Paper 11
Filed: November 21, 2024

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

PATENT OWNER'S PRELIMINARY RESPONSE
37 C.F.R. § 42.107

TABLE OF CONTENTS

TABLE OF AUTHORITIES iii

CURRENT EXHIBIT LIST v

CLAIM LISTING viii

I. INTRODUCTION 1

II. *FINTIV* FACTORS SUPPORT DISCRETIONARY DENIAL 2

A. Factor 1—Stay 4

B. Factor 2—Anticipated Conclusions 5

C. Factor 3—Investment 6

D. Factor 4—Overlap 7

E. Factor 5—Parties 9

F. Factor 6—Other Circumstances 10

III. OVERVIEW OF THE PATENT-AT-ISSUE 11

A. Family and Effective Filing Date 11

B. Brief Overview of the Patented Invention 12

C. Relevant Prosecution History 17

IV. OVERVIEW OF THE CITED REFERENCES 22

A. RFC 1112 (Aug. 1989) ("IGMPv1") 22

B. Overview of JP2004-343243A ("Murakami") 25

1. Nomenclature and Topology 25

2. Functionality 27

C. RFC 4601 ("PIM-SM") 34

D. U.S. Patent Appl. 2002/0150097 A1 ("Yen") Is Only Used for Dependent Claims 36

V. LEVEL OF ORDINARY SKILL IN THE ART 37

VI. CLAIM CONSTRUCTION 37

A. "Services" 37

B. "Common Key" 41

C. "Bearer Channel" 42

VII. PETITIONER'S PRIOR ART REFERENCES FAIL TO RENDER OBVIOUS ANY CHALLENGED CLAIM 43

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 Found in 1b/c and 9c, or Show That These Limitations Would Be Obvious 43

B. Petitioner Fails to Show Any Challenged Dependent Claims Are Obvious 62

VIII. CONCLUSION 62

TABLE OF AUTHORITIES

Cases

AGIS Software Dev. LLC v. Google LLC,
No. 2:19-CV-00359-JRG, 2021 WL 465424 (E.D. Tex. Feb. 9, 2021) 5

Apple Inc. v. Maxell, Ltd.,
IPR2020-00200-21 (PTAB Feb. 3, 2021) 7

Apple, Inc. v. Fintiv, Inc.,
IPR2020-00019-11 (PTAB Mar. 20, 2020) (precedential) 3, 8

Arthur A. Collins, Inc. v. N. Telecom Ltd.,
216 F.3d 1042 (Fed. Cir. 2000) 40

Cisco v. Ramot,
IPR2020-00122-15 (PTAB May 15, 2020) 10

Commscope Techs. LLC v. Dali Wireless, Inc.,
IPR2022-01242-23 (PTAB Feb. 27, 2023) 4

Corning Glass Works v. Sumitomo Elec. USA, Inc.,
868 F.2d 1251 (Fed. Cir. 1989) 63

Google LLC v. Agis Software Development, LLC,
IPR2020-00873 (PTAB Nov. 25, 2020) 8

In re Fine,
837 F.2d 1071 (Fed. Cir. 1988) 63

In re Gordon,
733 F.2d 900 (Fed. Cir. 1984) 57

In re Ratti,
270 F.2d 810 (CCPA 1959) 57

Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.,
868 F.3d 1013 (Fed. Cir. 2017) 43, 44

OpenSky Indus., LLC v. VLSI Tech. LLC,
IPR2021-01064-102 (PTAB Oct. 4, 2022) (precedential) 11

Polaris Powerled Techs., LLC v. Samsung Elecs. Am., Inc.,
No. 2:22-cv-00469-JRG, 2024 WL 1149223 (E.D. Tex. Mar. 15, 2024) 9

Sotera Wireless Inc. v. Masimo Corp.,
IPR2020-01019-12 (PTAB Dec. 1, 2020) (precedential) 10

Spectralytics, Inc. v. Cordis Corp.,
649 F.3d 1336 (Fed. Cir. 2011) 57

Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.,
200 F.3d 795 (Fed. Cir. 1999) 43

Statutes

35 U.S.C. § 314(a) 10

35 U.S.C. § 314(b) 5

35 U.S.C. § 316(a)(11) 5

Rules

37 C.F.R. § 42.65(a) 58

Other Authorities

Interim Procedure for Discretionary Denials in AIA Post-Grant
Proceedings with Parallel District Court Litigation (June 21. 2022) 3

CURRENT EXHIBIT LIST[1]

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	Declaration in Support of Motion for *Pro Hac Vice* Admission of Eric J. Enger
2002	Expert Declaration of Dr. Kerry I. Litvin
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.)

[1] Relevant portions of Patent Owner's exhibits may be highlighted to help the Panel find cited sections.

No.	Brief Description
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
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, *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)

No.	Brief Description
2016	Texas Eastern, U.S. District Court—Judicial Case Load Profile excerpt from Federal Court Management Statistics (June 30, 2024), *available at* https://www.uscourts.gov/sites/default/files/data_tables/fcms_na_distprofile0630.2024.pdf
2017	Defendant's Preliminary Invalidity Contentions Cover Pleading, *Iarnach Technologies Ltd. v. Charter Communications, Inc.* et al., No. 2:23-cv-00230-JRG (E.D. Tex. served Sept. 5, 2024).
2018	Declaration of Eric J. Enger

CLAIM LISTING[2]

	Limitation
1pre	**1.** A method for encrypting multicast service in a passive optical network system, the method comprising:
1a	an optical line terminal (OLT) generating a common key,
1b	and using the common key to encrypt multicast service data of all different multicast services in a same bearer channel and then sending encrypted data,
1c	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; and
1d	said OLT sending the common key applied in encrypting the multicast service data via a management control channel to an optical network unit (ONU) that is activated successfully and applies to receive said multicast service data.
2	**2.** The method of claim **1**, further comprising: after obtaining the common key, said ONU using said common key to decrypt all the multicast service data, which the ONU applies to receive, in the bearer channel.
3	**3.** The method of claim **2**, further comprising: said OLT generating the common key and setting an aging time for the common key, and after the aging time arrives, it regenerating a new common key, and using the new common key to encrypt the multicast service data in the bearer channel, and sending the new common key to the ONU that is activated successfully and applies for the multicast service data.
4	**4.** The method of claim **2**, wherein: in the step of said OLT sending the common key to the ONU that is activated successfully and applies to receive said multicast service data, said OLT also sends the ONU a bearer channel identification of the bearer channel where all multicast service data are encrypted with the common key.

[2] For consistency Patent Owner follows Petitioner's numbering convention.

	Limitation
5	**5.** The method of claim **1**, further comprising: said OLT generating the common key and setting an aging time for the common key, and after the aging time arrives, it regenerating a new common key, and using the new common key to encrypt the multicast service data in the bearer channel, and sending the new common key to the ONU that is activated successfully and applies for the multicast service data.
6	**6.** The method of claim **1**, wherein: the step of said OLT sending the common key applied in encrypting the multicast service data to the ONU that is activated successfully and applies to receive said multicast service data comprises: the OLT judging that the ONU is activated successfully and applies to receive the multicast service data, and actively sending the common key applied in encrypting the multicast service data to said ONU; or the ONU sending a key request to the OLT, and said OLT detecting that the ONU is activated successfully and applies to receive the multicast service data, then the OLT sending the common key applied in encrypting said multicast service data to the ONU.
7	**7.** The method of claim **1**, wherein: the multicast service data in different bearer channels use different common keys or the same common key.
8	**8.** The method of claim **1**, wherein: in the step of said OLT sending the common key to the ONU that is activated successfully and applies to receive said multicast service data, said OLT also sends the ONU a bearer channel identification of the bearer channel where all multicast service data are encrypted with the common key.
9a	**9.** A device for encrypting multicast service in a passive optical network system, and the device comprising a key generation unit, an encryption unit and a sending unit, wherein: said key generation unit is configured to: generate a common key;

	Limitation
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;
9c	said sending unit is configured to: send the encrypted multicast service data, and send the common key applied in encrypting the multicast service data via a management control channel to an optical network unit (ONU) that is activated successfully and applies to receive the multicast service data
10	**10.** The device of claim **9**, wherein, said device also comprises an aging time setting unit, and said aging time setting unit is configured to: set an aging time for the common key, and when the aging time arrives, notifying said key generation unit to regenerate a common key.
11	**11.** The device of claim **9**, wherein: said sending unit is configured to apply following methods to send the common key applied in encrypting the multicast service data to the ONU that is activated successfully and applies to receive the multicast service data: after judging that the ONU is activated successfully and applies to receive the multicast service data, actively sending the common key applied in encrypting the multicast service data to said ONU; or, after receiving a key request from the ONU, judging that the ONU is activated successfully and applies to receive the multicast service data, and then sending the common key applied in encrypting the multicast service data to the ONU.
12	**12.** The device of claim **9**, wherein, said sending unit is also configured to: send the common key to the ONU which is activated successfully and applies to receive the multicast service data, and also send the ONU a bearer channel identification of the bearer channel where all multicast service data are encrypted with the common key.
13a	**13.** The device of claim **11**, wherein, said sending unit is also configured to: send the common key to the ONU which is activated successfully and applies to receive the multicast service data, and

	Limitation
13b	also send the ONU a bearer channel identification of the bearer channel where all multicast service data are encrypted with the common key.

I. INTRODUCTION

Charter Communications, Inc. ("Petitioner") petitions for *inter partes* review of claims 1–13 ("Challenged Claims") of U.S. Patent No. Patent 8,942,378 ("'378 Patent" or "Patent-at-Issue"). Paper 1 ("Petition" or "Pet."). The Board should deny Charter's Petition for at least two reasons.

First, the Board should discretionarily deny the Petition under *Fintiv* because, due to a parallel district court proceeding involving the same parties and invalidity challenges, institution will: (1) increase, rather than limit litigation costs as Congress intended; and (2) give rise to potential conflicts between the PTAB and district court proceedings. Each of the *Fintiv* factors shows discretionary denial is appropriate.

Second, if the Board decides not to deny the Petition under *Fintiv*, the Board should deny institution on the merits. All Challenged Claims require the method/system to ***encrypt all different multicast services in a same one bearer channel with a same common key***. Indeed, the Examiner explicitly identified this limitation as one reason for finding the claims patentable over prior art during prosecution. Yet, Petitioner's primary Murakami reference uses ***different*** bearer channels and ***different*** encryption keys for different multicast services.

Petitioner admits that Murakami does not disclose encrypting all different multicast services in a same one bearer channel with a same common key, as claimed. So, there is no anticipation. And with respect to obviousness, Petitioner

ignores Murakami's fundamental design that uses different bearer channels/encryption keys per multicast service and nonetheless tries to show how two additional references, IPMGv1 and PIM-SM, invalidate the claim.

In the end, though, the best Petitioner can say is that those two references permit multiple "sources" to address a multicast group. But a "source" as used in those references refers to ***an IP address***—it does not refer to the claimed different "***services***" that a service provider provides to users, such as an internet TV service or a video conferencing service. So even the combination of Murakami with IPMGv1 and PIM-SM does not render the Challenged Claims obvious.

Because all Challenged Claims require encrypting all different multicast services in a same one bearer channel with a same common key, and the cited prior art does not teach or suggest that limitation, Petitioner has not shown that any claim is invalid. Patent Owner discusses these and other issues in more detail herein.

II. *FINTIV* FACTORS SUPPORT DISCRETIONARY DENIAL

Patent Owner has asserted the '378 Patent in District Court litigation, *Iarnach Technologies Ltd. v. Charter Communications, Inc. et al.*, No. 2:24-cv-00230 (E.D. Tex. filed Apr. 05, 2024) ("E.D. Tex. Litigation"). *See* Pet.§ II(B); Paper 5 § II.

Under the PTAB's precedential *Fintiv* opinion, the Board should consider the following non-exclusive factors when determining whether efficiency and integrity of the system are best served by denying review because the issues in the IPR are

likely to be resolved by a parallel District Court litigation:

1. whether the court granted a stay or evidence exists that one may be granted if a proceeding is instituted;
2. proximity of the court's trial date to the Board's projected statutory deadline for a final written decision;
3. investment in the parallel proceeding by the court and the parties;
4. overlap between issues raised in the petition and in the parallel proceeding;
5. whether the petitioner and the defendant in the parallel proceeding are the same party; and
6. other circumstances that impact the Board's exercise of discretion, including the merits.

Apple, Inc. v. Fintiv, Inc., IPR2020-00019-11 (PTAB Mar. 20, 2020) (precedential). However, as further clarified by the Director,[3] "the PTAB will not rely on the *Fintiv* factors to discretionarily deny institution in view of parallel district litigation where a petition presents compelling evidence of unpatentability," Interim Procedure at 2, or "where a petitioner presents a stipulation not to pursue in a parallel proceeding the same grounds or any

[3] Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings with Parallel District Court Litigation, at 2 (June 21. 2022), *available at*, https://www.uspto.gov/¬sites/¬default/¬files/¬documents/-interim_proc_discretionary_denials_aia_parallel_district_court_litigation_memo_20220621.pdf.

grounds that could have reasonably been raised before the PTAB," *id.* at 2. The Director "intended for PTAB panels to only consider compelling merits if they first determined that Fintiv factors 1–5 favored a discretionary denial." *Commscope Techs. LLC v. Dali Wireless, Inc.*, IPR2022-01242-23, at 4 (PTAB Feb. 27, 2023).

A. Factor 1—Stay

Petitioner has not filed a motion to stay the E.D. Tex. Litigation, despite Petitioner's promise to file one "pre-institution." *See* Pet. 11. However, even if Petitioner does seek a stay, this factor is not "neutral" like Petitioner suggests. *Id.* Rather, as Petitioner acknowledges, this factor is neutral only "[i]n the absence of specific evidence" showing how a district court litigation would rule on such a motion. *Sand Revolution II, LLC, v. Continental Intermodal Grp.—Trucking LLC*, IPR2019-01393-24, at 7 (PTAB June 16, 2020) (informative). And the E.D. Tex. Litigation Court has a policy of denying all "pre-institution" motions to stay. *See, e.g.*, *AGIS Software Dev. LLC v. Google LLC*, No. 2:19-CV-00359-JRG, 2021 WL 465424, at *1 (E.D. Tex. Feb. 9, 2021) (denying motion to stay with permission to try again "following the PTAB's institution decision regarding the last of the patents-in-suit to be acted upon by the PTAB . . . *consistent with this Court's well-established practice where institution decisions remain pending*.") (emphasis added). So, Petitioner's pre-institution motion for stay (if filed) will be

denied per the Court's practice.

Moreover, Petitioner represented to the Board that it "will be filing additional petitions of the two other patents asserted in the underlying litigation" either "concurrently" with this Petition or "soon hereafter." Pet. 12. While Petitioner filed an additional petition against U.S. Patent No. 9,287,982, *see* IPR2024-01287 ("'982 Petition"), it has been more than three months and Petitioner has not lived up to its promise to "soon" file a petition against U.S. Patent No. 9,674,035. As such, even if the Board instituted this IPR petition and the '982 Petition, the Eastern District of Texas Court would still not stay the litigation since the '035 Patent is not subject to an IPR petition. *AGIS*, 2021 WL 465424, at *1.

Thus, there is strong evidence that the Court will not stay litigation in the current situation, and Factor 1 favors denial.

B. Factor 2—Anticipated Conclusions

Petitioner filed this Preliminary Response at or around November 21, 2024. The statutory deadline for this Panel to issue an institution decision is therefore about February 21, 2025, 35 U.S.C. § 314(b), and a final written decision ("FWD") would not issue until about February 21, 2026, 35 U.S.C. § 316(a)(11).

Jury selection in the E.D. Tex. Litigation is scheduled to begin February 9, 2026. Ex. 1011 at 1. And, per the Director's Procedure, the Panel may also consider the entire district's time-to-trial statistics, Interim Procedure at 8–9 &

n.12, that show the average time to trial from filing in civil cases as 21.6 months, Ex. 2016, which indicates an anticipated statistical date of approximately December 14, 2025.

In either case, the E.D. Tex. Litigation is scheduled to end slightly before or around the same time the FWD would issue. Having judgments in parallel proceedings ending at the same time merely ensures duplicative invalidity work by both parties, the District Court, and the PTAB, and raises the opportunity for inconsistent outcomes in the two forums. These are the very issues that *Fintiv* addresses, so Factor 2 favors denial. *See* Interim Procedure at 1 (explaining that *Fintiv* allows the PTAB to address inefficiency and potential conflict among the PTAB and district court).

C. Factor 3—Investment

Petitioner disregards the foreseeable progress in the parallel case and only discusses the situation that existed when Petitioner filed its Petition. Pet. 13. However, the Board may consider after-arising events that occur before the institution decision. *See, e.g.*, *Apple Inc. v. Maxell, Ltd.*, IPR2020-00200-21, at 4 (PTAB Feb. 3, 2021) ("We do not agree with Patent Owner that our analysis of *Fintiv* Factor 4 must be constrained to the facts as they existed when the Petition was filed").

Before the Petition, Patent Owner provided detailed, highly-technical

infringement contentions spanning about 170 pages. Ex. 2018 ¶3. After the Petition, Petitioner provided Patent Owner with its invalidity contentions totaling more than 2,500 pages. *See* Ex. 2017. Moreover, the parties have conducted extensive litigation discovery, including producing and reviewing over 17,000 pages of documents, answering tens of interrogatories on myriad topics, issuing third-party subpoenas, and taking a deposition. Ex. 2018 ¶¶4–7. An additional deposition is scheduled prior to the institution decision. *Id*. ¶8.

Given the substantial investment in the parallel district court, Factor 3 favors denial.

D. Factor 4—Overlap

In the parallel litigation, Petitioner has provided invalidity contentions for claims 1–4, 6–7, and 9–12 of the '378 Patent, including contentions involving the same references at issue in this IPR. Ex. 2017 at 1 & 5–7. So, there is a large overlap of claims and prior art.[4] This means there will be substantial duplication in the two forums and opportunity for inconsistent decisions. This supports discretionary denial.

Additionally, even though three dependent Challenged Claims are not

[4] The only Challenged Claims not asserted in the parallel litigation are dependent claim 5 (regarding using a new key after aging time has expired) and dependent claims 8/13 (regarding sending a bearer channel identification).

included in the litigation invalidity contentions, this does not necessarily support institution. This tribunal recognizes that "it may still be inefficient to proceed because the district court may resolve validity of enough overlapping claims to resolve key issues in the petition." *Fintiv,* IPR2020-00019-11 at 13. This is especially true where a petitioner does not explain why the different challenged claims are materially different, like here. *Google LLC v. Agis Software Development, LLC*, IPR2020-00873-16, at 13 (PTAB Nov. 25, 2020). Indeed, other than depending from different claims, Claim 5 is identical to Challenged Claim 2 and Claims 8/13 are identical to Challenged Claim 4.

Also, as shown in the substantive section of this Preliminary Response, Patent Owner believes the validity of the Patent-at-Issue may be decided from limitations found in the independent claims. *See* § VII *infra*. As such, the resolution of the claims elected in the district court will likely resolve validity of enough overlapping claims to resolve the key issues in this proceeding.

Moreover, as noted above, despite Petitioner's assurances that it "will be filing additional petitions of the two other patents asserted in the underlying litigation challenging all claims," Pet. 12, Petitioner has not filed a IPR petition for the '035 Patent, so Petitioner's current petitions will not "dispose of all issues raised in

the underlying litigation" as Petitioner asserts.[5] *Id.*

Finally, Petitioner has offered no stipulation to not raise "any grounds that could have reasonably been raised in the petition," so it has not mitigated the possibility of duplicative work or the possibility of conflicting decisions. *Cf. Sotera Wireless Inc. v. Masimo Corp.*, IPR2020-01019-12, at 13 (PTAB Dec. 1, 2020) (precedential).

Factor 4, then, also favors denial.

E. Factor 5—Parties

Petitioner and Patent Owner are the same parties as in the district court. And "[i]f the petitioner and the defendant in the parallel proceeding are the same, this factor weighs in favor of discretionary denial." *See, e.g.*, *Cisco v. Ramot*, IPR2020-00122-15, at 10–11 (PTAB May 15, 2020).

[5] For Factor 1, the scenario where Petitioner does not file an '035 Patent IPR petition also supports that a motion to stay the E.D. Tex. Litigation would be unsuccessful. *See, e.g.*, *Polaris Powerled Techs., LLC v. Samsung Elecs. Am., Inc.*, No. 2:22-cv-00469-JRG, 2024 WL 1149223, at *6 (E.D. Tex. Mar. 15, 2024) (refusing a partial stay of the case where less than all patents were before the PTAB because this "would in effect require the Court to hold two entirely separate trials" and "[s]uch an approach would create significant inefficiencies that would more than offset any simplification gained through the IPR process") (citation and quotation omitted).

F. Factor 6—Other Circumstances

Under "other circumstances," Petitioner argues that the Patent-at-Issue is necessary to be Standards Compliant, and Petitioner asserts that cancellation will remove some industry-wide "unnecessary encumbrance." Pet. 12. However, Petitioner cites no authority that the Board should treat standards essential patents differently in a discretionary denial analysis. Moreover, despite implementing the DPoE v2.0 standards, Petitioner nonetheless states it does not infringe the '378 Patent. Ex. 2018 ¶9. Accordingly, the Board should be skeptical about Petitioner's position that canceling the Challenged Claims will unencumber the DPoE v2.0 standards.

Given that the first five factors favor denial, the Board should consider whether the Petition is "compelling." *Commscope*, IPR2022-01242-23, at 4. "Compelling" is a much higher standard than for institution and means the analysis "plainly lead[s] to a conclusion that one or more claims are unpatentable." *OpenSky Indus., LLC v. VLSI Tech. LLC*, IPR2021-01064-102, at 49 (PTAB Oct. 4, 2022) (precedential).

And Patent Owner submits that, as shown in the merits section of this Preliminary Response, Petitioner has not even met the normal institution standard per 35 U.S.C. § 314(a) to show a "reasonable likelihood" of prevailing, much less the higher "compelling" standard required to trump every other factor. The Petition

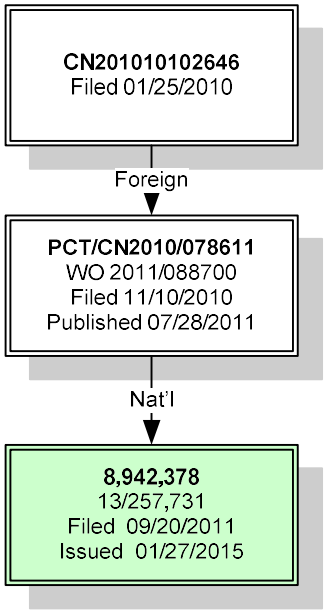
is not "compelling."

In sum, each of the six *Fintiv* factors individually suggest the Board should deny this position. And when the factors are considered collectively, they weigh heavily in favor of denying institution.

III. OVERVIEW OF THE PATENT-AT-ISSUE

A. Family and Effective Filing Date

The '378 Patent is part of the following family.



As seen, the '378 Patent has an earliest possible priority date—which is also the '378 Patent's actual effective priority date—of January 25, 2010 ("Effective Priority Date").[6] So, the Board should judge the '378 Patent under

[6] Patent Owner provides the Dr. Kerry Litvin's ("Dr. Litvin's") declaration in support of this Preliminary Response. Ex. 2002 ¶¶1–3. Dr. Litvin is eminently

(Footnote continued on next page)

the pre-AIA regime.

B. Brief Overview of the Patented Invention[7]

The Patent-at-Issue concerns the "passive optical network" ("PON") environment. Ex. 1001 1:7–10. PON is "passive" because the network distributes data through *unpowered* devices and "optical" because its transmission lines transmit data using *light* wave frequencies. Ex. 2002 ¶26. The PON network has an Optical Line Terminal ("OLT") at the office side that sends data to multiple Optical Network Units ("ONUs") at the customer end. *Id.* 1:14–19.

The '378 Patent teaches "a method and device for encrypting multicast service[s] in a passive optical network (PON) system to . . . reduce the complexity of [the] OLT encryption mechanism and the burden of the OLT." *Id.* 1:59–62. Specifically, the '378 Patent encrypts 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 a key that the OLT provides to the ONUs via a "separate management control channel"

---

qualified in the field of encrypting multicast service data in passive optical network PON systems. *Id.* ¶¶4–15 & App'x A. Patent Owner asked Dr. Litvin to assume this was the Effective Priority Date. *Id.* ¶¶16–17.

[7] Dr. Litvin provided his own overview of the '387 Patent similar to that presented here with additional expert commentary. *Id.* ¶¶26–40.

after the ONU is successfully activated, *see, e.g.*, *id.* 2:4–7, 2:33–34, 8:3–5. A second ONU may receive all multicast services on an encrypted bearer channel encrypted with the same common key on the same bearer channel. *See, e.g., id*. claim 7; Ex. 2002 ¶36.

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[8] port or the logical link identification (LLID) channel of the EPON[9] port." *Id.* 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 an OMCI[10] channel in the GPON system, . . . an extended OAM channel in the EPON system [or] a digital channel." *Id.* 4:9–15.

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

---

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

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

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

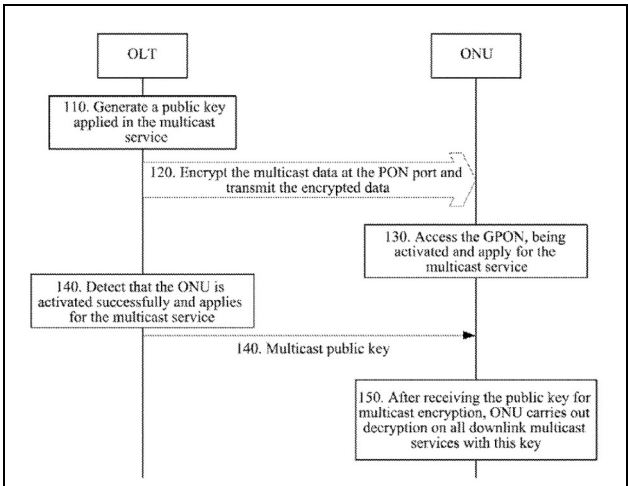


FIG. 1

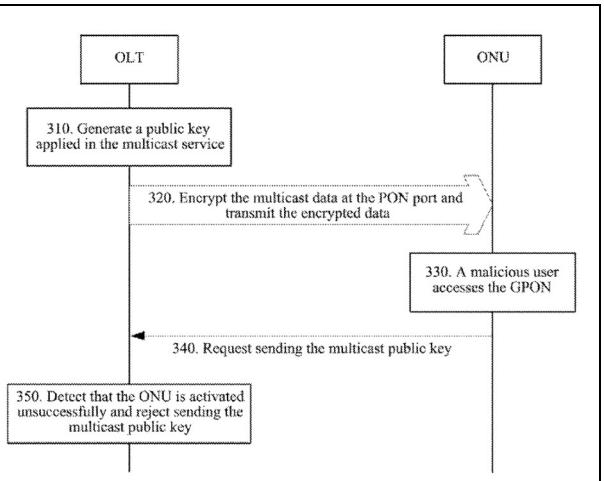


FIG. 3

In these Fig. 1 and Fig. 3 embodiments, the first two steps are the same. At steps 110/310, the OLT generates a key for encrypting multicast services. And in steps 120/320, the encrypted multicast service data is sent to the ONT. *Id.* 4:44–47. However, in the Fig. 1 embodiment, at step 130, a legal user accesses the GPON and applies for a 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 the applied for multicast service and "***all downlink multicast services***" on this bearer channel with this key. *Id.* 5:1–3 (emphasis added). That is, the OLT need not create and share a new key for a subsequent multicast service. Whereas in the Fig. 3 embodiment, a malicious user is unable to use the data in the encrypted multicast channel at all. Indeed, 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. *Id.* 5:54–67.

Moreover, the '378 Patent contemplates that the OLT may set an "aging time" for the keys the OLT sends 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.* 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 Figure 2 embodiment shows this aging time variation:

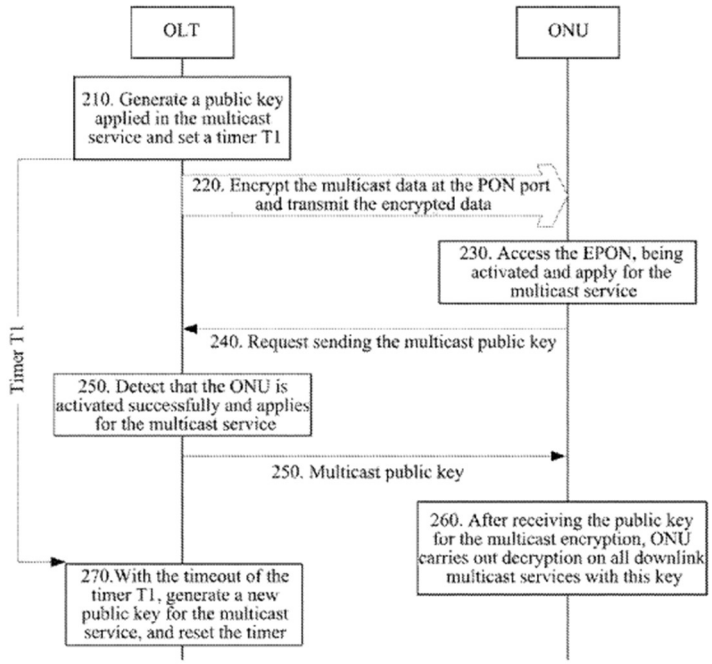


FIG. 2

As seen, steps 210–260 are like the Figure 1 embodiment. But 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, after which "***all multicast services***" may be decrypted with the new key. *Id.* 5:33–35 (emphasis added).

The last embodiment is shown in Figure 4. Here the '378 Patent contemplates there may be more than one encrypted multicast bearer channel, so the OLT must let the ONU know what bearer channel and key to use for all different multicast services sent on the specified bearer channel. *See, e.g.*, *id.* 6:9–20, 6:41–47 & claim 4.

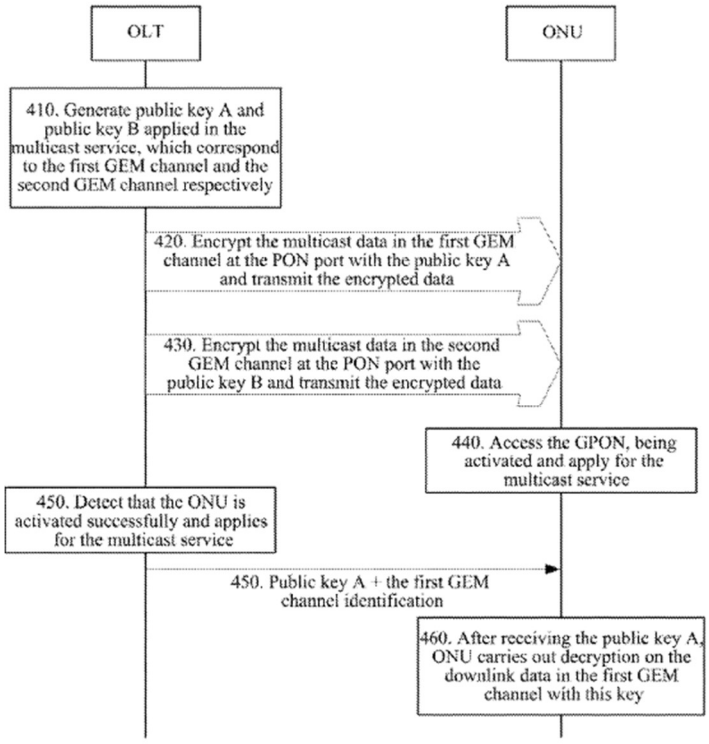


FIG. 4

In step 450, after the OLT detects the ONU successfully activates and applies for a multicast service, the OLT provides the ONU with both the bearer channel identification and the key that applies to the bearer channel for all multicast services sent on this bearer channel. *Id.* 6:26–30.

C. Relevant Prosecution History[11]

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

> 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. And the Applicant clarified that the amendments capture that one bearer channel includes a plurality of service channels to bear ***all multicast services***. *Id.* 352. The Applicant contrasted the new claim limitations with *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).

On May 21, 2014, the Examiner admitted that "He does not teach all multicast

[11] Dr. Litvin also presents a similar recounting of the key prosecution events in his expert report for his reference therein. Ex. 2002 ¶¶41–48.

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

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 relied upon a new reference, Ex. 2003, Jiang *et al.*, Multicast Broadcast Services Support in OFDMA-Based WiMAX Systems, IEEE COMMUNICATIONS MAGAZINE (Aug. 2007) ("*Jiang2007*"), for this limitation.

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*.

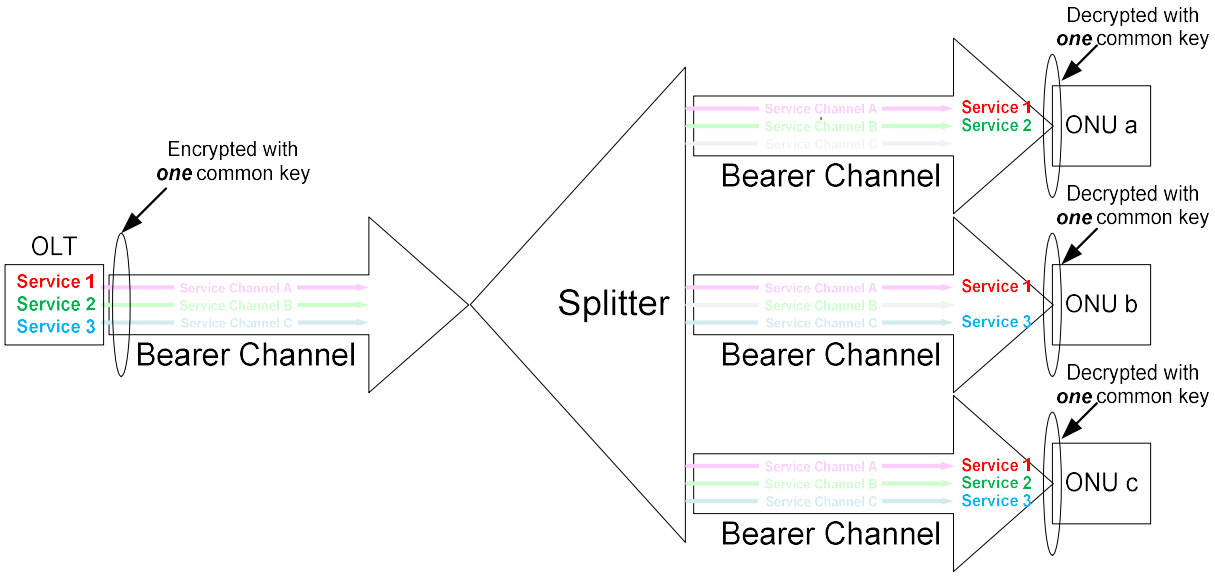
Ex. 2003 at PDF 5 (original page 82) (emphasis added); *see also* Ex. 1002 at 374 (citing *Jiang2007* at 82).

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). That is, the Applicant made it clear that the amendments meant one bearer channel carries a plurality of service channels for all multicast services encrypted by the same key. Patent Owner illustrates this description below.



The Applicant further explained that, for two reasons, *Jiang2007* does not meet the "using the common key to encrypt multicast service data of all multicast services in a bearer channel" limitation. 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," and those "skilled in the art would know that the handoff between the different BSs and one MS should be on different bearer channels."[13] *Id.* (emphasis removed). Applicant's point was that *Jiang2007* also used its key on ***different*** bearer channels. *Id.* The Applicant summed up the difference between the claims and *Jiang2007* saying, "*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).

On September 16, 2014, the Examiner issued a final rejection. *Id.* 393, 399.

[13] The Applicant was referencing the fact that neighboring base stations generally communicate with mobile devices with non-overlapping channels to avoid interference. Ex. 2002 ¶45.

The Examiner agreed that "Applicant made a valid argument that *Jiang2007* teaches the common key for all BS encrypting the same MBS program," i.e., same service. *Id.* 401. But the Examiner nonetheless believed 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.* (emphasis added).

On November 11, 2014, the Applicant amended the claims such that they took their final form, as seen in Claim 1 below:

> an optical line terminal (OLT) generating a common key, and 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 multicast services in the same one bearer channel use a same common key to carry out encryption

Id. 416. This change made clear that the claims were directed to ***different*** multicast services in the ***same*** bearer channel at the same time (as opposed to the same multicast service in a different bearer channel at another time). Accordingly, the Applicant 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.

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: "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 ***all*** multicast services for an ONU on service channels in a ***single*** bearer channel using a common key.

IV. OVERVIEW OF THE CITED REFERENCES[14]

Patent Owner describes RFC 1112 (Aug. 1989) ("IGMPv1") first, because it will be beneficial background information prior to examining Murakami.

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

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.* 2. "A

[14] Dr. Litvin also presents a similar overview of Petitioner's relied upon references with additional expert commentary for his further reference therein. Ex. 2002 ¶¶49–99.

multicast datagram [addressed to this single IP destination address] is delivered to all members of its destination host group." *Id.* 1. "A host may be a member of more than one group at a time." *Id.*

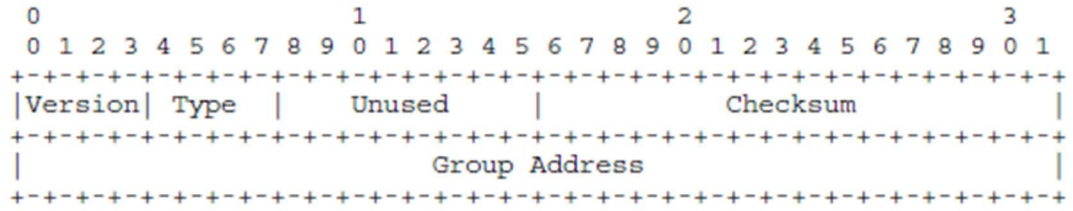
When a "host transmits an IP multicast datagram . . . [it] reaches all immediately-neighboring members of the destination host group [and] [i]f the datagram has an IP time-to-live greater than 1, the multicast router(s) attached to the local network take[s] responsibility for forwarding it towards all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

"Host groups are identified by class D IP addresses ['IPAs'], i.e., those with '1110' [0x0E] as their high-order four bits." *Id.* 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.* 6.

"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.* 5.

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.* 8.

"IGMP messages are encapsulated in IP datagrams" as shown:



Id. 11. A Type (bits 4–7) of "1" indicates a message is a "Host Membership Query" or just "Query," while a Type of "2" indicates a message is a "Host Membership Report" or just "Report." *Id.* 11–12. A multicast router sends a Query, which is the equivalent of asking "what group(s) is/are everyone in?" *Id.* 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.* 11–12. A member responds to a Query, letting the multicast router know what groups the member is a part of, by sending Report messages. *Id.* 12. "In a Host Membership Report message, the group address field holds the IP host group address of the group being reported." *Id.*

"Multicast routers send Queries periodically to refresh their knowledge of memberships present on a particular network. If no Reports are received for a

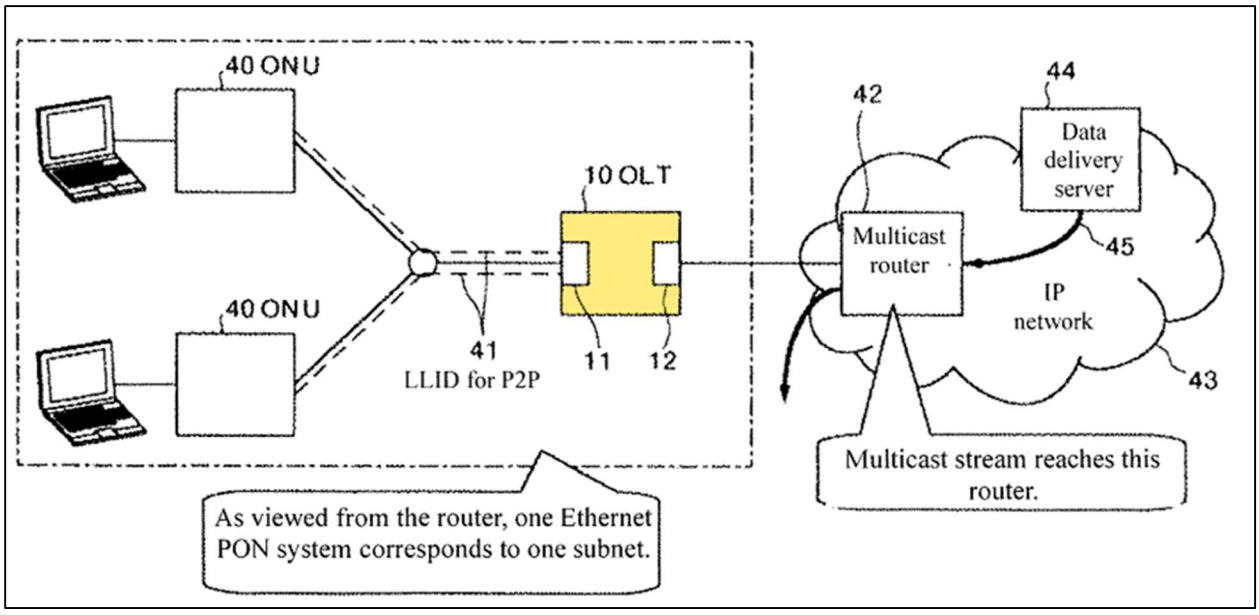
particular group after some number of Queries, the routers assume that group has no local members and they need not forward remotely-originated multicasts for that group onto the local network." *Id.* at 13.

In short, IGMPv1 describes the basic functionality of IP multicasting.

B. Overview of JP2004-343243A ("Murakami")

1. Nomenclature and Topology

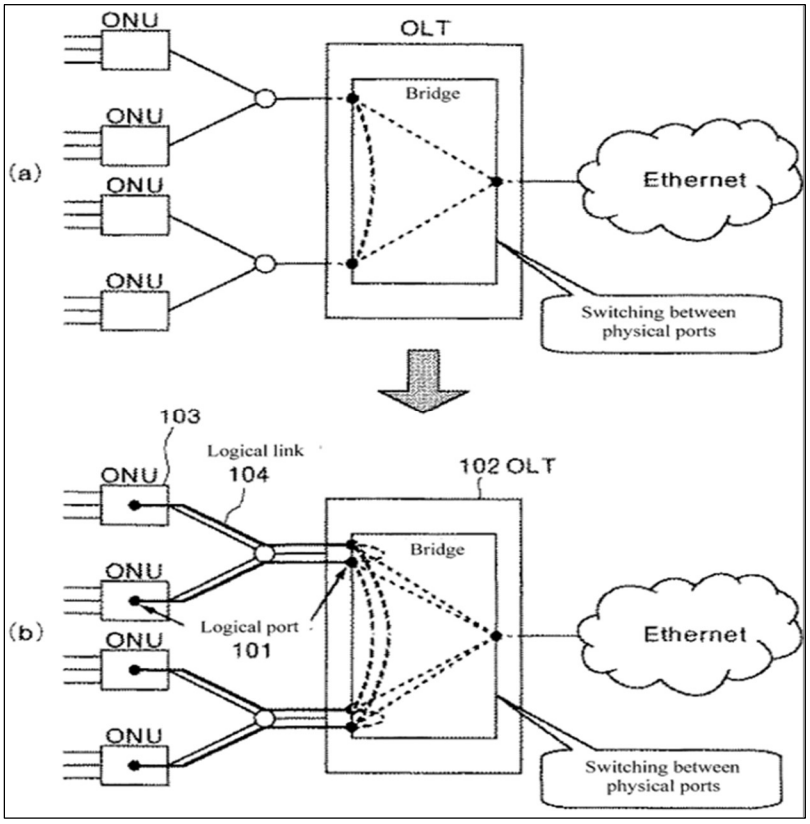
Murakami concerns a central office where OLTs (yellow) act as a transparent bridge between (1) an Ethernet network using Media Access Control ("MAC") frames and the Internet Group Management Protocol ("IGMP") (right side) and (2) multiple subscriber-side units ONUs (left side). Ex. 1005 [0001–03]. This is illustrated below.



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]. There is 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."[15] *Id.*

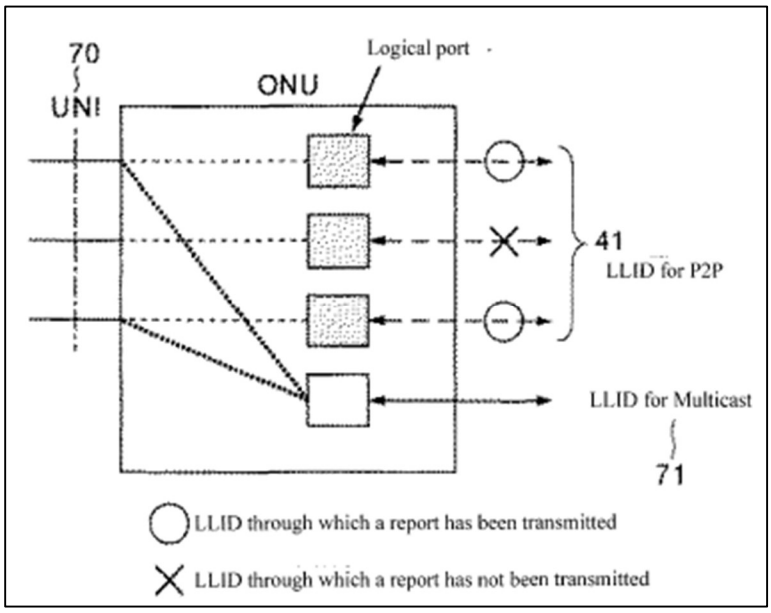
Murakami contrasts its logical port switching shown in Figure 4 (above) and Figure 8(b) (below) with the conventional OLT physical PON interface switching shown in Figure 8(a) (below) where the OLT "switches on a per physical-port basis." *Id.* [0016].



[15] Patent Owner discusses this encryption in more detail below in this section on page 22.

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

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].

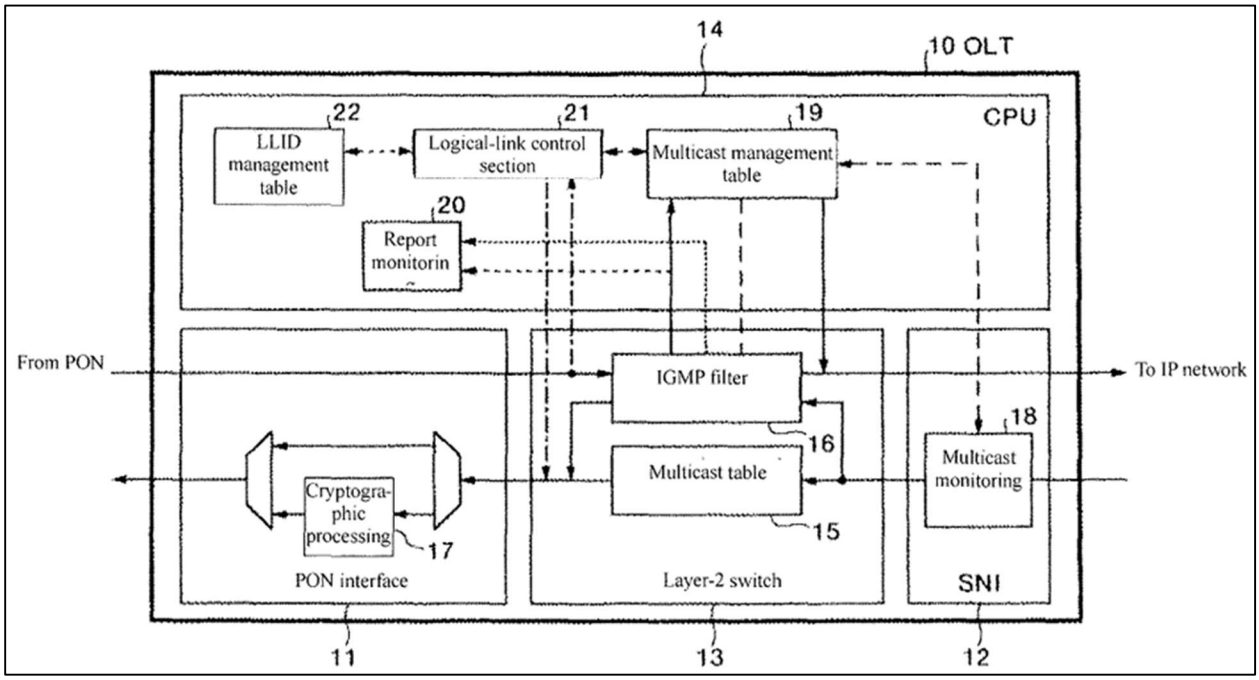
"Logical *ports* 101 . . . are connected through logical *links* 104." *Id.* [0016] (emphasis added). The OLT assigns each logical link a Logical Link Identifier ("LLID") that is unique in the PON. *Id.* [0017–18].

2. Functionality

Murakami provides multicast communication security using logical links without requiring routing functions on the subscriber (ONU) side. *Id.* at Abstract and [0011]. Specifically, its "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."[16] *Id.* [0013].

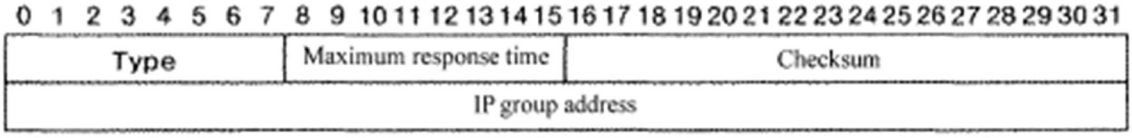
Murakami Figure 1 shows a block diagram of an OLT:



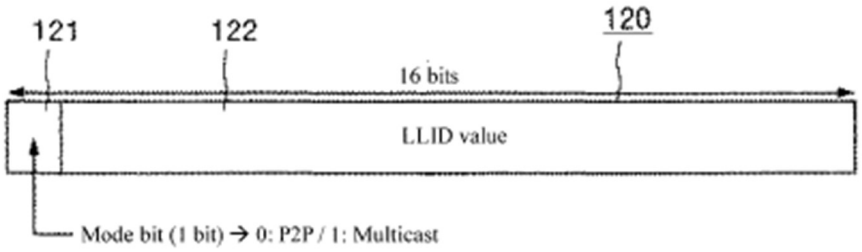
Id. Fig. 1. As can be seen from the figure, the OLT includes a PON interface to ONUs (left) and an interface to the IP network (right). *Id.* [0019].

[16] With IGMP, a multicast router identifies its members by periodically multicasting "query messages." *Id.* [0004]; *see also* IGMPv1, § IV.A *supra*. The router detects a member is part of a group when the member "replies with a report message." Ex. 1005 [0004]. 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.*

Murakami explains its operation via 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[17] and a "Type" of Type 2.[18] *Id.* [0027].

When the OLT finds a Report message, it searches through the Multicast Management Table ("MMT") shown below "using the IP group address as the

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

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

key."[19] *Id.* [0029].

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
⋮	⋮	⋮	⋮	⋮

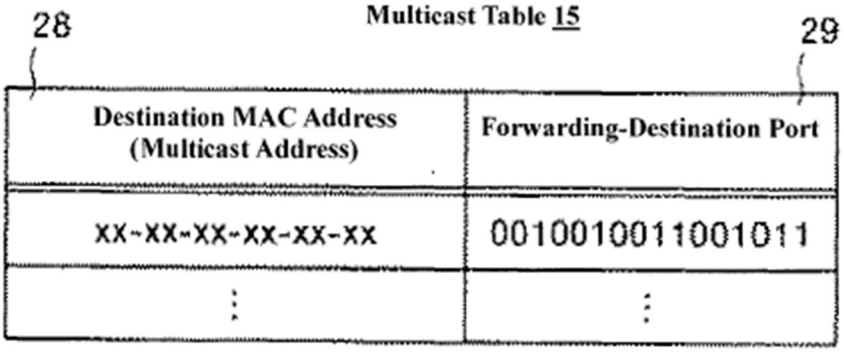
Id. Fig. 3. If the multicast address from the IP datagram is not in the table, the OLT creates a new entry in the MMT for the multicast address, populates the physical access port (aka PON interface) at which the Report arrived, and fills in the P2P LLID that is found in the MAC preamble for the ONU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

At this time, the OLT "generates a new encryption key used [for] multicast communication" and selects an unused LLID which 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

[19] The use of the word "key" here can be confusing without the proper context. Here "key" refers to a unique index into the MMT—not a cryptographic key.

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

Additionally, as this is the first Report message for this IP multicast group address, the Layer-2 ("L2") switch of the OLT will add an entry in a 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.[20] The table index is a unique Multicast MAC Address, and the

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

Forwarding-Destination Port column is a bitmap where a "1" indicates that the data is to be forwarded to a port. *Id.* This example is for 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 group destination MAC addresses 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

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].

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 creates and uses a different encryption key and multicast LLID. *Id.* [0037–39].

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].

In short, Murakami teaches how to handle routing of multicast communications at the OLT by snooping the ethernet IGMP communications and setting up new keys and LLIDs per multicast group while preventing non-subscribed ONUs from "eavesdropping" and getting a key to a non-subscribed service .

C. RFC 4601 ("PIM-SM")

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

PIM-SM's functionality is largely irrelevant to Murakami, Ex. 2002 ¶79, and Petitioner only relies on PIM-SM's uncontroversial teachings that (1) multiple "sources" may address a tree and (2) IGMPv3 allows for "source" specific group joins. Nonetheless, Patent Owner recapitulates the basics of PIM-SM.

With PIM-SM, 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 and 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 add a branch to the RP tree:

> 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.

With an RPT tree in place, a "multicast data sender" may "just start[] sending data destined for a multicast group," which the RP then "forwards [] 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.*

"[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.*

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.*

When a receiver knows a particular source address 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.

D. U.S. Patent Appl. 2002/0150097 A1 ("Yen") Is Only Used for Dependent Claims

Because Patent Owner addresses the missing and non-obvious limitation found in the independent claims—hence all claims—and Petitioner only uses Yen for dependent claims 3, 5, and 10, Patent Owner does not address Yen in this Preliminary Response.

V. LEVEL OF ORDINARY SKILL IN THE ART

Petitioner proposes a person of ordinary skill in the art ("POSITA") at the '378 Patent's effective priority date "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 (emphasis added). Petitioner's use of "or"s means this proposal encompasses "2–3 years industry experience . . . maintaining back-end networking equipment," generally, and does not even require experience maintaining passive optical network ("PON") equipment.

Patent Owner believes that this minimum education and experience is too low. Rather, a POSITA at the time of the inventions would have at least a bachelor's degree in electrical engineering, computer science, or a similar degree ***plus*** at least two years of experience in ***optical networks***. *See* Ex. 1001 1:7–10 ("The present invention relates to . . . a method and device for encrypting multicast service data in passive optical network (PON) system."); *see also* Ex. 2002 ¶¶18–24. A higher level of experience would compensate for a lower education and *vice versa*.

VI. CLAIM CONSTRUCTION

A. "Services"

Petitioner has not formally proposed a claim construction for the term "services"; however, the Petition equates "sources" with "services" by arguing that

"[d]ata from . . . different ***sources*** constitutes multicast ***service*** data of different multicast services, as recited in the claims." Pet. 32 (citing Ex. 1003 ¶91). This is incorrect.

The '378 Patent does not explicitly define "service." Nonetheless, the Patent uniformly uses the word "service" approximately 150 times, including in the title and the abstract. Ex. 1001 *passim*; *see also id.* (54), (57). The term is not explicitly defined because, as set forth in the GPON specification referenced by the '378 Patent, *id.* 1:34–35, services are "described by the name that is clearly recognized by everyone," Ex. 2005 at 8; Ex. 2002 ¶¶100–02. For instance, a POSITA would understand that services include "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. Ex. 2005 at 10–11; Ex. 2002 ¶101 (citing Ex. 2015). That is, a "service" is the intangible activity that a user on the PON network is provided.[21] *See, e.g.*, Ex. 2006 (defining "service" as "[a] customer-based or user-oriented function."); Ex. 2002 ¶102–03. To take a real-world example, Netflix and Hulu each

[21] "Services" is often used in the longer phrase "goods and services," where the former reference is to *physical* commodities, or *tangible* material products, while the latter reference is to intangible activities. Ex. 2011 at 1.

would be considered as companies providing a video streaming ***service***. *See, e.g.*, Ex. 2009 at 3.

In contrast, the '378 Patent never uses the word "source." Rather, as used in the cited prior art references, a "source" is the IP address from which a low-level data packet is sent. Ex. 2002 ¶104; *see also* 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); *see also Arthur A. Collins, Inc. v. N. Telecom Ltd.*, 216 F.3d 1042, 1044–45 (Fed. Cir. 2000) ("Even when prior art is not cited in the written description or the prosecution history, it may assist in ascertaining the meaning of a term to a person skilled in the art."). This meaning of "source" as "a place from which data is taken" is the common meaning in the relevant field. Ex. 2002 ¶104 (citing Ex. 2010).

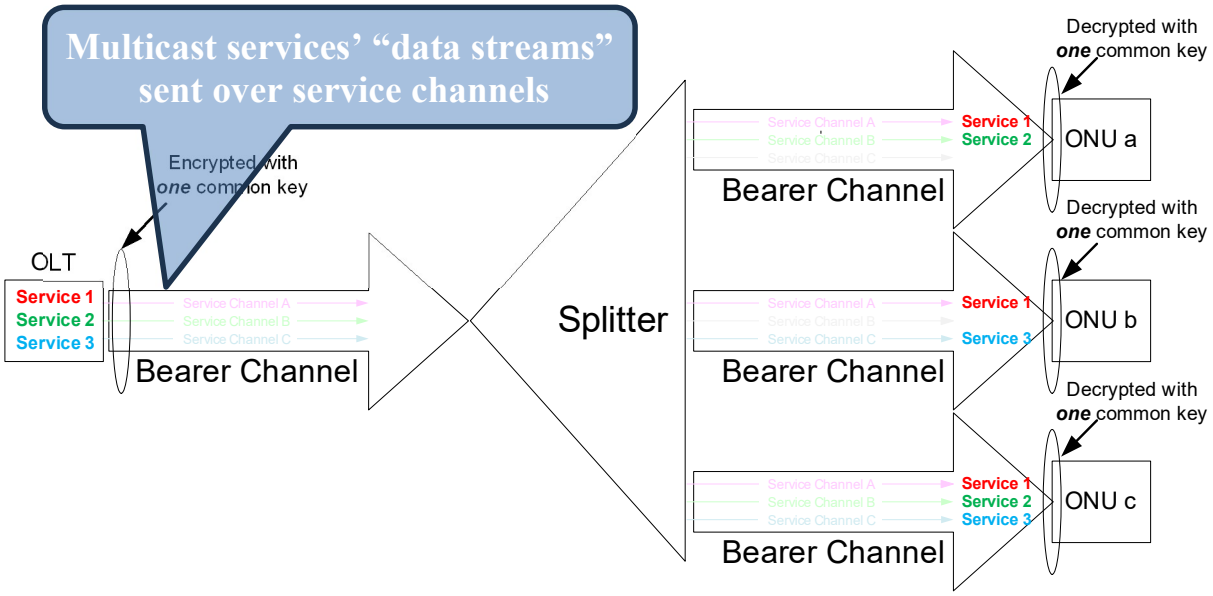
And the two words are not equivalent; one ***service*** in a network implementing the PIM-SM specification may have multiple ***sources***. Ex. 2002 ¶¶104–05. For example, "a video-conferencing ***service***" may have "many ***sources*** come and go." Ex. 2007 at 2 (emphasis added); Ex. 2002 ¶106. Or 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).

Petitioner's basis for equating "service" and "source"—against the plain meaning of the words as understood by a POSITA—is Petitioner's allegation that "[d]uring prosecution of the '378 Patent, the applicant acknowledged that different multicast '***data streams'*** equated to multicast service data of different multicast services." Pet. 32 (referencing the Aug. 12, 2013, Applicant Arguments/Remarks Made in an Amendment, Ex. 1002 at 352) (emphasis added). However, this is no rational reason to equate ***source*** with ***service***. Ex. 2002 ¶¶107–08.

Indeed, the Applicant did not use the word "source." Instead, 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 referenced "data stream" of the "service channel" is the claimed "service data" of the "service," respectively.

Applicant's terminology is also consistent with the further clarification the applicant made regarding *Jiang2007*, where the Applicant discussed services being sent on service channels in a bearer channel as shown below. *See id.* 384; *see also* Ex. 2002 ¶109.



In short, the claimed "services" are different from "sources." The former refers to the intangible activities that service providers on the PON network provide a user, such as digital broadcast services. The latter refers to an address, paradigmatically an IP address.

B. "Common Key"

Patent Owner agrees with Petitioner that a "common key" is used in symmetric encryption, where the same key is used for both encryption and decryption. And, in the context of the Patent-at-Issue, the key is also "common" because it is common among all the multicast services sent on a single bearer channel. Ex. 2002 ¶110. However, Patent Owner asserts this is the plain and ordinary meaning of "common key," so this term does not need an explicit construction. *See, e.g.*, Ex. 2004, U.S. Patent No. 7,194,090 1:29–33 ("In the common key encryption system, decryption is carried out by employing a key

(common key or secret key) that is identical to a key employed for encryption."); *see also Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (citing *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)) (explaining that the Board need not construe terms not in controversy because they are not material to the obviousness dispute).

C. "Bearer Channel"

Patent Owner disagrees with Petitioner's view that a "bearer channel" is limited to a logical channel of the PON. Pet. 15. While the '378 Patent describes a logical channel of the PON as a bearer channel in the section titled "Preferred Embodiments of the Present Invention," Ex. 1001 4:4–8 (different capitalization), the Patentee also noted that "[t]he above description is the preferred embodiments of the present invention rather than restriction of the present invention, and for those skilled in the field, there are various modifications and variations in the present invention [and] all these types of modification, equivalent replacement or variations should belong to the protection scope of the present invention," *id.* 7:32–39.

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. *See, e.g.*, Limitation 1b; Ex. 2002 ¶111.

Nonetheless, Patent Owner agrees that the bearer channel *can be* a logical channel of the PON, so it does not appear that this term is required for resolution of

the institution decision or that the Board needs to construe this term. *Nidec Motor Corp.*, 868 F.3d at 1017.

VII. 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 Found in 1b/c and 9c, 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**;

These limitations capture the Patent-at-Issue's goal to reduce encryption complexity by having an OLT designate and encrypt ***all different multicast services in a same one bearer channel with a same common key***. Ex. 2002 ¶¶33, 169. But, as now discussed, Murakami teaches to use ***different*** keys and bearer channels for ***different*** services. Ex. 2002 ¶¶112–32. Further, neither IGMPv1's teaching that a host that is not part of a multicast group may address a group, nor PIM-SM's teaching that multiple IP addresses (i.e., "sources") may address a Rendezvous Point for a multicast group, changes this fact. Ex. 2002 ¶¶133–69.

As previously discussed, Murakami indexes its MMT by "Multicast Address

(IP Group Address)" as the first column shows below.

Multicast Management Table 19

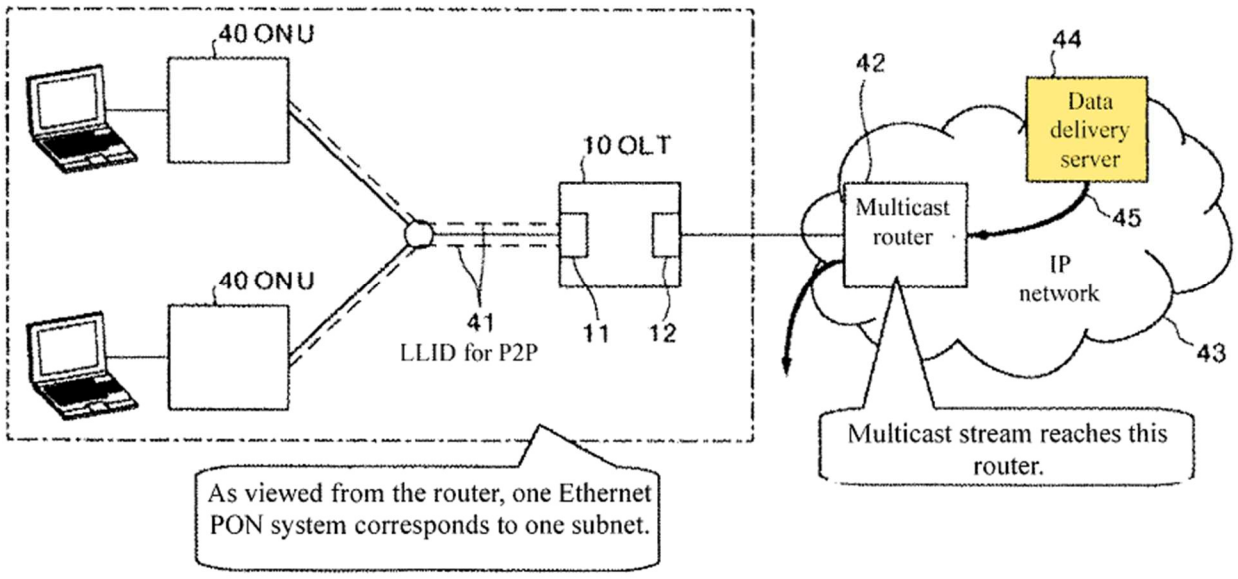
Multicast Address (IP Group Address)	Access Port	ONU (LLID for P2P)	LLID for multicasting	Encryption key
yyy.yyy.yyy.yyy	2	1 3	100	#1
	4	2 5	110	#3
⋮	⋮	⋮	⋮	⋮

Id. Fig. 3 (highlighting added); Ex. 2002 ¶118. And a POSITA understands that each multicast IP group address corresponds to a different service. Ex. 2002 ¶¶114, 119.

Indeed, "content providers will expect that their assigned multicast addresses are unique" because "applications will not expect data from separate sessions to arrive on the same multicast address." *Id.* ¶¶119–22 (citing Ex. 2014). Therefore, IP group address "yyy.yyy.yyy.yyy" corresponds to one service ("YYY Service"), and the next row would be another multicast group address for a different service, say "zzz.zzz.zzz.zzz" ("ZZZ Service"). *Id.* ¶123. Murakami assigns unique LLIDs and encryption keys for each multicast group, as it is building the MMT. *Id.* ¶¶124–25. Therefore, the OLT uses a different bearer channel (a different multicast LLID) and a different encryption key when sending the YYY Service to an ONU than the

OLT will use when sending the ZZZ Service to the exact same ONU. *Id.*

To further explain by example, consider a service from an internet service provider that may be multicasting a basic video package such as live TV ("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. *Id.* ¶126.



Ex. 1005, Fig. 4 (highlighting added). As IGMPv1 notes, this service, an upper-layer protocol module,[22] "us[es] the same 'Send IP' operation used to send unicast IP datagrams . . . [but] merely specifies an IP host group address, rather

[22] Upper layer protocol is referring to the OSI model, whereby the application sits in "upper" Layer 7, while IGMP specifies behavior at the "lower" Level 3. Ex. 2002 ¶¶89–95.

than an individual IP address, as the destination." Ex. 1006 at 5. This is in accord with Murakami (and IGMPv1 and IGMPv2), Ex. 1005 [00013], where a "host group" is "identified by a single IP destination address." Ex. 1006 at 1, 12; Ex. 2002 ¶¶49, 159, 162. The multicast IP group addresses correspond to the "service channels" by which different multicast services are sent, like the Applicant alluded to during prosecution. *See* Ex. 1002 at 384; *see also* the illustration in § III.C *supra* on page **Error! Bookmark not defined.**

For instance, an ONU on Access Port 2 of an OLT assigned P2P LLID 1—call it "ONU A"—may send an IGMP Report to multicast IP destination address 224.0.0.4 that subscribes to the IPTV group multicast destination 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. Ex. 2002 ¶127.

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. *Id.*

And because no other ONUs on Access Port 2 have subscribed to this service, and the OLT encrypted the key for this service with the ONU A P2P encryption key, *see* 1005 [0032], no other ONU may decrypt this service. Ex. 2002 ¶128.

Now, if the same ONU A also subscribed to an intraoffice video conferencing service ("VC") provided by the ISP, ONU A would send another IGMP Report message indicating its desire to join the VC multicast IP destination address, say 224.0.0.5. Ex. 2002 ¶129. 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.*; Ex. 2002 ¶129.

More importantly, Murakami explicitly discloses that 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] (emphasis added); and (2) "***generates a new encryption key used in this multicast***

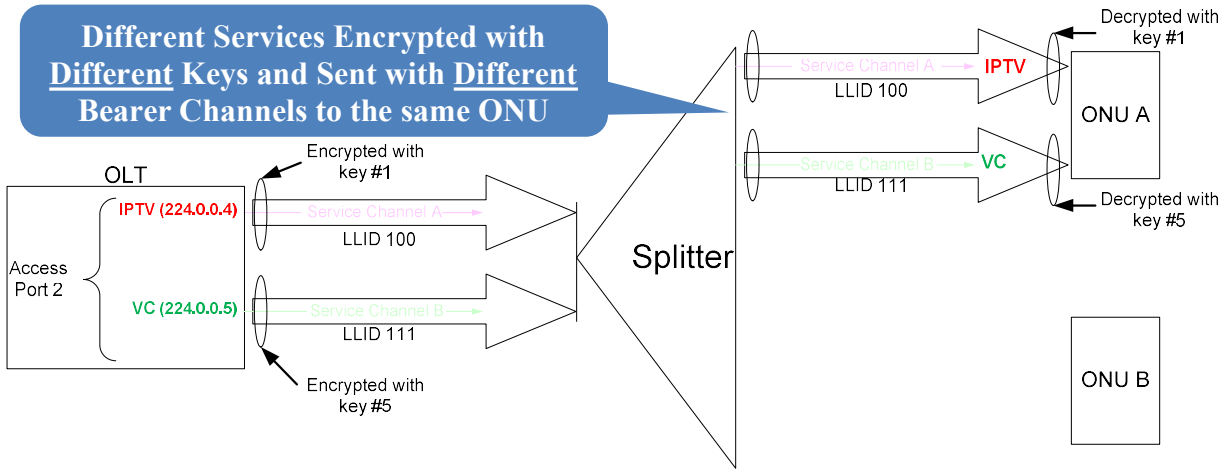
communication and transmits it to the point-to-point logical link 41," *id.* [0031] (emphasis added); Ex. 2002 ¶130. Therefore, the MMT would look as follows after the OLT snoops the two Report messages subscribing to the different services. *Id.*

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**

Again, Murakami 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. *Id.*

In short, for subsequent data sent in these service channels, i.e., addressed to these two multicast groups, Murakami's OLT would use bearer channel LLID 100 and encryption key #1 for the IPTV service and bearer channel LLID 111 and encryption key #5 for the VC service. *Id.* ¶131. 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—not the claimed "using the common key to encrypt multicast service data of all different multicast services in a

same bearer channel," as illustrated below.[23] *Id.*



So, Murakami's architecture does not satisfy the Challenged Claims because it does not route all different services on the same bearer channel using the same common key. *Id.*

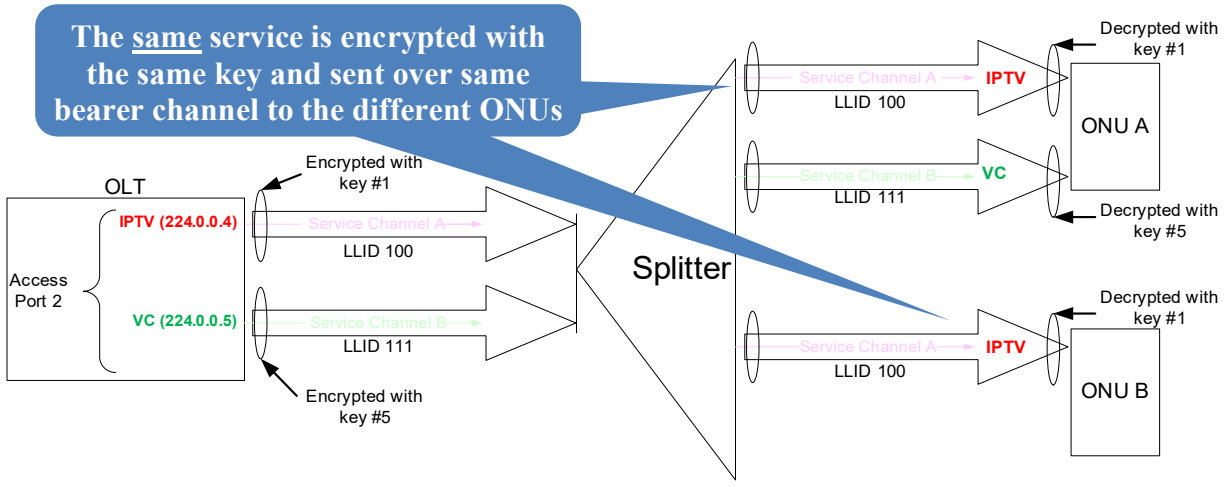
This is why Petitioner is particularly focused on the case where two ONUs are attached to the same PON serviced by the same OLT transceiver. *See, e.g.*, Pet. 22 (discussing "two ONUs ***belonging to a multicast group***, each connected to the OLT's physical port 2, receiving multicast data communications via a downstream logical link having LLID 100") (emphasis added). However, if the two ONUs belonged to the same ***group***, they would be receiving the same ***service***. Ex. 2002 ¶132.

[23] The encrypted data would also be sent to ONU B; however, this is not shown to simplify the illustration as ONU B does cannot process this data as it does not have the encryption keys #1 and #5. Ex. 2002 ¶131 n.12.

Extending the example, if another ONU on Access Port 2 that had P2P LLID 3—call it "ONU B"—sent a Report to also join the IPTV service, Murakami would give the IPTV encryption key #1 to ONU B and the table may now look as so. *Id.*

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**

As seen, different ONUs—listed in the third column of the first row (yellow)—will receive the encrypted data of the ***same*** multicast service—specified by the multicast IP group address and listed in the first column—on LLID 100. This situation is illustrated below. *Id.*



That is, just as a POSITA would expect from the MMT indexed by multicast

group address, 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." *Id*. Indeed, 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')."").

As such, 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 because PIM-SM teaches that communications to a multicast group can be drawn from different ***sources***, not ***services***, and the cited to IPMGv1 section says nothing concerning multiple sources ***or*** services. Ex. 2002 ¶133.

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 sending source need not be part of the group of receivers. IGMPv1 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. And IGMPv1 certainly does not address encrypting, much less encrypting all different multicast services on the same bearer channel with the same common key. Ex. 2002 ¶134.

For PIM-SM, the specification does say that "source***s***" (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 all 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.[24] Ex. 2002 ¶135.

The fact that a multicast group may have multiple sources does not even imply multiple services. As Iarnach's expert, Dr. Litvin, explains: a ***single*** service taking advantage of the PIM-SM protocol may have ***multiple*** sources. Ex. 2002 ¶¶136–49 (citing Ex. 2013). For instance, a presentation ***service*** may have one ***source*** for video and another ***source*** for audio. Ex. 2002 ¶144; *see also* Ex. 2007 at 2.

[24] This makes sense as IGMPv1 and PIM-SM are concerned with the OSI lower levels rather than the upper application level where a "service" resides. Ex. 2002 ¶¶96–99.

Moreover, the two sources for the same service may be addressed to the same RPT for a single multicast group where receiver applications use the two source streams. Ex. 2002 ¶145. Or alternatively, a single multicast service may have multiple sources to provide: (1) redundant data to obviate single source failures, *see* Ex. 2008 at 2; (2) different geographic sources of data to improve latency; and (3) different channel sources that a receiving application may choose (e.g., one source of the IPTV service providing C-SPAN content and another source of the IPTV service providing PBS content). Ex. 2002 ¶¶146–48. Therefore, PIM-SM's disclosure that its architecture allows sending data to a RPT from different ***sources*** is not a teaching that ***any*** different ***services*** would or should send ***service*** data to the same multicast group—much less that ***all*** different services would or should. *Id.* ¶149.

Ultimately, 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 completely misaligned with Murakami's teachings. Ex. 2002 ¶¶150–69. 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. Ex. 2002 ¶150.

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 as so:

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

This table illustrates that Petitioner is making a results-driven suggestion in an attempt to meet the claim limitations by requiring "all different multicast services in the same one bearer channel use a same common key." Ex. 2002 ¶150.

Additionally, Murakami teaches away from Petitioner's proposal to force multiple services on the same group to arrive at the Patent-at-Issue's invention

because Murakami at least implicitly "warned against the very modification made by the patentee." *Spectralytics, Inc. v. Cordis Corp.*, 649 F.3d 1336, 1343 (Fed. Cir. 2011), *abrogated on unrelated grounds by Halo Elecs., Inc. v. Pulse Elecs., Inc.*, 579 U.S. 93 (2016) (considering the standard for awarding enhanced damages); *see also* Ex. 2002 ¶151. Specifically, Murakami explicitly says its per multicast group encryption key design is meant to prevent the stored encryption key for a service "from being eavesdropped by another ONU," *see* Ex. 1005 [0032], whereas the Patent-at-Issue embraced providing the same key to multiple ONUs to decrypt any service in the bearer channel. Ex. 2002 ¶160.

Murakami also teaches away from Petitioner's proposal because Petitioner's redesign would "change . . . the basic principles under which the [prior art] was designed to operate." *In re Ratti*, 270 F.2d 810, 813 (CCPA 1959); *see also In re Gordon*, 733 F.2d 900, 902 (Fed. Cir. 1984) (finding teaching away where proposed modification "rendered [prior art] inoperable for its intended purpose"). Under Petitioner's proposal, an ONU that is subscribed to any service in the shared group may decrypt and eavesdrop on services that only another ONU has subscribed, thereby fundamentally changing Murakami's operation meant to prevent a service's encryption key "from being eavesdropped by another ONU." Ex. 1005 [0032]; Ex. 2002 ¶¶29, 79, 125, 130, 132, 151.

Moreover, 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—are also undeveloped and unsound. Pet. 34–38; Ex. 2002 ¶¶152–69. Petitioner begins its motivation to combine arguments with the strawman that "Murakami did not suggest restricting its system to a single source of data and/or a single multicast service"—implying that this is Patent Owner's position or the only way Patent Owner may rebut that the "encrypt all different multicast services in a same one bearer channel with a same common key" is obvious. Pet. 33 (citing Ex. 1003 ¶94).

This is not Patent Owner's position. As set forth above, Patent Owner's stance is that multicast services may have multiple sources of data and Murakami suggests using different keys and bearer channels for the different multicast services (regardless of the number of sources a service has). This is why Murakami/IGMPv1/PIM-SM do not render the "encrypt all different multicast services in a same one bearer channel with a same common key" claim language obvious—not because Murakami may only be used with a single service or source of data.

Petitioner then 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, and each multicast service may have its 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 already may get "data from more than one different multicast service" without forcing different multicast services to share a single multicast group. Ex. 2002 ¶¶153–59.

Petitioner also argued, relying solely on its expert, that having different services address a single multicast group would "deliver that data to a subscriber in a single bearer channel more efficiently." Pet. 34. (citing Ex. 1003 ¶93). However, Dr. Rouskas simply parrots the conclusion and provides no reason why sending multiple services to a single multicast group is "more efficient" than sending data from multiple services via each service's dedicated multicast group. Without disclosing the underlying facts or data on which the opinion is based, Dr. Rousska's unexplained opinion "is entitled to little or no weight." 37 C.F.R. § 42.65(a).

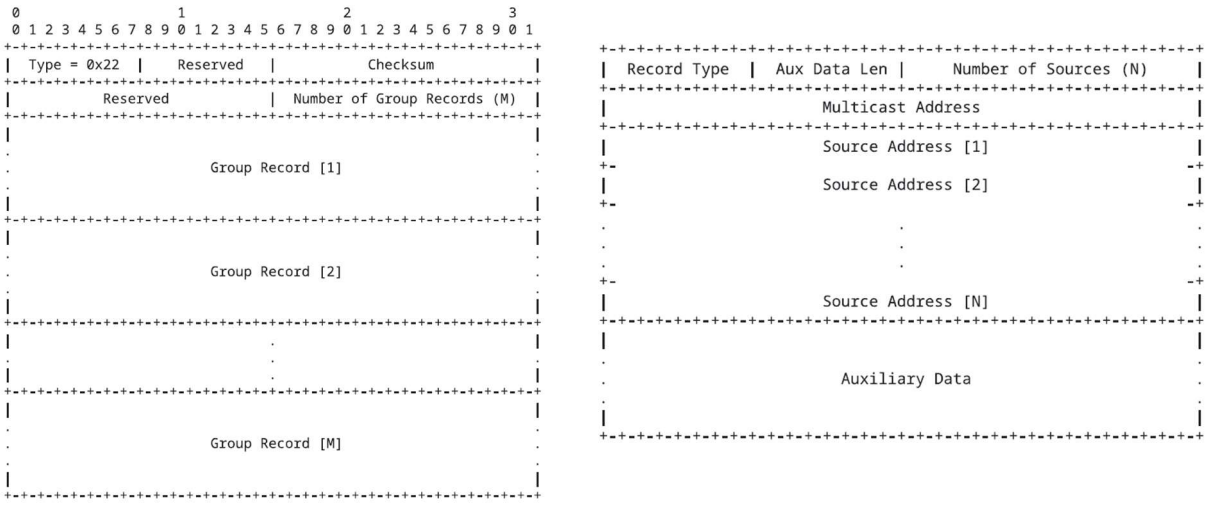
Petitioner further says that a POSITA would design a system whereby different multicast services would be sent to a single multicast group to "ensure compatibility with published standards protocols, such as RFC 4601," "so that it could enjoy the benefits of the advances in IGMP standards (*i.e.* IGMPv3)," "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. While Petitioner is less than clear regarding its vision for the role of IGMPv3's introduction of "source-specific joins," whereby a receiver may "join a group and specify that it only wants to receive traffic for a group if that traffic comes from a particular source," Ex. 1007 at 7, it appears that not only is Petitioner suggesting that a POSITA would scrap Murakami's different key/channel per multicast group design and have all services use only a single multicast group, but that the reimagined system would have all 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.

And 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 (emphasis added). But Petitioner's plan to use a single group and IGMPv3's source filtering ***requires just that***. Ex. 2002 ¶¶164–66. 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. Ex. 2002 ¶¶165–66.

With IGMPv3, Report messages have the following format shown on the left and each group record in the Report message has the format shown on the right:



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/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"). So, because Murakami would have to differentiate multicast data based upon its source, and "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 (emphasis added), such a design is not obvious. Ex. 2002 ¶¶165–66.

Additionally, Petitioner's suggestion would ***not*** "ensure compatibility with published standards protocols." Pet. 34. Specifically, requiring source specific joins means that no IGMPv1 or IGMPv2 applications would work; these protocols do not support source specific joins. *See* Ex. 2012 at 2; Ex. 2002 ¶168.

Finally, and perhaps most telling, is what Petitioner has not said. Despite PIM-SM having been available for nearly two decades, Petitioner and its expert have not provided a single example of multiple services sharing a multicast group address. *See generally* Pet; Ex. 2002 ¶167.

In the end, Murakami's design that allows for millions of different multicast bearer channels using different keys for different services is the opposite of the '378 Patent. Contrary to Murakami, the '378 reduces encryption complexity by having an OLT designate and encrypt a bearer channel used to send the encrypted data for ***all*** different multicast services using the ***same*** common encryption key. And IMPGv1's teaching that a ***source*** outside a multicast group can address a multicast group does not change Murakami's fundamental design. Nor does PIM-SM's teachings that multiple ***sources*** that can come from a ***single*** service and may address a multicast group 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 neither taught nor rendered obvious by Murakami, IGMPv1, or PIM-SM, whether considered individually or collectively. Ex. 2002 ¶¶112–17, 160–62, 169.

B. Petitioner Fails to Show Any Challenged Dependent Claims Are Obvious

Because Petitioner failed to show it would be obvious to modify Murakami in light of IGMPv1/PIM-SM such that Murakami would "encrypt multicast service data of all different multicast services born in a same one bearer channel with a same common key" as set forth in Section VII.A, Petitioner has also failed to meet its burden to show a reasonable likelihood that any dependent claims are unpatentable. *In re Fine*, 837 F.2d 1071, 1076 (Fed. Cir. 1988) ("Dependent claims are nonobvious under section 103 if the independent claims from which they depend are nonobvious.").

VIII. CONCLUSION

Patent Owner believes the Board should discretionarily deny the Petition as wastefully duplicative and providing an opportunity for inconsistent outcomes. Nonetheless, Patent Owner also has shown the Petition should be denied on the merits.

The '378 Patent claims the invention of encrypting multicast service data of all different multicast services via a bearer channel using a same common key. As

the Patent-at-Issue explains, the advantage of this setup is that it will "***reduce the complexity of [the] OLT encryption mechanism and the burden of the OLT***." *Id.* 1:59–62 (emphasis added).

In contrast, Murakami's goal is to remove complexity ***from the subscriber end of the PON network***, i.e., "without requiring routing functions on the ***subscriber side or the subscriber-side units (ONUs)***." *See, e.g.*, Ex. 1005 [0011] (emphasis added). Murakami achieves this goal by ***increasing*** the complexity and the burden of the OLT. Specifically, rather than simply encrypting multicast service data of all different multicast services via a bearer channel with a same common key and leaving the routing to the downstream portion of the network, Murakami must snoop Level 3 routing protocol messages, *id.* [0013], maintain a Multicast Management Table that can have millions of snooped IP group addresses (each with a corresponding multicast LLID and encryption key), *id.* [0029], and implement a Layer-2 switch that coordinates with the MMT to apply the correct encryption key for the different groups, *id.* [0034].

Petitioner's invocation of two secondary low-level protocol specifications does not change Murakami's fundamental architecture. At most, IGMPv1 merely says that a source need not be part of a group to address the group, and PIM-SM merely notes that multiple ***sources*** may address a multicast group. But as shown, a single service expects to have a ***uniquely reserved multicast group address***. And a

single service relying upon PIM-SM may have multiple ***sources***. *See* Exs. 2007 & 2008. So, the use of multiple sources on a PIM-SM tree does not mean ***all services*** would or should share a multicast group. Moreover, Petitioner's suggestion to use only one multicast group address and rely upon user side source specific joins is (1) misaligned with Murakami's fundamental one key/channel per group design and (2) greatly increases the OLT's burden and complexity.

In short, Murakami's approach is the opposite of the Patent-at-Issue's, and Murakami's design does not render the '378 Patent's claimed invention obvious, even when IGMPv1 and PIM-SM are considered. For that reason, Patent Owner respectfully suggests that the Board should deny institution.

Dated: November 21, 2024

Respectfully submitted,

/Blaine A. Larson/

Blaine A. Larson (Reg. No. 69,132)

HEIM PAYNE & CHORUSH, LLP
609 Main Street, Suite 3200
Houston, Texas 77002
Tel: (713) 221–2000
Fax: (713) 221–2021
blarson@hpcllp.com

Counsel for Patent Owner,
IARNACH TECHNOLOGIES, INC.

CERTIFICATE OF WORD COUNT

Per § 42.24(a)–(b) the undersigned certifies that the number of words in the paper, PATENT OWNER'S PRELIMINARY RESPONSE, is:

12,832

The word count does not include the table of contents, table of authorities, certificate of service, word count, exhibits list, or claim listing.

To arrive at this count, the undersigned has relied upon the word count feature of the word-processing system used to prepare the paper.

Dated: November 21, 2024

/Blaine A. Larson/
Blaine A. Larson (Reg. No. 69,132)

CERTIFICATE OF SERVICE

The undersigned certifies that on the twenty-first day of November, 2024, a complete and entire copy of the foregoing "PATENT OWNER'S PRELIMINARY RESPONSE," including exhibits, if any, was served on the following counsel of record via email per Petitioner' consent to electronic service. *See* Paper 1 at 3:

Raymond R. Ricordati III	rricordatti@marshallip.com
Thomas L. Duston	tduston@marshallip.com

Dated: November 21, 2024 /Blaine A. Larson /
Blaine A. Larson (Reg. No. 69,132)

Counsel for Patent Owner,
IARNACH TECHNOLOGIES, INC.