(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
26 September 2002 (26.09.2002)

PCT

(10) International Publication Number
WO 02/075548 A1

(51) International Patent Classification[7]: G06F 11/30, 12/14, H04L 9/00, 9/32

(21) International Application Number: PCT/US02/08577

(22) International Filing Date: 20 March 2002 (20.03.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/276,923	20 March 2001 (20.03.2001)	US
60/276,953	20 March 2001 (20.03.2001)	US
60/276,955	20 March 2001 (20.03.2001)	US
10/023,043	17 December 2001 (17.12.2001)	US

(71) Applicant: WORLDCOM, INC. [US/US]; 500 Clinton Center Drive, Clinton, MS 39056 (US).

(72) Inventor: MCDYSAN, David, E.; 2159 Astoria Circle #104, Herndon, VA 20170 (US).

(74) Agent: GROLZ, Edward, W.; Scully, Scott, Murphy & Presser, 400 Garden City Plaza, Garden City, NY 11530 (US).

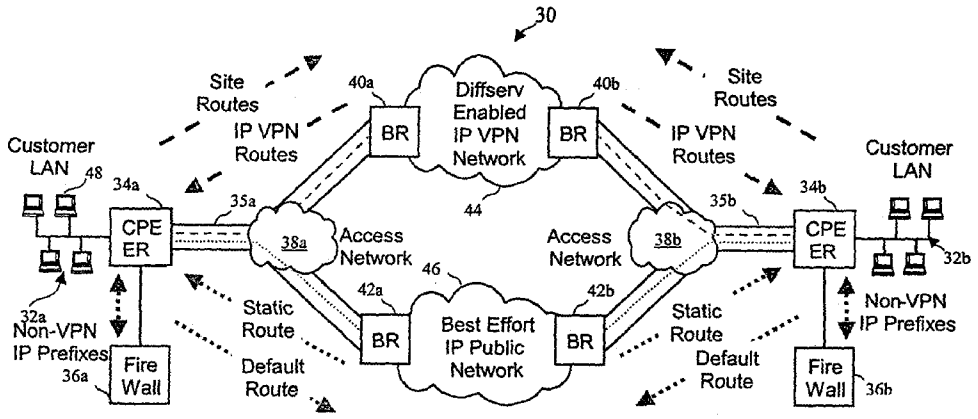
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: SYSTEM, METHOD AND APPARATUS THAT EMPLOY VIRTUAL PRIVATE NETWORKS TO RESIST IP QoS DENIAL OF SERVICE ATTACKS



(57) Abstract: A network architecture (30) in accordance with the present invention includes a communication network that supports one or more network-based Virtual Private Networks (VPNs) (44, 46). The communication network includes a plurality of boundary routers (40, 42) that are connected by access links (35) to CPE edge routers (34) belonging to the one or more VPNs (44, 46). To prevent traffic from outside a customer's VPN (e.g., traffic from other VPNs or the Internet at large) from degrading the QoS (Quality of service) provided to traffic from within the customer's VPN, the present invention gives precedence to intra-VPN traffic over extra-VPN traffic on each customer's access link through access link prioritization or access link capacity allocation, such that extra-VPN traffic cannot interfere with inter-VPN traffic. Granting precedence to intra-VPN traffic over extra-VPN traffic in this manner entails special configuration of network elements and protocols, including partitioning between intra-VPN and extra-VPN traffic on the physical access link using layer 2 multiplexing and the configuration of routing protocols to achieve logical traffic separation. By configuring the access networks, the VPN boundary routers (40, 42) and CPE edge routers (34) and the routing protocols of the edge and boundary routers in this manner, the high-level service of DoS (Denial of Service) attack prevention is achieved.

WO 02/075548 A1

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.