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 13
   - 2.6. Proof of Service 14
3. IDENTIFICATION OF CLAIMS BEING CHALLENGED (§42.104(B)) 14
4. BACKGROUND OF TECHNOLOGY 14
   - A. Layered Network Protocols 15
   - B. TCP/IP 16
   - C. Protocol Offload and Fast-Path Processing 20
   - D. Direct Memory Access 22
5. OVERVIEW OF THE 948 PATENT 23
6. 948 PATENT PROSECUTION HISTORY 25
7. CLAIM CONSTRUCTION 27
   - 7.1. Applicable Law 27
   - 7.2. Construction of Claim Terms 27
8. PERSON HAVING ORDINARY SKILL IN THE ART 27
9. DESCRIPTION OF THE PRIOR ART 28
   - 9.1. Thia 28
   - 9.2. Tanenbaum96: A. Tanenbaum, Computer Networks, 3rd ed. (1996) 32
   - 9.3. Stevens2: TCP-IP Illustrated, Vol.2 38
   - 9.4. Motivations To Combine 40

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

9.4.1. Thia in combination with Tanenbaum96 40
9.4.2. Thia in combination with Tanenbaum96 and Stevens2 43
10. GROUND #1: 44
10.1. Claim 1 45
10.1.1. [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 45
10.1.2. [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; 47
10.1.3. [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; 50
10.1.4. [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; 52
10.1.5. [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; 54
10.1.6. [1.5] if the first packet has any of the exception conditions, then protocol processing the first TCP header by the protocol processing stack; 56
10.1.7. [1.6] if the second packet has any of the exception conditions, then protocol processing the second TCP header by the protocol processing stack; 56
10.1.8. [1.7] if the packets do not have any of the exception conditions, then bypassing host protocol processing of

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

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. 57

10.2. Claim 3 61

10.2.1. [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. 61

10.3. Claim 6 62

10.3.1. [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. 62

10.4. Claim 7 64

10.4.1. [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. 64

10.5. Claim 8 64

10.5.1. [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. 64

10.6. Claim 9 65

10.6.1. [9.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: 65

10.6.2. [9.1] receiving, by the network interface, a first packet having a header including source and destination Internet Protocol (IP) addresses and source and destination Transmission Control Protocol (TCP) ports; 65

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

10.6.3. [9.2] protocol processing, by the host computer, the first packet, thereby initializing a TCP connection that is defined by the source and destination IP addresses and source and destination TCP ports; 66

10.6.4. [9.3] receiving, by the network interface, a second packet having a second header and payload data, wherein the second header has IP addresses and TCP ports that match the IP addresses and TCP ports of the TCP connection; 67

10.6.5. [9.4] receiving, by the network interface, a third packet having a third header and additional payload data, wherein the third header has IP addresses and TCP ports that match the IP addresses and TCP ports of the TCP connection; 68

10.6.6. [9.5] checking, by the network interface, whether the second and third 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;.....69

10.6.7. [9.6] if the second packet has any of the exception conditions, then protocol processing the second packet by the host computer;.....69

10.6.8. [9.7] if the third packet has any of the exception conditions, then protocol processing the third packet by the host computer;.....70

10.6.9. [9.8] if the second and third packets do not have any of the exception conditions, then storing the payload data of the second and third packets 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 of the second and third packets.....70

10.7. Claim 11 71

10.7.1. [11] The method of claim 9, wherein storing the payload data of the second and third packets together

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.