US007941526B1

(12) **United States Patent**
Hope et al.

(10) **Patent No.: US 7,941,526 B1**
(45) **Date of Patent: May 10, 2011**

(54) **TRANSMISSION OF SYSLOG MESSAGES OVER A ONE-WAY DATA LINK**

(75) Inventors: **James Hope**, Greenwich, CT (US); **Ronald Mraz**, South Salem, NY (US); **Andrew Holmes**, Darien, CT (US)

(73) Assignee: **Owl Computing Technologies, Inc.**, Ridgefield, CT (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 368 days.

(21) Appl. No.: **11/788,156**

(22) Filed: **Apr. 19, 2007**

(51) **Int. Cl.**
G06F 15/173 (2006.01)

(52) **U.S. Cl.** **709/224**

(58) **Field of Classification Search** 709/224
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,672,601	A	6/1987	Ablay	370/277
5,282,200	A	1/1994	Dempsey et al.	370/245
5,703,562	A	12/1997	Nilsen	
5,769,527	A	6/1998	Taylor et al.	362/85
5,983,332	A	11/1999	Watkins	711/202
6,108,787	A	8/2000	Anderson et al.	
6,262,993	B1	7/2001	Kirmse	370/463
6,269,398	B1	7/2001	Leong et al.	
6,415,329	B1	7/2002	Gelman et al.	
6,546,422	B1	4/2003	Isoyama et al.	709/225
6,665,268	B1	12/2003	Sato et al.	370/242
6,728,213	B1	4/2004	Tzeng et al.	370/235
6,731,625	B1	5/2004	Eastep et al.	
6,792,432	B1	9/2004	Kodavaila et al.	707/103 R
6,807,166	B1 *	10/2004	Ohura	370/352
6,954,790	B2	10/2005	Forslow	
6,988,148	B1 *	1/2006	Sheth	709/245
7,007,301	B2	2/2006	Crosbie et al.	
7,016,085	B2 *	3/2006	Gonzalez et al.	358/405
7,020,697	B1	3/2006	Goodman et al.	
7,095,739	B2	8/2006	Mamillapalli et al.	370/390
7,134,141	B2	11/2006	Crosbie et al.	

(Continued)

FOREIGN PATENT DOCUMENTS

WO WO 2004/105297 A2 12/2004

OTHER PUBLICATIONS

Ian Eaton, "The Ins and Outs of System Logging Using Syslog," 2003, SANS Institute, Australia.

(Continued)

Primary Examiner — David Y Eng
(74) *Attorney, Agent, or Firm* — Amster, Rothstein & Ebenstein LLP

(57) **ABSTRACT**

A special syslog daemon on a send node, wherein the send node is connected to a receive node by a one-way data link, the special syslog daemon configured to receive a syslog message from a syslog sender, insert a portion of IP information of the syslog sender in the body of the received syslog message and route the resulting syslog message to the one-way data link so that the resulting syslog message can be sent through the one-way data link to a syslog receiver communicatively coupled to the receive node. The present invention resolves the potential conflict between syslog and one-way data transfer applications that are configured to remove IP information from data prior to its passage through a one-way data link, thereby leading to a further enhancement of network security through their combination.

10 Claims, 2 Drawing Sheets