

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

MICROSOFT CORPORATION,
Petitioner,

v.

DAEDALUS BLUE, LLC,
Patent Owner.

IPR2021-00832
Patent 8,381,209 B2

Before SALLY C. MEDLEY, HYUN J. JUNG, and
ARTHUR M. PESLAK, *Administrative Patent Judges*.

MEDLEY, *Administrative Patent Judge*.

DECISION
Denying Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

Microsoft Corporation (“Petitioner”) filed a Petition for *inter partes* review of claims 1–8 of U.S. Patent No. 8,381,209 B2 (Ex. 1001, “the ’209 patent”). Paper 1 (“Pet.”). Daedalus Blue, LLC (“Patent Owner”) filed a Preliminary Response. Paper 6 (“Prelim. Resp.”). In accordance with Board authorization, Petitioner filed a Reply to the Preliminary Response (Paper 9) and Patent Owner filed a Sur-Reply (Paper 10).

Institution of an *inter partes* review is authorized by statute when “the information presented in the petition . . . and any response . . . shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” 35 U.S.C. § 314(a). Upon consideration of the Petition, the Preliminary Response, and the evidence of record, we decline to institute review of the challenged claims of the ’209 patent.

A. Related Matters

The parties indicate that related district court litigations are *Daedalus Blue, LLC v. Microsoft Corp.*, No. 6:20-cv-01152 (W.D. Tex.) (“the district court case”) and *Daedalus Blue, LLC v. Oracle Corp. et al.*, No. 6:20-cv-00428 (W.D. Tex.) (terminated). Pet. 4; Paper 4, 2.

B. The ’209 Patent

The ’209 patent relates to “virtual machine migration with filtered network connectivity which includes enforcing network security and routing at a hypervisor layer at which a virtual machine partition is executed and which is independent of guest operating systems.” Ex. 1001, 1:11–15. The ’209 patent describes that “in order to perform maintenance on or provide a fail-over for a processor device or machine, it is desirable to move or

migrate a virtual machine (VM) from one processor machine or device to another.” *Id.* at 2:27–30. The ’209 patent seeks to address shortcomings of conventional approaches for VM migration (*id.* at 4:31–40), which include “a complex update scheme to update the ACLs [access control lists] in the real switches and the filters in the firewalls,” and “very little network security” (*id.* at 3:6–11).

Figure 4, reproduced below, illustrates an embodiment for “securing a filtered network, including enforcing network security and routing at a hypervisor layer.” *Id.* at 8:31–34.

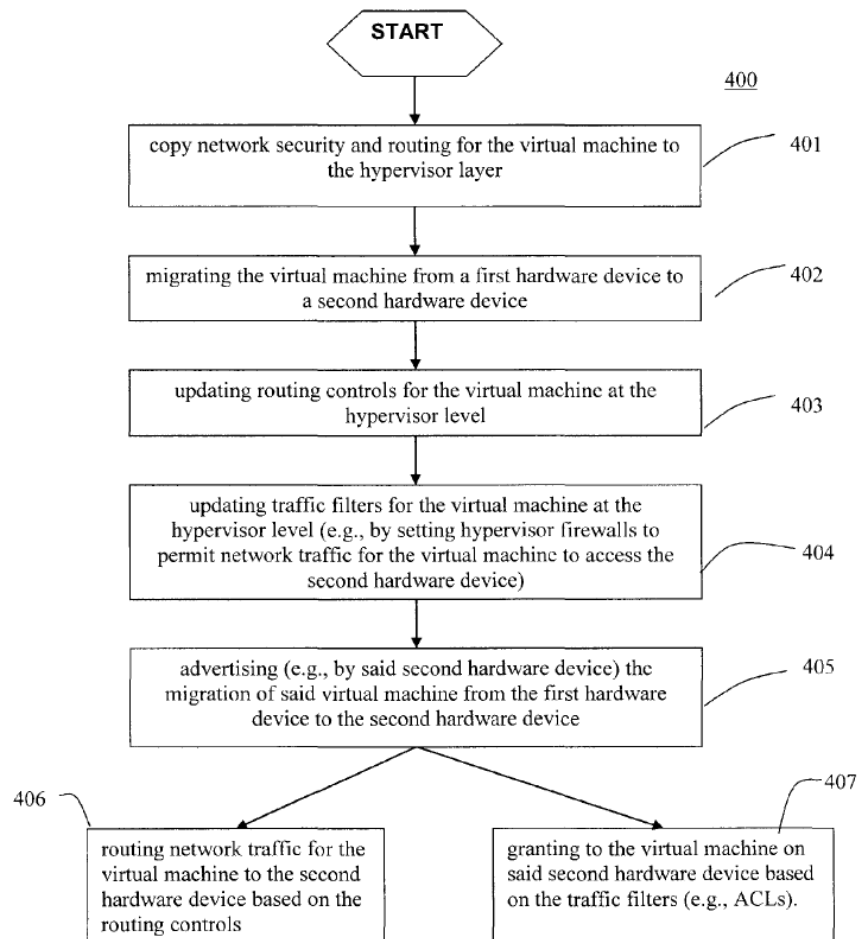


FIGURE 4

Figure 4 shows a method, beginning with step 401, which “copies network security and routing for the virtual machine to the hypervisor layer.” *Id.* at 8:37–39. Then, the method “migrates the virtual machine from a first hardware device to a second hardware device” in step 402, “updates routing controls for the virtual machine at the hypervisor level” in step 403, “updates traffic filters for the virtual machine at the hypervisor level” in step 404, “and advertises the migration of the virtual machine from the first hardware device to the second hardware device” in step 405. *Id.* at 8:39–46. In steps 406 and 407, network traffic for the virtual machine is routed to the second hardware device based on the routing controls and access is granted to the virtual machine on the second hardware device based on the traffic filters. *Id.* at 8:47–51.

The ’209 patent describes that by copying security and routing to the hypervisor layer, “the user will see no difference in operation.” *Id.* at 9:25–28. For example, “the first and second device . . . would each act the same, and preferably, would each have the same internet protocol (IP) address.” *Id.* at 9:29–31. Moreover, because “the hypervisor layer provides traffic filtering and routing updating,” “the real switches do not need to be updated at the first and second hardware devices.” *Id.* at 9:39–42.

C. Illustrative Claim

Petitioner challenges claims 1–8 of the ’209 patent. Claim 1 is independent, and claims 2–8 depend therefrom. Claim 1 is reproduced below.

1. A computer implemented method of controlling network security of a virtual machine, the method comprising enforcing network security and routing at a hypervisor layer via dynamic updating of routing controls initiated by a

migration of said virtual machine from a first device to a second device.

Ex. 1001, 15:39–43.

D. Asserted Grounds of Unpatentability

Petitioner asserts that claims 1–8 are unpatentable based on the following grounds (Pet. 7):¹

Claims Challenged	35 U.S.C §	References/Basis
1, 3, 6	103(a) ²	Dhawan ³ , Clark ⁴
2, 4, 5	103(a)	Dhawan, Clark, Warfield ⁵
7, 8	103(a)	Dhawan, Clark, Chandika ⁶

¹ Although Petitioner adds the general knowledge of a person of ordinary skill in the art to the express statement of each alleged ground of unpatentability (Pet. 7, 36, 45, 55), that is not necessary. Obviousness is determined from the perspective of one with ordinary skill in the art. We leave out the express inclusion of the general knowledge of one with ordinary skill.

² The Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284 (2011) (“AIA”), amended 35 U.S.C. § 103. The ’209 patent was filed on January 3, 2007. Ex. 1001, code (22). Because the filing date is before the effective date of the applicable AIA amendments, we refer to the pre-AIA version of 35 U.S.C. § 103.

³ U.S. Pat. App. Pub. No. US 2007/0079307 A1, published Apr. 5, 2007 (Ex. 1005, “Dhawan”).

⁴ “Live Migration of Virtual Machines” (Ex. 1006, “Clark”). Petitioner asserts a publication date of May 3, 2005, and a public accessibility date of February 28, 2006. Pet. 6 (citing Ex. 1009).

⁵ “Isolation of Shared Network Resources in XenoServers” (Ex. 1007, “Warfield”). Petitioner asserts a publication date of November 2002, and a public accessibility date of December 2002. Pet. 7–10 (citing Exs. 1024–1045).

⁶ U.S. Patent No. 8,107,370 B2, filed Apr. 6, 2005, issued Jan. 31, 2012 (Ex. 1008, “Chandika”).

II. DISCUSSION

A. Claim Construction

In this *inter partes* review, claims are construed using the same claim construction standard that would be used to construe the claims in a civil action under 35 U.S.C. § 282(b). 37 C.F.R. § 42.100(b) (2020). The claim construction standard includes construing claims in accordance with the ordinary and customary meaning of such claims as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent. *See id.*; *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–14 (Fed. Cir. 2005) (en banc).

*“enforcing . . . at a hypervisor layer via
dynamic updating of routing controls”*

Claim 1 recites “enforcing network security and routing at a hypervisor layer via dynamic updating of routing controls.” Ex. 1001, 15:40–42. Patent Owner argues that in the district court case, Petitioner proposes construing this phrase to mean “upon migration, automatically changing the routing controls at a hypervisor layer to rout network traffic for the virtual machine to the second device.” Prelim. Resp. 15 (citing Ex. 2010, 4). Although Patent Owner argues that it does not agree with the proposed construction or propose its own construction (*id.* at 15–16), Patent Owner’s arguments regarding why the prior art fails to meet the phrase are based on a construction that the phrase requires “dynamic updating of routing controls *at the hypervisor layer.*” *Id.* at 30–39. We understand Petitioner also to construe the phrase to require “dynamic updating of routing controls *at the hypervisor layer.*” Pet. 38; Ex. 1003 ¶¶ 130, 132. The parties’ proposed construction is consistent with the Specification of the

'209 patent. Ex. 1001, 5:8–16, 5:24–25, 5:59–60, 6:11–15, 8:41–42, 9:39–40, 9:58–62, 10:40–42, Fig. 4 step 403. Thus, for purposes of this Decision we agree with the parties' construction that "enforcing network security and routing at a hypervisor layer via dynamic updating of routing controls" requires "dynamic updating of routing controls at the hypervisor layer."

For purposes of this Decision, we need not expressly construe any other claim terms. *See Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999) (holding that "only those terms need be construed that are in controversy, and only to the extent necessary to resolve the controversy"); *see also Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co. Matal*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (citing *Vivid Techs.* in the context of an *inter partes* review).

B. Principles of Law

A patent claim is unpatentable under 35 U.S.C. § 103(a) if the differences between the claimed subject matter 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. *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of ordinary skill in the art;⁷ and (4) when in evidence, objective

⁷ Relying on the testimony of Dr. Markus Jakobsson, Petitioner offers an assessment as to the level of ordinary skill in the art and the knowledge of a person of ordinary skill in the art at the time of the '209 patent. Pet. 21–25 (citing Ex. 1003 ¶¶ 51, 56–75). For example, Dr. Jakobsson states that a person having ordinary skill in the art "would have had at least a bachelor's

indicia of nonobviousness. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

C. Asserted Obviousness of Claims 1, 3, and 6 over Dhawan, and Clark

Petitioner contends claims 1, 3, and 6 are unpatentable under 35 U.S.C. § 103(a) as obvious over Dhawan and Clark. Pet. 36–45. In support of its showing, Petitioner relies upon the declaration of Dr. Markus Jakobsson. *Id.* (citing Ex. 1003).

1. Dhawan

Dhawan “relates in general to the field of information handling systems and, more specifically, to the flexible and secure transfer of packets by carrier virtual machines.” Ex. 1005 ¶ 2. Dhawan describes that “virtual machine migration is generally implemented on physical servers that share a common pool of data storage resources.” *Id.* ¶ 11. “When a virtual machine migrates to other nodes a virtual volume manager, working in concert with virtual machine manager, can provide the necessary routing and redirection functionality to transport data stored in VSDs [Virtual Storage Devices] across SAN and LAN fabrics.” *Id.* Dhawan recognizes a need, however, “for an improved way of securely managing data and processes across physical hosts.” *Id.* ¶ 16.

degree in computer science, computer engineering, or an equivalent degree and at least three years of work experience in the field of cloud computing, virtual machines, computer networks and systems, and/or a similar field.” Ex. 1003 ¶ 51. Patent Owner does not propose an alternative assessment. *See* Prelim. Resp. 14. To the extent necessary, and for purposes of this Decision, we accept the assessment offered by Petitioner as it is consistent with the ’209 patent and the asserted prior art.

Figure 1, reproduced below, illustrates an embodiment of an information handling system. *Id.* ¶ 35.

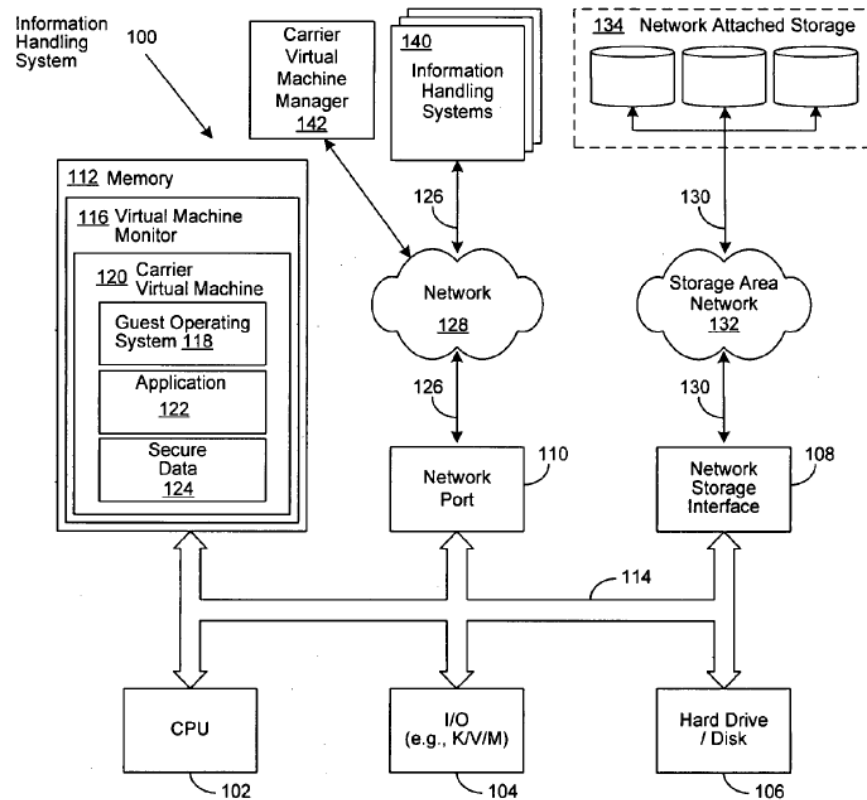


FIGURE 1

Figure 1 shows that information handling system 100 includes virtual machine monitor 116 residing in system memory 112 and supporting a guest operating system 118. *Id.* Virtual machine monitor 116 implements carrier virtual machine 120, which can interact with application 122 and secure data 124. *Id.* Virtual machine carrier manager 142 manages virtual machine packets and implements routing and policy management for the virtual machines. *Id.*

Figure 4, reproduced below, illustrates a TCP/IP network for implementing carrier virtual machines. *Id.* ¶ 41.

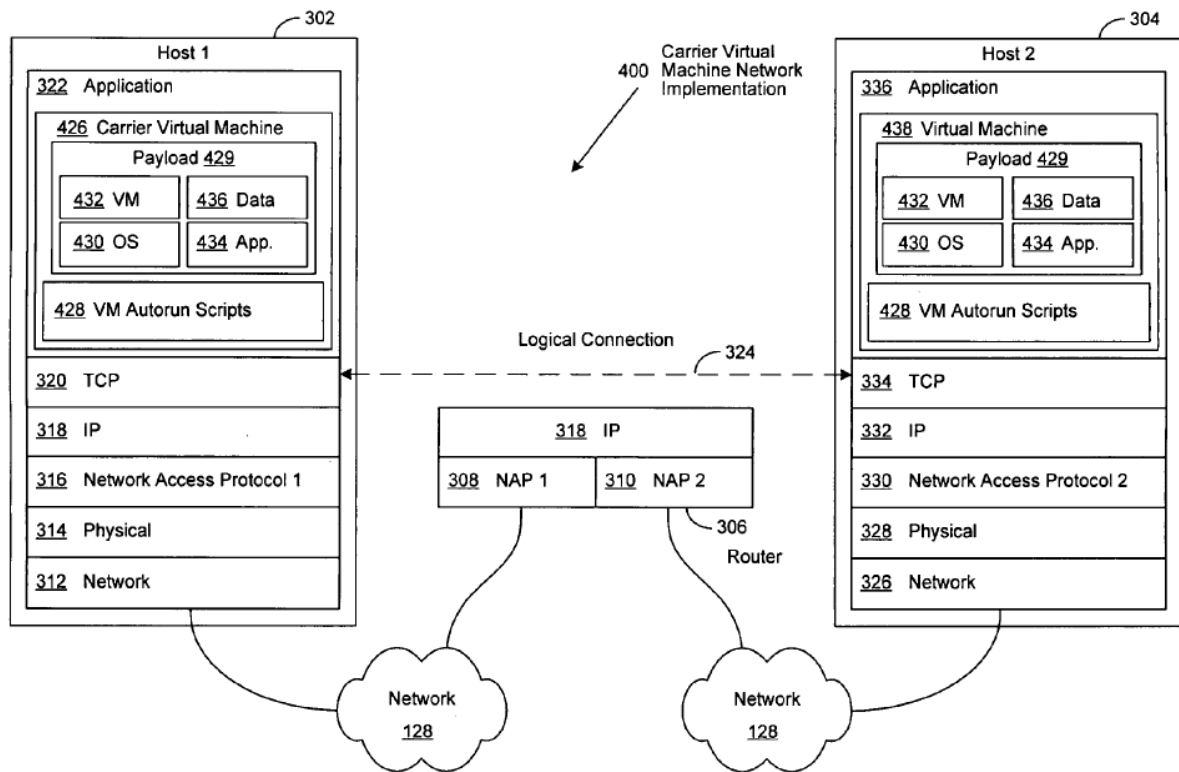


Figure 4

Figure 4 shows host 302 connected to host 304 through network 128. *Id.* Application 322 on host 302 includes carrier virtual machine 426, which contains “virtual machine autorun scripts 428, and a payload 429 that includes operating systems 430, other virtual machines 432, applications 434, and data 436.” *Id.* ¶ 42. “[C]arrier virtual machine 426 is migrated from participating physical host 302 using a multi-layer communications protocol stack . . . through network 128 to router 306.” *Id.* ¶ 43. Thereafter, carrier virtual machine 426 completes its migration to host 304 as virtual machine 438, and “carrier virtual machine 426 on participating physical host ‘1’ 302 can be destroyed (if required by security policies).” *Id.*

Figure 5a, reproduced below, illustrates a carrier virtual machine. *Id.* ¶ 46.

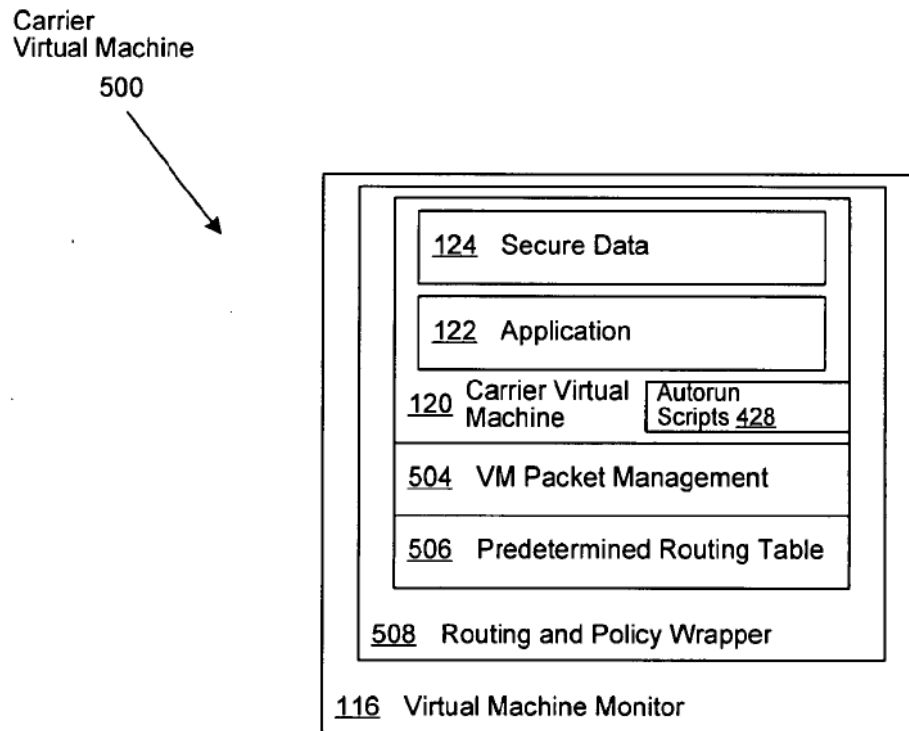


Figure 5a shows carrier virtual machine 120 associated with VM packet management 504 and predetermined routing table 506. *Id.* VM packet management 504 includes “security mechanisms such as access control lists (ACLs), usage policies, directory roles, etc.” *Id.* ¶ 47. “[P]redetermined routing table 506 manages originating and terminating network address” and “can translate between physical network addresses and virtual network addresses.” *Id.* ¶ 48. Further, “virtual machine monitor 116 can interact with routing and policy wrapper 508 to access information contained by predetermined routing table 506 and/or VM packet management 504 to facilitate the secure transfer of data across a network environment.” *Id.* ¶ 50.

2. Clark

Clark relates to “[m]igrating operating system instances across distinct physical hosts.” Ex. 1006, 1. In particular, Clark is “concerned with the migration of live, in-service OS instances on fast ne[t]works with only tens

of milliseconds of downtime.” *Id.* at 2. Clark describes a process that begins “with an active VM on physical host *A*.” *Id.* at 4. “A request is issued to migrate an OS from host *A* to host *B*,” and “all pages are transferred from *A* to *B*.” *Id.* The OS is suspended at host *A*, and its network traffic is redirected to host *B*. *Id.* After commitment of the migration transaction, “host *A* may now discard the original VM, and host *B* becomes the primary host.” *Id.* “Post-migration code runs to reattach device drivers to the new machine and advertise moved IP addresses.” *Id.*

3. Discussion

Claim 1 recites “enforcing network security and routing at a hypervisor layer via dynamic updating of routing controls initiated by a migration of said virtual machine from a first device to a second device.” Ex. 1001, 15:40–43. Petitioner contends “Dhawan discloses this limitation or at least renders it obvious when combined with Clark.” Pet. 36. First, Petitioner argues that “Dhawan teaches a migration of a virtual machine from a first device to a second device.” *Id.* at 36–38 (citing Ex. 1005 ¶¶ 17, 20, 43).

Second, Petitioner argues that the virtual machine migration “initiates dynamic updating of routing controls,” because “the routing controls that once directed traffic to the virtual machine at the first physical host must be updated to route that traffic to the virtual machine’s new physical location on the second host.” *Id.* at 37 (citing Ex. 1003 ¶ 135; Ex. 1005 ¶ 20). Petitioner further argues that “routing table 506—which ‘manages originating and terminating network addresses’—maps between the virtual network addresses and their new corresponding physical network addresses.” *Id.* at 37–38 (citing Ex. 1005 ¶ 48). Petitioner contends that

Dhawan's virtual machine monitor (hypervisor) "interact[s] with routing and policy wrapper 508 to access information contained by predetermined routing table 506 . . . to facilitate the secure transfer of data across a network environment." *Id.*, [0050] (***i.e., dynamically updating routing controls at the hypervisor layer***).

Id. at 38. As explained above, we agree with the parties' construction that "enforcing network security and routing at a hypervisor layer via dynamic updating of routing controls" requires "updating of routing controls at the hypervisor layer." Patent Owner argues, and we agree, that Petitioner fails to show how "'*interact[ing] with*' or '*accessing*' information is [] '*updating*,' . . . of routing controls' 'at a hypervisor layer.'" Prelim.

Resp. 34. In particular, Dr. Jakobsson testifies, in a conclusory manner, that Dhawan's "hypervisor [virtual machine monitor] updates the migrated virtual machine's routing controls." Ex. 1003 ¶ 132; *id.* ¶ 130.

Dr. Jakobsson further testifies, however, that "the virtual machine migration *initiates updating routing table 506*," not updating of routing controls *at the hypervisor layer* (virtual machine monitor). *Id.* ¶ 135 (citing Ex. 1003 ¶ 48); *id.* ¶ 136 ("a POSITA would have understood that when a virtual machine's physical address changes due to a physical migration, *the routing table must be updated* to reflect that change if the migrated virtual machine is to continue receiving network traffic."). Petitioner fails to explain sufficiently how the virtual machine monitor ("hypervisor") interacting with the routing and policy wrapper 508 to access information contained by routing table 506 results in "dynamic updating of routing controls at the hypervisor layer" as asserted. Pet. 38; Ex. 1003 ¶¶ 135–136.

Petitioner argues that to the extent Dhawan does not teach dynamically updating the routing controls, Clark teaches this limitation. Pet.

38. Specifically, Petitioner contends Clark teaches a virtual machine migration that a person of ordinary skill in the art would have understood as initiating an advertisement that “causes the routing controls to dynamically update.” *Id.* at 38–39 (citing Ex. 1003 ¶¶ 138–139; Ex. 1006, 4). Petitioner further contends that using ARP (Address Resolution Protocol) to advertise reconfigures peers to send packets to the new physical address. *Id.* at 39 (Ex. 1006, 4). Petitioner asserts that the reconfigurations are dynamic because they occur continuously with each advertisement consistent with a routing protocol. *Id.* Petitioner then contends that “Clark’s hypervisor layer, *i.e.*, virtual machine monitor, facilitates the dynamic routing updates.” *Id.* at 39 (citing Ex. 1006, 2, 7). Petitioner contends a person of ordinary skill in the art would have modified Dhawan’s method in view of Clark “to dynamically update routing controls by advertising the virtual machine migration” to “ensure[] that the virtual machine’s data traffic is routed to the correct location post-migration.” *Id.* at 39–40 (citing Ex. 1003 ¶¶ 141–142).

Although Petitioner points out that Clark’s virtual machine monitor “facilitates the dynamic routing updates,” it appears to us that Petitioner is not relying on Clark’s virtual machine monitor to meet the claimed hypervisor layer, but rather is proposing to include using Clark’s ARP. *Id.* at 38–40; Ex. 1003 ¶¶ 141–144. In any event, to the extent Petitioner is relying on Clark’s virtual machine monitor as the claimed hypervisor, we agree with Patent Owner (Prelim. Resp. 37–38) that Petitioner has failed to show that Clark’s virtual machine monitor (hypervisor) *facilitating* dynamic routing updates is the same as updating routing controls at the hypervisor layer.

Each of claims 3 and 6 depends directly from independent claim 1. For claims 3 and 6, Petitioner does not present arguments or evidence that

remedy the deficiencies in Petitioner’s contentions identified above with regard to claim 1. Pet. 41–45. For all of the above reasons, we are not persuaded that Petitioner has established a reasonable likelihood that Petitioner would prevail in its challenge that claims 1, 3, and 6 are unpatentable under 35 U.S.C. § 103(a) as obvious over Dhawan and Clark.⁸

D. Asserted Obviousness of Claims 2, 4, and 5 over Dhawan, Clark, and Warfield

Petitioner contends claims 2, 4, and 5 are unpatentable under 35 U.S.C. § 103(a) as obvious over Dhawan, Clark, and Warfield. Pet. 45–55.

1. Warfield

Warfield relates to “virtualizing network resources so that they may be shared across a set of isolated virtual machines (VMs).” Ex. 1007, 2. In particular, Warfield “describes the design approach that has been taken for the first public release of the XenoServers hypervisor, *Xen*.” *Id.* at 4. “Individual virtual machines may have one or more virtual interfaces, each of which appears as a point-to-point Ethernet link to an IP router.” *Id.* Xen’s network system “consists of a virtual firewall router, which is a rule-based packet classification/forwarding engine (based on the Linux netfilter/IPTables code) responsible for simple, fast packet handling.” *Id.* Warfield’s described “approach presents a model in which VMs appear as isolated as they would be were they separate physical machines on a shared switching element.” *Id.* at 5.

⁸ Because we find Petitioner has not shown a reasonable likelihood of prevailing on this challenge for the reasons discussed above, we do not reach Patent Owner’s remaining arguments.

2. Discussion

Each of claims 2, 4, and 5 depends either directly or indirectly from independent claim 1. For claims 2, 4, and 5, Petitioner does not present arguments or evidence that remedy the deficiencies in Petitioner's contentions identified above with regard to claim 1. Pet. 45–55.

Accordingly, for the same reasons discussed above, we are not persuaded that Petitioner has established a reasonable likelihood that Petitioner would prevail in its challenge that claims 2, 4, and 5 are unpatentable under 35 U.S.C. § 103(a) as obvious over Dhawan, Clark, and Warfield.

E. Asserted Obviousness of Claims 7 and 8 over Dhawan, Clark, Chandika, and the Knowledge of a Person of Ordinary Skill in the Art

Petitioner contends claims 7 and 8 are unpatentable under 35 U.S.C. § 103(a) as obvious over Dhawan, Clark, and Chandika. Pet. 55–61.

1. Chandika

Chandika describes “systems and methods for interconnecting a restricted device and a network,” and in particular, “a device for accessing the network [that] has various input ports, with each port having an associated parameter whose value is either restricted or unrestricted.”

Ex. 1008, 1:55–60. In an embodiment, an access device has packet detectors 220 that include content addressable memory (CAM) 222. *Id.* at 4:33–36.

The device can extract fields from the header of each received packet for packet detectors 220 to examine. *Id.* at 4:37–41. If extracted fields are found via a lookup in CAM 222, “then the packet matches a restricted pattern and thus the packet is restricted.” *Id.* at 4:42–45. CAM 222 can be “configured to hold access parameters based on access control lists (ACLs),”

which “allow dynamic configuration of the set of restricted patterns that are to be detected.” *Id.* at 4:51–55.

2. *Discussion*

Each of claims 7 and 8 depends either directly or indirectly from independent claim 1. For claims 7 and 8, Petitioner does not present arguments or evidence that remedy the deficiencies in Petitioner’s contentions identified above with regard to claim 1. Pet. 55–61. Accordingly, for the same reasons discussed above, we are not persuaded that Petitioner has established a reasonable likelihood that Petitioner would prevail in its challenge that claims 7 and 8 are unpatentable under 35 U.S.C. § 103(a) as obvious over Dhawan, Clark, and Chandika.

III. CONCLUSION

For the foregoing reasons, we determine that Petitioner has not shown a reasonable likelihood that it would prevail in showing that any of the challenged claims of the ’209 patent are unpatentable.

IV. ORDER

Accordingly, it is:

ORDERED that the Petition is *denied* as to all challenged claims, and no trial is instituted.

IPR2021-00832
Patent 8,381,209 B2

FOR PETITIONER:

Donald Daybell
ORRICK, HERRINGTON & SUTCLIFFE LLP
D2bptabdocket@orrick.com

FOR PATENT OWNER:

Lauren Robinson
Brenda Entzminger
Bunsow De Mory LLP
lrobinson@bdiplaw.com
bentzminger@bdiplaw.com