Trials@uspto.gov
571-272-7822

Paper 41
Entered: May 18, 2015

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

ERICSSON INC.,
Petitioner,

v.

INTELLECTUAL VENTURES I LLC,
Patent Owner.

Case IPR2014-00527
Patent 7,496,674 B2

Before JOSIAH C. COCKS, WILLIAM A. CAPP, and DAVID C. McKONE, *Administrative Patent Judges.*

CAPP, *Administrative Patent Judge.*

FINAL WRITTEN DECISION
35 U.S.C. § 318(a) and *37 C.F.R. § 42.73*

Ericsson Inc. ("Ericsson") filed a corrected Petition (Paper 8, "Pet.") requesting *inter partes* review of claims 1–22 of U.S. Patent No. 7,496,674 B2 (Ex. 1001, the "'674 patent"). We instituted an *inter partes* review of claims 1–22 of the '674 patent. Paper 11. After institution of trial, Intellectual Ventures I LLC ("Intellectual Ventures") filed a Patent Owner's Response (Paper 21, "PO Resp.") and Ericsson filed a Reply (Paper 28, "Reply").[1] This case is before the Board for a Final Written Decision following an Oral Hearing on the merits conducted April 15, 2015, the transcript for which is entered as Paper 40 ("Tr.").

After considering the evidence and arguments of counsel, we determine that Ericsson has met its burden of showing, by a preponderance of the evidence, that claims 1–22 of the '674 patent are unpatentable.

I. BACKGROUND

A. The '674 Patent (Ex. 1001)

The '674 patent, titled "System, Method, and Base Station Using Different Security Protocols on Wire And Wireless Portions of Network," relates to a method and apparatus for sending and receiving datagrams on wired and wireless portions of a network. Ex. 1001, claims 1, 13. The invention implements security protocols on transmissions over wired and wireless portions of the network. *Id.* A first security protocol is

[1] In its Patent Owner's Response, Intellectual Ventures asserts that Ericsson has failed to identify all real parties in interest. PO Resp. 2–3. This assertion is not supported by any evidence and, instead, merely alleges that we should draw an inference from the fact that Ericsson has named certain foreign affiliates as real parties in interest in other IPR proceedings. *Id.* Intellectual Ventures's contention is speculative in nature and will not be given further consideration in this Decision.

implemented on transmissions over the wired portion of the network. *Id.* A second and different security protocol is implemented over the wireless portion of the network. *Id.*

The invention employs a wireless base station. *Id*. The base station interfaces with both the wired and wireless portions of the network. *Id.* Processing of datagrams to implement the first and second security protocols is performed in the base station. *Id.*

B. Challenged Claims

Ericsson challenges claims 1–22. Claims 1, 13, and 18 are independent claims. Claim 1 (with paragraph indentation added) is reproduced below:

> 1. A method comprising:
>
> receiving a first packet from a wired data network in a wireless base station that is coupled to the wired data network,
>
> wherein the first packet is protected according to a first security protocol on the wired data network, and
>
> wherein a target device of the first packet communicates with a source of the first packet, at least in part, over a wireless network on which the wireless base station communicates;
>
> processing the first packet in the wireless base station according to the first security protocol;
>
> determining that the first packet is targeted at the target device, wherein the determining is performed by the wireless base station, and
>
> wherein the first packet comprises a header coded with address information identifying the target device; and
>
> applying a second security protocol employed on the wireless network to the first packet, wherein the second security protocol is different from the first security protocol, and wherein the applying is performed in the wireless base station.

C. The Asserted Grounds of Unpatentability

We instituted a trial on claims 1–22 of the '674 patent based on the alleged grounds of unpatentability set forth in the table below, as further supported by the Declaration of Armand M. Makowski, Ph.D. (Ex. 1013).

References	**Basis**	**Claims Challenged**
Stadler (Ex. 1003)[2]	§ 102	1–6 and 10–22
Stadler and Davison (Ex. 1010)[3]	§ 103	7–9
Rai (Ex. 1004)[4]	§ 103	1, 10–13, 17, 18, and 22
Rai and Davison	§ 103	2–9, 14–16, and 19–21

II. CLAIM INTERPRETATION

In an *inter partes* review, claim terms in an unexpired patent are given their broadest reasonable construction in light of the specification of the patent in which they appear. *See* 37 C.F.R. § 42.100(b); *In re Cuozzo Speed Techs., LLC*, 778 F.3d 1271, 1281–82 (Fed. Cir. 2015). Under the broadest reasonable interpretation standard, claim terms are given their ordinary and customary meaning as would be understood by one of ordinary skill in the art in the context of the entire disclosure. *In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007).[5]

---

[2] J. Scott Stadler and Jay Gelman, *Performance Enhancement for TCP/IP On a Satellite Channel*, 1 IEEE MILITARY COMMUNICATIONS CONFERENCE 270–76 (Oct. 19–21, 1998).

[3] U.S. Patent No. 6,829,242 B2 to Davison et al., titled *Method and Apparatus For Associating PVC Identifiers With Domain Names of Home Gateways*, issued Dec. 7, 2004.

[4] U.S. Patent No. 6,414,950 B1 to Rai et al., titled *Sequence Delivery of Messages*, issued July 2, 2002.

[5] Citing *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc).

1. "security protocol"

The term "security protocol" appears in each independent claim. In our Decision to Institute, we construed "security protocol" on a preliminary basis to mean a "protocol that provides protective measures for communications." Paper 11, 6. We explained that this construction is broad enough to encompass, but is not limited to, techniques for encryption, authentication, and other measures to protect the confidentiality of information. *Id.* At that time, we did not decide whether "tunneling" *per se* must be considered a "security protocol." *Id.*

Intellectual Ventures insists that the following construction, which was previously proposed in Patent Owner's Preliminary Response, should be adopted.

> Intellectual Ventures's proposed construction:
>
> "a protocol that provides security measures," where "security" means a condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences.

PO Resp. 4–5; Prelim. Resp. 3, 5. Apart from the claims, the term "security protocol" appears in the title of the '674 patent and appears only once in the specification in connection with a discussion of IPSec (Internet Protocol Security). Ex. 1001, 46:17–41. The term is not defined in the specification either expressly or by implication.[6] Intellectual Ventures concedes that the term is broad enough to encompass authentication and encryption techniques. PO Resp. 5.

[6] Intellectual Ventures concedes that the specification does not define "security protocol." PO Resp. 5.

Intellectual Ventures's primary concern appears to be that "security protocol" does not encompass "tunneling" *per se*. PO Resp. 5–11. Intellectual Ventures supports its position with quotations from an industry publication and testimony from its expert. *Id.* (quoting Ex. 2005, 54–55; Ex. 2015 ¶ 37 (Newman)).

Ericsson argues that a tunneling protocol satisfies the security protocol limitation in claim 1 because it allows an encrypted message to be sent over the Internet without revealing the source address or the destination address. Reply 12. Ericsson also argues that a tunneling protocol provides a protective measure in that it allows a destination address to avoid being stored on a router. *Id.* at 13. Ericsson, however, does not explain how or why merely avoiding storage of a destination address on a router protects a communication. Ericsson's position is undermined by its own evidence. For example, the Kagan article states that:

> IPSec is the preferred solution for IP environments, because it has security built in. PPTP and L2TP are most appropriate for multiprotocol environments, but both require additional support to deliver data privacy, integrity, and authentication.

Ex. 1007, 269.[7]

A court may revisit and alter its construction of claim terms as the record in a case develops. *See Pressure Prods. Med. Supplies, Inc. v. Greatbatch Ltd*, 599 F.3d 1308, 1322 (Fed. Cir. 2010). After receiving additional evidence and argument from the parties, we alter the preliminary construction of "security protocol" in our Decision to Institute to clarify that

[7] Richard S. Kagan, *Virtual Private Networks – New Strategies for Secure Enterprise Networking*, IEEE WESCON/98 CONFERENCE PROCEEDINGS 267–72 (Sept. 15–17, 1998) (Ex. 1007).

tunneling *per se* is not a security protocol. We are persuaded by Intellectual Ventures's evidence that tunneling merely provides an unsecured conduit for allowing third party communications to be carried over a public network such as the Internet. To the extent that tunneling is associated with secure communications, the security is provided by a feature or technique that may be used in conjunction with tunneling, such as encryption or authentication. However, the fact that security protocols may be used in conjunction with tunneling does not indicate that tunneling *per se* provides security. In other words, unsecure communication may occur via tunneling. If the sender or recipient desires to make such communication secure, a security feature must be used in conjunction with tunneling.

2. "packet"

The term "packet" is used in each independent claim of the '674 patent. Neither party proposed a construction for "packet" prior to our Decision to Institute. In their respective Patent Owner's Response and Petitioner's Reply, the parties proposed the following constructions.

Intellectual Ventures's proposed construction:

a header and a payload.

PO Resp. 13.

Ericsson's proposed construction:

a packet does not require a header.

Reply 3.

A claim construction analysis begins with, and is centered on, the claim language itself. *See Interactive Gift Express, Inc. v. Compuserve, Inc.*, 256 F.3d 1323, 1331 (Fed. Cir. 2001). In the claims, a packet is something that can be protected by a security protocol. Ex. 1001, claim 1. It can

comprise a header coded with address information identifying a target device. *Id.* It can be encrypted and decrypted. *Id.* at claim 2. It can be processed to authenticate its source. *Id.* at claim 3. It can be received from a wired data network. *Id.* at claim 18. It can be transmitted wirelessly. *Id.* at claim 10.

Claim terms generally are construed in accordance with the ordinary and customary meaning that they would have to one of ordinary skill in the art in light of the specification and the prosecution history. *See Aventis Pharma S.A. v. Hospira, Inc.*, 675 F.3d 1324, 1329 (Fed. Cir. 2012).[8] The person of ordinary skill in the art, through whose eyes a patent claim is construed, is deemed to read the claim term not only in the context of a particular claim in which the disputed term appears, but in the context of the entire patent, including the specification. *Phillips*, 415 F.3d at 1313. The overall context in which "packet" is used in the '674 patent relates to communication over packet switched networks, an alternative technology to circuit switch networks. Ex. 1001, 3:48–64.

> Packet switching makes more efficient use of available bandwidth than does traditional circuit switching. Packet switching breaks up traffic into so-called "packets" which can then be transported from a source node to a destination for reassembly.

Id.

In the context of the specification of the '674 patent, a packet can be subjected to data compression algorithms (Ex. 1001, 44:13–22) and encryption (*Id.* at 46:15–29). Particularly with respect to Intellectual

[8] The Federal Circuit imposes a stringent standard for narrowing a claim term beyond its plain and ordinary meaning. *Id.* at 1330 (citing *Thorner v. Sony Computer Entm't Am. L.L.C.*, 669 F.3d 1362 (Fed. Cir. 2012)).

Ventures's contention that a "packet" should be construed as a header and a payload, the specification indicates that an entity referred to as a packet can be created and brought into existence prior to being assigned a header.

> Packet switching breaks a media stream into pieces known as, for example, packets, cells or frames. Each packet *can then be* encoded with address information for delivery to the proper destination and can be sent through the network.

Ex. 1001, 30:33–36 (emphasis added).

> The packet-switched network instead breaks a message into pieces known as packets of information. Such packets *can then be* encapsulated with a header which designates a destination address to which the packet must be routed.

Ex. 1001, 34:9–12 (emphasis added).

In view of the foregoing, we will construe a "packet" as a piece or segment of a data/media stream that serves as a unit of transmission over a packet switched network. To the extent that the "packet" of claims 1, 13, and 18 is required to have a header, such requirement is imposed by the express claim language "comprises a header" and is not imposed by virtue of the definition of "packet" *per se*.

III. MOTIONS TO EXCLUDE EVIDENCE

Intellectual Ventures moves the Board to exclude the following exhibits from evidence: Ex. 1003, 1007, 1020, and 1021. Paper 32. Intellectual Ventures also moves to exclude excerpts from the cross-examination of its expert, Dr. Newman. *Id.* Ericsson opposes the motion. Paper 36. Intellectual Ventures replied to Ericsson's opposition. Paper 37.

A. Exhibit 1003 (Stadler)

Ericsson asserts Stadler, among other things, as an anticipation reference under 35 U.S.C. § 102 against claims 1–6 and 10–22. Pet. 18–31. Intellectual Ventures objected to Stadler on the grounds of hearsay and lack of authenticity. Ex. 2026. Intellectual Ventures now moves to exclude Stadler on such grounds. Paper 32.

1. Hearsay

On its face, Stadler appears to be a work that was sponsored by the Department of the Air Force. Ex. 1003, 1. In the lower left hand corner of the first page, it bears an IEEE copyright line. *Id.* The IEEE copyright line contains a publication date, a price, and what appears to be an ISSN code.[9]

Intellectual Ventures argues that Ericsson has not offered any admissible evidence that tends to establish that Stadler was available to the public before the filing date of the '674 patent. Paper 32, 1–2. Intellectual Ventures argues that the date information in Stadler is hearsay because it is submitted for its alleged truth. *Id.* at 3. Intellectual Ventures argues that Ericsson could have established a date of public availability through the submission of a librarian's declaration and, because Ericsson did not do this, we should presume that no admissible evidence exists that Stadler was publically available before the critical date.

Ericsson counters that the publication information provided by the IEEE establishes that Stadler was publically available in 1998. Paper 36, 5. We agree. We accept the publication information on the IEEE copyright

[9] Ex. 1003, 1 ("0-7803-4506-1/98/$10.00 © 1998 IEEE"). *See* IEEE Editorial Style Manual, IEEE Periodicals, © 2014 IEEE, page 8 (hereinafter "IEEE Style Manual").

line on page 1 of Stadler as evidence of its date of publication and public accessibility. IEEE is a well-known, reputable compiler and publisher of scientific and technical publications, and we take Official Notice that members in the scientific and technical communities who both publish and engage in research rely on the information published on the copyright line of IEEE publications. The information published on the copyright line of Stadler thus falls under an exception to the hearsay rule as lists, etc., generally relied on by the public or by persons in particular occupations. Fed. R. Evid. 803(17). [10]

As an alternative ground for admitting Exhibit 1003, we invoke the so-called "residual exception" of Federal Rule of Evidence 807. The copyright line of IEEE publications is added by IEEE as the publisher, not the author, and is added in accordance with the IEEE Style Manual. The assignment of a publication date in the copyright line of an IEEE publication has equivalent circumstantial guarantees of trustworthiness as with other exceptions to the hearsay rule. It is offered as evidence of a material fact, namely, whether Stadler predates the date of invention and is, therefore, prior art to the '674 patent. We consider the publication date on the copyright line to be more probative on the point for which it is offered than any other evidence that Ericsson could have obtained through reasonable efforts. In particular, we note our disagreement with Intellectual Ventures that a librarian's declaration would have been more probative of the publication date of Stadler than the publication date that IEEE published in

[10] We also note that the assignment of an ISSN or ISBN code by a publisher furnishes a circumstantial guarantee of trustworthiness sufficient to justify admission of otherwise hearsay evidence. *See* ADVISORY COMMITTEE NOTES to Fed. R. Evid. 803.

its copyright line on the face of Stadler. Finally, admitting Stadler as prior art in view of the publication date on the IEEE copyright line will best serve the purpose of the Federal Rules of Evidence and the interests of justice. An IPR proceeding may only be based on patents and "printed publications." 35 U.S.C. § 311(b). Allowing IPR petitioners to rely on the IEEE publication date in an IPR proceeding, which is an administrative proceeding designed and intended to afford expedited and efficient relief, serves the interests of justice.

2. Authenticity

Intellectual Ventures also challenges Stadler on the grounds of authenticity. Intellectual Ventures argues that Stadler appears to be an improper collection of documents. Paper 32, 5 (citing Fed. R. Evid. 1003).

Ericsson argues that Stadler is authenticated under Fed. R. Evid. 901(b), 902(6), or 902(7). Paper 36, 12. Ericsson argues that the standard for admissibility under Fed. R. Evid. 901(a) is slight. *Id.* (citing *United States v. Turner*, 718 F.3d 226, 232 (3d Cir. 2013)).

We are persuaded that Ericsson has laid a proper foundation for admission of Stadler. We are able to discern that Stadler itself consists of pages 270 through 276. *See* Ex. 1003. We are also able to discern that the three pages of web printout material that Ericsson appended to Exhibit 1003 is merely for the purpose of laying a foundation for the admission of pages 270–76 of Stadler.

In this case, Ericsson has laid a sufficient foundation to establish that Stadler is authentic under Fed. R. Evid. 901(b)(4). Copies of Stadler are immediately accessible to the public through IEEE's on-line library system. Intellectual Ventures's counsel concedes that there is no reason to believe

that the copy of Stadler introduced into the record by Ericsson has been forged or altered. Tr. 37–38.

For the foregoing reasons, Intellectual Ventures's motion to exclude Stadler is DENIED.

B. Exhibit 1020

Exhibit 1020 appears to be an abstract for Stadler (Ex. 1003) obtained from the IEEE Explore on-line library. It appears to be offered for no other reason than to establish a foundation for the admissibility of Stadler. Inasmuch as we have determined that Stadler is admissible apart from consideration of Exhibit 1020, we DENY Intellectual Ventures's motion to exclude Exhibit 1020 as MOOT.

C. Exhibit 1021

Exhibit 1021 is a declaration of an employee from the Ericsson's counsel's law firm. It appears to be offered for no other reason than to establish a foundation for the admissibility of Stadler. Inasmuch as we have determined that Stadler is admissible apart from consideration of Exhibit 1021, we DENY Intellectual Ventures's motion to exclude Exhibit 1021 as MOOT.

D. Kagan (Exhibit 1007)

Kagan, like Stadler, is an IEEE publication. Like Stadler, Kagan contains an IEEE copyright line on the bottom left hand corner of the first page. *See* Ex. 1007, 267. Intellectual Ventures and Ericsson exchange similar arguments with respect to Kagan as we have considered previously

with respect to Stadler above. For essentially the same reasons, we DENY Intellectual Ventures's motion to exclude Kagan.

E. Newman Deposition Testimony (Exhibit 1022: 39:13–40:8 and 43:10–44:3)

Intellectual Ventures moves to exclude portions of the cross-examination deposition testimony of its expert, Dr. Newman. Paper 32, 11–14. Intellectual Ventures argues that the testimony is excluded properly under Fed. R. Evid. 611(b) as outside the scope of direct examination. *Id.*

Courts are admonished to exercise caution in limiting the cross-examination of a witness whose credibility could have an important influence on the outcome of the trial. *See Harbor Ins. Co. v. Schnabel Co., Inc.*, 946 F.2d 930, 935 (D.C. Cir. 1991). In the testimonial excerpts under consideration, Dr. Newman repeatedly admitted a lack of familiarity with the subject matter of the '674 patent. *See, e.g.*, Ex. 1022, 39:16–17 ("I really haven't spent very much time looking at this . . . ."). This testimony goes to Dr. Newman's credibility and, therefore, does not exceed the proper scope of cross-examination.

Intellectual Ventures's motion to exclude the portions of the cross-examination testimony of Dr. Newman's deposition is DENIED.

IV. ANTICIPATION BY STADLER

To anticipate a patent claim under 35 U.S.C. § 102, "a reference must describe . . . each and every claim limitation and enable one of skill in the art to practice an embodiment of the claimed invention without undue experimentation." *Am. Calcar, Inc. v. Am. Honda Motor Corp.*, 651 F.3d 1318, 1341 (Fed. Cir. 2011) (citing *In re Gleave*, 560 F.3d 1331, 1334 (Fed.

Cir. 2009)). Anticipation of a patent claim is a question of fact. *In re Montgomery*, 677 F.3d 1375, 1379 (Fed. Cir. 2012). Ericsson contends that Stadler anticipates claims 1–6 and 10–22 of the '674 patent.

A. Stadler (Ex. 1003)

Stadler discloses a Wireless IP Suite Enhancer (WISE) system that implements the TCP/IP (Transmission Control Protocol / Internet Protocol) suite in a wireless environment. Ex. 1003, 273. Figure 1 of Stadler is reproduced below:

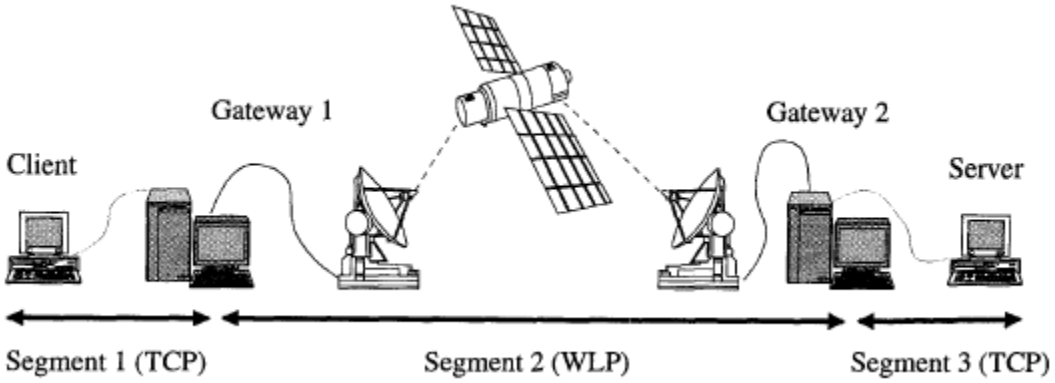

Figure 1 depicts a communication system divided into three segments, with a wired communication connection from a Client computer to Gateway 1, a wireless connection from Gateway 1 to Gateway 2, and a wired connection from Gateway 2 to a Server. *Id.*

In Stadler, the client-to-gateway and gateway-to-server segments use unmodified TCP/IP. *Id.* The client-to-gateway and gateway-to-server segments use IPSec as an encryption technique. *Id*. at 270. The gateway-to-gateway wireless segment uses a special Wireless Link Protocol ("WLP"). *Id.* at 273. Communications are converted from TCP to WLP upon entering the wireless sub-network and back to TCP upon exiting. *Id.* Stadler

discloses that encryption can be used to protect communications from eavesdropping during the wireless segment. *Id.*

B. Independent Claims 1, 13, and 18

1. The "packet" limitations

Intellectual Ventures essentially argues that Stadler does not anticipate claim 1 because it fails to transmit a "first packet" from the client to the server. PO Resp. 14–21. Intellectual Ventures contends that after a "first packet" arrives from the client at gateway 1, it ceases to exist and is replaced by a new and different packet that is constructed to be compatible with the wireless protocol that is used between gateway 1 and gateway 2. *Id.* at 19. Thus, according to Intellectual Ventures, Stadler does not apply a "second security protocol" to the "first packet," because the "first packet" ceases to exist before any "second security protocol" can be applied to it.

Ericsson argues that the identity and integrity of the original packets received at the first WISE gateway are preserved such that the same packet of data that is received at the WISE gateway over the wired link is the same packet of data that is transmitted over the wireless link. Reply 4–7.

Intellectual Ventures's "first packet" theory is predicated on a narrow interpretation of "packet" that we do not endorse. The better interpretation of Stadler is that after a first packet is received from the client at gateway 1, the first packet, including the header thereof, merely undergoes a transformation of form to facilitate its transmission over the wireless segment of the communication system. The information that is transmitted is not "new and different" as argued by Intellectual Ventures, rather, it is essentially the same information targeted at the same addressee as the original packet. Ex. 2017, 38:13–20 (Makowski) ("the final information will

always be there . . . the final destination is always carried somewhere as part of the encapsulation process").

Claim 1 contemplates that a packet will be "processed" in the wireless base station according to a first security protocol. Ex. 1001, claim 1. The claim also contemplates that a second security protocol is applied to the first packet at the wireless base station. *Id.* Claim 2 contemplates that the processing of the first security protocol at the wireless base station in accordance with claim 1 may entail decryption. *Id.* at claim 2. Claim 3 contemplates that the second security protocol that is applied at the wireless base station in accordance with claim 1 may entail encryption. *Id.* at claim 3. Thus, claim 1 contemplates that a "packet" will undergo processing that transforms the form of the packet without destroying its identity as a "packet."

2. Fragmentation

Intellectual Ventures next argues that the payloads that are transmitted over Stadler's wireless segments are not the same payloads transmitted over the wired segment. PO Resp. 21. Intellectual Ventures characterizes Stadler's disclosure of fragmenting the original packets transmitted over the wired segment into fragments for transmission over the wireless segment as forming entirely "new packets." *Id.* Intellectual Ventures supports its position with declaration testimony from Dr. Newman. Ex. 2015 ¶¶ 55–57 ("The clear indication based on 'fragmentation' is that the WLP packets do not have the same payload as received TCP packets.").

Ericsson replies that Stadler's fragmentation technique is no different than the time division multiplexing technique disclosed in columns 53 and 54 of the '674 patent. Reply 6. On cross-examination, Intellectual

Ventures's expert, Dr. Newman, was unable to explain how the fragmentation technique in Stadler differed, in any patentably distinct manner, from the time division multiplexing technique taught in the '674 patent. Ex. 1022, 37:3–44:24.

3. Applying a Second Protocol to the First Packet

Intellectual Ventures argues that Stadler fails to apply a second protocol to the first packet within the meaning of claims 1, 13, and 18. PO Resp. 25. This position is predicated on Intellectual Ventures's earlier position that Stadler deconstructs packets at the wireless gateway and then constructs new and different packets for transmission across the wireless segment. *Id.* Thus, according to Intellectual Ventures to the extent that Stadler discloses application of a second security protocol, it would not be applied to the same "first packet" received from the wired network. *Id.*

In reply, Ericsson points to portions of Stadler that disclose application of encryption to the data that is transmitted over the wireless link. Reply 7 (citing Ex. 1003, 275–76). Stadler discloses that it is advantageous to encrypt wireless transmissions in bulk. Ex. 1003, 275–76. We are persuaded that such bulk encryption over the wireless segment is sufficiently distinct from the IPSec encryption utilized over the wired segment to constitute a second security protocol. *Id.*

4. Determining, at the Wireless Base Station, that the First Packet is Targeted at the Target Device

Intellectual Ventures argues that Stadler fails to satisfy the determining step of claim 1. PO Resp. 26. Intellectual Ventures argues that

the claim language requires an active step not something that occurs passively. *Id.* at 28.

In reply, Ericsson points to cross-examination testimony from Dr. Newman that essentially concedes that the determining step is satisfied by Stadler. Reply 9; Ex. 1022, 57:6–58:9. Ericsson also relies on the following passage from Stadler as satisfying the determining step.

> The system operation is as follows. IP packets not containing TCP segments (or whose TCP headers cannot be read) that arrive at the periphery of the wireless network will go up the protocol stack to the IP layer where the standard routing functions will be performed. The packet will go down the protocol stack through the LLLL and over the wireless link. Any errors encountered during transmission will be corrected by the two peer LLLL layers transparently to IP. TCP packets on the other hand, will pass all the way up the protocol stack to the WISE server. Here the TCP connection will be terminated and a virtual circuit will be set up through the LLLL to the WISE server on the other side of the wireless link. This will cause the receiving WISE server to establish a TCP connection to the intended recipient. Once the connections are all established the data is passed over the wireless link to the receiving WISE server where it is relayed (via the TCP connection) to the intended recipient.

Reply 8; Ex. 1003, 274–75. We agree with Ericsson that Stadler's disclosure that it "will cause the receiving WISE server to establish a TCP connection to the intended recipient," is sufficient to satisfy the determining step.

5. Findings of Fact Regarding Claims 1, 13, and 18

To summarize the foregoing, the evidence presented by the parties supports the following findings of fact by a preponderance of the evidence:

1. Stadler packetizes a media stream and transmits such over a combination of wired and wireless channels such that the media stream that is received by the server is essentially the same media stream that is transmitted by the client.

2. Stadler's media stream packets arrive at and are received by a server that is an intended recipient or target device.

3. The '674 patent contemplates that a "first packet" will undergo transformation in form while being processed and transmitted over a communications network comprised of wired and wireless segments such that a "first packet" does not lose its identity as the "first packet" merely because it undergoes such transformation.

4. The change that a Stadler packet header undergoes in the process of being converted from a TCP/IP protocol over the wired segment to the WISE protocol over the wireless segment involves a mere transformation in form as evidenced by the fact that the addressee information remains sufficiently intact that the media stream ultimately is routed to the intended recipient or target device. Thus, while the information in the header is transformed at the wireless base station, it is not destroyed, thereby necessitating creation of a new and different header.

5. Because Stadler's first packet is merely transformed, but not destroyed, at the wireless base station, Stadler applies a second protocol to the first packet as opposed to a different and newly created packet.

6. The transformation in form that a first packet undergoes in the process of being transmitted from the client to server in Stadler is

not patentably distinct from the transformation in form that a first packet undergoes during transmission in accordance with the '674 patent.

7. Stadler's wireless base station determines that the first packet is targeted at the target device.

In view of the foregoing, we find that Ericsson has established, by a preponderance of the evidence, that Stadler anticipates claims 1, 13, and 18 of the '674 patent.

C. Dependent Claims 2–6, 10–12, 14–17, and 19–22.

1. Claims 2, 4–6, 10–12, 14, 16, 17, 19, 21, and 22.

Intellectual Ventures does not argue for the separate patentability of these claims apart from the arguments that we have considered above with respect to claims 1, 13, and 18. We have reviewed Ericsson's Petition and supporting evidence and find that Ericsson has established by a preponderance of the evidence that Stadler anticipates each of these claims. Pet. 26–32.

2. Different encryption algorithm (Claims 3, 15, and 20)

Intellectual Ventures argues that Stadler fails to disclose a second security protocol that uses a different encryption algorithm from the first security protocol. PO Resp. 29–31. Intellectual Ventures's expert, Dr. Newman, testifies that, at the time of the invention, a variety of encryption algorithms were used with IPSec. Ex. 2015 ¶ 66. Dr. Newman characterizes Stadler as being silent on the specific algorithm used for encryption over the wireless segment. *Id.* Dr. Newman concludes that there is no way to know whether Stadler's wireless encryption is the same or

different from the encryption algorithm used over the wired segment. *Id.* ¶ 67.

In the Petition, Ericsson relies on Stadler's disclosure of bulk encryption techniques used over the wireless segment as satisfying the limitation directed to a different encryption algorithm. Pet. 27, 29, 31. Ericsson's Petition is supported by declaration testimony from its expert, Dr. Makowski, explaining that the protocol applied at the Stadler gateway is a security protocol and that it is different from the IPSec protocol used over the wired segment of Stadler. Ex. 1013 ¶ 52.

After considering the evidence and argument presented by both parties, we find that Ericsson's position is supported by a preponderance of the evidence. At the wireless base station, Stadler transforms incoming data stream packets before they are transmitted over the wireless segment. The TCP/IP headers are replaced with a shorter WLP header. Ex 1003, 273. The TCP/IP data undergoes data compression so that fewer bytes need to be sent over the wireless segment. *Id.* The WISE architecture has the capability to allow TCP connections to be compressed independently or in bulk. *Id.* at 275. Stadler discloses that it is advantageous, though not required, to compress independently and encrypt in bulk. *Id.* The WISE system is characterized as very flexible and may be configured in several different manners depending on the type of encryption that will be used. *Id.* at 273. In other words, more than one single type of encryption is contemplated by Stadler. Given the foregoing description, we think that it is more likely than not that a person of ordinary skill in the art would understand that Stadler is not restricted to using the exact same encryption algorithm over both the wired and wireless segments. In other words, a person of ordinary skill in

the art would understand that embodiments of Stadler would be practiced where the encryption algorithm over the wired segment differs from the encryption algorithm used over the wireless segment.

Ericsson has shown, by a preponderance of the evidence, that claims 3, 15, and 20 are anticipated by Stadler.

V. OBVIOUSNESS OVER STADLER AND DAVISON

Ericsson asserts that claims 7–9 are obvious over the combination of Stadler and Davison. A patent is invalid for obviousness:

> if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.

35 U.S.C. § 103. Obviousness is a question of law based on underlying factual findings: (1) the scope and content of the prior art; (2) the differences between the claims and the prior art; (3) the level of ordinary skill in the art; and (4) objective indicia of nonobviousness. *See Graham v. John Deere Co. of Kansas City*, 383 U.S. 1, 17–18 (1966). Courts must consider all four *Graham* factors prior to reaching a conclusion regarding obviousness. *See Eurand, Inc. v. Mylan Pharms., Inc. (In re Cyclobenzaprine Hydrochloride Extended–Release Capsule Patent Litig.)*, 676 F.3d 1063, 1076–77 (Fed. Cir. 2012). As the party challenging the patentability of the claims at issue, Ericsson bears the burden of proving obviousness by a preponderance of the evidence. 35 U.S.C. § 316(e).

A. Scope and Content of the Prior Art – Davison (Ex. 1010).

Davison describes a network in which a virtual private network may be provided. Ex. 1010, 1:33–37. Davison states that any protocol that allows tunneling or tunneling-like features may be used to initiate a tunnel session, such as L2TP, L2F, PPTP, or IPSec. *Id.* at 5:20–34. It explains that conventional tunneling protocol security features may be employed to prevent a home gateway from masquerading as a home gateway to a different network. *Id.* at 3:9–17.

B. Differences Between the Prior Art and the Claimed Invention

We previously have found that Stadler discloses all of the limitations of claim 1, from which claims 7– 9 each depend. *See supra* Section IV. Claims 7–9 further require that the first security protocol is compliant with PPTP, L2F, and L2TP tunneling protocols, respectively. Ex. 1001. As set forth in Section V.A. *supra,* Davison discloses that any protocol that allows tunneling or tunneling-like features may be used to initiate the tunnel session, such as L2TP, L2F, PPTP, or IPSec. Ex. 1010, 5:20–34. Intellectual Ventures does not dispute that Davison discloses these tunneling protocols.

C. Level of Ordinary Skill in the Art

Ericsson's Petition does not attempt to define or describe a level of ordinary skill in the art. Ericsson's expert, Dr. Makowski, assumes, based on information provided to him, that the level of skill in the art is evidenced by the prior art references. Ex. 1013 ¶ 6. Based on this assumption, Dr. Makowski testifies that a person of ordinary skill in the art at the time of

the invention was aware of techniques involved in translating security protocols in a communication system. *Id.*

Intellectual Ventures's Patent Owner's Response does not define or describe a level of ordinary skill in the art. Intellectual Ventures's expert, Dr. Newman, assumes, based on information provided to him, that a person of ordinary skill in the art is a person with a bachelor's degree in electrical or computer engineering with three to five years of experience analyzing and/or designing systems incorporating security protocols on telecommunication and cellular networks. Ex. 2015 ¶ 28. Although Dr. Newman testifies that he "agrees" with the position that Intellectual Ventures has taken on the level of ordinary skill, his testimony is not based on any underlying factual analysis.

Merely reciting a college degree and a number of years of experience provides little guidance as to the actual capabilities of a person of ordinary skill in the art. Neither party presents a detailed evidentiary showing under the factors recited in *Environmental Designs, Ltd. v. Union Oil Co.*, 713 F.2d 693, 696–97 (Fed. Cir. 1983).[11] Notwithstanding the scant evidence on skill level presented by the parties, the level of skill in the art often can be determined from a review of the prior art. *See Litton Indus.*

[11] Factors pertinent to a determination of the level of ordinary skill in the art include: (1) educational level of the inventor; (2) type of problems encountered in the art; (3) prior art solutions to those problems; (4) rapidity with which innovations are made; (5) sophistication of the technology; and (6) educational level of workers active in the field. Not all such factors may be present in every case, and one or more of these or other factors may predominate in a particular case. *See id.* These factors are not exhaustive but are merely a guide to determining the level of ordinary skill in the art. *See Daiichi Sankyo Co. Ltd., Inc. v. Apotex, Inc.*, 501 F.3d 1254, 1256 (Fed. Cir. 2007).

Products, Inc. v. Solid State Sys. Corp., 755 F.2d 158, 163–64 (Fed. Cir. 1985). Based on our review of the prior art, the applicable field of endeavor is telecommunication networking. The person of ordinary skill in this field would have been generally familiar with communication protocols used over the Internet. Ex. 1010, 5:20–34. The person of ordinary skill in the art also would have had some familiarity with using IPSec encryption over a TCP/IP protocol wired communications system. Ex. 1003, 275; Ex. 1010, 5:22; Ex. 1007, 268–269. The person of ordinary skill in the art also would have had familiarity with conventional tunneling protocol security features. Ex. 1010, 3:14–15; Ex. 1007. The person of ordinary skill in the art also would have had familiarity with wireless communication systems and using authentication and encryption as security features over wireless communication systems. Ex. 1009, iv.

D. Secondary Considerations of Non-Obviousness

Evidence of secondary considerations of non-obviousness, when present, must always be considered en route to a determination of obviousness. *See Cyclobenzaprine*, 676 F.3d at 1075–76. However, the absence of secondary considerations is a neutral factor. *See Custom Accessories, Inc., Jeffrey-Allan Industries, Inc.*, 807 F.2d 955, 960 (Fed. Cir. 1986). Neither party introduced evidence on secondary considerations of non-obviousness. Consequently, we will focus our attention on the first three *Graham* factors.

E. Whether the Prior Art Could Have Been Combined or Modified to Achieve the Claimed Invention

The evidence establishes that Stadler and Davison, together, disclose all of the limitations of claims 7–9, respectively. However, Intellectual Ventures argues against the combinability of the two references and makes essentially the same argument with respect to each claim. PO Resp. 31–35. Essentially, Intellectual Ventures argues that Ericsson's stated reason for combining Stadler and Davison is flawed. *Id.* Intellectual Ventures characterizes Ericsson's proposed combination as substituting PPTP, L2F, and/or L2TP for IPSec because the respective tunneling protocols are known substitutes for IPSec. *Id.* Intellectual Ventures then argues that such a substitution would leave the proposed combination without a security protocol because PPTP, L2F, and L2TP merely provide unsecured tunneling conduits for communications. *Id.*

Ericsson argues that it would have been obvious to modify the system of Stadler to use any of the PPTP, L2F, and L2TP tunneling procedures of Davison, respectively, in place of IPSec. Pet. 33–34. Ericsson asserts that such modification merely would have involved substituting one known element for another to yield a predictable result. *Id.*

The Supreme Court instructs courts to take an expansive and flexible approach in determining whether a patented invention was obvious at the time it was made. *See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 415 (2007). The existence of a reason for a person of ordinary skill in the art to combine references is a question of fact. *See In re Constr. Equip. Co.*, 665 F.3d 1254, 1255 (Fed. Cir. 2011). A reason 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. *Perfect Web Techs., Inc. v. InfoUSA, Inc.*, 587 F.3d 1324, 1328–29 (Fed. Cir. 2009) (quoting *KSR*, 550 U.S. at 418–21).

Intellectual Ventures's argument mischaracterizes Ericsson's position as substituting PPTP, L2F, or L2TP for IPSec without using any security features in conjunction with the PPTP, L2F, or L2TP tunneling protocols. We do not interpret Davison as espousing unsecured transmission during tunneling sessions in lieu of using IPSec. Instead, Davison teaches secured transmissions using encryption and authentication techniques. Ex. 1010, 4:66–5:19. Davison also teaches the use of a tunneling protocol in conjunction with "conventional tunneling protocol security features." *Id.* at 3:13–17. Thus, taken in the proper context, Davison explains that such secure communication can take place using "any protocol that allows tunneling or tunneling-like features," including PPTP, L2F, and L2TP. *Id.* at 5:20–33.

As we understand Ericsson's proposed obviousness combination, Davison's communication that is secured using authentication, encryption or both and utilized with either PPTP, L2TP, or L2F tunneling protocols, is substituted for IPSec over Stadler's wired transmission segment. We have considered Ericsson's evidence and find it persuasive. Where "a patent claims a structure already known in the prior art that is altered by the mere substitution of one element for another known in the field, the combination must do more than yield a predictable result." *KSR*, 550 U.S. at 416. The Patent Owner Response provides neither evidence nor persuasive technical

reasoning to controvert Ericsson's persuasive position that such combination entails nothing more than substituting one known element for another to yield a predictable result.

F. Ultimate Conclusion of Obviousness

After considering all of the underlying factual considerations, the ultimate conclusion of obviousness is a question of law. *Pfizer, Inc. v. Apotex, Inc*., 480 F.3d 1348, 1359 (Fed. Cir. 2007). "[T]he great challenge of the obviousness judgment is proceeding without any hint of hindsight." *Star Scientific, Inc., v. R.J. Reynolds Tobacco Co*., 655 F.3d 1364, 1375 (Fed. Cir. 2011).

All things considered, Ericsson has carried its burden of proof that claims 7–9 of the '674 patent are unpatentable as obvious over Stadler and Davison.

VI. OBVIOUSNESS OVER RAI AND DAVISON

Ericsson asserts that claims 2–9, 14–16, and 19–21 are unpatentable as obvious over the combination of Rai and Davison. Intellectual Ventures presents separate arguments for the patentability of claims 2, 14, and 19 (PO Resp. 44), claim 7 (*id*. at 45), claim 8, (*id*. at 46), claim 9 (*id*.), claims 3, 15, and 20 (*id*. at 47), and claims 5 and 6 (*id*.).

A. Scope and Content of the Prior Art – Rai (Exhibit 1004)

Rai provides users with remote wireless access to the public Internet, private intranets, and Internet service providers. Ex. 1004, 2:31–33. Rai discloses base station 64 that is connected between wired network 38 and wireless network airlinks. *Id.* at Fig. 4, 10:29–11:58. Rai's base station

provides "computer users with remote access to the internet and to private intranets using virtual private network services over a high speed, packet switched, wireless data link." *Id.* at 4:64–66.

Rai's base station includes access point 82 that applies a MAC (media access control) layer protocol to packets sent over the air link. Ex. 1004, Figs. 7, 11. "PPP frames traveling from the end system to the IWF are sent over the MAC and air link to the base station." *Id.* at 8:21–23.

B. Differences Between the Prior Art and the Claimed Invention

1. "first security protocol" – Rai (claims 1, 13, and 18)[12]

Ericsson contends that the Xtunnel protocol disclosed in Rai satisfies the element in claim 1 directed to "the first packet is protected according to a first security protocol on the wired data network." Pet. 34. A similar contention is made with respect to claims 13 and 18. Pet. 37, 40. Ericsson's expert, Dr. Makowski, characterizes Rai's XTunnel protocol as the "first security protocol" of claims 1, 13, and 18, because a tunneling protocol performs an operation of securing a particular path for packets to travel from a source to its destination. Ex. 1013 ¶ 59.

Intellectual Ventures disputes that XTunnel protocol is a security protocol within the meaning of claims 1, 13, and 18. According to Intellectual Ventures, the XTunnel protocol merely ensures that PPP data frames that are sent are all received correctly and in the correct order and

[12] Each of claims 2–9, 14–16, and 19–21 ultimately depend from one of independent claims 1, 13, and 18. Claims 2–9, 14–16, and 19–21, thus, include a "first security protocol," which is required by the independent claims.

that the sender does not overwhelm the receiver causing data to be lost due to buffer overflow. PO Resp. 37. Intellectual Ventures's expert, Dr. Newman, testifies that such data delivery mechanisms have nothing to do with providing confidentiality or authenticity of the data or data frames. Ex. 2015 ¶ 73.

After considering the evidence and arguments of the parties, we agree with Intellectual Ventures's position that the XTunnel protocol of Rai does no more than provide an unsecure conduit for communications which may be capable of use with actual security protocols. However, XTunnel, by itself, is not a security protocol. Ericsson not has carried its burden of establishing that Rai discloses a first security protocol over the wired data network.

2. "first security protocol" – Davison (claims 1, 2, 13, 14, 18, and 19)

Claims 2, 14, and 19 depend from claims 1, 13, and 18, respectively, and each add limitations that the first security protocol comprises encryption that is decrypted by the processing step. Ex. 1001. Ericsson concedes that Rai does not explicitly disclose that the XTunnel protocol includes encryption. Pet. 43. However, Ericsson relies on Davison as disclosing conventional tunneling protocol security features including IPSec. *Id.* at 44; Ex. 1010, 3:9–17. Ericsson relies on the disclosure of IPSec in Davison as satisfying the encryption limitation in claims 2, 14, and 19. Pet. 43–44.

Intellectual Ventures does not dispute that Davison discloses the encryption limitation of claims 2, 14, and 19. PO Resp. 44–45. Based on the evidence provided, we find that Davison satisfies the encryption limitation of claims 2, 14, and 19. We find further that Davison's disclosure

of conventional tunnel protocol security features including IPSec satisfies the "first security protocol" limitation of claims 1, 13, and 18.

3. "second security protocol – Rai (claims 1, 13, and 18)

Ericsson contends that the MAC layer protocol disclosed in Rai satisfies the element in claim 1 directed to "applying a second security protocol employed on the wireless network." Pet. 36. A similar contention is made with respect to claims 13 and 18. Pet. 39, 41. Ericsson's expert, Dr. Makowski, testifies that it readily would have been understood to a person of ordinary skill in the art that the use of the MAC layer for a wireless LAN as shown in Rai followed the 802.11 standard. Pet. 33–34; Ex. 1013 ¶ 64. Dr. Makowski testifies that the 802.11 standard includes the Wired Equivalency Privacy (WEP) algorithm, which includes security features such as authentication and encryption. Ex. 1013 ¶ 64.

Intellectual Ventures argues that Ericsson has not explained its obviousness position adequately. PO Resp. 39. Intellectual Ventures argues that Rai does not mention the 802.11 standard. *Id.* at 40.

Intellectual Ventures's arguments are not persuasive. The 802.11 standard informs us that:

> The medium access control (MAC) supports operation under control of an access point as well as between independent stations. The protocol includes *authentication*, association, and reassociation services, an operational *encryption/decryption* procedure, power management to reduce power consumption in mobile stations, and a point coordination function for time-bounded transfer of data.

Ex. 1009, iv (emphasis added). While Rai does not mention the 802.11 standard expressly, it does disclose that PPP frames are sent over the MAC and air link. Ex. 1004, 8:21–23. An artisan must be presumed to know

something about the art apart from what the references disclose. *See In re Jacoby*, 309 F.2d 513, 516 (CCPA 1962). Here, the 802.11 standard informs us as to what a person of ordinary skill in the art would understand Davison's disclosure of the MAC protocol entails. Thus, we are persuaded that Rai's reference to use of the MAC protocol is sufficient to inform a person of ordinary skill in the art that a security protocol is employed on the wireless network.

4. The "determining . . . target" element – Rai (claims 1, 13, and 18)

Ericsson contends that the determining step of claims 1, 13, and 18 is satisfied by disclosures in columns 8, 9, and 17 of Rai. Pet. 35, 38, 40. Ericsson's position is supported by declaration testimony from Dr. Makowski. *Id.*; Ex. 1013 ¶ 62.

Intellectual Ventures argues that Ericsson's recited passages in Rai merely refer to assignment of an IP address, which Intellectual Ventures contends is different from determining that a packet is targeted at a target device as recited in the claims. PO Resp. 43. Intellectual Ventures argues that Ericsson neglects to explain how the determining step is performed by the wireless base station as opposed to being performed by another structure disclosed in Rai. *Id.*

In reply, Ericsson notes that Rai describes that the base station de-tunnels down link frames and relays them over the air link to the "end system," which Ericsson equates with the target device. Reply 14 (citing Ex. 1004, 8:32–34). Ericsson argues that the base station must make a determination that the packet is targeted at the end system in order to send the packet to the end system. Reply 14–15. We agree with Ericsson on this

point. Ericsson has shown by a preponderance of the evidence that Rai satisfies the determining element of claims 1, 13, and 18.

5. "different encryption algorithm" (claims 3, 15, and 20)

Claims 3, 15, and 20, depend from claims 2, 14, and 18, respectively and add limitations requiring that the second security protocol comprises encryption according to a different encryption algorithm from the first security protocol. Ex. 1001. In its Petition with respect to claims 2, 14, and 20, Ericsson relies on Davison's disclosure of conventional tunneling protocol security features, including IPSec, as the first security protocol. Pet. 43–44. Ericsson relies on the MAC layer protocol as the second security protocol. Pet. 47, 48, 49. Dr. Makowski testifies that the MAC layer protocol uses the Wired Equivalency Privacy (WEP) algorithm from the 802.11 standard. Ex. 1013 ¶ 64 (citing Ex. 1009, 62–70). Dr. Makowski describes the WEP algorithm as a second and different security protocol. *Id*.

Intellectual Ventures argues that the Petition is insufficient to carry Ericsson's burden of proof, because the Petition fails to identify the encryption algorithm that is used on either the wired network or the wireless network. PO Resp. 47. Intellectual Ventures presents supporting testimony from Dr. Newman. *Id.*; Ex. 2015 ¶ 84. Dr. Newman's testimony, however, does not address any similarities or differences between IPSec encryption and WEP encryption. Thus, Dr. Newman does not address the actual factual issue raised by the Petition, which is whether the MAC protocol used over the wireless segment of Rai is different from the IPSec protocol used over a wired network as disclosed by Davison.

We determine that Ericsson's position has merit, and observe that there is an absence of persuasive evidence from Intellectual Ventures

controverting Ericsson's position. We find that Ericsson has met its burden of showing that the MAC protocol of Rai, which we find includes the WEP encryption algorithm of standard 802.11, is different from the IPSec encryption algorithm of Davison.

C. Level of Ordinary Skill in the Art

We apply the same level of ordinary skill in the art for the grounds of unpatentability over the combination of Rai and Davison as described above for the combination of Stadler and Davison.

D. Secondary Considerations of Non-Obviousness

As with the grounds of unpatentability over Stadler and Davison, neither party introduced evidence on secondary considerations of non-obviousness.

E. Whether the Prior Art Could Have Been Combined to Achieve the Claimed Invention

The evidence establishes that Rai and Davison, together, disclose all of the limitations of claims 2–9, 14–16, and 19–21. Nevertheless, Intellectual Ventures raises a number of arguments against the combinability of the two references with respect to various challenged claims.

1. Claims 2, 14, and 19.

Intellectual Ventures argues that Ericsson's obviousness argument is conclusory and, therefore, insufficient. PO Resp. 45. Intellectual Ventures argues that even if IPSec could be substituted for XTunnel, Ericsson does not explain why one with ordinary skill in the art would make that substitution. *Id.*

Intellectual Ventures presents testimony from Dr. Newman that the specifications for XTunnel contain requirements that IPSec cannot provide. *Id.*; Ex. 2015 ¶ 80. However, the features described in paragraph 80 of Dr. Newman's declaration as differences between XTunnel and IPSec do not appear to relate to the subject matter of claims 2, 14, and 19. The issue before us is whether the prior art renders the invention, as claimed, obvious, not whether unclaimed features in one reference must be included in the process of combining two references to achieve the claimed invention. *See* 35 U.S.C. § 103; *see also KSR*, 550 U.S. at 420 (in many cases a person of ordinary skill will be able to fit the teachings of multiple patents together like pieces of a puzzle).

Ericsson contends that it would have been obvious to a person of ordinary skill in the art to modify Rai to replace the XTunnel protocol with the IPSec protocol. Pet. 44. According to Ericsson, a person of ordinary skill in the art would have done this in order to provide a tunnel that was secure. *Id.* Ericsson's position is supported by declaration testimony from Dr. Makowski. *Id.*; Ex. 1013 ¶¶ 65–67.

Intellectual Ventures previously argued that the XTunnel protocol fails to provide secure communications. PO Resp. 36. We are of the opinion that the prospect of obtaining security for communications by using IPSec is a sufficient reason to substitute IPSec for XTunnel. Ericsson has established, by a preponderance of the evidence, that a person of ordinary skill in the art would have combined Rai and Davison to achieve the invention of claims 2, 14, and 19 of the '674 patent.

2. Claims 3, 15, and 20

Intellectual Ventures does not argue against the combinability of Davison and Rai with respect to claims 3, 15, and 20, apart from the argument that the prior art fails to disclose two different encryption algorithms, an argument that we rejected in Section VI.B.5 above. A person of ordinary skill in the art would have combined Rai and Davison to achieve these claims for essentially the same reason discussed in the preceding section with respect to claims 2, 14, and 19.

3. Claim 4

Claim 4 depends from claim 2 and adds a limitation that the first security protocol comprises authentication. Ex. 1001. Ericsson relies on Davison as satisfying the authentication element. Pet. 47. Intellectual Ventures does not challenge Ericsson's position on claim 4 apart from the arguments made opposing Ericsson's case with respect to claim 1. PO Resp. 44. We find that Ericsson has carried its burden of showing that a person of ordinary skill in the art would have combined Davison and Rai to achieve the invention of claim 4 for essentially the same reason discussed in preceding sections with respect to claims 2, 3, 14, 15, 19, and 20.

4. Claims 5 and 6

Claim 5 depends from claim 4 and claim 6 depends from claim 1. Ex. 1001. Each claim adds a limitation that the first security protocol is compliant with IPSec. *Id.* For each of claims 5 and 6, Ericsson relies on Davison as disclosing IPSec. Pet. 48. Intellectual Ventures argues that Ericsson provides no rationale for combining Davison and Rai. PO Resp. 48.

As discussed previously with respect to claim 2 (*see* Section VI.E.1 above), Ericsson argues that it would have been obvious to a person of ordinary skill in the art to modify Rai to replace the XTunnel protocol with IPSec for the purpose of providing a secure tunnel. Pet. 44. Ericsson's position is supported by declaration testimony from Dr. Makowski. *Id.*; Ex. 1013 ¶¶ 65–67. In view of the similarity between claims 2, 5, and 6, Ericsson's rationale for combining Davison with Rai for claim 2 suffices for claims 5 and 6.

5. Claims 7–9

Intellectual Ventures raises essentially identical arguments against Ericsson's proposed combination of Rai and Davison as rendering each of claims 7–9 unpatentable. PO Resp. 45–47. With respect to each claim, Intellectual Ventures argues that Ericsson's proposed substitution of PPTP, L2F, and L2TP tunneling protocols, respectively, for IPSec is flawed, because Rai does not mention IPSec. *Id.* Intellectual Ventures supports its position with testimony from Dr. Newman that a person of ordinary skill in the art would not have substituted PPTP, L2F, or L2TP tunneling protocols for IPSec because such a substitution of tunneling protocols would leave communications unsecured and vulnerable to hostile acts or influences. Ex. 2015, ¶¶ 81–83.

Intellectual Ventures's arguments mischaracterize Ericsson's position. Ericsson's Petition points out that the '674 patent acknowledges that the PPTP, L2P, and L2TP were well known before the date of the invention. Pet. 45. Ericsson further points out that the '674 patent acknowledges that these tunneling protocols were known substitutes for IPSec. *Id.* Ericsson relies on Davison as disclosing that, when using permanent virtual circuits,

conventional tunneling protocol security measures may be employed to prevent a home gateway from masquerading as a home gateway to a different network by providing an incorrect domain identifier. *Id.*; Ex. 1010, 3:9–17. Ericsson further relies on Davison as disclosing that any protocol that allows tunneling or tunneling-like features may be used to initiate a tunnel session. Ex. 1010, 5:20–34. Although Davison indicates that IPSec could be used as the tunneling protocol, it also indicates that PPTP, L2F, or L2TP could be used in lieu of IPSec. *Id.*

Thus, as we understand the Petition, Ericsson is not proposing to substitute unsecured PPTP, L2F, or L2TP tunnel communications for secure IPSec tunnel communications. Rather, we understand that Ericsson is relying on Davison's "conventional tunneling protocol security features" as a first security protocol to be used with PPTP, L2P, or L2TP tunneling communications in connection with claims 7–9, respectively. Pet. 45; Ex. 1010, 3:13–17.

We are unpersuaded by Intellectual Ventures's arguments and find that Ericsson has shown, by a preponderance of the evidence, that a person of ordinary skill in the art would have found it obvious to combine Davison with Rai to achieve the invention of claims 7–9.

6. Claims 16 and 21

Claim 16 depends from claim 14 and claim 21 depends from claim 19. Ex. 1001. Each claim adds a limitation that the first security protocol further comprises authentication. *Id.* For each of claims 16 and 21, Ericsson relies on Davison as disclosing authentication. Pet. 48–49. Ericsson's position is supported by declaration testimony of Dr. Makowski. *Id.*; Ex. 1013 ¶ 23.

Intellectual Ventures does not challenge Ericsson's position on claims 16 and 21 apart from the arguments made opposing Ericsson's case with respect to claim 1. PO Resp. 44. We find that Ericsson has carried its burden of showing that a person of ordinary skill in the art would have combined Davison and Rai to achieve the invention of claims 16 and 21 for essentially the same reason discussed in proceeding sections with respect to claims 2, 3, 14, 15, 19, and 20.

F. Ultimate Conclusion of Obviousness

Upon consideration of all the evidence, it is our opinion that Ericsson has carried its burden of proof that claims 2–9, 14–16, and 19–21 of the '674 patent are unpatentable as obvious over Davison and Rai.

VII. OBVIOUSNESS OVER RAI

Ericsson asserts that claims 1, 10–13, 17, 18, and 22 are unpatentable as obvious over Rai. Pet. 33–43. Intellectual Ventures presents separate arguments for the patentability of claims 1, 13, and 18. PO Resp. 36–43. In opposing the grounds of unpatentability with respect to claims 10–12, 17, and 22, each of which depends from either claims 1, 13, or 18, Intellectual Ventures relies on the arguments asserted with respect to claims 1, 13, and 18.

A. Claims 1, 13, and 18

Claims 1, 13, and 18 are independent claims. Ex. 1001. Claims 2, 14, and 19 depend from claims 1, 13, and 18, respectively. *Id.* We previously have determined that each of claims 2, 14, and 19 is unpatentable as obvious. *See supra* Section VI.F.

Settled law maintains that a broader independent claim cannot be nonobvious where a dependent claim stemming from that independent claim is invalid for obviousness. *See Soverain Software LLC v. Victoria's Secret Direct Brand Mgmt., LLC*, 778 F.3d 1311, 1315 (Fed. Cir. 2015). In view of our determination that each of claims 2, 14, and 19 is unpatentable over Rai and Davison, we determine that each of claims 1, 13, and 18 also is unpatentable as obvious over those references.

B. Claims 10–12, 17, and 22

Claim 10 depends from claim 1 and adds a limitation that the wireless base station wirelessly transmits the first packet. Ex. 1001. Ericsson argues that Rai satisfies this limitation. Pet. 41; Ex. 1004, 8:32–34. Intellectual Ventures does not challenge this assertion.

Claim 11 depends from claim 1 and adds a limitation that a second packet is wirelessly received in the wireless base station that is protected by a second security protocol. Ex. 1001. Ericsson argues that Rai satisfies this limitation. Pet. 42; Ex. 1004, 8:21–29, Figs. 7, 11, 17, 20, 26. Ericsson supports its position with declaration testimony from Dr. Makowski. Pet. 42; Ex. 1013 ¶ 64. Intellectual Ventures does not challenge this assertion.

Claim 12 depends from claim 11 and adds a limitation that the wireless base station transmits the second packet on the wired network. Ex. 1001. Ericsson argues that Rai satisfies this limitation. Pet. 42; Ex. 1004, 8:21–29, Fig. 11. Ericsson supports its position with declaration testimony from Dr. Makowski. Pet. 42; Ex. 1013 ¶ 64. Intellectual Ventures does not challenge this assertion.

Claim 17 depends from claim 13 and adds a limitation that the controller is configured to process a second packet received by the second interface and the controller is configured to process the second packet according to the second security and apply the first security protocol to the second packet. Ex. 1001. Ericsson argues that Rai satisfies this limitation. Pet. 42–43; Ex. 1004, 8:21–29, Figs. 7, 11, 17, 20, 26. Ericsson supports its position with declaration testimony from Dr. Makowski. Pet. 42; Ex. 1013 ¶ 64. Intellectual Ventures does not challenge this assertion.

Claim 22 depends from claim 18 and adds a limitation that the controller is configured to process a second packet received from the wireless network and the controller is configured to process the second packet according to the second security and apply the first security protocol to the second packet. Ex. 1001. Ericsson argues that Rai satisfies this limitation. Pet. 42–43; Ex. 1004, 8:21–29, Figs. 7, 11, 17, 20, 26. Ericsson supports its position with declaration testimony from Dr. Makowski. Pet. 43; Ex. 1013 ¶ 64. Intellectual Ventures does not challenge this assertion.

Thus, in opposing the grounds of unpatentability with respect to claims 10–12, 17, and 22, Intellectual Ventures relies solely on the arguments asserted with respect to claims 1, 13, and 18. We have reviewed the evidence submitted by Ericsson in support of its contentions with respect to claims 10–12, 17, and 22 and find it sufficient to establish the facts, as asserted. Under the circumstances, we find that Ericsson has carried its burden of showing, by a preponderance of the evidence, that claims 10–12, 17, and 22 are unpatentable as obvious over Rai.

IV. ORDER

In view of the foregoing, it is ORDERED as follows:

1. Claims 1–6 and 10–22 of U.S. Patent No. 7,496,674 B2 have been shown to be unpatentable as anticipated by Stadler;

2. Claims 7–9 of U.S. Patent No. 7,496,674 B2 have been shown to be unpatentable as obvious over Stadler and Davison; and

3. Claims 1–22 of U.S. Patent No. 7,496,674 B2 have been shown to be unpatentable as obvious over Rai and Davison.

This is a final decision. Parties to the proceeding seeking judicial review of the decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

PETITIONER:

Todd Baker
Robert Mattson
Sameer Gokhale
OBLON, MCCLELLAND, MAIER & NEUSTADT, L.L.P
cpdocketbaker@oblon.com
cpdocketmattson@oblon.com
cpdocketgokhale@oblon.com

PATENT OWNER:

Herbert Hart
Jonathan Sick
Steven
Hampton
MCANDREWS, HELD & MALLOY, LTD.
hhart@mcandrews-ip.com
jsick@mcandrews-ip.com
shampton@mcandrews-ip.com

James Hietala
Tim Seeley
INTELLECTUAL VENTURES MANAGEMENT
jhietala@intven.com
tim@intven.com