IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

| | | |
|---|---|---|
| CROSSROADS SYSTEMS, INC., | § | |
| | § | |
| Plaintiff, | § | |
| | § | CIVIL ACTION NO. 1:10-CV-652-SS |
| v. | § | |
| | § | JURY DEMANDED |
| (1) 3PAR, INC., | § | |
| (2) AMERICAN MEGATRENDS, INC., | § | |
| (3) RORKE DATA, INC., | § | |
| (4) D-LINK SYSTEMS, INC., | § | |
| (5) CHELSIO COMMUNICATIONS, INC., | § | |
| (a Delaware Corporation), | § | |
| (6) ISTOR NETWORKS, INC., and | § | |
| (7) CHELSIO COMMUNICATION, INC., | § | |
| (a California Corporation), | § | |
| | § | |
| Defendants. | § | |

## SUPPLEMENTAL DECLARATION OF JOHN LEVY, Ph.D.

I, John Levy, Ph.D., make the following declaration based on my own personal knowledge and, if called to testify before the court, could and would testify as follows:

1. Attached hereto are true and correct copies of:

Exhibit A: *NFS Version 3 Protocol Specification*, Internet Engineering Steering Group, RFC 1813, June, 1995;

Exhibit B: *NFS Version 3 Design and Implementation* by Pawlowski et al., USENIX Summer 1994, June 9, 1994;

Exhibit C: Portions of *Fibre Channel – Gigabit Communications and I/O for Computer Networks*, by Alan F. Benner, McGraw-Hill, 1996, p. 17 (Figure 2.1 – Fibre Channel Structural Hierarchy);

EXHIBIT: 1021
NAME: CQ
DATE:
SAMANTHA DOWNING, CSR

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

Exhibit D: Portions of *American National Standard for Information Technology- Fibre Channel-Arbitrated Loop (FC-AL)*, ANSI X3.272-1996;

Exhibit E: *SCSI-3 Block Commands (SBC),* ANSI NCITS 306-1998;

Exhibit F: *Fibre Channel Protocol for SCSI (FCP),* ANSI INCITS 269-1996;

Exhibit G: Portions of *International Standard for Information Technology – High-Performance Parallel Interface – Part 1: Mechanical, Electrical and Signaling Protocol Specification (HIPPI-PH)*, ISO/IEC 11518-1-1995;

Exhibit H: Portions of *American National Standard for Information Technology- Small Computer System Interface-2*, ANSI INCITS 131-1994 (R1999);

Exhibit I: *ISO/OSI, IEEE 802.2, and TCP/IP* by Tao Zhou, 1997, http://www.windowsitpro.com/article/tcpip/iso-osi-ieee-802-2-and-tcp-ip.aspxl;

Exhibit J: *Storage Vendors Push the Capacity Envelope: Infoworld* October 27, 1997 Volume 19, Issue 43, p. 48;

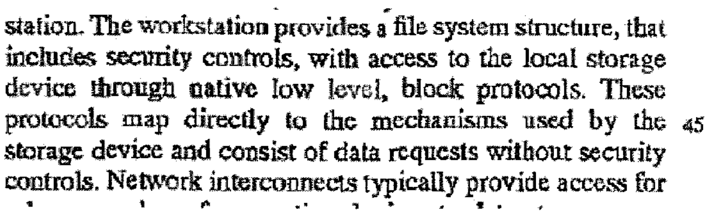
Exhibit K: *Internet Small Computer Systems Interface (iSCSI),* Internet Engineering Task Force RFC 3720, April, 2004;

Exhibit L: *OSI Reference Model—The ISO Model of Architecture for Open Systems Interconnection,* by Hubert Zimmermann, IEEE Transactions on Communications, vol. COM-28, no. 4, April, 1980.

**NLLBP and "Allow Access . . . Using NLLBP"**

2. The term native low level block protocol ("NLLBP") is not a term of art. The Patents-In-Suit describe a NLLBP:

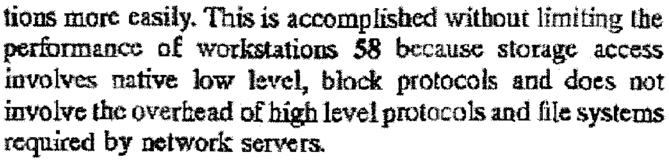
DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.



> station. The workstation provides a file system structure, that includes security controls, with access to the local storage device through native low level, block protocols. These protocols map directly to the mechanisms used by the storage device and consist of data requests without security controls. Network interconnects typically provide access for

Col. 1, ll. 42-47.[1]

3. A person of ordinary skill in the art at the time of filing (the filing date of Dec. 31, 1997 of United States Patent No. 5,941,972) would understand from the specification that an NLLBP is a protocol used to access a local storage device that is appropriate for that device. Additionally, the Patents-In-Suit describe that:

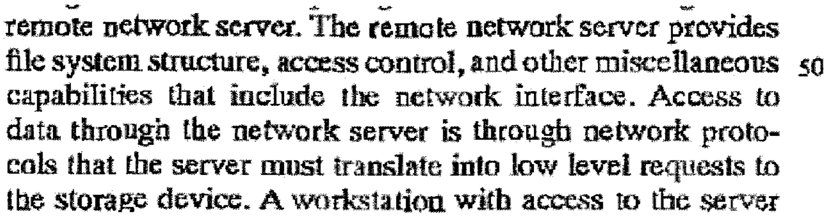


> tions more easily. This is accomplished without limiting the performance of workstations 58 because storage access involves native low level, block protocols and does not involve the overhead of high level protocols and file systems required by network servers.

Col. 5, ll. 1-5.

4. Therefore, a person of ordinary skill in the art at the time of filing would understand that NLLBPs do not involve the overhead of high level protocols and file systems typically required by network servers.

5. The Patents-In-Suit also use the term "network protocol." The Patents-In-Suit state, for example:



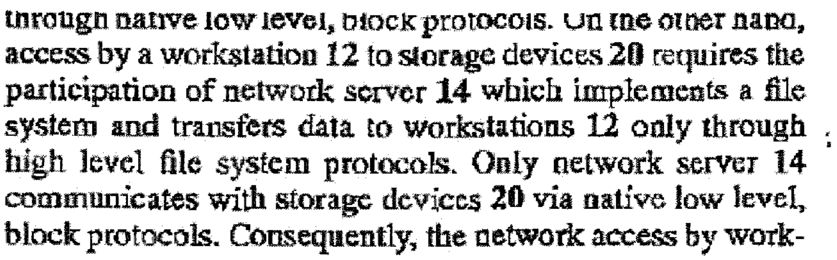
> remote network server. The remote network server provides file system structure, access control, and other miscellaneous capabilities that include the network interface. Access to data through the network server is through network protocols that the server must translate into low level requests to the storage device. A workstation with access to the server

Col. 1, ll. 49-54.

[1] All cites are to United States Patent No. 6,425,035 (the "'035 Patent") unless otherwise specified.

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

6. Thus, according to the Patents-In-Suit, a network protocol is a protocol that is used to access data through a network server, which the network server must then translate into low level requests to the storage device. The Patents-In-Suit specifically describe what is translated:



> through native low level, block protocols. On the other hand, access by a workstation 12 to storage devices 20 requires the participation of network server 14 which implements a file system and transfers data to workstations 12 only through high level file system protocols. Only network server 14 communicates with storage devices 20 via native low level, block protocols. Consequently, the network access by work-

Col. 3, ll. 17-23.

7. A person of ordinary skill in the art at the time of filing would understand that it is data access requests in high level file system protocols that are translated into low level requests to access data on storage devices. Therefore, a person of ordinary skill in the art at the time of filing would understand that a "network protocol" as used in the Patents-In-Suit is a protocol used to access data on a network server that includes high level file system protocols that are translated into low level requests by the network server in order to access storage.

8. To provide additional context, Figure 1 of the Patents-In-Suit illustrates a conventional network that provides access to storage devices through a network server.

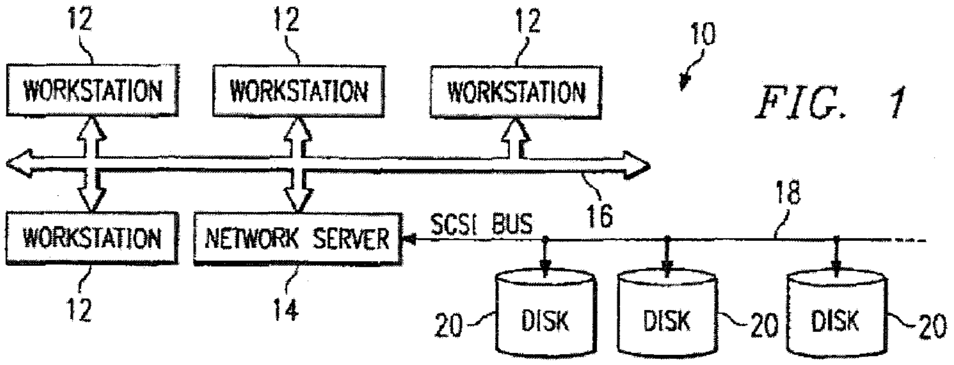


FIG. 1

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

9. To better understand how data is transferred in systems such as those depicted in Figure 1, some background on the operation of networks is helpful. This background is meant to provide a high-level understanding. Networks are best understood as having layers. Each layer uses the facilities and features of the layer below it. Conversely, each layer provides other, typically more abstract, facilities and features to the layer above it. Each layer in a network defines a protocol establishing rules for interaction between (two or more) devices connected through the network.

10. To provide a more specific example based on Figure 1, a network server 14 can be a network file server providing file access services to the networked workstations 12 and, for example, transferring information using Network File System (NFS), Remote Procedure Call (RPC) and Transmission Control Protocol / Internet Protocol (TCP/IP) protocols on the network. The network layers of the example of Figure 1, in which network server 14 uses NFS/RPC and TCP/IP protocols over an Ethernet network transport medium 16, can be visualized as shown in Table 1 below.

| *Network Layer* | *Typical usage* | *Purpose* |
|---|---|---|
| Network Application | **Network File System (NFS)** | **File access commands / responses** |
| Presentation/Session | Remote Procedure Call (RPC) | Invoke remote software / return response |
| Transport/Network | "datagram" delivery – addressing, routing, disassembly to and reassembly from packets (TCP/IP) | Encapsulate messages |
| Data Link / Physical | Data framing, hardware addressing, electrical signaling (Ethernet) | Deliver packets |

**Table 1**

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

# 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**