UNITED STATES PATENT AND TRADEMARK OFFICE

_____

BEFORE THE PATENT TRIAL AND APPEAL BOARD

_____

APPLE INC.,
Petitioner

v.

MPH TECHNOLOGIES OY,
Patent Owner

_____

Case IPR2019-00825
U.S. Patent No. 9,762,397

_____

**PETITIONER APPLE INC.'S REQUEST FOR REHEARING OF
DECISION DENYING INSTITUTION OF *INTER PARTES* REVIEW**

Mail Stop PATENT BOARD
Patent Trial and Appeal Board
U.S. Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

TABLE OF CONTENTS

I.   Introduction

Apple Inc. respectfully requests rehearing of the Board's November 6, 2019

decision denying institution of *inter partes* review of U.S. Patent No. 9,762,397.

Paper 7 ("DI"). In its decision, the Board asserted that "RFC3104 does not describe

any message ever being sent from address Nb to address Na," and "Dr. Goldschlag

does not explain how RFC3104's 'tunneling' operation results in the understanding

that a message sent to RSIP server N via address Nb is also sent to address Na."

DI, 11-12. The Board misapprehended the evidence relied on by Dr. Goldschlag to

support his opinion. In particular, a message sent from host Y to host X in

RFC3104 must necessarily flow through addresses Nb and Na of RSIP server N, as

explained by the Petition and Dr. Goldschlag's declaration.

II.   Standard of Review

"A party dissatisfied with a decision may file a request for rehearing,

without prior authorization from the Board." 37 C.F.R. § 42.71(d). The "burden of

showing a decision should be modified lies with the party challenging the

decision," and the request "must specifically identify all matters the party believes

the Board misapprehended or overlooked, and the place where each matter was

previously addressed in a motion, an opposition, or a reply." *Id.*

III.   Argument and Relief Requested

The Board based its institution denial on Apple's alleged failure to

demonstrate that RFC3104 renders obvious claim 1's recitation of "the

intermediate computer receiving a secure message having a first source address sent to an address of the intermediate computer" and "the intermediate computer sending the secure message in the secure connection to the destination address by using the address of the intermediate computer as a second source address." DI, 10-13. The Board respectfully misapprehended the evidence cited in the Petition, which shows that messages sent from host Y to host X in RFC3104 must flow through both RSIP server N's interface receiving packets at address Nb *and* RSIP server N's interface sending packets from address Na. Thus, any packet sent to address Nb must also be sent to address Na. Apple respectfully requests that the Board grant rehearing and institute trial of claims 1 and 2 of the '397 patent.

A. RFC3104 itself discloses that messages sent from host Y are sent to address Na of RSIP server N.

RFC3104 discloses that "IPsec packets from Y destined for X arrive at RSIP server N," and "[i]f N is able to find a matching mapping, it tunnels the packet to X according to the tunneling mode in effect." EX1004, 5; Pet., 38. This process is shown in the figure provided in RFC3104, as annotated in the Petition and Dr. Goldschlag's declaration:
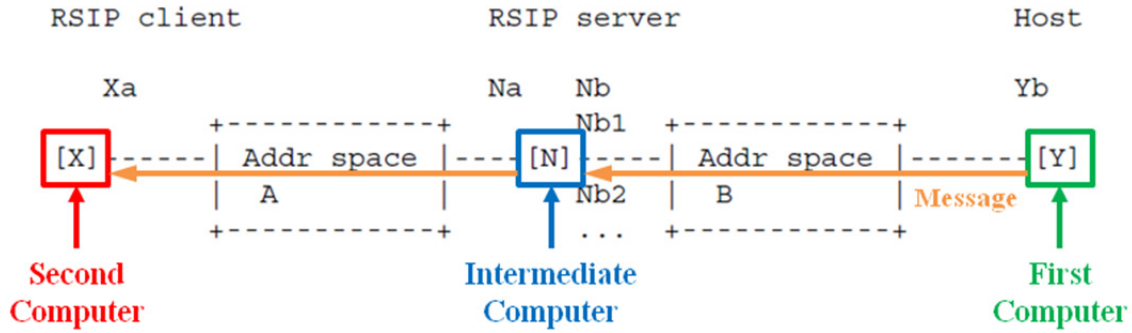
EX1004, 2 (annotated); Pet., 38; EX1002, ¶103.

As illustrated in the figure, RSIP server "N has two addresses: Na on address space A, and Nb on address space B. For example, A could be a private address space, and B the public address space of the general Internet." EX1004, 3; Pet., 26; EX1002, ¶83.
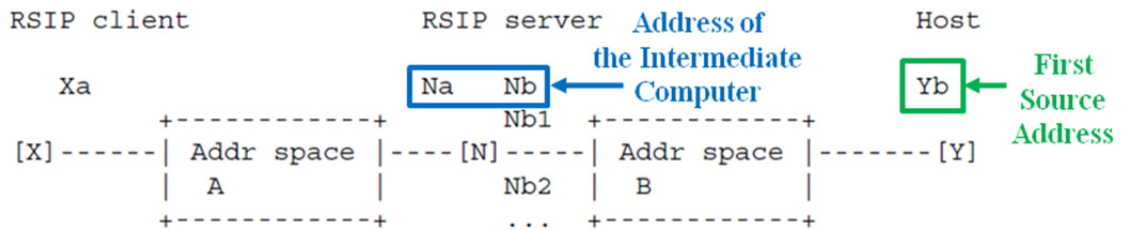
EX1004, 2 (annotated); Pet., 29; EX1002, ¶88.

Importantly, the parties do not dispute that a message sent from host Y is received at address Nb of RSIP server N (e.g., N's public interface), and then the same message is subsequently sent from address Na of server N (e.g., N's private interface) to host X. *See, e.g.*, Pet., 38-39, POPR, 18 ("RFC3104 teaches an RSIP Server N receiving a message at address Nb (from Host Y) and sending it out to RSIP Client X from address NA"). Thus, the message must flow through both

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.