

http://www.linkedin.com/pub/kerry-litvin/10/996/543

Results-driven intellectual property technical expert and technology development leader with visionary foresight, a keen eye towards new innovations, and solving difficult problems. Extensive optical network architecture, optical transport, optical sub-systems, and component expertise within the broadband cable and telecommunications industry. Demonstrated ability to advance the state-of-the-art in all of these areas. "Go to" person when building relationships with customers and suppliers in order to achieve technologically based business goals. Strong background in Fiber Optic Engineering, TV Signal Transmission Over Fiber, Electrical Engineering, Applied Physics, RF/Microwave/Millimeter-Wave/Wireless Engineering, Mathematical Modeling, Technical Due-Diligence, and Intellectual Property Matters. *14* issued patents.

AREAS of OPTICAL EXPERTISE

- DWDM and CWDM Optical Networks
- FTTH/PON
- QAM TV Transmission Over Optical Fiber
- BC/NC Video Overlay Architecture
- RFOG
- Optical Transport
- Polarization Multiplexing
- Commercial Transport/Ethernet Over Fiber
- Broadband HFC Products & Architecture
- Dispersion and Dispersion Compensation
- Nonlinear Optical Distortions/Raman Effects
- CSO, CTB, CNR, Distortion Analysis
- Optical Layer Monitoring OTDR/OFDR
- Polarization Mode Dispersion

PROFESSIONAL EXPERIENCE & CAREER ACCOMPLISHMENTS

H-Bar Omega LLC, Huntingdon Valley, PA **6/2014-Present**

Founder and President

Independent consultancy providing technological due diligence support to investment managers at private equity firms, venture capital firms, hedge funds, and other private or public financial institutions all with keen monetary interests in cutting-edge and/or commodity: 1) optical communication devices, components, and technologies, 2) optical sensing devices, components, and technologies, 3) fiber optic telecommunications networking systems and technologies, and 4) broadband fiber optic, wired, or wireless communication components, subsystems, and networks.

- ***Extensively involved with intellectual property law matters in all areas and aspects of optical fiber communications technologies, broadband communications technologies, optical sensor and instrumentation technologies, and photonics.***
- ***Patent litigation expert analysis and consulting in all aspects of fiber optic and broadband communications networks, systems, components, and instrumentation. Extensive inter partes review (IPR) experience in fiber optic communications.***
- ***Provided technical evaluations of approximately 3000 patents to date regarding both IP portfolio asset valuation and the potential for patent infringement including creating evidence of use (claim) charts as required.***

The consultancy was founded to:

- Completely address the financial community's needs to fully understand the implications of potential high-technology investment opportunities from expert technological, engineering, and scientific perspectives so that any investment decisions can be made in an entirely informed and unbiased manner.
- Provide expert technical and engineering support to direct industry participants; by servicing the broadband/fiber-optic/telecommunications/high-technology industries; including providing technical, engineering, and regulatory support to industry players both on the equipment manufacturer and the service provider sides of this market equation.
- Assist litigants with expert witness support in all related legal and/or regulatory matters in cases pertinent to the expertise of the consultancy.

HUAWEI TECHNOLOGIES COMPANY, Ltd. (d.b.a. Futurewei), Bridgewater, NJ **6/2011-12/2013**

Principal Research and Development Engineer, Access Optical Network Product Line

Responsible for overseeing and initiating innovative technology advances applicable to passive optical network (PON) communication system architectures. Report directly to the VP of R&D for Access Optical Networks. Charged with leading a worldwide engineering staff in a variety of applied research and development efforts related to fiber optic data and video transport technologies. Subject matter expert in mathematical and system modeling of optical communication networks, subsystem components, and devices.

- Developed system models and hardware for coherent PON architectures.
- Developed system models and hardware for dynamic spectrum managed PON architectures.
- Developed system models and hardware for wavelength division multiplexed PON architectures.
- Developed system models and hardware for self-seeded colorless PON transmitter technology.

- Developed Coherent OFDR technology for optical metrology and optical network integrity monitoring.
- Developed Raman Crosstalk Mitigation technology allowing for TV signal video overlay with 10G data transport on PONs.
- Successfully supported various FSAN and ITU standards initiatives promoted by Huawei/Futurewei.

ARRIS (formally MOTOROLA MOBILITY / HOME), Horsham, PA **2000-2010**

Principal Staff Engineer: Advanced Optical Communications Technology Applied R&D

Responsible for overseeing and initiating innovative technology developments applicable to broadband optical communication networks deployed by traditional cable industry MSO's and telecommunication industry service providers. Subject matter expert in optical communication networks, subsystem components, and devices. Lead engineers and technician staff in a variety of applied research and development efforts related to fiber optic and photonic communication technology. Advised senior management.

- Pioneered CWDM fiber deep architecture and technology that, for the first time ever, allowed multiple near zero dispersion 13xx nm broadcast signals to co-propagate on a single fiber network with minimal Raman crosstalk. This reduces cost and complexity for MSO's while expanding network capacity and reach enhancing the potential for increased revenues with an expedient return on investment.
- Invented a methodology for selecting DWDM optical channel wavelengths that minimizes four-wave mixing crosstalk in fiber-deep networks allowing MSO's to increase network capacity while minimizing the impact on signal quality.
- Awarded multiple patents for inventions related to all-optical "networks/architectures of the future."
- Recipient of two corporate *"Bravo Awards"* for excellence in technical contributions.
- Provided key insights and developed methodologies to counteract the impacts of fiber nonlinear effects and dispersion on analog and QAM signals in broadcast/narrowcast overlay HFC networks. These inputs were critical to ultimately achieving promised industry leading network performance goals for major MSO customers. The measures increased both reach and signal splits enhancing the network economy of scales.
- Diagnosed the limitations and impacts of the original FTTH/PON architectures with regard to optical signal transmission in both the upstream and downstream paths. Resulted in adjusting the standard upstream data transmission rate from OC-3 to OC-12 in order to minimize the crosstalk impact on analog video transmission.
- Acted in an expert "behind-the-scenes" advisory role to senior management providing critical technical and scientific insights and strategic guidance when addressing MSO and other customer concerns regarding potential future products and network architecture proposals. Responded to customer requests for proposals or requests for information.
- Advised on issues impacting customer field installed equipment. Key player in providing assistance to field engineers and MSO's in resolving system failures and difficult to diagnose subpar optical performance problems that arose unexpectedly.
- Managed optical component venders to ensure optimal price and performance points were met.
- ***Responsible for technological due diligence with regard to start-up company investment prospects.***
- ***Responsible for intellectual property rights reviews and provided expert advice to corporate IP attorneys.***
- ***When Motorola, was named as a defendant, in a patent infringement lawsuit brought by British Telecom, I provided detailed technical support work for the Motorola corporate I.P. legal team to bolster the company's defense. I provided extensive technical/engineering/scientific analytical support to General Instruments (Motorola) corporate legal/IP department in the form of written reports and presentations to the defense team. British Telecom (BT) accused General Instruments/Motorola (and other companies) of integrating their patented technology for removing or suppressing stimulated Brillouin scattering (SBS) into optical transmitters in violation of their patent rights. US4560246A US4560246B1 The final outcome was a negotiated licensing agreement for incorporating this technology into the commercial optical transmitters being sold to their customers at that time.***

LOCKHEED MARTIN MISSILES AND SPACE, Newtown, PA **1995-2000**

Staff Engineer: Millimeter-Wave, Microwave, and Photonic Component Design

Responsible for the design of military grade space qualified satellite communication hardware for a variety of U.S. government agency customers. Also responsible for the analysis of the end-of-life and expected worst case performance of a 60 GHz secure satellite cross-link. Additional functions included a substantial effort in applied IR&D and proposal authoring and presentations in the area of optical DWDM distribution of microwave signals on-board spacecraft.

- Developed the first 60 GHz space qualified power amplifier utilizing monolithic millimeter-wave integrated circuit technology for the ACSS military satellite program. This implementation provided substantial cost reductions to the U.S. military while also significantly increasing the life expectancy and reliability of the amplifier. Subsequently, the useful lifetime of the entire satellite communications constellation was positively impacted.
- Developed fiber optic communication/data links for satellite payload applications.
- As a Kaizen team member, provided manufacturing continuous process improvement innovations which lead to higher first run yields and reduced production and re-engineering costs on custom manufactured hybrid microwave and millimeter-wave circuits.

HUGHES RESEARCH LABORATORIES (HRL), Malibu, CA **1989-1994**

Howard Hughes Doctoral Fellow

The extremely competitive Howard Hughes doctoral fellowship supported my Ph.D. studies at Cornell University. As part of the fellowship program I spent regular periods of time as a fulltime researcher working at HRL in the area of monolithic microwave and millimeter-wave integrated circuit design, modeling, fabrication, and laboratory evaluation using material systems such as AlInAs/GaInAs on InP. These efforts lead to world class performance in the areas of millimeter-wave amplifier gain and noise figure.

- Developed ultra low-noise monolithic millimeter-wave and microwave integrated circuit amplifiers having world record noise performance (0.78 dB @ 12 GHz, < 1.2 dB up to14 GHz).
- Developed monolithic millimeter-wave integrated circuit amplifiers with 8 dB gain at 55 GHz.

EDUCATION

Cornell University, Ithaca, NY

Ph.D. in Electrical Engineering with a minor in Applied Physics

Howard Hughes Doctoral Fellow

Dissertation: "Metal-Semiconductor-Metal Photodiodes With Applications in Monolithic Optical Receiver Circuits Capable of Detecting and Amplifying a Millimeter-Wave Modulation Signal Being Transmitted Via an Optical Carrier"

Advisors: Professor Lester F. Eastman (chair), Professor Harold Craighead, Dr. Richard Compton

California Institute of Technology, Pasadena, CA

M.S. in Electrical Engineering

Institute Graduate Fellow

Research Project: Microwave power combining by placing an array of Gunn diode sources in a quasi-optical free-space cavity.

Advisor: Professor David Rutledge

Drexel University, Philadelphia, PA

B.S. in Electrical Engineering

GPA 3.8 on a 4.0 scale, graduated with high honors, top 2%.

Senior Advisors: Professors Peter Herczfeld and Afshin Daryoush

HONOR SOCIETY MEMBERSHIPS

- **Eta Kappa Nu (National Electrical Engineering Honor Society)**
- **Tau Beta Pi (National Engineering Honor Society)**