UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CAVIUM, INC.

Petitioner

v.

ALACRITECH, INC.

Patent Owner

Case IPR. No. **Unassigned**

U.S. Patent No. 8,805,948

Title: INTELLIGENT NETWORK INTERFACE SYSTEM AND METHOD FOR PROTOCOL PROCESSING

Petition For *Inter Partes* Review of U.S. Patent No. 8,805,948 Under 35 U.S.C. §§ 311-319 and 37 C.F.R. §§ 42.1-.80, 42.100-.123

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

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

TABLE OF CONTENTS

Page

1. INTRODUCTION 1
2. REQUIREMENTS FOR PETITION FOR INTER PARTES REVIEW 1
   - 2.1. Grounds for Standing (37 C.F.R. § 42.104(a)) 1
   - 2.2. Notice of Lead and Backup Counsel and Service Information 1
   - 2.3. Notice of Real-Parties-in-Interest (37 C.F.R. § 42.8(b)(1)) 2
   - 2.4. Notice of Related Matters (37 C.F.R. § 42.8(b)(2)) 2
   - 2.5. Fee for Inter Partes Review 14
   - 2.6. Proof of Service 14
3. IDENTIFICATION OF CLAIMS BEING CHALLENGED (§42.104(B)) 14
4. **THERE IS NO FACTUAL BASIS FOR THE BOARD TO DENY INSTITUTION UNDER 35 U.S.C. §314(A) OR §325(D)** 17
5. BACKGROUND OF TECHNOLOGY 21
   - A. Layered Network Protocols 22
   - B. TCP/IP 23
   - C. Protocol Offload and Fast-Path Processing 27
   - D. Direct Memory Access 29
6. OVERVIEW OF THE 948 PATENT 30
7. 948 PATENT PROSECUTION HISTORY 32
8. CLAIM CONSTRUCTION 34
   - 8.1. Applicable Law 34
   - 8.2. Construction of Claim Terms 34
9. PERSON HAVING ORDINARY SKILL IN THE ART 34
10. DESCRIPTION OF THE PRIOR ART 35
    - 10.1. Thia 35
    - 10.2. Tanenbaum96: A. Tanenbaum, Computer Networks, 3rd ed. (1996) 39

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

10.3. Stevens2: TCP-IP Illustrated, Vol.2 45
10.4. Motivations To Combine 47
10.4.1. Thia in combination with Tanenbaum96 47
10.4.2. Thia in combination with Tanenbaum96 and Stevens2 50
11. GROUND #1: 51
11.1. Claim 1 52
11.1.1. [1.P] A method for network communication by a host computer having a network interface that is connected to the host by an input/output bus, the method comprising....................52
11.1.2. [1.1] running, on the host computer, a protocol processing stack including an Internet Protocol (IP) layer and a Transmission Control Protocol (TCP) layer, with an application layer running above the TCP layer; 54
11.1.3. [1.2] initializing, by the host computer, a TCP connection that is defined by source and destination IP addresses and source and destination TCP ports;................57
11.1.4. [1.3] receiving, by the network interface, first and second packets, wherein the first packet has a first TCP header and contains first payload data for the application, and the second packet has a second TCP header and contains second payload data for the application;....................59
11.1.5. [1.4] checking, by the network interface, whether the packets have certain exception conditions, including checking whether the packets are IP fragmented, checking whether the packets have a FIN flag set, and checking whether the packets are out of order; 61
11.1.6. [1.5] if the first packet has any of the exception conditions, then protocol processing the first TCP header by the protocol processing stack; 63

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

11.1.7. [1.6] if the second packet has any of the exception conditions, then protocol processing the second TCP header by the protocol processing stack; 63

11.1.8. [1.7] if the packets do not have any of the exception conditions, then bypassing host protocol processing of the TCP headers and storing the first payload data and the second payload data together in a buffer of the host computer, such that the payload data is stored in the buffer in order and without any TCP header stored between the first payload data and the second payload data. 64

11.2. Claim 3 68

11.2.1. [3] The method of claim 1, wherein storing the first payload data and the second payload data together in a buffer of the host computer is performed by a direct memory access (DMA) unit of the network interface. 68

11.3. Claim 6 69

11.3.1. [6] The method of claim 1, including comparing, by the network interface, the IP addresses and TCP ports of the packets with the source and destination IP addresses and source and destination TCP ports that define the TCP connection...69

11.4. Claim 7 71

11.4.1. [7] The method of claim 1, wherein checking whether the packets have certain exception conditions includes checking whether the packets have a RST flag set.............71

11.5. Claim 8 71

11.5.1. [8] The method of claim 1, wherein checking whether the packets have certain exception conditions includes checking whether the packets have a SYN flag set. 71

11.6. Claim 17 72

11.6.1. [17.P] An apparatus for network communication, the apparatus comprising: 72

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

11.6.2. [17.1] a host computer running a protocol stack including an Internet Protocol (IP) layer and a Transmission Control Protocol (TCP) layer, the protocol stack adapted to establish a TCP connection for an application layer running above the TCP layer, the TCP connection being defined by source and destination IP addresses and source and destination TCP ports; 74

11.6.3. [17.2] a network interface that is connected to the host computer by an input/output bus, the network interface adapted to parse the headers of received packets to determine whether the headers have the IP addresses and TCP ports that define the TCP connection and to check whether the packets have certain exception conditions, including whether the packets are IP fragmented, have a FIN flag set, or are out of order, the network interface having logic that directs any of the received packets that have the exception conditions to the protocol stack for processing, and directs the received packets that do not have any of the exception conditions to have their headers removed and their payload data stored together in a buffer of the host computer, such that the payload data is stored in the buffer in order and without any TCP header stored between the payload data that came from different packets of the received packets..76

11.7. Claim 19 80

11.7.1. [19] The apparatus of claim 17, wherein the network interface includes a direct memory access (DMA) unit that is adapted to store the payload data in the buffer. 80

11.8. Claim 21 81

11.8.1. [21] The apparatus of claim 17, wherein the exception conditions include having a RST flag set. 81

11.9. Claim 22 82

11.9.1. [22] The apparatus of claim 17, wherein the exception conditions include having a SYN flag set. 82

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

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.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**

fastcase®
Smarter legal research.