

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

CHARTER COMMUNICATIONS, INC.,  
Petitioner,

v.

IARNACH TECHNOLOGIES, INC.,  
Patent Owner.

---

Case IPR: 2024-XXXXX  
U.S. Patent No. 8,942,378

PETITION FOR *INTER PARTES* REVIEW  
UNDER 35 U.S.C. §312 AND 37 C.F.R. §42.104

(Claims 1-13)

## TABLE OF CONTENTS

|                                                                                | Page |
|--------------------------------------------------------------------------------|------|
| I. INTRODUCTION .....                                                          | 1    |
| II. MANDATORY NOTICES .....                                                    | 2    |
| A. Real Party in Interest .....                                                | 2    |
| B. Related Matters.....                                                        | 2    |
| C. Lead and Back-Up Counsel and Service Information .....                      | 2    |
| D. Fee Payment Authorization (37 C.F.R. §§42.103(a) and<br>42.15(a)) .....     | 3    |
| III. GROUNDS FOR STANDING.....                                                 | 3    |
| IV. THE '378 PATENT.....                                                       | 3    |
| A. Specification.....                                                          | 3    |
| B. Prosecution History .....                                                   | 6    |
| V. DISCRETIONARY DENIAL INAPPROPRIATE.....                                     | 9    |
| VI. LEVEL OF SKILL .....                                                       | 13   |
| VII. CLAIM CONSTRUCTION .....                                                  | 13   |
| A. “common key” .....                                                          | 13   |
| B. “bearer channel” .....                                                      | 15   |
| VIII. PRIOR ART.....                                                           | 15   |
| A. JP2004-343243A (“Murakami”) (EX1004, EX1005 (English<br>Translation)) ..... | 15   |
| B. RFC 1112 (EX1006) .....                                                     | 16   |
| C. RFC 4601 (EX1007) .....                                                     | 17   |

**TABLE OF CONTENTS**  
(Continued)

|                                                                                                                                                               | <b>Page</b> |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| D. U.S. Patent Appl. 2002/0150097 A1 (“Yen”).....                                                                                                             | 18          |
| IX. IDENTIFICATION OF HOW THE CLAIMS ARE<br>UNPATENTABLE.....                                                                                                 | 19          |
| A. Challenged Claims & Statutory Grounds.....                                                                                                                 | 19          |
| B. Ground 1: Claims 1-2, 4, 6-10, 12-13 are Obvious in light of<br>JP2004-343243A in view of RFCs 1112 and 4601 and the<br>knowledge of persons of skill..... | 19          |
| 1. Independent Claim 1 .....                                                                                                                                  | 19          |
| a. Element 1 [preamble] .....                                                                                                                                 | 19          |
| 2. Claim 2.....                                                                                                                                               | 43          |
| 3. Claim 4.....                                                                                                                                               | 44          |
| 4. Claim 6.....                                                                                                                                               | 45          |
| 5. Claim 7.....                                                                                                                                               | 46          |
| 6. Claim 8.....                                                                                                                                               | 46          |
| 7. Claim 9.....                                                                                                                                               | 47          |
| a. Element 9[a].....                                                                                                                                          | 47          |
| b. Element 9[b] .....                                                                                                                                         | 49          |
| c. Element 9[c].....                                                                                                                                          | 50          |
| 8. Claim 11 .....                                                                                                                                             | 51          |
| 9. Claim 12.....                                                                                                                                              | 52          |
| 10. Claim 13.....                                                                                                                                             | 53          |

**TABLE OF CONTENTS**  
(Continued)

|                                                                                                                                                                                                               | <b>Page</b> |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| a.    Element 13[a].....                                                                                                                                                                                      | 53          |
| b.    Element 13[b] .....                                                                                                                                                                                     | 53          |
| C.    Ground 2: Claims 3, 8, 11 are Obvious in light of JP2004-343243A in view of RFCs 1112 and 4601 and knowledge of persons of skill, and in further view of U.S. Patent Appl. 2002/0150097 A1 (“Yen”)..... | 54          |
| 1.    Claim 3.....                                                                                                                                                                                            | 54          |
| a.    Element 3[a].....                                                                                                                                                                                       | 54          |
| b.    Element 3[b] .....                                                                                                                                                                                      | 58          |
| c.    Element 3[c].....                                                                                                                                                                                       | 59          |
| d.    Element 3[d] .....                                                                                                                                                                                      | 60          |
| 2.    Claim 5.....                                                                                                                                                                                            | 60          |
| a.    Element 5[a].....                                                                                                                                                                                       | 60          |
| b.    Element 5[b] .....                                                                                                                                                                                      | 61          |
| c.    Element 5[c].....                                                                                                                                                                                       | 61          |
| d.    Element 5[d] .....                                                                                                                                                                                      | 61          |
| 3.    Claim 10.....                                                                                                                                                                                           | 61          |
| D.    No Evidence of Sufficient Secondary Factors .....                                                                                                                                                       | 63          |
| X.    CONCLUSION.....                                                                                                                                                                                         | 63          |

---

**TABLE OF AUTHORITIES**

**Cases**

|                                                                                                                    |            |
|--------------------------------------------------------------------------------------------------------------------|------------|
| <i>Advanced Bionics, LLC v. MED-EL Elektromedizinische Geräte GmbH,</i><br>IPR2019-01469 (PTAB Feb. 13, 2020)..... | 9, 10      |
| <i>Apex Inc. v. Raritan Computer, Inc.,</i><br>325 F.3d 1364 (Fed. Cir. 2003) .....                                | 47         |
| <i>Apple Inc. v. Fintiv, Inc.,</i><br>IPR2020-00019 (PTAB Mar. 20, 2020) .....                                     | 10, 11     |
| <i>B. Braun Medical Inc., v. Abbott Laboratories,</i><br>124 F.3d 1419 (Fed. Cir. 1997) .....                      | 47         |
| <i>Brown &amp; Williamson Tobacco Corp. v. Philip Morris, Inc.,</i><br>229 F.3d 1120 (Fed. Cir. 2000) .....        | 62         |
| <i>Catalina Mktg. Int’l, Inc. v. Coolsavings.com, Inc.,</i><br>289 F.3d 801 (Fed. Cir. 2002) .....                 | 20         |
| <i>Google, LLC v. Flypsi, Inc.,</i><br>IPR2023-00361 (PTAB July 31, 2023) .....                                    | 11         |
| <i>In re Bigio,</i><br>381 F.3d 1320 (Fed. Cir. 2004) .....                                                        | 16         |
| <i>In re ICON Health &amp; Fitness, Inc.,</i><br>496 F.3d 1374 (Fed. Cir. 2007) .....                              | 16         |
| <i>KSR Int’l Co. v. Teleflex Inc.,</i><br>550 U.S. 398 (2007).....                                                 | 35, 36     |
| <i>Markforged Inc. v. Continuous Composites, Inc.,</i><br>IPR2022-00679 (PTAB Oct. 25, 2022).....                  | 12         |
| <i>Netflix, Inc. v. DivX, LLC,</i><br>80 F.4th 1352 (Fed. Cir. 2023) .....                                         | 27, 29, 54 |
| <i>Nokia of Am. Corp. v. TQ Delta,</i><br>IPR2022-00471 (PTAB Aug. 18, 2022).....                                  | 10         |

**TABLE OF CONTENTS**  
(Continued)

|                                                                                                                           | <b>Page</b>    |
|---------------------------------------------------------------------------------------------------------------------------|----------------|
| <i>Ormco Corp. v. Align Tech., Inc.</i> ,<br>463 F.3d 1299 (Fed. Cir. 2006) .....                                         | 62             |
| <i>Phillips v. AWH Corp.</i> ,<br>415 F.3d 1303 (Fed. Cir. 2005) ( <i>en banc</i> ) .....                                 | 13             |
| <i>Plantronics, Inc. v. Aliph, Inc.</i> ,<br>724 F.3d 1343 (Fed. Cir. 2013) .....                                         | 32             |
| <i>Samsung Elecs. v. Netlist, Inc.</i> ,<br>IPR2022-00063 (PTAB May 5, 2022) .....                                        | 11             |
| <i>Sand Revolution II, LLC v. Continental Intermodal Group–Trucking LLC</i> ,<br>IPR2019-01393 (PTAB June 16, 2020) ..... | 11, 12         |
| <i>Williamson v. Citrix Online, LLC</i> ,<br>792 F.3d 1339 (Fed. Cir. 2015) .....                                         | 46, 47         |
| <i>Zup v. Nash Mfg.</i> ,<br>896 F.3d 1365 (Fed. Cir. 2018) .....                                                         | 32             |
| <br><b>Statutes</b>                                                                                                       |                |
| 35 U.S.C. §102(b) .....                                                                                                   | 16, 17         |
| 35 U.S.C. §112 .....                                                                                                      | 46, 48, 49, 61 |
| 35 U.S.C. §314 .....                                                                                                      | 10             |
| 35 U.S.C. §325(d) .....                                                                                                   | 9, 10          |
| <br><b>Other Authorities</b>                                                                                              |                |
| 83 Fed. Reg. 197 (Oct. 11, 2018) .....                                                                                    | 13             |
| <br><b>Rules</b>                                                                                                          |                |
| 37 C.F.R. §42.100(b) .....                                                                                                | 13             |

**TABLE OF CONTENTS**  
*(Continued)*

|                           | <b>Page</b> |
|---------------------------|-------------|
| 37 C.F.R. §42.104(a)..... | 3           |

**PETITIONER’S EXHIBIT LIST**

|        |                                                                                                                                      |
|--------|--------------------------------------------------------------------------------------------------------------------------------------|
| EX1001 | U.S. Patent No. 8,942,378                                                                                                            |
| EX1002 | Prosecution History of U.S. Patent No. 8,942,378                                                                                     |
| EX1003 | Declaration of Dr. George Rouskas                                                                                                    |
| EX1004 | JP2004-343243A                                                                                                                       |
| EX1005 | Certified English Translation of JP2004-343243A                                                                                      |
| EX1006 | RFC 1112                                                                                                                             |
| EX1007 | RFC 4601                                                                                                                             |
| EX1008 | U.S. Patent Appl. 2002/0150097 A1 (“Yen”)                                                                                            |
| EX1009 | Complaint, <i>IARNACH TECHNOLOGIES, INC. v. CHARTER COMMUNICATIONS, INC., et al.</i> , Case No. 2:24-cv-00230 (E.D. Tex.)            |
| EX1010 | RFC 2362                                                                                                                             |
| EX1011 | Docket Control Order, <i>IARNACH TECHNOLOGIES, INC. v. CHARTER COMMUNICATIONS, INC., et al.</i> , Case No. 2:24-cv-00230 (E.D. Tex.) |

## **I. INTRODUCTION**

Pursuant to 35 U.S.C. §§311, 314(a), and 37 C.F.R. §42.100, CHARTER COMMUNICATIONS, INC. (“Petitioner”) respectfully requests that the Board cancel as unpatentable Claims 1-13 of U.S. Patent No. 8,942,378 (“’378 Patent,” EX1001).

The ’378 Patent is directed to securing multicast communications—*i.e.*, point to multipoint communications in which multiple recipients receive the same data from a single transmitter. The ’378 Patent claims the obvious an unremarkable method of encrypting that data before transmission to prevent unauthorized eavesdropping, and then providing recipients with the key used to encrypt the data so that it can be decrypted upon receipt. The applicant did not dispute that the prior art taught such a method. While the applicant persuaded the examiner that this prior art did not explicitly describe use of this method for multicast communications comprising data relating to more than one multicast service, it was well-known to persons of ordinary skill in the art that multicast communications routinely comprised data of more than one service.

Prior art reflecting this known fact was not presented to, nor before, the examiner at the time the patent application was allowed. This Petition seeks to correct this miscarriage.

## II. MANDATORY NOTICES

### A. Real Party in Interest

Pursuant to 37 C.F.R. §42.8(b)(1), Petitioner certifies that the real party-in-interest is CHARTER COMMUNICATIONS, INC.

### B. Related Matters

Pursuant to 37 C.F.R. §42.8(b)(2), to the best knowledge of the Petitioner, the '378 Patent is involved in the following case (the "Litigation"):

| Case Heading                                                       | Number        | Court     | Filed         |
|--------------------------------------------------------------------|---------------|-----------|---------------|
| IARNACH TECHNOLOGIES, INC. v. CHARTER COMMUNICATIONS, INC., et al. | 2:24-cv-00230 | E.D. Tex. | April 5, 2024 |

### C. Lead and Back-Up Counsel and Service Information

#### Lead Counsel

Raymond R. Ricordati III, Esq.  
Marshall, Gerstein & Borun LLP  
233 S. Wacker Drive  
6300 Willis Tower  
Chicago, IL 60606

Phone: (312) 474-6300  
Fax: (312) 474-0448  
rricordatti@marshallip.com  
USPTO Reg. No. 62,856

#### Back-up Counsel

Thomas L. Duston, Esq.  
Marshall, Gerstein & Borun LLP  
233 S. Wacker Drive  
6300 Willis Tower  
Chicago, IL 60606

Phone: (312) 423-3446  
Fax: (312) 474-0448  
tduston@marshallip.com

Please address all correspondence to lead and back-up counsel. Petitioner consents to service by email at the addresses above.

**D. Fee Payment Authorization (37 C.F.R. §§42.103(a) and 42.15(a))**

Payment of required fees is submitted herewith. The Patent Office is authorized to charge Deposit Account No. 13-2855 for all additional fees.

**III. GROUNDS FOR STANDING**

Petitioner certifies the '378 Patent is eligible for IPR and Petitioner is not barred or estopped from requesting this IPR. 37 C.F.R. §42.104(a).

**IV. THE '378 PATENT**

The '378 Patent issued from U.S. Patent Application No. 13/257,731, filed November 10, 2010, and claims priority to Chinese Patent Application 201010102646 filed January 25, 2010. Based on Patent Owner's ("PO's") claimed priority, the '378 Patent would be evaluated under the rules preceding the adoption of the America Invents Acts.

**A. Specification**

The '378 Patent describes a conventional method for encrypting multicast service data in a passive optical network (PON) system. The '378 Patent acknowledges that the structure of a PON system was known and that various mechanisms for encrypting service data in a PON system existed in the art. EX1001, 1:14-19, 32-39.

For example, the '378 Patent explains that a PON system was known to employ a plurality of optical network units (ONU) associated with users. EX1001, 1:14-19. These ONUs received data packets sent from an upstream Optical Line Terminal (OLT), after they interconnected with the PON and were authorized to receive such communications. *Id.*

The '378 Patent further acknowledges that encryption mechanisms were known. EX1001, 1:32-39. The '378 Patent illustrates the OLT's use of a key to encrypt the multicast communication before their transmission to one or more ONUs. For this purpose, the OLT unsurprisingly generates a key (*i.e.*, step 110). EX1001, Fig. 1. The OLT then encrypts the multicast data to be sent (*i.e.*, step 120). *Id.*

ONUs power on and access the PON network, registering with the network and applying for multicast service (*i.e.*, step 130). *Id.* The '378 Patent acknowledges that the procedures for registration and authorization were previously fully described in published industry protocols, and for that reason, asserts that it need not provide details to explain that process further to a person of ordinary skill in the art ("POSA"). EX1001, 4:51-53.

In response, the OLT shares the key used to encrypt the multicast communication with the ONU authorized to receive it (*i.e.*, step 140). EX1001, Fig. 1. The key both encrypts and decrypts the multicast data (*i.e.*, the key is common to both processes).

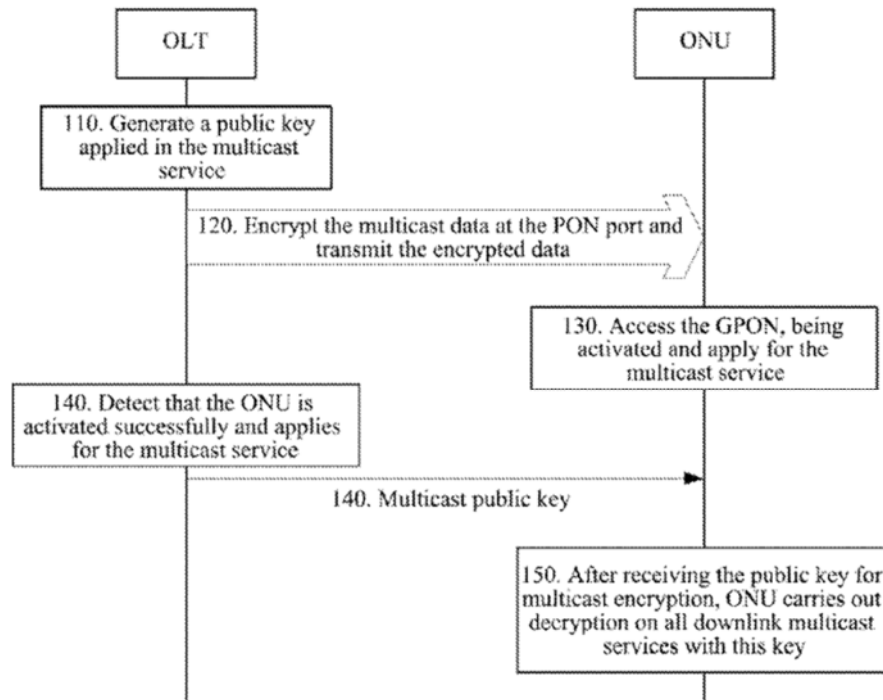


FIG. 1

EX1001, Figure 1.

Figure 2 further depicts use of a key valid for only a limited period of time. The OLT generates a common key and sets a timer (T1) (*i.e.*, step 210). EX1001, Fig. 2. Use of this key proceeds as described above. However, upon expiration of the timer, the OLT regenerates a new common key and resets the timer (*i.e.*, step 270):

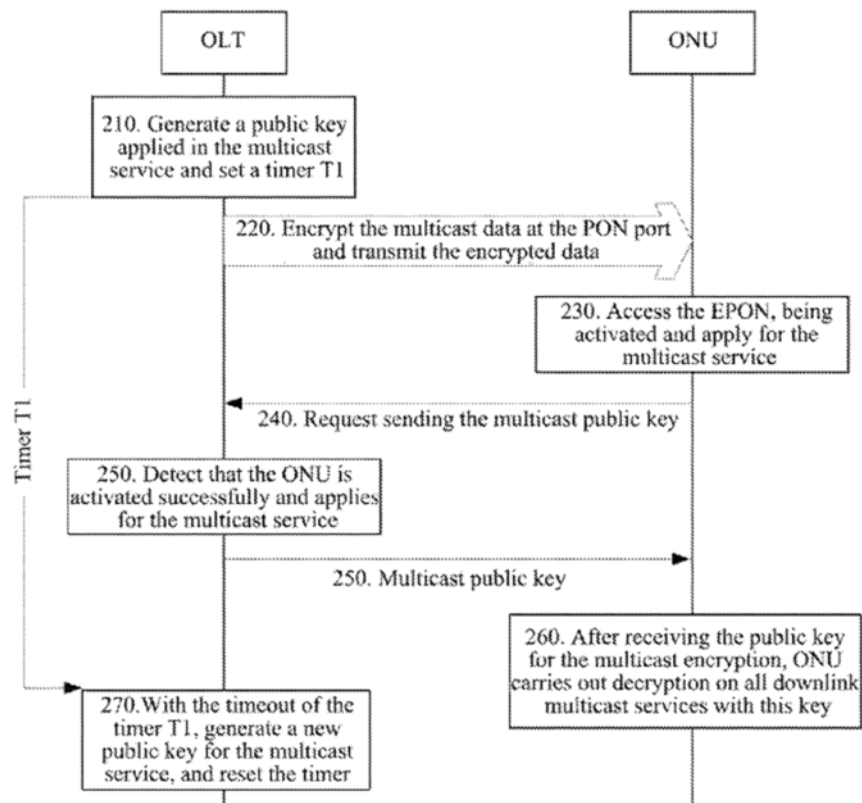


FIG. 2

EX1001, Figure 2.

## B. Prosecution History

The claims of the application were initially rejected as anticipated by Chinese Patent No. 1855834 (“He”) dated November 1, 2006. EX1002, 208-10. The examiner determined that He taught a method for encrypting multicast services in a passive optical network system in which an optical line terminal (OLT) generated a common key, used that key to encrypt multicast service data sent in a bearer channel, and then sent that key via a separate management control channel to an optical network unit (ONU) that is activated successfully and applies to receive said multicast

service data, after which it is used to decrypt the encrypted data. *Id.* The examiner noted that He also taught the remaining elements of the certain of the remaining dependent claims. *Id.* (observing that He taught use of the key to decrypt the multicast communications, that the key is sent once the ONU is detected/judged to have been activated successfully and to have applied to receive the key, that the OLT sent the ONU an identifier for the bearer channel, as well as the various independent/dependent apparatus claims drawn to the same method).

The examiner further concluded claims remaining that regenerated the key following expiration of an aging time, were obvious in light of He in further view of Chinese Patent No. 1866857 (“Jiang”) dated November 22, 2006. EX1002, 210-12. The examiner determined that He and Jiang were analogous art because they were from the same field, namely the provision of secure communications between computer systems. *Id.* The examiner noted that Jiang taught the application of an expiration time to a key and the generation of a new key following expiration. *Id.*

In response to the examiner’s rejection, the applicant contended that He described the encryption of a multicast “bit-stream,” and argued that He did not disclose the encryption of multiple multicast communications in a bearer channel with the common key. EX1002, 321-24 (arguing that a bearer channel differed from a multicast bit-stream, asserting that multiple multicast bit-streams could be carried in

a single bearer channel). The applicant did not otherwise dispute the examiner's reading of He, nor his application of the timing disclosures present in Jiang.

The examiner rejected the applicant's efforts to distinguish He. The examiner noted that based on He, he had rejected a dependent claim (then Claim 6) that recited the encryption of all multicast service data in a bearer channel with the common key. EX1002, 328-31.

The applicant responded by amending the claims to positively recite that the common key was used to encrypt "all multicast services in a bearer channel" and that "all multicast services in the same one bearer channel use a same common key to carry out encryption." EX1002, 341-44. The applicant again argued that He disclosed the transmission of only a single data stream and failed to disclose examples involving transmission of more than one data stream. EX1002, 351-54 ("HE's invention provides a method for realizing multicast in PON, in which the OLT allocates the multicast service which is applied for to occupy one downlink service channel, and the OLT generates one key for this multicast service."). Again, the applicant did not otherwise dispute the examiner's application of He and/or Jiang.

The examiner responded that the amended claims remained obvious in light of the disclosures in He and Jiang. The examiner noted that Jiang disclosed the encryption of all multicast services in a bearer channel, rendering the claims obvious in light of He's remaining disclosures. EX1002, 373-78 (noting that Jiang disclosed

that “BS in the same MBS zone use the same key for encrypting the same MBS program”).

To gain allowance, the applicant again amended its claims. The applicant required that a common key be used to encrypt multicast service data “of all different multicast services in a same bearer channel[.]” EX1002, 416-19. The examiner ultimately issued the claims after concluding that the prior art then of record did not explicitly disclose that data of “different” multicast services on a single bearer channel would be encrypted with the same common key. EX1002, 436-40.

## **V. DISCRETIONARY DENIAL INAPPROPRIATE**

This Petition relies on references not identified during any stage of the prosecution of the ’378 Patent. Under 35 U.S.C. §325(d), the art and arguments must have been previously presented to the Office during prosecution. *See Advanced Bionics, LLC v. MED-EL Elektromedizinische Geräte GmbH*, IPR2019-01469, Paper 6, at 8 (PTAB Feb. 13, 2020) (precedential). This Petition thus presents new issues warranting an exercise of discretion to institute trial. 35 U.S.C. §325(d).

The grounds asserted herein rely upon uncited JP2004-343243A (“Murakami”), RFCs 1112 and 4106, and U.S. Patent Appl. 2002/0150097 A1 (“Yen”). These references were not before the Examiner, and thus were never evaluated by the Examiner, either alone or in combination with other references. The Board has consistently declined to exercise discretion under Section 325(d) when a reference

was not disclosed during prosecution. *Advanced Bionics* at 9 n.10 (discretionary denial dependent upon “the extent to which the asserted art was evaluated during examination”).

Applicant distinguished prior art by arguing that none of the prior art of record alone or in combination taught using the common key to encrypt multicast service data of all different multicast services in a same bearer channel. Murakami in view of RFCs 1112 and 4106 teaches all recited limitations, including that which the applicant argued distinguished its invention from the prior art. This Petition thus presents new arguments not previously addressed by the Examiner. Denial is therefore inappropriate under 35 U.S.C. §325(d).

Discretionary denial also is inappropriate under 35 U.S.C. §314. Under the Director’s Interim Procedure for Discretionary Denials, the PTAB will not deny institution based on *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11 (PTAB Mar. 20, 2020) (precedential) if there is compelling evidence of unpatentability. This Petition provides such evidence, and thus, concludes the *Fintiv* analysis. *Nokia of Am. Corp. v. TQ Delta*, IPR2022-00471, Paper 11 at 19-21 (PTAB Aug. 18, 2022).

Regardless, the *Fintiv* factors strongly favor institution.

**1. Potential for Stay**

Petitioner will seek a pre-institution stay, but without “specific evidence” how the court will rule, this factor is neutral. *Sand Revolution II, LLC v. Continental Intermodal Group–Trucking LLC*, IPR2019-01393, Paper 24 at 7 (PTAB June 16, 2020) (informative).

## **2. Timing of Trial**

Jury selection is scheduled to begin on February 9, 2026. EX1011, 1. A trial would thus likely occur about the same time as a final written decision would be expected 18 months from the filing of this petition. *Google, LLC v. Flypsi, Inc.*, IPR2023-00361, Paper 9 at 8-9 (PTAB July 31, 2023) (finding trial occurring at least two months *before* deadline only “slightly” favored institution).

Moreover, Petitioner filed this petition with diligence, filing three weeks after receiving Patent Owner’s list of asserted claims, and eight months before the §315(b) deadline. Factor 2 thus is neutral or weighs against denial. *Fintiv*, Paper 11 at 11 (“expeditiously” filed petitions “weigh[] against [denial]”).

## **3. Litigation Investment**

Other than preliminary infringement contentions, the parties have invested little in the litigation, weighing against denial. *Samsung Elecs. v. Netlist, Inc.*, IPR2022-00063, Paper 13 at 8 (PTAB May 5, 2022) (granting institution where no “claim construction and merits determinations” had occurred).

**4. Issue Overlap**

This petition challenges all claims of the '378 patent whereas only claims 1-4, 6-7, and 9-12 are asserted in the underlying litigation. In addition, Petitioner is or will be filing additional petitions of the two other patents asserted in the underlying litigation challenging all claims, including non-asserted claims, concurrently or soon hereafter. Collectively, these petitions will dispose of all issues raised in the underlying litigation and others not at issue. A combined trial here will address claims the district court will not address, which weighs against denial. *Markforged Inc. v. Continuous Composites, Inc.*, IPR2022-00679, Paper 7 at 32-33 (PTAB Oct. 25, 2022).

**5. Litigation Parties**

Petitioner is the defendant in district court, which is typical. *Sand Revolution II*, Paper 24 at 12-13.

**6. Other Considerations**

The claims are being asserted against Charter's systems for complying with the DPoE v2.0 specification, so their cancelation will provide for the public good by removing this unnecessary encumbrance on the standard, weighing against denial. EX1009, ¶¶ 41-46 ("The Accused Instrumentalities include the functionality necessary for Charter to provide DPoE v2.0 compliant networks to its customers . . .").

## **VI. LEVEL OF SKILL**

A person having ordinary skill in this art (“POSA”) 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.

## **VII. CLAIM CONSTRUCTION**

Words in a claim are given their plain meaning, as understood by a POSA in view of the patent and file history. *Changes to the Claim Construction Standard for Interpreting Claims in Trial Proceedings Before the Patent Trial and Appeal Board*, 83 Fed. Reg. 51,340 (Oct. 11, 2018) (codified at 37 C.F.R. §42.100(b)); *Phillips v. AWH Corp.*, 415 F.3d 1303, 1313 (Fed. Cir. 2005) (*en banc*). For purposes of this Petition only, other than the following terms, Petitioner proposes that no claim language requires express construction to resolve the grounds herein. Petitioner reserves the right to propose additional and/or alternative claim constructions in other proceedings in response to arguments that may be advanced therein by PO.

### **A. “common key”**

Each claim of the ’378 Patent recites a “common key.” The term is nowhere found in the specification. *See, e.g.*, EX1001, Claim 1. Instead, the specification refers to a “public” key. *See generally* EX1001.

As initially filed, the claims also used the term “public” key. EX1002, 129-131. During prosecution, however, the examiner noted that the “key” recited in the claims and described in the specification was not a “public” key as generally understood. As the examiner commented,

The term “public key” in claims 1-13 is used by the claim to mean “common key”, while the accepted meaning is of the term “public key” in the art is one of the pair of public/private keys in asymmetric encryption. One key locks or encrypts the plaintext, and the other unlocks or decrypts the ciphertext. **Neither key can perform both functions by itself.** The public key may be published without compromising security, while the private key must not be revealed to anyone not authorized to read the messages.

EX1002, 207.

The examiner observed that the claimed “key” was “common” because it was used to both encrypt and decrypt the communication. This interpretation of the “key” was consistent with the specification. The Applicant agreed with the Examiner’s findings and replaced the term “public key,” as recited in the original claims, with the term “common key” to overcome the Examiner’s indefiniteness rejection. EX1002, 313-316.

In view of the Examiner’s findings, the Applicant’s claim amendments, and the express disclosures of the ’378 Patent, a POSA would understand that the claimed “common key” is a key used to both encrypt and decrypt communications. EX1003, ¶26-33.

**B. “bearer channel”**

Each claim of the '378 Patent recites a “bearer channel.” For example, independent Claim 1 recites “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 different multicast services in the same one bearer channel use a same common key to carry out encryption[.]” EX1001, Claim 1.

The term “bearer channel” is expressly defined in the '378 Patent. The specification discloses that the claimed “bearer channel is a logical channel of the PON, and it can be the general encapsulation model (GEM) channel born by the GPON port or the logical link identification (LLID) channel of the EPON port[.]” EX1001, 4:4-8. In view of this disclosure, a POSA would understand that the claimed “bearer channel” is a logical channel of the PON that may be a LLID or GEM. EX1003, ¶34.

The term “bearer channel” should therefore be construed to mean “a logical channel of the PON that can be a LLID or GEM.”

**VIII. PRIOR ART**

**A. JP2004-343243A (“Murakami”) (EX1004, EX1005 (English Translation))**

Entitled “Method and Central Office Unit for Multicast Communication in PON System,” Murakami was published December 2, 2004. EX1005, 1(54), 1(43).

Murakami qualifies as prior art to the '378 Patent under 35 U.S.C. §102(b)(pre-AIA).

Murakami is concerned with same field of endeavor as inventions claimed in the '378 Patent. EX1003, ¶57. Specifically, both the invention and Murakami are concerned with secure, multicast communications, particularly those made in passive optical networks. *Id.* A reference is analogous art if from the same field of endeavor as the claimed invention. *In re Bigio*, 381 F.3d 1320, 1325 (Fed. Cir. 2004).

Murakami's disclosures are also reasonably pertinent to the problems which the application sought to solve, such that Murakami would have "logically commended itself to an inventor's attention in considering his problem." EX1003, ¶58; *In re ICON Health & Fitness, Inc.*, 496 F.3d 1374, 1379-80 (Fed. Cir. 2007). Murakami discloses a method of securing multicast communications to prevent unauthorized access. *Id.*

**B. RFC 1112 (EX1006)**

Entitled "Host Extensions for IP Multicasting," RFC 1112 is an internet standard that was not cited or discussed by the Examiner during prosecution. RFC 1112 was published in August 1989. EX1006, 1. RFC 1112 qualifies as prior art to the '378 Patent under 35 U.S.C. §102(b)(pre-AIA).

RFC 1112 is concerned with same field as the '378 Patent. RFC 1112 “specifies the extensions required of a host implementation of the Internet Protocol (IP) to support multicasting” and “is the recommended standard for IP multicasting in the Internet.” EX1003, ¶60 (quoting EX1006, p. 1). RFC 1112 is relevant to problems which inventors of the '378 Patent sought to solve. EX1003, ¶60.

**C. RFC 4601 (EX1007)**

Entitled “Protocol Independent Multicast – Sparse Mode IPIM-SM): Protocol Specification (Revised),” RFC 4601 discloses a multicast routing protocol that was not cited or discussed by the Examiner during prosecution. RFC 4601 was published in August 2006. EX1007, 1. RFC 4601 qualifies as prior art to the '378 Patent under 35 U.S.C. §102(b)(pre-AIA).

RFC 4601 is concerned with same field as the '378 Patent. The '378 Patent concerns the content of multicast communications in a bearer channel and the encryption of those communications. RFC 4601 describes source data forming multicast communications, and protocols for delivering them to users. RFC 4601 “specifies an Internet standards track protocol” (*i.e.*, Protocol Independent Multicast – Sparse Mode (PIM-SM)), which “is a multicast routing protocol.” EX1003, ¶62 (quoting EX1007, p. 1).

RFC 4601 is also relevant to problems which inventors of the '378 Patent sought to solve. EX1003, ¶63. The '378 Patent addresses multicast communications

consisting of more than one multicast service. RFC 4601 describes systems and methods for constructing such multicast communications. *Id.*

**D. U.S. Patent Appl. 2002/0150097 A1 (“Yen”)**

U.S. Patent Appl. 2002/0150097 A1 (“Yen”), entitled “Method and apparatus for secured multicasting,” was published October 17, 2002. EX1008, 1(54), 1(43).

Yen describes a method and apparatus for conducting secured multicast communications in a passive optical network having an optical line terminal (“OLT”), and multiple network devices, such as optical network terminals (“ONT”). Yen describes using a multicast encryption key to encrypt multicast data. ONTs employ the same key to decrypt those communications. Yen describes an OLT that periodically updates this multicast encryption key. EX1003, ¶65 (citing EX1008, 1(57)).

Yen is concerned with the same field of endeavor as the inventions claimed in the ’378 Patent. Specifically, both the invention and Yen are concerned with securing communications, particularly multicast communications made in passive optical networks. EX1003, ¶66.

Yen’s disclosures are also reasonably pertinent to the problems which the application sought to solve, such that Yen would have logically commended itself to an inventor's attention in considering his problem. Yen discloses a method of securing multicast communications to prevent unauthorized access. EX1003, ¶67.

## IX. IDENTIFICATION OF HOW THE CLAIMS ARE UNPATENTABLE

### A. Challenged Claims & Statutory Grounds

The Petition presents two grounds for unpatentability:

| Ground | Claims              | Basis (Pre-AIA 35 U.S.C. § 103)                                                                                                                                          |
|--------|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1      | 1-2, 4, 6-10, 12-13 | Obvious in light of JP2004-343243A in view of RFCs 1112 and 4601 and the knowledge of persons of skill.                                                                  |
| 2      | 3, 5, 11            | Obvious in light of JP2004-343243A in view of RFCs 1112 and 4601 and the knowledge of persons of skill, and in further view of U.S. Patent Appl. 2002/0150097 A1 (“Yen”) |

### B. Ground 1: Claims 1-2, 4, 6-10, 12-13 are Obvious in light of JP2004-343243A in view of RFCs 1112 and 4601 and the knowledge of persons of skill

#### 1. Independent Claim 1

Murakami explicitly discloses all but one element of independent Claim 1 (*i.e.*, “all **different** multicast services”). EX1003, ¶68 (citing EX1001, Claim 1 (emphasis added)). This remaining element is implicitly disclosed by Murakami and would have been obvious to a POSA based upon Murakami’s disclosures, particularly in view of RFCs 1112 and 4601 and in light of his knowledge. *Id.*

#### a. Element 1 [preamble]

|                                                                                                       |
|-------------------------------------------------------------------------------------------------------|
| A method for encrypting multicast service in a passive optical network system, the method comprising: |
|-------------------------------------------------------------------------------------------------------|

The preamble is not a limitation. *Catalina Mktg. Int’l, Inc. v. Coolsavings.com, Inc.*, 289 F.3d 801, 808 (Fed. Cir. 2002). To the extent deemed a limitation, however, Murakami discloses this element.

Murakami discloses “[a] method for multicast communication in a PON system,” which “distribute[s] encryption keys for use in the multicast communication.” EX1003, ¶70 (citing EX1005, Claim 1); *see also id.* (citing EX1005, 1(57) (“ONUs and OLT 10 are connected via an optical transport medium so as to transmit and receive data between the ONUs and OLT 10 . . . [and] OLT 10 snoops IGMP<sup>1</sup> messages so as to control the setting of logical links for multicasting according to the result of the snooping and **distribute encryption keys for use in multicast communications.**”) (emphasis added)).

|                                                                              |
|------------------------------------------------------------------------------|
| <b>Element 1[a]:</b> an optical line terminal (OLT) generating a common key, |
|------------------------------------------------------------------------------|

Murakami discloses this element. Murakami discloses that “**OLT 10 generates a new encryption key** used in this multicast communication[.]” EX1003, ¶71 (citing EX1005, [0031] (emphasis added)).

|                                                                            |
|----------------------------------------------------------------------------|
| <b>Element 1[b]:</b> and using the common key to encrypt multicast service |
|----------------------------------------------------------------------------|

---

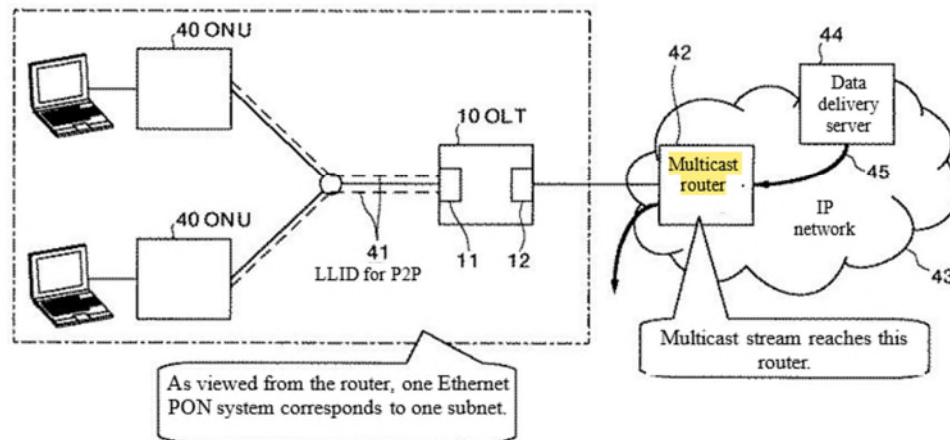
<sup>1</sup> “IGMP” refers to the Internet Group Management Protocol. “Snooping” is a process by which network switches eavesdrop on conversations between hosts (*i.e.*, customer premises equipment) and routers to map which links need which multicast transmissions. “Snooping” prevents hosts from receiving traffic for a multicast group they have not joined. EX1003, ¶1004, n.4.

data of all different multicast services in a same bearer channel and then sending encrypted data,

Murakami discloses this element. Murakami discloses use of a bearer channel in the form of a logical link. EX1003, ¶72 (citing EX1005, 1(57) (disclosing “a PON system in which communications are carried out through the use of logical links”)).

Murakami explains its OLT is equipped with a service node interface 12 that connects to an IP network via multicast router 42. EX1003, ¶73 (citing EX1005, [0026]). Multicast data from delivery servers on the IP network are routed through the Multicast Router 42 to OLTs for subsequent broadcast to ONUs and their associated subscribers. *Id.* This arrangement is depicted in Figure 4, below:

Figure 4



EX1003, ¶73 (citing EX1005, Fig. 4 (yellow annotation added)).

Communications in Murakami's PON system are carried out through "logical links." EX1003, ¶74 (citing EX1005, 1(57)). Using PON interface 11, the OLT connects with one or more ONUs via optical fiber and a passive optical splitter. *Id.* (citing EX1005, [0020]). Murakami describes communicating with ONUs through logical links. *Id.* (citing EX1005, 1(57)). Murakami describes the establishment of logical links 120 for both point-to-point **and multicast communications**. EX1003, ¶74 (citing EX1005, [0018] ("LLID 120 can be specified for point-to-point or multicasting, the only difference is mode bit 121, as shown in Figure 10[.]")).

Murakami discloses that ONUs comprising a multicast group can receive multicast services on a downstream logical link. EX1003, ¶75. For example, in Figure 3, Murakami illustrates 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:<sup>2</sup>

---

<sup>2</sup> Multicast Management Table 19 also illustrates a separate logical channel is established between the physical ports on the OLT and each ONU individually for point-to-point communications. EX1003, ¶75, n.1 (citing EX1005, Fig. 3 (as indicated by "LLIDs for P2P" 1, 2, 3, and 5)).

Figure 3

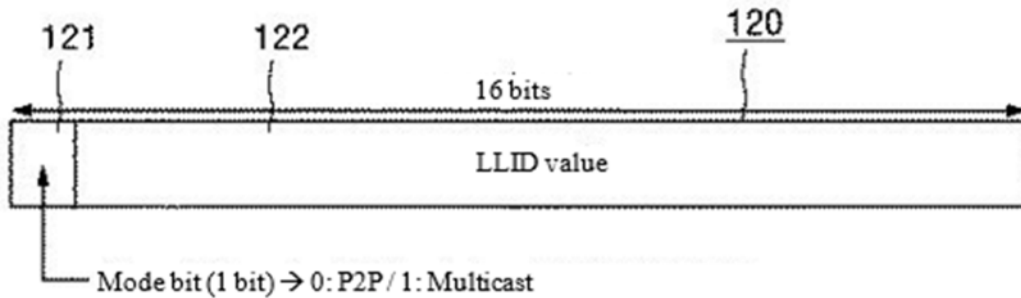
**Multicast Management Table 19**

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

EX1005, Fig. 3.

“A logical link is identified by an LLID value, which is a unique identifier in PON.” EX1003, ¶76 (citing EX1005, [0018]). “The LLID is defined in the preamble for the MAC frame and consists of 16 bits that include a mode bit, as shown in Figure 10.” *Id.* Murakami’s Figure 10 depicts this data structure:

Figure 10

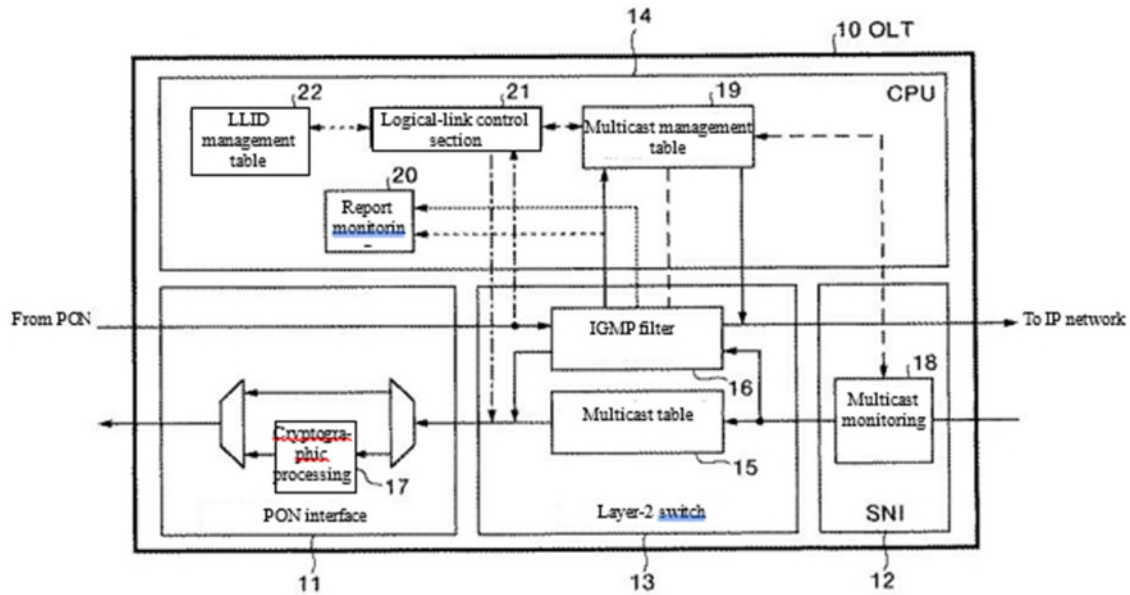


EX1003, ¶76 (citing EX1005, Fig. 10).

These logical links are bearer channels. EX1003, ¶ 77. They bear the multicast communications downstream to ONUs. *Id.* The '378 Patent acknowledges that a “logical channel” identified by a “logical link identification (LLID)” constitutes a “bearer channel.” *Id.* at ¶77 (citing EX1001, 4:4-8 (“Said bearer channel is a logical channel of the PON, and it can be the general encapsulation model (GEM) channel born by the GPON port **or the logical link identification (LLID) channel** of the EPON port[.]”) (emphasis added)).

Murakami further discloses encrypting multicast service data of all multicast services communicated in this bearer channel. According to Murakami, “PON interface 11 is provided with cryptographic processing section 17 for encrypting multicast data.” EX1003, ¶78 (citing EX1005, [0023]). The structure of the OLT, with its PON interface, is depicted in Figure 1:

Figure 1



EX1005, Fig. 1.

The OLT encrypts all data of all multicast services communicated in a particular bearer channel (*i.e.*, logical link) with a key. EX1003, ¶79. Murakami describes encrypting all multicast frames received from the IP-network and destined for a particular multicast group with a key before transmitting them via the logical links. *Id.* “[M]ulticast data arriving from SNI interface 12 are forwarded to the access port . . . , **encrypted with the encryption key corresponding to the multicast communication concerned (the encryption key corresponding to the encryption**

**key index<sup>3</sup> in the entry whose destination IP address matches the IP multicast address in the Multicast Management Table),** and then transmitted to PON interface 11.” EX1003, ¶79 (citing EX1005, [0034] (emphasis added)); *see also id.* (citing EX1001, Claim 7). “Multicast Management Table 19” is stored on the OLT and managed by its CPU 14 using “report monitoring section 20.” EX1003, ¶79 (citing EX1005, [0024], [0031], Fig. 1).

The Multicast Management Table 19 records information for each multicast group denoted by a unique IP Group address. EX1003, ¶80. For each multicast group, Multicast Management Table 19 associates the ONUs in that group with the OLT physical ports to which they are connected, with the logical link on that port over which multicast communications are made to each particular ONU, and with the encryption key used to encrypt the multicast communications on that link. *Id.* (citing EX1005, [0025], Fig. 3).

An example of Multicast Management Table 19 is shown in Murakami’s Figure 3. Murakami explains “there are two access ports (ports 2 and 4) for the multicast communication with the destination IP address of ‘yyy.yyy.yyy.yyy,’ allowing access by a total of four ONUs[.]” EX1003, ¶81 (citing EX1005, [0025]). “For port 2,

---

<sup>3</sup> The value recorded in Table 19 for the encryption key is an “index,” with the actual encryption key being managed by cryptographic processing section 17 of PON interface 11. *Id.* at ¶79 (citing EX1005, [0025]).

the LLID of the multicast logical link is 100, and the encryption key is #1,” and “[f]or port 4, the LLID of the multicast logical link is 110, and the encryption key is #3.” *Id.*

Figure 3

**Multicast Management Table 19**

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

EX1005, Fig. 3.

In other words, all data for the different group multicast services communicated via link 100 to ONUs 1 and 3 (as denoted by their point-to-point LLIDs) is encrypted with encryption key #1 and all multicast data for all services communicated via link 110 to the remaining two ONUs is encrypted with encryption key #3. A POSA would understand that Murakami discloses that all multicast data for all different multicast services transmitted on the same bearer channel (LLID 100 or

110) to ONUs that are members of a multicast group is encrypted with the same encryption key. EX1003, ¶82.

To the extent Murakami does not explicitly disclose delivery in a logical link (*i.e.* bearer channel) of all multicast data from *different* sources encrypted with a common key, such a disclosure would have been implicit in Murakami, or 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. EX1003, ¶78-100.

RFCs 1112 and 4601 teach that (1) a multicast group is defined by an IP multicast address, (2) the content of communications to each such multicast group can be drawn from different services, and (3) all data packets from these different services are sent to members of the group. EX1003, ¶83. RFCs 1112 and 4601 are prior art pursuant to 35 U.S.C. ¶103(b). Each was published more than one year before the earliest claimed priority date for the '378 Patent.

RFCs 1112 and 4601 are both from the same field of endeavor as the '378 Patent. *See Netflix, Inc. v. DivX, LLC*, 80 F.4th 1352, 1358 (Fed. Cir. 2023) (noting that one test used to define the scope of analogous art is “whether the art is from the same field of endeavor, regardless of the problem addressed”). The '378 Patent relates to the field of multicast communications. EX1003, ¶84 (citing EX1001, 1:7-10) (noting that invention relates to communication of multicast service data). Both RFCs relate to the composition of multicast communications and protocols relating

to its transmission. EX1003, ¶84 (citing EX1006, 1 (RFC 1112 describing “IP multicasting”); EX1007, 4 (describing a protocol for routing communications to multicast groups)).

Murakami expressly notes that it employs IGMP, including versions 1 and 2. EX1003, ¶85 (citing EX1005, [0027]). RFC 1112 describes what a POSA would understand to be version 1 of the Internet Group Management Protocol (IGMP). EX1003, ¶85 (citing EX1006, 11-15). IGMP Version 2 is defined in similar terms in the successor RFC 2362. EX1003, ¶85 (citing EX1010). RFC 4601 specifically implements the service model initially described in RFC 1112. EX1003, ¶85 (citing EX1007, 6 (“Like all multicast routing protocols that implement the service model from RFC 1112[3], PIM-SIM must be able to route data packets from sources to receivers without either the sources or receivers knowing a priori of the existence of the others.”)).

Murakami’s architecture and RFC 1112’s multicasting model are consistent. Similar to the ’378 Patent’s description, RFC 1112 also characterizes “IP multicasting” as the transmission of an “IP datagram” to a “‘host group,’ a set of zero or more hosts identified by **a single IP destination address**.” EX1003, ¶86 (citing EX1006, 1 (emphasis added)); *compare* EX1001, Fig. 3 (showing members of multicast group identified by single IP group address). RFC 4601 expressly implements the service model described in RFC 1112. EX1003, ¶86 (citing EX1007, 6).

RFC 4601 describes the implementation of RFC 1112's service model by means of a configuration nearly identical to that of Murakami. RFC 4601 describes transmitting multicast data to a router that has been configured as a "root" for the multicast group. EX1003, ¶87 (citing EX1007, 4-6 (describing multiple sources transmitting multicast data to a Rendezvous Point (RP))). As depicted above, Murakami similarly describes use of a multicast router 42 delivering multicast data to OLT 10 received from a data delivery server 45 in an IP network 43. EX1003, ¶87 (citing EX1005, Fig. 4); *id.* at ¶96 (citing EX1005, [0026] (noting that describes an infrastructure for receiving multicast data from a plurality of sources); EX1007, 4, 6, and 8 (describing a "multicast receiver" that communicates with a "local router" that forwards "join messages" (*i.e.* expressions of interest in receiving multicast traffic) to a router configured to be used as a root of the "non-source specific" distribution)).

The RFCs are properly considered analogous art. EX1003, ¶88; *Netflix*, 80 F.4th at 1359 (explaining analogous requires no more than that references share a general field of endeavor).

At least as early as August 1989, RFC 1112 disclosed to a POSA that multicast communications can be composed of data from a plurality of sources. Ex1003, ¶89. As noted above, RFC 1112 confirmed that "IP multicasting" involves transmission

of an IP datagram to “a single IP destination address” representing one or more recipients (*i.e.* hosts). *Id.* (citing EX1006, 1). Any number of sources may direct such IP datagrams to this single destination address. *See, e.g., id.* (noting IP datagrams can be sent by sources other than those constituting hosts).

RFC 4601 in turn further confirms that the implementation of the IGMP model described in RFC 1112 includes multicast data drawn from a plurality of sources. EX1003, ¶90 (citing EX1007, 4 (“This document specifies a protocol for efficiently routing multicast groups that may span wide-area (and inter-domain) internets.”)). In fact, in the earlier versions of IGMP referenced by Murakami, a receiver joining a multicast group was not permitted to opt out of receipt of **all** multicast communications. EX1003, ¶97 (citing EX1007, 7 (noting that expanded IGMPv3 now “permits a receiver to join a group and specify that it only wants to receive traffic for a group if that traffic comes from a particular source”)).

RFC 4601 further explains that IGMPv3 maintained functionality permitting a host to receive **all** multicast data from a plurality of sources. For example, hosts seeking to join a multicast group can issue a request to “join[] group G **for all sources to that group.**” EX1003, ¶90 (citing EX1007, 6 (emphasis added)). Data sent by this plurality of sources is ultimately distributed to hosts (recipients) via a *shared tree*—“shared” because it is employed “**by all sources sending to that group.**” *Id.* (citing EX1007, 6 (emphasis added)).

Data from these different sources constitutes multicast service data of different multicast services, as recited in the claims. EX1003, ¶91. During prosecution of the '378 Patent, the applicant acknowledged that different multicast “data streams” equated to multicast service data of different multicast services. *Id.* (citing EX1002, 352 (arguing that nowhere did He encrypt “all multicast data streams” carried in a single bearer channel, as required by the claims). A POSA would understand, and it would have been obvious to such a person, that multicast data transmitted from a plurality of different sources can and would encompass data relating to different multicast services. *Id.* In view of the RFC disclosures that *multiple different sources* (*i.e.* a plurality of different data streams) can send data packets to the *same* multicast group, a POSA would understand that Murakami’s multicasting communications can involve *different* multicast services sent to the *same* multicast group. Murakami’s OLT transmits all of these multicast services on the *same* multicast LLID/bearer channel, encrypting them with the same key. *Id.*

A POSA would have been understood from Murakami’s reference to use of IGMP that its multicast communications comprised different multicast services originate from a plurality of sources. Moreover, A POSA would also have been motivated to employ the systems and methods described in Murakami to communicate multicast data encompassing different multicast services, as described in these

RFCs. EX1003, ¶92. A “motivation to combine may be found explicitly or implicitly in market forces; design incentives; the ‘interrelated teachings of multiple patents’; ‘any need or problem known in the field of endeavor at the time of invention and addressed by the patent’; and the background knowledge, creativity, and common sense of the person of ordinary skill.” *ZUP, LLC v. Nash Mfg., Inc.*, 896 F.3d 1365, 1371 (Fed. Cir. 2018) (quoting *Plantronics, Inc. v. Aliph, Inc.*, 724 F.3d 1343, 1354 (Fed. Cir. 2013)).

Murakami described a system intended for the secure communication of multicast communications to multicast groups and a POSA would have been motivated to communicate known configurations of such multicast data, drawn from different sources as described in these RFCs. EX1003, ¶93. Murakami did not suggest restricting its system to a single source of data and/or a single multicast service. *Id.* Doing so would render Murakami’s system incompatible with published industry protocols. EX1003, ¶94.

As discussed above, the Internet Group Management Protocol (IGMP) discussed in these RFCs and implemented in Murakami’s system, encompassed communication of a plurality of multicast data services to recipients via a single group IP address. EX1003, ¶93 (citing EX1005, [0003]). A POSA would have been motivated to employ such a system to communicate conventional configurations of multicast data, such as data drawn from different sources as described in these RFCs. *Id.*

A POSA would have been motivated 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 and to deliver that data to a subscriber in a single bearer channel more efficiently. *Id.* A POSA would employ Murakami's system to deliver encrypted data of all different multicast services in its bearer channel because doing so would ensure compatibility with published standards protocols, such as RFC 4601, as so that it could enjoy the benefits of the advances in IGMP standards (*i.e.* IGMPv3). *Id.* A POSA would also have been motivated to employ the IGMP protocols described in RFC 4601, with its retained ability to join all sources of different multicast services, because the advances provided by RFC 4601 also enabled more selection of more selective data sources. *Id.* As discussed below, Murakami's system and methods are compatible with multicast data consisting of different multicast services and are employable with more recent IGMP standards. *Id.*

Indeed, a POSA would not have undertaken to differentiate multicast data composed of data from a plurality of sources based upon its source. EX1003, ¶94. Nor would a POSA have otherwise sought to differently encrypt that data based upon its original source. *Id.* Murakami's disclosures (*e.g.* data entries reflected in Multicast Management Table 19) do not contemplate differentiating between sources of multicast data received by multicast router 42 and transmitted to OLT 10. *Id.* Doing

so would have required Murakami's system to monitor the source addresses of multicast communications and establish either unique logical links for each source, or different encryption keys therefor, or both. *Id.* Such an arrangement would require establishing more than one logical channel for each port devoted to multicast content originating each different source, unnecessarily multiplying the number of logical channels, adding unneeded complexity to the establishment and maintenance of such channels, and pointlessly increasing processing overhead. *Id.* Alternatively, separately encrypting data based upon its source, multiplies the number of unique keys needed to encrypt these multicast communications, increases the complexity surrounding the generation, assignment, maintenance of the keys securing such communications, complicates the process of decryption that now must assess the data's origin to determine the proper key for decryption, and unnecessarily increases the processing overhead at both the OLT and ONU which must differentiate content based upon source and process differently with respect to the keys used to encrypt/decrypt. *Id.*

A POSA would have reasonably expected success in combining data from these different services in the multicasting made to ONUs on a particular bearer channel, and in encrypting that data with the key disclosed in Murakami. EX1003, ¶95. A reasonable expectation is shown where a POSA could have combined the elements as claimed by known methods with no change in their respective functions,

and the combination would have yielded nothing more than predictable results. *See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 416 (2007).

Murakami describes an infrastructure that can receive multicast data from a plurality of sources for communication to ONUs. Ex1003, ¶96. Consistent with the architecture recited in RFC4601, Murakami explains that the IP network 43 streams multicast data from data delivery servers 45 to the multicast router 42, where it is passed to the OLT. EX1003, ¶96 (*compare* EX1005, [0026] (“multicast data 45 from data delivery server 44 in IP network 43 reaches multicast router 42 connected to OLT 10”) *with* EX1007, 4, 6, and 8 (describing a “multicast receiver” that communicates with a “local router” that forwards “join messages,” *i.e.* expressions of interest in receiving multicast traffic, to a router configured to be used as a root of the “non-source specific” distribution)).

Murakami also employs the IGMP protocols incorporated in RFC 4601. EX1003, ¶97 (citing EX1005, Fig. 4 and [0027]; EX1007, 6 (noting that the PIM-SM protocol routes packets from sources to receivers in a manner consistent with the service model described in RFC 1112)). In fact, earlier versions of IGMP explicitly referenced by Murakami did not permit a host joining a multicast group to opt out of receiving all different multicast communications. EX1003, ¶97 (citing EX1007, 7 (noting that expanded IGMPv3 now “permits a receiver to join a group

and specify that it only wants to receive traffic for a group if that traffic comes from a particular source”)).

A POSA would have reasonably expected success in combining data from these different services in the multicasting made to ONU’s on a particular bearer channel, and in encrypting that data with the key disclosed in Murakami. EX1003, ¶95; *see KSR Int’l Co.*, 550 U.S. at 416 (reasonable expectation shown where POSA could have combined the elements as claimed by known methods with no change in their respective functions, and the combination would have yielded nothing more than predictable results). Murakami describes an infrastructure for receiving multicast data from a plurality of sources for communication to ONUs. EX1003, ¶96. As depicted above, Murakami describes use of a multicast router 42 connected to a data delivery server 45 in an IP network 43. *Id.* at ¶87 (citing EX1005, Fig. 4). Consistent with the descriptions in RFC4601, Murakami explains that the IP network streams multicast data to the multicast router 42, where it is passed to the OLT. *Id.* at ¶96 (*compare* EX1005, [0026] (“multicast data 45 from data delivery server 44 in IP network 43 reaches multicast router 42 connected to OLT 10”) *with* EX1007, 4, 6, and 8 (describing a “multicast receiver” that communicates with a “local router” that for-wards “join messages” (i.e., expressions of interest in receiving multicast traffic) to a router configured to be used as a root of the “non-source specific” distribution))).

Murakami also employed IGMP protocols. EX1003, ¶97 (citing EX1005, Fig. 4 and [0027]). As discussed above, these IGMP protocols contemplated multicast data from different sources (*i.e.* services). *Id.* at ¶93 (citing EX1007, 4 (noting that the ability to selectively receive multicast data from different sources not introduced until IGMPv3). Moreover, as discussed above, Murakami’s architecture could accommodate the newer version of IGMP which maintained the ability for a host to join all different multicast services.

Murakami’s encryption key is a “common key.” EX1003, ¶98. It is a single key used both to encrypt and decrypt the multicast data communicated on a particular bearer channel. This would have been evident to a POSA from Murakami’s discussion of sharing the key used to encrypt the information with the ONUs for purposes of decrypting that information. *Id.*

Murakami explains that when an ONU registers with the OLT as a member of a multicast group, the OLT accesses the Multicast Management Table 19 to determine if there already exists an ONU communicating on the same physical port who is a member of this multicast group. EX1003, ¶99 (citing EX1005, [0029]). If so, the OLT adds an entry to the Multicast Management Table 19 associating the newly registered ONU with the multicast group address. *Id.* (citing EX1005, [0035]-[0036]). The entry also associates the ONU with the physical port on which such multicast group communications are to occur. *Id.* (citing EX1005, [0037]). The

LLID of the logical link on which it and the other previously registered ONUs are to receive the multicast data is denoted for the new ONU. *Id.* The entry made in the Multicast Management Table 19 also specifies the index number of the encryption key to be used for transmissions of multicast data on this logical link to the previously registered and newly registered ONUs. *Id.* (citing EX1005, [0039]). The OLT then “transmits [that encryption key] to the point-to-point logical link 41” connecting the OLT with the particular, newly registered ONU. *Id.* **The ONU uses the same encryption key to decrypt the received multicast data.** *Id.* (citing EX1005, Claim 5 (“after setting up the multicasting logical link, uses a point-to-point logical link pre-set for the aforementioned subscriber-side unit to distribute an encryption key, which is to be used in the aforementioned multicast logical link”)).<sup>4</sup>

Thus, Murakami discloses using a common key to encrypt multicast service data of all *different* multicast services in a same bearer channel and then sending the encrypted data, and/or a POSA would have considered it obvious to use a common key to encrypt multicast service data of all different multicast services in a same bearer channel and then send the encrypted data, based upon the disclosures in Murakami, RFCs 1112 and 4601, and his knowledge. EX1003, ¶100.

---

<sup>4</sup> Murakami describes a similar process where the registering ONU is the first to register on a particular port as a member of a multicast group. EX1003, ¶99, n.3 (citing EX1005, [0029-0031]).

**Element 1[c]:** 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

Murakami discloses this element and/or a POSA would have considered it obvious based upon the disclosures in Murakami, RFCs 1112 and 4601, and his knowledge. EX1003, ¶101; *see* Element 1[b], above.

**Element 1[d]:** 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.

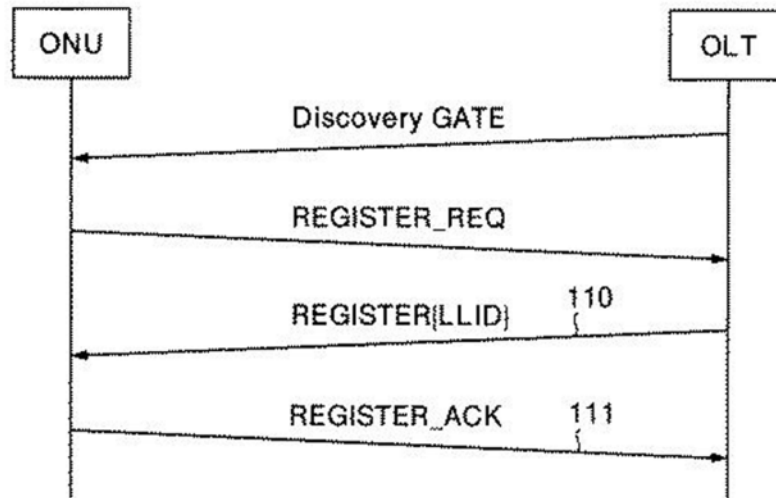
Murakami discloses this element. EX1003, ¶102. Murakami communicates the common key to an ONU only after it has been activated successfully and applies to receive the multicast service. *Id.*; *see* Element 1[b], above. Indeed, the applicant made no claim of novelty for this step. *Id.* (citing EX1001, 5:17-19 (“the specific procedure of registration and multicast service application has been defined relevantly in the EPON protocol and will be omitted here”) and 4:51-53 (“the specific procedure of registration and multicast service application has been defined relevantly in the GPON protocol and will be omitted here”)).

For example, Murakami describes an OLT which receives a report message at interface 11 from an ONU. EX1003, ¶103. The OLT snoops this message using IGMP filter section 16. *Id.* (citing EX1005, [0045]). The OLT 10 snoops the message

“to control the setting of logical links for multicasting” and to “distribute encryption keys for use in multicast communication.” *Id.* (citing EX1005, 1(57)).

The OLT 10 captures “report messages” from the ONU which also have a MAC frame destination address that is a multicast address. EX1003, ¶104 (citing EX1005, [0027]). In this manner, the ONU applies to receive multicast services via the OLT from the multicast router 42. *Id.* “OLT 10 then sets up a multicast logical link for the ONU that has made access.” *Id.* (citing EX1005, [0030]). The OLT transmits REGISTER message 110 containing said LLID to point-to-point logical link 41 of the ONU concerned. EX1003, ¶104 (citing EX1005, [0031] and Fig. 9). “The ONU concerned, upon receipt of the REGISTER message 110, uses the LLID stored in message 110 as the LLID of the multicast logical link and transmits REGISTER\_ACK message 111”, confirming that REGISTER message 110 has been correctly received. *Id.* (citing EX1005, [0031]). These exchanges are illustrated in Figure 9, below:

Figure 9



*Id.* (citing EX1005, Fig. 9).

Only after the ONU has thus been activated successfully does the OLT now communicate the appropriate encryption key. EX1003, ¶105 (citing EX1005, [0032] (“Now, said encryption key may be included in REGISTER message 110.”). The REGISTER message is encrypted to prevent the stored encryption key from being eavesdropped by another ONU not authorized to receive the multicast data. *Id.* The encryption key is communicated to the ONU on a point-to-point logical link established between the OLT and the particular ONU different from the logical link on which the OLT will communicate multicast data to the ONU. *Id.* A POSA would understand that this point-to-point logical link is “a management control channel,” EX1003, ¶105.

A POSA would understand in view of these disclosures that Murakami discloses that the OLT sends the common key applied in encrypting the multicast service data via a management control channel to an ONU *that is activated successfully* and who *applies to receive said multicast service data*. EX1003, ¶106.

The method recited in Claim 1 would have been obvious to a POSA at least as early as the date of RFC 4601's publication. EX1003, ¶107.

## 2. Claim 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. |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Murakami discloses this element. EX1003, ¶108; see Elements 1[b] and 1[d], above. To the extent that Murakami does not expressly disclose use of the common key to decrypt the multicast service data, such use would have been obvious to a POSA based upon Murakami's disclosures and the knowledge of a POSA. *Id.*

A POSA would have understood that Murakami discloses a system in which an ONU is the terminus of communications with a subscriber receiving multicast communications. EX1003, ¶109 (citing EX1005, [0057] (noting that an ONU may, but need not, accommodate multiple user network interfaces (*i.e.* subscriber ports))). In such a case, the ONU must necessarily decrypt the multicast communication intended for the recipient associated with that ONU for the multicast communication for the multicast communication to be of any use for that subscriber. *Id.*

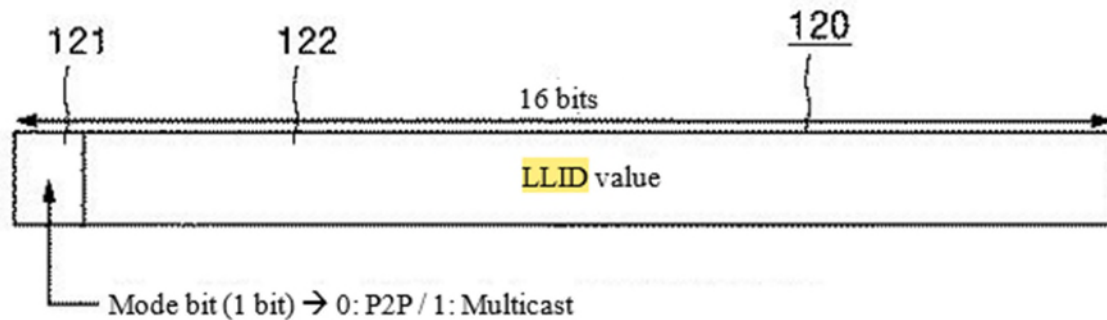
The method recited in Claim 2 would have been obvious to a POSA at least as early as the date of RFC 4601's publication. EX1003, ¶110.

### 3. Claim 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.

Murakami discloses this element. EX1003, ¶111; *see also* Claim 2, above. Murakami discloses that the OLT sends the ONU a bearer channel identification of the bearer channel where all multicast service data are encrypted with the common key. *Id.* Murakami describes sending each successfully activated ONU who has applied to receive multicast service data a “REGISTER message 110 containing the LLID thus selected,” informing it of the bearer channel upon which multicast service data will be transmitted. *Id.* (citing EX1005, [0037]-[0038] (“upon receipt of the REGISTER message 110, [the ONU] uses the LLID stored in said REGISTER message 110 as the LLID of the multicast logical link”) and [0018] (“The LLID is selected in the OLT and notified to the ONU.”)). The structure of the message sent by the OLT to the ONU is illustrated in Figure 10 and depicts the inclusion of the LLID identifying the bearer channel:

Figure 10



EX1003, ¶111 (citing EX1005, Fig. 10 (yellow annotation added)).

The method recited in Claim 4 would have been obvious to a POSA at least as early as the date of RFC 4601's publication. EX1003, ¶112.

#### 4. Claim 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.

Murakami discloses the elements of Claim 6. EX1003, ¶113. Murakami describes the step of an OLT actively 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. *Id.*; see also Element 1[d] and Claim 4, above.

Murakami discloses that this step may comprise ONU sending a key request to the OLT, and said OLT both judging and detecting that the ONU is activated successfully and applies to receive the multicast service data, then the OLT actively sending the common key applied in encrypting said multicast service data to the ONU. EX1003, ¶114; *see also* Element 1[d] and Claim 4, above.

The method recited in Claim 6 would have been obvious to a POSA at least as early as the date of RFC 4601's publication. EX1003, ¶115.

## **5. Claim 7**

|                                                                                                                                           |
|-------------------------------------------------------------------------------------------------------------------------------------------|
| The method of claim 1, wherein: the multicast service data in different bearer channels use different common keys or the same common key. |
|-------------------------------------------------------------------------------------------------------------------------------------------|

Murakami discloses this element. Murakami discloses that different bearer channels (*e.g.* LLIDs 100 and 110) use different common keys (*e.g.* Encryption Key #1 and Encryption Key #3). EX1003, ¶116; *see* Element 3[d], above. The method recited in Claim 7 would have been obvious to a POSA at least as early as the date of RFC 4601's publication. *Id.*

## **6. Claim 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. |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Murakami discloses this element. EX1003, ¶117; *see also* Claim 4, above. The method recited in Claim 8 would have been obvious to a POSA at least as early as the date of RFC 4601’s publication. *Id.*

**7. Claim 9**

**a. Element 9[a]**

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;

Murakami discloses this element. EX1003, ¶118. Murakami discloses a device for encrypting multicast service in a passive optical network system. *Id.*; *see also* Element 1[a], above.

Murakami discloses such a system having an encryption unit and a sending unit. EX1003, ¶119; *see also* Element 9[b]-9[c], below.

Murakami discloses such a system having a key generation unit configured to generate a common key. EX1003, ¶120. The term “key generation unit” is properly construed in accordance with 35 U.S.C. §112, paragraph 6 (pre-AIA). Claim terms that fail to recite sufficiently definite structure or else recites function without reciting sufficient structure for performing that function, are to be construed as encompassing only that specific structure disclosed in the patent’s specification that is clearly linked with the performance of the recited function. *See Williamson v. Citrix Online, LLC*, 792 F.3d 1339, 1349 (Fed. Cir. 2015). The words of the claim are

understood by POSAs to have a sufficiently definite meaning as the name for structure, although that structure may cover a broad class of structures. *See Apex Inc. v. Raritan Computer, Inc.*, 325 F.3d 1364, 1372-73 (Fed. Cir. 2003). While there is a presumption that a claim term is not a means-plus-function limitation if it does not employ the term “means,” this presumption is overcome if the claim terms merely serve as a generic placeholder and thus does not limit the scope of the claim to any specific manner or structure for performing the claimed function. *See Williamson*, 792 F.3d at 1349. The construction of such terms is limited to what a POSA would understand from the specification constitutes the corresponding structure, material, or acts clearly linked or associated with the claimed function. *See B. Braun Medical Inc., v. Abbott Laboratories*, 124 F.3d 1419, 1424 (Fed. Cir. 1997).

The limitation “key generation unit” would not have been understood by a POSA at the time of the priority date as having a sufficiently definite meaning as a name for particular structure or class of structures. Ex1003, ¶122. The limitation recites the function of key generation, without reciting sufficient structure for generating a key. *Id.*

In the ’378 Patent specification, the only structure explicitly linked to the performance of the key generating function is the OLT. EX1003, ¶124 (citing EX1001, Abstract (“an Optical Line Terminal (OLT) generating a public key”), 1:66-67 (same), 2:13 (same), 3:48, 61-62 (same), Figs. 1-4 and accompanying discussion

(same)). Whether or not construed pursuant to §112, paragraph 6, however, the patent specification acknowledges that at least an OLT constitutes the claimed key generation unit. Ex1003, ¶125.

As discussed above, Murakami discloses an OLT that generates a common key. Ex1003, ¶126; *see also* Element 1[a], above.

**b. Element 9[b]**

|                                                                                                                                                                     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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; |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Murakami discloses this element. EX1003, ¶127. Murakami discloses a device for encrypting multicast service in a passive optical network system having an encryption unit configured to encrypt multicast service data of all different multicast services born in a same one bearer channel with a same common key. *Id.* at ¶131; *see also* Element 1[b], above.

The term “encryption unit” is properly construed in accordance with 35 U.S.C. §112, paragraph 6 (pre-AIA). EX1003, ¶128. In the ’378 Patent specification, the only structure explicitly linked to the performance of the encrypting function is the OLT. EX1003, ¶129 (citing EX1001, Abstract (“an Optical Line Terminal (OLT) generating a public key, and using the public key to encrypt the multicast service data in a bearer channel”), 1:66-2:1 (same), 2:13-16 (same), 3:48-49, 61-65 (same), Figs. 1-4 and accompanying discussion (same)). Whether or not construed

pursuant to §112, paragraph 6, however, the patent specification acknowledges that at least an OLT constitutes the claimed encryption unit. EX1003, ¶130.

As discussed above, Murakami discloses an OLT that encrypts multicast service data of all different multicast services borne in a same one bearer channel with a same common key. EX1003, ¶131; *see* Element 1[b], above.

**c. Element 9[c]**

|                                                                                                                                                                                                                                                                                                             |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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. |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Murakami discloses this element. EX1003, ¶132. Murakami discloses a device for encrypting multicast service in a passive optical network system having an encryption unit configured to encrypt multicast service data of all different multicast services born in a same one bearer channel with a same common key.

The term “sending unit” is properly construed in accordance with 35 U.S.C. §112, paragraph 6 (pre-AIA). EX1003, ¶133. In the ’378 Patent specification, the only structure explicitly linked to the performance of the sending function is the OLT. EX1003, ¶134 (citing EX1001, Abstract (“an Optical Line Terminal (OLT) . . . transmitting the encrypted data . . . and said OLT sending the public key”), 1:66-2:4 (same), 2:13-18 (same), 3:47-52 (same), Figs. 1-4 and accompanying discussion

(same)). Whether or not construed pursuant to §112, paragraph 6, however, the patent specification acknowledges that at least an OLT constitutes the claimed sending unit. EX1003, ¶135.

As discussed above, Murakami discloses an OLT that sends the encrypted multicast service data, as well as sends 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. EX1003, ¶136; *see also* Element 1[d], above.

The device recited in Claim 9 would have been obvious to a POSA at least as early as the date of RFC 4601's publication. EX1003, ¶137.

## **8. Claim 11**

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>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.</p> |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Murakami discloses this element. EX1003, ¶138. Murakami discloses a device recited in Claim 9. *Id.*; *see also* Claim 9, above.

Murakami describes the step of an OLT actively 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. EX1003, ¶139; *see also* Claim 6 and Element 1[d], above.

Murakami discloses that this step may comprise ONU sending a key request to the OLT, and said OLT both judging and detecting that the ONU is activated successfully and applies to receive the multicast service data, then the OLT actively sending the common key applied in encrypting said multicast service data to the ONU. EX1003, ¶140; *see also* Claim 6 and Element 1[d], above.

The device recited in Claim 11 would have been obvious to a POSA at least as early as the date of RFC 4601's publication. EX1003, ¶141.

## **9. Claim 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. |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Murakami discloses this element. EX1003, ¶142. Murakami discloses the device recited in Claim 9. *Id.*, ¶143; *see also* Claim 9, above. Murakami discloses a device having a said sending unit configured to send the common key to the ONU which is activated successfully and applies to receive the multicast service data. *See* Claim 11, above.

Murakami discloses a device having a sending unit configured to send the common key to the ONU which is activated successfully and applies to receive the multicast service data. EX1003, ¶143; *see also* Claim 11, above.

Murakami also discloses that the sending unit (OLT) sends the ONU a bearer channel identification of the bearer channel where all multicast service data are encrypted with the common key. EX1003, ¶144; *see also* Claim 4, above.

The device recited in Claim 12 would have been obvious to a POSA at least as early as the date of RFC 4601's publication. EX1003, ¶145.

**10. Claim 13**

**a. Element 13[a]**

|                                                                                                                                                                                                 |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Murakami discloses this element. EX1003, ¶146. Murakami discloses the device recited in Claim 11. *Id.*; *see also* Claim 11, above. Murakami also discloses the device having a sending unit (OLT) configured to send the common key to the ONU which is activated successfully and applies to receive the multicast service data. EX1003, ¶147; *see also* Claim 11, above.

**b. Element 13[b]**

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

Murakami discloses this element. EX1003, ¶148. Murakami discloses the device's sending unit (OLT) is also configured to send the ONU a bearer channel identification of the bearer channel where all multicast service data are encrypted with the common key. *Id.*; *see also* Claim 12, above.

The device recited in Claim 13 would have been obvious to a POSA at least as early as the date of RFC 4601's publication. EX1003, ¶149.

**C. Ground 2: Claims 3, 8, 11 are Obvious in light of JP2004-343243A in view of RFCs 1112 and 4601 and knowledge of persons of skill, and in further view of U.S. Patent Appl. 2002/0150097 A1 (“Yen”)**

**1. Claim 3**

**a. Element 3[a]**

|                                                                                                                                 |
|---------------------------------------------------------------------------------------------------------------------------------|
| The method of claim 2, further comprising: said OLT generating the common key and setting an aging time for the common key, and |
|---------------------------------------------------------------------------------------------------------------------------------|

Murakami discloses the OLT generating the common key. Ex1003, ¶150; *see also* Elements 1[b] and 1[d], above. Murakami discloses the method recited in Claim 2, and/or such a method would have been obvious to a POSA at the time of Murakami's publication. *Id.*; *see also* Claim 2, above.

A POSA would have deemed it obvious to set an aging time for the common key based upon the disclosures in Murakami in view of Published U.S. Patent Appl. 2002/0150097 A1 (“Yen”). EX1003, ¶151. Yen was published October 17, 2002, and is prior art under 35 U.S.C. §103(e). EX1008, 1(43). Yen is analogous prior art.

EX1003, ¶151. It is from the same field of endeavor as Murakami and the invention and is also reasonably pertinent to the particular problem with which the inventor is involved (*i.e.*, securing multicast communications). EX1003, ¶151 (citing EX1008, [0002] (“The present invention is directed to a method and apparatus for secured multicasting [in a PON].”)); *see also Netflix*, 80 F.4th at 1358. Yen describes a “multicasting churning key scheme [that] provides privacy against eavesdropping by unauthorized or potentially malicious third parties.” EX1003, ¶151 (citing EX1008, [0018]; *compare* EX1001, 7:50-58 (describing invention’s concerns with malicious users stealing the multicast service content)).

Yen’s churning key is the equivalent of the claimed common key. EX1003, ¶152. According to Yen, its churning key may be sent by the OLT to all ONUs authorized to receive the multicast broadcast for subsequent use by each ONU in descrambling the multicast communication. *Id.* (citing EX1008, [0027] (“However, prior to transmitting the scrambled message to all the subscribing ONTs, the OLT preferably sends to all the other subscribing ONTs the group leader ONT’s churning key.”) and [0029] (“OLT selects **a common, multicast, churning key** and sends the churning key to all the subscribing ONTs.”) (emphasis added)).<sup>5</sup>

---

<sup>5</sup> While Yen describes soliciting the churning key from the lead ONU, rather than initially generating it via the OLT, this distinction is irrelevant to Yen’s teachings of

(Footnote Continued . . .)

Yen further discloses setting a “key interval” at the time a churning key is distributed. EX1003, ¶153 (citing EX1008, [0016] (teaching that a “churning key is then updated at a given churning **key interval**”) (emphasis added) and [0031] (noting that the key interval is set by the OLT)).

A POSA would have been motivated to add Yen’s key aging feature to Murakami’s system and method in order to further ensure secure communication. EX1005, ¶154. Murakami expressed concerns that subscriber authorizations could become stale and proposed, in that circumstance, that authorization expire. *Id.* (citing EX1005, Claim 8, [0028] (describing the maximum response-time field that specifies the maximum amount of waiting time before a report message is received), and [0048] (explaining that system entries in Multicasting Management Table 19 are deleted for ONUs that have failed to respond within a particular interval)).

---

securing that distributed key against malicious users by means of predetermined obsolescence. EX1003, ¶152, n.5. In addition, while Yen includes embodiments in which the ONUs instead receive a value representing the difference between a churning key suggested by each ONU and that suggested by the lead ONU, by which each ONU is then able to calculate the lead ONU’s churning key, this represents merely an alternative embodiment. *Id.*

A POSA would have been motivated to periodically change the common key to defeat efforts to hack the system to gain access. For example, sunsetting decryption keys reduces the time available to hackers seeking to mount a successful brute-force attack. EX1003, ¶155.

Dr. Rouskas provides an analogy. In the movie *The Imitation Game* Alan Turing and his British colleagues attempt to break the German's enigma code during World War II. Their efforts to crack this code through typical cryptographic techniques proves futile, however, because each day the Germans reset the code, rendering the preceding progress towards breaking that code useless. In other words, the Germans set a twenty-four (24) hour aging time for the key where, after the aging time arrived, a new key was generated. EX1003, ¶156.

A POSA would have been motivated to incorporate Yen's key aging method to further protect the multicast communications against unauthorized interception, and to ensure that only ONU's in authorized communication with the OLT remain recipients of multicast communications. EX1003, ¶157. Applying Yen's aging method to the common key also necessitates that the key be regenerated once its aging time has elapsed, so that communications may continue with the multicast group. EX1003, ¶158.

A POSA would have reasonably expected that Murakami's system and methods could have been modified to incorporate Yen's sunsetting feature. EX1003,

¶159. A POSA would have reasonably expected that Murakami’s system and methods could have been modified to incorporate Yen’s sunsetting feature. Murakami describes a system capable of soliciting responses from ONUs concerning their authorization and desire to receive multicast communications (*i.e.* Query messages). *Id.* (citing EX1005, [0004] (noting that in widely used methods “[a] multicast router ***periodically*** multicasts query messages (Query messages) and acknowledges its members by the presence or absence of report messages (Report messages) from each host”) (emphasis added)). A POSA would have known to schedule such a communication by the OLT upon the expiration of a pre-set interval, and to invoke its key generation process as if the ONUs were newly applying for access. *Id.* (citing Ex1005, [0027]-[0041] (describing process of populating Multicast management Table 19 with entries relating to members of multicast group and the generation of encryption keys for same)).

**b. Element 3[b]**

|                                                                     |
|---------------------------------------------------------------------|
| after the aging time arrives, it regenerating a new common key, and |
|---------------------------------------------------------------------|

This element would have been obvious to a POSA in light of the disclosures in Murakami in view of Yen. EX1003, ¶160. Murakami discloses the ability of the OLT to generate new common keys for use in encrypting multicast communications. *Id.* (citing EX1005, [0027]-[0041] (“OLT 10 generates a new encryption key used

in this multicast communication[.]”)). Yen teaches the establishment of a key interval upon the expiration of which the OLT will establish a new “churning key” and distribute that key to all affected ONUs for use in decrypting multicast communications. *Id.* (citing EX1008, [0031] (disclosing that upon the expiration of the key interval, the OLT establishes a new churning key and “then send[s] to all the subscribing ONTs the new churning key as the updated multicast key”) and 1(57) (“[T]he central network device [*i.e.*, OLT] periodically updates the multicast encryption key[.]”)).

For the reasons set for the above in connection with Element 3[a], a POSA would have been motivated to regenerate a new common key upon expiration of the aging time and would have expected that such a facility could have been incorporated into the system/method disclosed in Murakami. EX1003, ¶161.

**c. Element 3[c]**

|                                                                                           |
|-------------------------------------------------------------------------------------------|
| using the new common key to encrypt the multicast service data in the bearer channel, and |
|-------------------------------------------------------------------------------------------|

This element would have been obvious to a POSA in light of the disclosures in Murakami in view of Yen. EX1003, ¶162. As noted above, Murakami discloses the use of a common key to encrypt multicast services data in the bearer channel. *See* Elements 1[a]-1[d]. Yen teaches the establishment of a time for updating such a key. *Id.*; *see also* Elements 3[a]-3[b].

**d. Element 3[d]**

sending the new common key to the ONU that is activated successfully and applies for the multicast service data.

This element would have been obvious to a POSA in light of the disclosures in Murakami in view of Yen. EX1003, ¶163. As noted above, Murakami discloses sending a common key to ONUs that are successfully activated and who apply to receive the multicast service data. *Id.*; *see also* Elements 1[a]-1[d]. Yen similarly teaches the updating of such a key and its distribution to ONUs that have been activated successfully and who have applied to receive multicast service data. *Id.*; *see also* Elements 3[a]-3[b].

For the reasons set for the above in connection with Element 3[a], a POSA would have been motivated to send the new common key to the ONU that is activated successfully and applies for the multicast service data in order that such an ONU could decrypt those communications. EX1003, ¶164; *see also* Claim 2, above.

The method recited in Claim 3 would have been obvious to a POSA at least as early as the date of RFC 4601's publication. EX1003, ¶165.

**2. Claim 5**

**a. Element 5[a]**

The method of claim 1, further comprising: said OLT generating the common key and setting an aging time for the common key, and

Murakami discloses this element. EX1003, ¶166; *see* Element 3[a], above.

**b. Element 5[b]**

after the aging time arrives, it regenerating a new common key, and

Murakami discloses this element. EX1003, ¶167; *see* Element 3[b], above.

**c. Element 5[c]**

using the new common key to encrypt the multicast service data in the bearer channel, and

Murakami discloses this element. EX1003, ¶168; *see* Element 3[c], above; *see also* Element 1[b], above.

**d. Element 5[d]**

sending the new common key to the ONU that is activated successfully and applies for the multicast service data.

Murakami discloses this element. EX1003, ¶169; *see* Element 3[d], above.

The method recited in Claim 5 would have been obvious to a POSA at least as early as the date of RFC 4601's publication. EX1003, ¶170.

**3. Claim 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.

Murakami discloses this element. EX1003, ¶171. Murakami discloses a device recited in Claim 9. *Id.*; *see* Claim 9, above.

Murakami discloses such a system having an aging time setting unit 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. EX1003, ¶172. The limitation “aging time setting unit” would not have been understood by a POSA at the time of the priority date as having a sufficiently definite meaning as a name for particular structure or class of structures. *Id.* at ¶173. The limitation recites the function of setting an aging time, without reciting sufficient structure for doing so. *Id.* The term “aging time setting unit” is properly construed in accordance with 35 U.S.C. §112, paragraph 6 (pre-AIA).

In the ’378 Patent specification, the only structure explicitly linked to the performance of the aging time setting unit function is the OLT. EX1003, ¶174 (citing EX1001, 2:13 (“said OLT generating the public key and setting an aging time for the public key”), 3:61-63 (same), Fig. 2 and accompanying discussion (same)). Whether or not construed pursuant to §112, paragraph 6, however, the patent specification acknowledges that at least an OLT constitutes the claimed aging time setting unit. EX1003, ¶175.

Yen discloses an OLT sets an aging time or the common key. EX1003, ¶176; *see* Element 3[a], above. As discussed above, it would have been obvious to a POSA based upon the disclosures in Murakami and Yen to have an OLT that is notified of the expiration of an aging time in order that it regenerates a common key. EX1003, ¶176; *see* Element 3[a]-[b], above.

The method recited in Claim 10 would have been obvious to a POSA at least as early as the date of RFC 4601's publication. EX1003, ¶178.

**D. No Evidence of Sufficient Secondary Factors**

The “ultimate determination of whether an invention is obvious is a legal question based on the totality of the evidence.” *See Brown & Williamson Tobacco Corp. v. Philip Morris, Inc.*, 229 F.3d 1120, 1131 (Fed. Cir. 2000). In its recent Complaint, PO has pointed to no evidence, such as “commercial success[,] long felt but unsolved needs[,] and failure of others,” as indicia of non-obviousness.<sup>6</sup> Nor can a lack of invention cannot be outweighed by secondary factors. *Id.* The Petition overwhelmingly demonstrates that the claims of the '378 Patent are not novel and are invalid as obvious.

**X. CONCLUSION**

For the reasons set forth above, there is a reasonable likelihood that at least one of the challenged claims is unpatentable. Petitioner respectfully requests *inter partes* review of Claims 1-13 be instituted and that those claims be cancelled.

---

<sup>6</sup> PO must also demonstrate a nexus between any secondary considerations and the purported invention. *See Ormco Corp. v. Align Tech., Inc.*, 463 F.3d 1299, 1311-12 (Fed. Cir. 2006). This the PO has similarly not done.

Dated: August 9, 2024

Respectfully submitted,

/s/ Raymond R. Ricordati III, Reg. No. 62,856  
Raymond R. Ricordati III (Reg. No. 62,856)  
rricordati@marshallip.com  
Lead Counsel for Petitioner

Thomas L. Duston  
tduston@marshallip.com  
Back-up Counsel for Petitioner  
(*pro hac vice* pending)

Customer No. 04743

MARSHALL, GERSTEIN & BORUN LLP  
233 South Wacker Drive  
6300 Willis Tower  
Chicago, Illinois 60606-6357  
Telephone: (312) 474-6300

MGBLitDocket@marshallip.com

**CERTIFICATE OF WORD COUNT**

Pursuant to 37 C.F.R. §42.24(d), Petitioner hereby certifies, in accordance with and reliance on the word count provided by the word-processing system used to prepare this Petition, that the number of words in this paper is 12,747. Pursuant to 37 C.F.R. §42.24(d), this word count excludes the table of contents, table of authorities, mandatory notices under §42.8, certificate of service, certificate of word count, appendix of exhibits, and any claim listing.

Dated: August 9, 2024

/s/ Raymond R. Ricordati III, Reg. No. 62,856  
Raymond R. Ricordati III (Reg. No. 62,856)  
Lead Counsel for Petitioner  
MARSHALL, GERSTEIN & BORUN LLP

**CERTIFICATE OF SERVICE**

The undersigned hereby certifies pursuant to 37 CFR § 42.6(e) and § 42.105 that on August 9, 2024, a true and correct copy of the foregoing “PETITION FOR *INTER PARTES* REVIEW” was served via UPS (Tracking No. 1Z0964W3NT92392149) on the Patent Owner at the following correspondence address of record as listed in the USPTO electronic filing system:

199393 - Atlantic IP  
c/o Lombard Geliebter LLP  
1325 Avenue of the Americas, 28th Floor  
New York, NY 10019

and was served via electronic mail upon counsel of record for the Patent Owner in the litigation in the U.S. District Court for the Eastern District of Texas:

*Iarnach Technologies Ltd. v. Charter Communications, Inc., et al.,  
Case No. 2:24-cv-00230*

Amir H. Alavi - aalavi@aatriallaw.com  
Demetrios Anaipakos - danaipakos@aatriallaw.com  
Masood Anjom - manjom@aatriallaw.com  
R. Allan Bullwinkel - abullwinkel@hpcllp.com  
Deron R. Dacus – ddacus@dacusfirm.com  
Eric J. Enger - eenger@hpcllp.com  
Andrea L. Fair - andrea@wsfirm.com  
Lily Rebecca Glick - lglick@hpcllp.com  
J. David Hadden – dhadden@fenwick.com  
Alden Harris - aharris@hpcllp.com  
Michael F. Heim - mheim@hpcllp.com  
Steven T. Juggle - sjuggle@aatriallaw.com  
Blaine A. Larson - blarson@hpcllp.com  
Christopher L. Larson – clarson@fenwick.com  
Michael D. McBride - mmcbride@aatriallaw.com

Christopher R. Pinckney - rpinckney@ aatriallaw.com  
Saina Shamilov – sshamilov@fenwick.com

/s/ Raymond R. Ricordati III, Reg. No. 62,856

Raymond R. Ricordati III (Reg. No. 62,856)

Lead Counsel for Petitioner