US007032242B1

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

(10) **Patent No.: US 7,032,242 B1**
(45) **Date of Patent: Apr. 18, 2006**

(54) **METHOD AND SYSTEM FOR DISTRIBUTED NETWORK ADDRESS TRANSLATION WITH NETWORK SECURITY FEATURES**

(75) Inventors: **David Grabelsky**, Skokie, IL (US); **Michael S. Borella**, Naperville, IL (US); **Ikhlaq Sidhu**, Vernon Hills, IL (US); **Danny M. Nessett**, Fremont, CA (US)

(73) Assignee: **3Com Corporation**, Marlborough, MA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/270,967**

(22) Filed: **Mar. 17, 1999**

Related U.S. Application Data

(63) Continuation-in-part of application No. 09/035,600, filed on Mar. 5, 1998, now Pat. No. 6,353,614.

(51) **Int. Cl.**
H04K 1/00 (2006.01)
H04L 9/00 (2006.01)
G06F 15/16 (2006.01)

(52) **U.S. Cl.** **726/11**; 726/3; 726/12; 726/26; 713/151; 713/153; 713/168; 709/201; 709/225; 709/229; 380/28; 380/270

(58) **Field of Classification Search** 713/201; 370/351, 356, 389
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,953,198 A 8/1990 Daly et al. 379/61
5,159,592 A 10/1992 Perkins

(Continued)

FOREIGN PATENT DOCUMENTS

WO WO 01/31888 5/2001

(Continued)

OTHER PUBLICATIONS

G. Montene, Internet Engineering Task Force, Internet Draft, "Negotiated Address Reuse" (NAR), <draft-montene-gro-aatn-nar-00.txt>, May 1998, pp. 1 to 22.

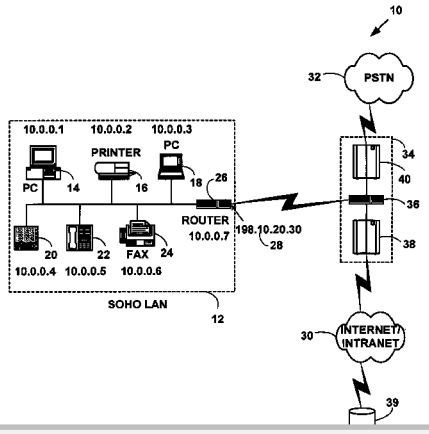
(Continued)

Primary Examiner—Gilberto Barron, Jr.
Assistant Examiner—A. Nobahar
(74) *Attorney, Agent, or Firm*—McDonnell Boehnen Hulbert & Berghoff LLP

(57) **ABSTRACT**

A method and system for distributed network address translation with security features. The method and system allow Internet Protocol security protocol ("IPsec") to be used with distributed network address translation. The distributed network address translation is accomplished with IPsec by mapping a local Internet Protocol ("IP") address of a given local network device and a IPsec Security Parameter Index ("SPI") associated with an inbound IPsec Security Association ("SA") that terminates at the local network device. A router allocates locally unique security values that are used as the IPsec SPIs. A router used for distributed network address translation is used as a local certificate authority that may vouch for identities of local network devices, allowing local network devices to bind a public key to a security name space that combines a global IP address for the router with a set of locally unique port numbers used for distributed network address translation. The router issues security certificates and may itself be authenticated by a higher certificate authority. Using a security certificate, a local network device may initiate and be a termination point of an IPsec security association to virtually any other network device on an IP network like the Internet or an intranet. The method and system may also allow distributed network address translation with security features to be used with Mobile IP or other protocols in the Internet Protocol suite.

33 Claims, 22 Drawing Sheets



U.S. PATENT DOCUMENTS

5,227,778	A		7/1993	Vacon et al.	
5,327,365	A		7/1994	Fujisaki et al.	364/717
5,497,339	A		3/1996	Bernard	364/705.5
5,526,353	A		6/1996	Henley et al.	370/60.1
5,526,489	A		6/1996	Nilakantan et al.	
5,550,984	A		8/1996	Gelb	
5,604,737	A		2/1997	Iwami et al.	370/352
5,606,594	A		2/1997	Register et al.	379/58
5,636,216	A		6/1997	Fox et al.	
5,654,957	A		8/1997	Koyama	370/355
5,708,655	A		1/1998	Toth et al.	
5,737,333	A		4/1998	Civanlar et al.	370/352
5,742,596	A		4/1998	Baratz et al.	370/356
5,754,547	A		5/1998	Nakazawa	370/401
5,793,657	A		8/1998	Nemoto	364/717.01
5,793,763	A		8/1998	Mayes et al.	
5,812,819	A		9/1998	Rodwin et al.	
5,828,846	A	*	10/1998	Kirby et al.	370/351
5,835,723	A		11/1998	Andrews et al.	395/200.56
5,862,331	A		1/1999	Herriot	395/200.49
5,867,495	A		2/1999	Elliott et al.	370/352
5,867,660	A		2/1999	Schmidt et al.	
5,872,847	A		2/1999	Boyle et al.	
5,889,774	A		3/1999	Mirashrafi et al.	370/352
5,892,924	A		4/1999	Lyon et al.	395/200.75
5,915,008	A		6/1999	Dulman	379/201
5,933,778	A		8/1999	Buhrmann et al.	455/461
5,950,195	A		9/1999	Stockwell et al.	
5,968,176	A	*	10/1999	Nessett et al.	713/201
5,983,350	A	*	11/1999	Minear et al.	713/201
6,011,782	A		1/2000	DeSimone et al.	
6,055,236	A		4/2000	Nessett et al.	
6,055,561	A		4/2000	Feldman et al.	709/200
6,058,421	A		5/2000	Fijolek et al.	709/225
6,079,021	A		6/2000	Abadi et al.	
6,101,189	A		8/2000	Tsuruoka	370/401
6,101,543	A		8/2000	Alden et al.	709/229
6,104,711	A		8/2000	Voit	370/352
6,115,751	A		9/2000	Tam et al.	709/240
6,134,591	A		10/2000	Nickles	
6,137,791	A		10/2000	Frid et al.	370/352
6,157,950	A		12/2000	Krishnan	709/223
6,172,986	B1		1/2001	Watanuki et al.	370/466
6,185,184	B1		2/2001	Mattaway et al.	370/230
6,195,705	B1		2/2001	Leung	709/245
6,212,183	B1		4/2001	Wilford	370/392
6,212,563	B1		4/2001	Beser	709/227
6,249,820	B1		6/2001	Dobbins et al.	709/238
6,266,707	B1		7/2001	Boden et al.	709/245
6,269,099	B1		7/2001	Borella et al.	370/389
6,353,614	B1		3/2002	Borella et al.	370/389
6,353,891	B1		3/2002	Borella et al.	713/201
6,438,612	B1	*	8/2002	Ylonen et al.	709/249
6,510,513	B1	*	1/2003	Danieli	713/156

FOREIGN PATENT DOCUMENTS

WO	WO 01/31888	A1	5/2001

OTHER PUBLICATIONS

George Tsirtis, Alan O'Neill, Internet Engineering Task Force, Internet Draft, "NAT Bypass for End 2 End 'Sensitive' Applications," <draft-tsirtsis-nat-bypass-00.txt>, Jan. 1998, pp. 1 to 5.

George Tsirtis, Pyda Srishuresh, Internet Engineering Task Force, Internet Draft, "Network Address Translation—Protocol Translation" (NAT-PT), <draft-ietf-ngtrans-natpt-04.txt>, Jan. 1999, pp. 1 to 13.

Jeffrey Lo, K, Taniguchi, Internet Engineering Task Force, Michael Borella, David Grabelsky, Ikhlaq Sidhu, Brian Petry, Internet Engineering Task Force, Internet Draft, "Distributed Network Address Translation," <draft-borella-aatn-dnat-01.txt>, Oct. 1998, pp. 1 to 21.

P. Srisuresh, G. Tsirsis, P. Akkiraju, A. Heffernan, Internet Engineering Task Force, Internet Draft, "DNS Extensions to Network Address Translators" (DNS_ALG), <draft-ietf-nat-dns-01.txt>, Oct. 1998, pp. 1 to 24.

P. Srisuresh, Internet Engineering Task Force, Internet Draft "Security for IP Network Address Translator (NAT) Domains," <draft-ietf-nat-security-00.txt.>, Nov. 1998, pp. 1 to 11.

P. Srisuresh, K. Eg, Internet Engineering Task Force, Internet Draft, "The IP Network Address Translator" (NAT), <draft-rfced-info-srisuresh-05.txt>, Feb. 1998, pp. 1 to 24.

P. Srisuresh, K. Egev, Internet Engineering Task Force, Internet Draft, "Traditional IP Network Address Translator (Traditional NAT)," <draft-ietf-nat-traditional-01.txt>, Oct. 1998, pp. 1 to 17.

P. Srisuresh, Matt Holdrege, Internet Engineering Task Force, Internet Draft, "IP Network Address Translator (NAT) Terminology and Consideration," <draft-ietf-nat-terminology-01.txt>, Oct. 1998, pp. 1 to 28.

Praveen Akkiraju, Yakov Rekhter, Internet Engineering Task Force, Internet Draft, "A Multihoming Solution Using NATs" <draft-akkiraju-nat-multihoming-00.txt>, Nov. 1998, pp. 1 to 32.

R. G. Moskowitz, Internet Engineering Task Force, Internet Draft, "Network Address Translation Issues with IPsec," <draft-moskowitz-net66-vpn-00.txt>, Feb. 5, 1998, p. 1 to 8.

R. Thay, N. Doraswa and R. Gle, Internet-Engineering-Task Force, Internet Draft "IP Security," <drat-ietf-ipsec-doc-roadmap-02.txt.>, Nov. 1997, pp. 1 to 12.

T. Hain, Internet Engineering Task Force, Internet Draft, "Architectural implications of NAT," <draft-iab-nat-implications-02.txt>, Oct. 1998, pp. 1 to 14.

W.T. Teo, S.W. Yeeow, R. Singh, Internet Engineering Task Force, Internet Draft, "IP Relocation Through Twice Network Address Translator," <draft-ietf-nat-rnat-00.txt>, Feb. 1999, pp. 1 to 20.

W.T. Teo, S.W. Yeow, R. Singh, Internet Engineering Task Force, Internet Draft, "Reverse Twice Network Address Translators" (RAT), <draft-teoyeow-mip-rat-01.txt>, Dec. 1998, pp. 1 to 20.

W.T. Teo, Y. Li, Internet Engineering Task Force, Internet Draft, "Mobile IP Extension for Private Internets Support," <draft-teoyli-mobileip-mvpn-02.txt>, Feb. 1999, pp. 1 to 24.

Yakov Rekhter, Internet Engineering Task Force, Internet Draft, "Implications of NATs on the TCP/IP Architecture," <draft-ietf-nat-arch-implications-00.txt>, Feb. 1999, pp. 1 to 7.

K. Egevang and P. Francis, "The IP Network Address Translator (NAT)", RFC 1631, Internet Engineering Task Force, www.ietf.org/rfc/rfc1631.txt, May 1994, pp. 1 to 10.

Borella, Michael, *Technology Update—Protocol Helps Stretch IPv4 Addresses*, "Network World", vol. 17, No. 3, Jan. 17, 2000, p. 43.

Kent, Stephen, *Evaluating Certification Authority Security*, Aerospace Conference, 1998 IEEE, Online, vol. 4, pp. 319-327 (Mar. 21-23, 1998).

Thayer, Rodney, *Bulletproof IP With Authentication and Encryption IPSec Adds a Layer of Armor to IP*, Data Communications, vol. 26, No. 16, pp. 55-58, 60 (Nov. 21, 1997).

Borella, M., Grabelsky, D., Lo, J., Tuniguchi, K., Internet Engineering Task Force, Internet Draft, "Realm Specific IP:

Borella, M., Grabelsky, D., Lo, J., Tuniguchi, K., Internet Engineering Task Force, Internet Draft, "Realm Specific IP: Procotol Specification <draft-ietf-nat-rsip-protocol-.07.txt>", Jul. 2000, pp. 1-49.
Montenegro, G., Internet Engineering Task Force, Internet Draft, "RSIP Support for End-to-End IPsec," <draft-ietf-nat-rsip-ipsec-04.txt>, Jul. 2000, pp. 1 to 17.
Borella, M., Lo, J., Grabelsky, D., Montenegro, G., Internet Engineering Task Force, Internet Draft, "Realm Specific IP: Framework <draft-ietf-nat-rsip-framework-05.txt>", Jul. 2000, pp. 1-30.
Borella, M., Montenegro, G., *RSIP: Address Sharing with End-to-End Security*, USENIX Conference, San Francisco, California, Mar. 9, 2000, pp. 1-9.
Handley, M., et al., *SIP: Session Initiation Protocol*, Network-Working Group, Request for Comments 2543, Mar. 1999, pp. 1 to 153.
ITU-T Recommendation H.225.0, *Call Signaling Protocols and Media Stream Packetization for Packet-Based Multimedia Communication Systems*, Series H: Audiovisual and Multimedia Systems—Infrastructure of Audiovisual Services—Transmission Multiplexing and Synchronization, (Feb., 1998).
ITU-T Recommendation H.323, *Packet-Based Multimedia Communications Systems*, Series H: Audiovisual and Multimedia Systems—Infrastructure of Audiovisual Services—Systems and Terminal Terminal Equipment for Audiovisual Services, (Feb. 1998).
McCanne et al., "The BSD Packet Filter: A New Architecture for User-Level Packet Capture," Proceedings of the 1993 Winter USENIX Technical Conference (Jan. 1993).
Postel, J., *User Datagram Protocol* , Request for Comments 768, Aug. 1980, pp. 1 to 3.
Postel, J., *Internet Protocol*, Request for Comments 791, Sep. 1981, pp. 1 to 45.
Postel J., *Internet Control Message Protocol*, Request for Comments 792, Sep. 1981, pp. 1 to 21.
Postel, J., *Transmission Control Protocol*, Request for Comments 793, Sep. 1981, pp. i to 84.
Postel, J., *File Transfer Protocol* (*FTP*), Request for Comments 959, Oct. 1985, pp. 1 to 69.
Jacobson, V., *TCP Extensions for High Performance*, Request for Comments 1323, May 1992, pp. 1 to 37.
Droms, R., *Dynamic Host Configuration Protocol*, Request for Comments 2131, Mar. 1997, pp. 1 to 45.
Stevens, W., *Advanced Sockets API for IPv6*, Request for Comments 2292, Feb. 1998, pp. 1 to 67.
Gilligan, R. et al., *Basic Socket Interface Extensions for IPv6*, Request for Comments 2553, Mar. 1999, pp. 1 to 41.
Srisuresh, P.,et al., *IP Network Address Translator*(*NAT*) *Terminology and Considerations*, Request for Comments 2663, Aug. 1999, pp. 1 to 30.
Maurice J. Bach, The Design of the Unix Operating System, Prentice Hall Software Series, 1986, pp. 382-390.
Durand, Alain, *Deploying Ipv6*, IEEE Internet Computing, http://computer.org/internet, Jan.-Feb. 2001, pp. 79-81.
3COM SIP Sloutions 1.0 benefits brochure. (4 total pages).
Sidhu, Ikhlaq and Bezaitis, Andrew, Eat or be eaten, www.americasnetwork.com/issues/99issues/991101/991191_eat.htm, printed May 10, 2000. (6 total pages).
Myers, Brad A.; Stiel, Herb; and Gargiulo, Robert, Collaboration Using Multiple PDAs Connected to a PC, Proceedings of the ACM 1998 conference on Computer supported cooperative work, Nov. 14-18, 1998, Seattle, WA. (total 11 pages).
Dalgic, Ismail; Borella, Michael; Dean, Rick; Grabiec, Jacek; Mahler, Jerry; Schuster, Guido; and Sidhu, Ikhlaq, True Number Portability and Advanced Call Screening in a SIP-Based IP Telephony System, *IEEE Communications Magazine*, vol. 37, No. 7, Jul. 1999, pp. 96-101. (8 total pages).
Handley/Schulzrinne/Schooler/Rosenberg, SIP: Session Initiation Protocol, Internet Engineering Task Force, draft-ietf-sip-rfc2543bis-02.ps. Sep. 4, 2000. (131 pages).
Borella, M., Lo., J., Grabelsky, D., Montenegro, G., IETF Proceedings presentation, Realm Specific IP: Protocol Specification <draft-nat-rsip-protocol-00.txt>, Apr. 9, 1999 (13 pages).
Marsan, Carolyn Duffy, The Next Best Things to Ipv6? Network World Fusion at http://www.nbwfusion.com/news/1999/0920ipv6.html, Mar. 29, 2000, pp. 1-3.
Borella, M., Lo, J., Grabelsky, D., Montenegro, G., Internet Engineering Task Force, Internet Draft, "Realm Specific IP: Framework <draft-ietf-nat-rsip-framework-.04.txt>", Mar. 2000, pp. 1-30.
IETF Mar. 1999 Proceedings, 2.7.10 Network Address Translators (nat), pp. 1-13.
Rosenberg, Jonathan D. and Shockey, Richard, The Session Initiation Protocol (SIP): A Key Component for Internet Telephony, ComputerTelephony.com, Jun. 2000, pp. 124-139.
Fenner, W., *Internet Group Management Protocol Version 2*, RFC 2236, Nov. 1997, pp. 1-24.
Mogul, J. et al., "*Internet Standard Subnetting Procedure*", RFC 950, Aug., 1985, pp. 1-18.
Schulzrinne et al., "*RTP: A Transport Protocol for Real-Time Applications*", RFC 1889, pp. 1-75.
Privat Jermone, "*Double Phase DHCP Configuration*", <draft-privat-dhc-doublephase-01.txt>, Internet Engineering Task Force, Sep. 1999, pps. 1-4.
Maughan, D. et al., "*Internet Security Association and Key Management Protocol*", RFC 2408, Nov. 1998, pps. 1-86.
Karn, P., "*Photuris Session-Key Management Protocol*", RFC-2522, Mar. 1999, pps. 1-58.
"*Random Number Generators*", Computational Science Education Projects, 1991, 1992, 1993, 1994, and 1995.
Foster, Ian, "*10 Random Numbers*", 1995.
Borella, Michael et al., "*Realm Specific IP: Protocol Specification*", <draft-ietf.nat-rsip-protocol-02.txt>, Internet Draft, Aug. 1999, pps. 1-27.
Gilligan, R. et al., "*Transition Mechanisms for IPv6 Hosts and Routers*", RFC 1933, Apr. 1996, pps. 1-22.
Afifi, H. et al., "*Method for IPv4-IPv6 Transition*", Proceedings IEEE International Symposium on Computers and Communications, Jul. 6-8, 1999, pps. 478-484.
"Cisco IOS Release 12.0 Network Protocols Configuration Guide, Part. 1", Configuring IP Addressing, Cisco Systems, 1998, pp. P1C-7 to P1C-58.
International Search Report for PCT Application Serial No. PCT/US00/07057, Dated Aug. 9, 2000.
"Cisco IOS Release 12.0 Network protocols Configuration Guide, Part 1", Configuring IP Addressing, CISCO Systems, 1998, pp. P1C-7 to PiC-58.
International Search Report for PCT Application Serial No. PCT/US00/07057, Dated Aug. 9, 2000.

* cited by examiner

FIG. 1

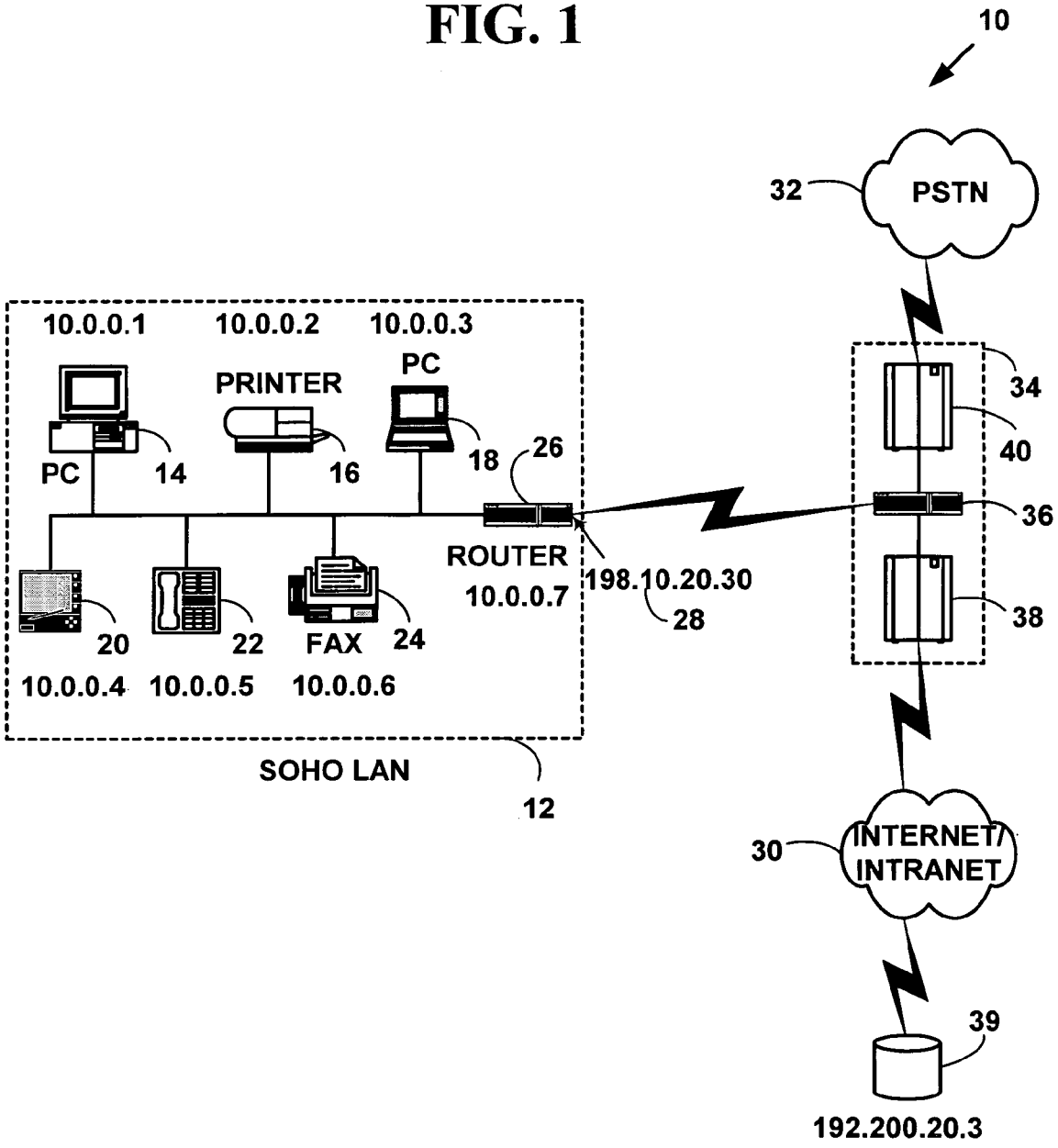
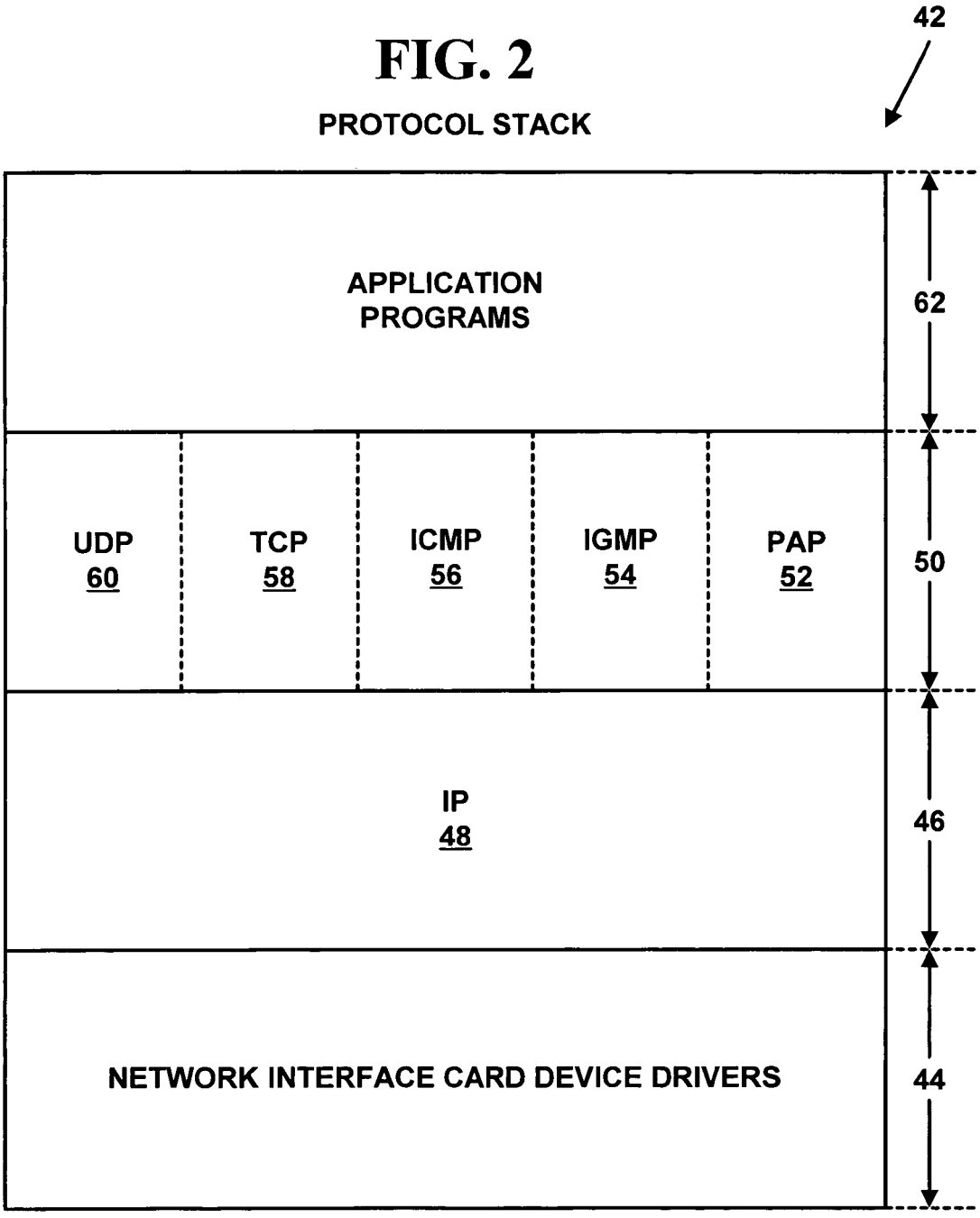


FIG. 2



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.