NOTE: This disposition is nonprecedential.

United States Court of Appeals for the Federal Circuit

TREND MICRO INC.,
Appellant

v.

CUPP COMPUTING AS,
Appellee

KATHERINE K. VIDAL, UNDER SECRETARY OF COMMERCE FOR INTELLECTUAL PROPERTY AND DIRECTOR OF THE UNITED STATES PATENT AND TRADEMARK OFFICE,
Intervenor

2020-2237, 2020-2238

Appeals from the United States Patent and Trademark Office, Patent Trial and Appeal Board in Nos. IPR2019-00561, IPR2019-00641.

Decided: October 25, 2022

STANLEY JOSEPH PANIKOWSKI, III, DLA Piper LLP (US), San Diego, CA, argued for appellant. Also represented by ROBERT BUERGI, MARK D. FOWLER, East Palo Alto, CA.

JAMES R. HANNAH, Kramer Levin Naftalis & Frankel LLP, Redwood Shores, CA, argued for appellee. Also represented by PAUL J. ANDRE; CRISTINA MARTINEZ, JEFFREY PRICE, New York, NY.

BENJAMIN T. HICKMAN, Office of the Solicitor, United States Patent and Trademark Office, Alexandria, VA, for intervenor. Also represented by KAKOLI CAPRIHAN, THOMAS W. KRAUSE, FARHEENA YASMEEN RASHEED.

Before DYK, TARANTO, and STARK, *Circuit Judges*.

TARANTO, *Circuit Judge*.

Trend Micro Inc. filed petitions in the Patent and Trademark Office seeking inter partes reviews (IPRs) under 35 U.S.C. §§ 311–19 of certain claims of two patents owned by CUPP Computing AS—claims 1, 7, and 16 of U.S. Patent No. 8,365,272 and claims 1, 6, and 7 of U.S. Patent No. 9,756,079. The PTO's Patent Trial and Appeal Board, after instituting and conducting the requested reviews, issued final written decisions holding each claim 1 to be unpatentable but rejecting Trend Micro's challenges to claims 7 and 16 of the '272 patent and claims 6 and 7 of the '079 patent. *Trend Micro Inc. v. CUPP Computing AS*, No. IPR2019-00561, 2020 WL 3709007, at *1 (P.T.A.B. July 6, 2020) (*IPR561 Decision*); *Trend Micro Inc. v. CUPP Computing AS*, No. IPR2019-00641, 2020 WL 3697863, at *1 (P.T.A.B. July 6, 2020) (*IPR641 Decision*). Trend Micro appeals the Board's holding regarding claims 7 and 16 of the '272 patent and claim 7 of the '079 patent. We vacate the Board's final written decisions on each appealed claim and remand.

I

A

The '272 patent is the grandparent of the '079 patent, so we cite only to the former's specification (replicated in relevant part in the latter). The specification discusses aspects of communication between (a) a computer (or a particular application on the computer) that is part of a particular network (*e.g.*, the computer's home network) and (b) computers or applications outside that network (*e.g.*, on a public network). In particular, it recognizes that such a computer or application may have an "internal" (*e.g.*, home-network) address that, for one or more reasons, should not be included as the source (originating) address in a communication sent outside that network.

Computers often communicate with one another using packets that adhere to an Internet Protocol, *i.e.*, using IP packets. Such a packet includes a header that contains a source IP address and a destination IP address, which typically identify the source and destination computers. The packet may also include source and destination port numbers to identify source and destination applications within the source and destination computers. IP addresses and port numbers are important for reliably communicating, by initial message and reply, between the source and intended destination.

Such reliable communication can be impaired when a computer that is part of a local (home) network is assigned an IP address that is unique within that network (for use in internal-to-the-network communication) but that is not unique within a broader public network (because another computer outside the local network may be using it). To deal with the problem, and its counterpart problem for non-unique port numbers, when a packet from such a local-network computer is destined for an external computer, the source's internal-network IP address and port number in the outgoing packet are often translated, before leaving the

local network, and replaced with a public-source IP address and port number that are (at the time) unique within the public network. This process is referred to as network address translation (NAT) and port address translation (PAT)—collectively, NPAT. Such translations can achieve the uniqueness needed for reply communication by the external computer and can protect the security and privacy of the internal-network computer and application addresses by situating the NPAT-processing unit as a firewall intermediary in the line of reply communication.

Computers must obtain public IP addresses from somewhere, and there are various means for doing so. For example, a computer administrator could manually assign an IP address. Commonly, though, computers use Dynamic Host Configuration Protocol (DHCP) to get an IP address, for use as a source address in outgoing packets, within a given network. Under DHCP, computers request IP addresses for use as public-source IP addresses in outgoing packets and receive (potentially renewable) leases for addresses for set times.

The parties agree that claims 7 and 16 of the '272 patent and claim 7 of the '079 patent deal specifically with outgoing communications from a computer application to addresses in networks that are external to the originating network, with such communications including a source address (useful to enable an eventual reply) and a destination address. In particular, the claims recite "dynamically isolating" the internal address of a computer application from an external network by translating the application's internal address so as to include a different origination address in the message sent to a computer outside the home network.

Claim 16 of the '272 patent reads:

> 16. A method within a computer of processing outgoing data, the method comprising:

> receiving the outgoing data from an application, the application being associated with an internal address;
>
> translating, using a network address translation engine within the computer, the internal address into a public address;
>
> routing, using a driver within the computer, at least a subset of the outgoing data to an external network using the public address, *thereby dynamically isolating the internal address from the external network*; and
>
> providing, using a network interface within the computer, the subset of the outgoing data to the external network.

'272 patent at col. 26, lines 37–48 (emphasis added). Claim 7 of the '079 patent reads:

> 7. A system comprising:
>
> a network interface configured to be coupled to an external network;
>
> a firewall in communication with the network interface, the firewall configured to perform both network-level security and application-level security on incoming data packets, the firewall being further configured to reject the incoming data packets if the incoming data packets include malicious content according to a security policy, the firewall being configured to allow the incoming data packets to pass to one or more applications if the incoming data packets do not include malicious content according to the security policy;
>
> a computer system in communication with the firewall, the computer system having one or more applications associated with at least one application address, the computer system being

> configured to send to the firewall outgoing data packets including an application identifier identifying a particular application of the one or more applications to the firewall; and
>
> an address translation engine configured to translate the at least one application address associated with the particular application of the one or more applications to an external address, *thereby dynamically isolating the particular application of the one or more applications from the external network*.

'079 patent, col. 26, lines 4–29 (emphasis added). Claim 7 of the '272 patent, col. 25, lines 34–57, is a system claim that is similar, for purposes of these appeals, to claim 7 of the '079 patent. And the parties have not shown that the "dynamically isolating" limitations of the three claims at issue differ from each other in any way material to these appeals, so we use the singular and refer to the "dynamically isolating" limitation.

B

In its IPR petitions, Trend Micro asserted that the claims are unpatentable under 35 U.S.C. § 103 (2008)[1] because their subject matter would have been obvious, at the relevant priority date in 2007, over certain combinations of prior-art references that include WO2006/069041 (Sikdar), which was published on June 29, 2006, and is undisputedly prior art. In addressing the "dynamically isolating"

---

[1] The parties do not dispute the Board's determination, *IPR561 Decision* at *6 n.5; *IPR641 Decision* at *6 n.6, that, for both patents at issue, the applicable version of § 103 is the version pre-dating the Leahy-Smith America Invents Act, Pub. L. No. 112-29, § 3(n)(1), 125 Stat. 293 (2011).

limitation of claims 7 and 16 of the '272 patent and claim 7 of the '079 patent—the claims on appeal now—Trend Micro asserted that Sikdar teaches that limitation. *See IPR561 Decision* at *13–15, 19–20; *IPR641 Decision* at *19–21. In ultimately rejecting Trend Micro's challenge to these three claims, the Board's sole stated basis was that Trend Micro failed to show that teaching in Sikdar. *IPR561 Decision* at *13–15, 19–20; *IPR641 Decision* at *19–22.[2]

In reaching that conclusion, the Board relied on a claim construction now accepted as correct by both parties. The Board construed "dynamically isolating" in its institution decisions *sua sponte* (applying the standard of *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc)), and it stated in its final written decisions that it was maintaining its earlier construction. J.A. 2139–41; *IPR561 Decision* at *7–10. It construed the phrase "as including the use of DHCP or other source of addresses in connection with a NAT engine to translate IP addresses." *IPR561 Decision* at *8. It added that the phrase "further refer[s] to an operation that occurs 'when and as needed.'" *Id.* With respect to the latter aspect, the Board explained that the term "dynamically" modifies "isolating," *id.* at *9, so that translation that occurs "beforehand, at device configuration[,] . . . would not be dynamic," *id.* The parties accept that construction on appeal. Opening Br. at 26–28; Response Br. at 18; Reply Br. at 5; Oral Arg. at 12:31–13:20.

The issue on appeal is whether, as the Board ultimately found, Sikdar fails to disclose what that construction requires. Sikdar discloses in relevant part a Reconfigurable Semantic Processor (RSP) capable of performing NAT and PAT. J.A. 836–39. The RSP, Sikdar

---

[2] The Board's construction of "dynamically isolating" and its obviousness analysis with respect to this claim limitation are the same in the two IPRs. We hereafter cite only to the Board's rulings in IPR2019-00561.

teaches, "can be programmed for NAT/PAT operations that convert IP addresses and/or port numbers for packets traveling thru the firewall 1062 between public IP addresses that are used for transporting the packet over public network 12 and private IP addresses that are used for transporting the packet over the private network 24." J.A. 836. The RSP in Sikdar includes a Semantic Processing Unit (SPU). J.A. 795–96, 914. Sikdar states that the SPU "generates the public IP address and port number for the packet" and that "the public IP address is usually the IP address assigned to firewall 1062." J.A. 838. Sikdar further states, regarding that embodiment, that there are typically "multiple unique private IP addresses associated with different network processing devices operating in private network 24" and that "only one, or a few, public IP addresses may be used to represent the multiple private IP addresses." *Id.* Sikdar also discloses an alternative embodiment, in which one-to-one mapping occurs, disclosing that "one or more IP addresses have an associated individual public IP address." J.A. 837.

In finding that Sikdar does not disclose the "dynamically isolating" limitation, the Board found that Sikdar uses the same public IP address, *i.e.*, the address of the firewall, as the source (originating) address for all outgoing communications and does not disclose the source from which Sikdar obtains that public IP address. *IPR561 Decision* at *14. In making that determination, the Board found that the SPU in Sikdar does not "actually" generate the public IP address used as the source address in outgoing packets. *Id.* Based on those findings, the Board determined that Sikdar does not disclose the translation of IP addresses "using DHCP or other source of addresses." *Id.* The Board also noted that Sikdar does not satisfy the "dynamically isolating" limitation because its "public IP address is not determined 'on the fly'" and because, "[i]nstead, the same firewall IP address is used." *Id.*

C

Trend Micro timely appealed the Board's final written decisions. We have jurisdiction under 28 U.S.C. § 1295(a)(4) and 35 U.S.C. §§ 141(c), 319.

II

We review the Board's legal conclusions de novo and its factual findings for substantial-evidence support. *Dynamic Drinkware, LLC v. National Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015). "A finding is supported by substantial evidence if a reasonable mind might accept the evidence to support the finding." *Id.* Obviousness is a question of law based on underlying findings of fact, including what the prior art teaches. *See*, *e.g.*, *In re Warsaw Orthopedic, Inc.*, 832 F.3d 1327, 1329-31 (Fed. Cir. 2016).

As we have noted, the parties agree that the Board's express construction of the claims—requiring "the use of DHCP or other source of addresses in connection with a NAT engine to translate IP addresses" and "an operation that occurs 'when and as needed'"—is correct. We need only decide whether substantial evidence supports the Board's finding that Sikdar does not disclose "dynamically isolating" under that construction. *See Seal-Flex, Inc. v. Athletic Track & Court Construction*, 172 F.3d 836, 842 (Fed. Cir. 1999) (accepting as correct a construction adopted by the district court that the parties did not dispute on appeal). We conclude that the Board's finding is not supported by substantial evidence. We do not see, and CUPP has not pointed us to, any evidence that would permit a reasonable finding that Sikdar fails to teach "dynamically isolating" under the agreed-on construction. We therefore reject that Board finding regarding Sikdar, as we have done in other cases where the evidence presented could not reasonably support a Board finding. *See*, *e.g.*, *Becton, Dickinson & Co. v. Baxter Corp. Englewood*, 998 F.3d 1337, 1340–42 (Fed. Cir. 2021); *Corning v. Fast Felt*

Corp., 873 F.3d 896, 901–03 (Fed. Cir. 2017); *Belden Inc. v. Berk-Tek LLC*, 805 F.3d 1064, 1077 (Fed. Cir. 2015).

Sikdar clearly discloses "the use of DHCP or other source of addresses in connection with a NAT engine to translate IP addresses." This claim construction does not require the use of DHCP or a source that is, in some narrowing way, similar or comparable to DHCP. By its broad terms, this construction simply requires any source of addresses—"DHCP or other source of addresses." Sikdar teaches this aspect of the claim construction in several ways: It discloses that the SPU "generates" the public IP address, says that this address is "usually" the address "assigned to" the firewall, and describes, in an alternative embodiment, a one-to-one mapping of private and public addresses. J.A. 837–38. These disclosures teach a "source of addresses in connection with a NAT engine to translate IP addresses."

In finding otherwise, the Board found that Sikdar does "not actually" generate the public IP address because "the public IP address is simply the firewall's public IP address," *IPR561 Decision* at *14, so that "Sikdar discloses using the same IP address (the IP address of the firewall) for all packets traveling from the private network to the public network," *id.* But even if Sikdar were limited to using an unvarying public IP address (of the firewall), it still falls within the claim construction, which nowhere requires variability of the swapped-in public IP address from packet to packet. Indeed, the Board explicitly rejected CUPP's initial argument to build into a claim construction a requirement that would "involve[] addresses that are not 'predetermined.'" *Id.* at *9. After all, as the Board explained, "dynamic" in the claim phrase refers to the act of translating (converting, swapping), not to variability of replacement addresses among packets. *Id.*

The Board's finding that, in Sikdar, "the public IP address is simply the firewall's public IP address," *id.* at *14,

is also unsupported by substantial evidence. The referred-to portion of Sikdar says only that the swapped-in address is "usually" the public address assigned to the firewall—not always. J.A. 838. And what "usually" allows, and indeed suggests, an alternative embodiment in Sikdar makes explicit. Specifically, Sikdar teaches what the Board acknowledges was a one-to-one-mapping embodiment. *IPR561 Decision* at *14 n.11. The Board dismissed that embodiment as irrelevant, *id.*, but it offered, and CUPP has furnished, no reasonable basis for that dismissal. In that embodiment, each private address within Sikdar's private network is associated with a corresponding public address for use on the public network. J.A. 837. That embodiment teaches the use of different swapped-in addresses where there is more than one private address.

Sikdar also discloses that translation occurs "when and as needed." Sikdar discloses that translation (*i.e.*, the swapping of addresses) occurs when "a device 1078 operating in private network 24 . . . send[s] packet 1072 through firewall 1062 to a destination public network 12." *Id.* In particular, the RSP "receives packet 1072 from local device 1078 in private network 24 that contains a private IP address 1070," and "[i]f the packet 1072 is directed to an endpoint 1056 in public network 12, the RSP 100 converts the private IP address 1070 into a public address 1052 that is used to route packet 1050 over public network 12 to endpoint 1056." *Id.* This conversion of an address, described precisely as taking place when an outgoing packet is in transit, occurs "when and as needed"—as packets pass through the RSP and "if" the packet containing a private source IP address is destined for a public network.

The Board lacked a reasonable basis (and hence lacked substantial evidence on which) to find that Sikdar fails to teach this aspect of the claim construction. The Board, for this aspect of the claim construction as for the "source of address" aspect, relied on its finding that "the public IP address assigned to the packets is the IP address of the

firewall," and it added that the "public IP address is not determined 'on the fly.'" *IPR561 Decision* at *14. But this reasoning, besides overlooking the "usually" and one-to-one-mapping aspects of Sikdar (discussed just above), departs from the simple "when and as needed" language of the unchallenged claim construction. That language refers only to the timing of the act of conversion for an outgoing communication, *i.e.*, the act of replacing a private-source address in a packet by a different, public address as packets pass through the translation engine. Sikdar plainly teaches that process. The language "when and as needed" does not address how many different public addresses are used as the replacements or when the replacements are identified (as opposed to when they are actually swapped in).

The Board did not cite, and CUPP has not pointed us to, any expert testimony that would permit a reasonable finding that Sikdar fails to teach "dynamically isolating" under the agreed-on construction. CUPP's expert, Dr. Medvidovic, opined that "the Board should find the [']272 [p]atent valid over the cited prior art" because Trend Micro's expert, Dr. Jakobsson, "fail[ed] to provide any analysis that would support a finding that the cited reference disclosed or suggested the use of DHCP or *a similar dynamic* source of addresses in connection with NAT translation." J.A. 2289–90 (emphasis added). Dr. Medvidovic's reasoning rests on a claim construction that is contrary to the one the Board adopted (and CUPP does not challenge): His rationale mistakenly treats "dynamic" as modifying "source" rather than "isolating"; and it requires a source "similar" to DHCP. Dr. Medivodovic's declaration thus does not support the Board's finding.

Dr. Jakobsson, for his part, testified that "the public IP address is generated somewhere." J.A. 2904. That testimony certainly does not point against the evidence, discussed above, showing that Sikdar teaches what the claim construction requires. It therefore cannot provide

substantial-evidence support for the Board's finding. That is so whether or not the Board reasonably characterized Dr. Jakobsson's testimony in this respect as "conclusory," adding that the testimony does not identify "how the public IP address disclosed in Sikdar, namely, the IP address of the firewall, is sourced." *IPR561 Decision* at *14. Even if we accept the characterization, substantial evidence is lacking for the Board's finding about Sikdar. The Board relied on the mistaken firewall-only reading of Sikdar and imported a requirement of identifying the address source, rather than simply having an address source; and it disregarded the facial sufficiency of Dr. Jakobsson's point that, of course, there must be a source (whose character is not limited to one similar to DHCP).

For the foregoing reasons, we conclude that no substantial evidence supports the Board's finding that Sikdar does not disclose "dynamically isolating." Rather, as we have explained, Sikdar does teach that requirement under the Board's express construction, which the parties accept. Trend Micro does not, however, ask for reversal of the final written decisions as to the appealed claims on this basis. It seeks only vacatur and remand to allow the Board to address issues (relevant to the appealed claims) that the Board has not yet addressed. *See* Trend Micro Opening Br. at 55; Response Br. at 38–39; Oral Arg. at 0:55–3:01. We follow that course, with the claim construction of "dynamically isolating" and Sikdar's teaching of that claim limitation now settled.

III

The Board's final written decisions on each appealed claim is vacated, and the case is remanded for further proceedings consistent with this opinion.

Costs awarded to Trend Micro.

VACATED AND REMANDED