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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 November 2003 (27.11.2003)

PCT

(10) International Publication Number
WO 03/098393 A2

(51) International Patent Classification⁷: G06F

(21) International Application Number: PCT/US03/15262

(22) International Filing Date: 15 May 2003 (15.05.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/378,055 16 May 2002 (16.05.2002) US
10/255,608 27 September 2002 (27.09.2002) US

(71) Applicant *(for all designated States except US)*: **MESHNETWORKS, INC.** [US/US]; 485 North Keller Road, Suite 250, Maitland, FL 32751 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **SCHMIDT, Jeffrey** [US/US]; 305 Bougival Court, Orlando, FL 32828 (US). **GUTIERREZ, Philip** [US/US]; 13225 Lake Live Oak Drive, Orlando, FL 32828 (US). **BARKER, JR., Charles** [US/US]; 6005 Westgate Drive, #2223, Orlando, FL 32835 (US).

(74) Agents: **BUCZYNSKI, Joseph** et al.; Roylance, Abrams, Berdo & Goodman, L.L.P., 1300 19th Street, N.W., Suite 600, Washington, DC 20036 (US).

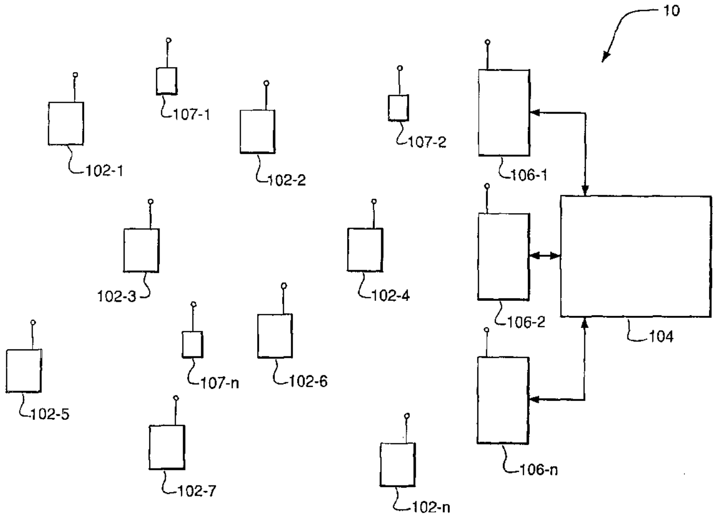
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, 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, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

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.

(54) **Title:** SYSTEM AND METHOD FOR A ROUTING DEVICE TO SECURELY SHARE NETWORK DATA WITH A HOST UTILIZING A HARDWARE FIREWALL



(57) **Abstract:** A system and method for providing the ability to selectively share data in a network routing device with an associated host. The system and method employs a hardware firewall in the routing device which restricts the host such that it can only access areas in shared memory which contains data destined for the host. The routing device CPU notifies the host of pending data and the location of that data in the shared memory. The hardware firewall is also notified of the location in shared memory which the host may access. When the host attempts to read the data, the firewall ensures that only the stated memory area or areas are accessed by the host. Once the data has been read by the host, the firewall is notified to cancel the host's ability to access the shared memory until such time as a new packet destined for the host arrives in the routing device.

A System And Method For A Routing Device To Securely Share Network Data With A Host Utilizing A Hardware Firewall

BACKGROUND OF THE INVENTION

Field of the Invention:

[0001] The present invention relates to a system and method for selectively sharing data contained in a network routing device with an associated host device. More particularly, the invention relates to a system and method for enabling routing device hardware to provide selective access by a host device to shared memory within the routing device, thus restricting the host's ability to access data not intended for use by the host. This application claims the benefit of U.S. Provisional Patent Application No. 60/378,055 entitled "A System And Method For A Routing Device To Securely Share Network Data With A Host Utilizing A Hardware Firewall", filed May 16, 2002, the entire contents of which being incorporated herein by reference.

Description of the Related Art:

[0002] In recent years, a type of mobile communications network known as an "ad-hoc" network has been developed. In this type of network, each user terminal is capable of operating as a base station or router for other mobile nodes, thus eliminating the need for a fixed infrastructure of base stations. Accordingly, data packets being sent from a source mobile node to a destination mobile node are typically routed through a number of intermediate mobile nodes before reaching the destination node.

[0003] More sophisticated ad-hoc networks are also being developed which, in addition to enabling mobile nodes to communicate with each other as in a conventional ad-hoc network, further enable the mobile nodes to access a fixed network and communicate with other types of user terminals, such as those on the public switched telephone network (PSTN) and on other networks, such as the Internet. Details of these types of ad-hoc networks are described in U.S. Patent Application Serial No. 09/897,790 entitled "Ad Hoc Peer-to-Peer Mobile Radio Access System Interfaced to the PSTN and Cellular Networks", filed on June 29, 2001, in U.S. Patent Application Serial No. 09/815,157 entitled "Time Division Protocol for an Ad-Hoc, Peer-to-Peer Radio Network Having Coordinating Channel Access to Shared Parallel Data Channels with Separate Reservation Channel", filed on March 22, 2001, and in U.S. Patent Application Serial No. 09/815,164 entitled "Prioritized-Routing for an Ad-Hoc, Peer-to-Peer, Mobile Radio Access System", filed on March 22, 2001, the entire content of each being incorporated herein by reference.

[0004] Generally, all nodes in a wireless ad-hoc peer-to-peer network provide similar core services and functionality, although their specific functionality can depend on their intended purposes, such as use as an access point, fixed router or mobile terminal. Although each node can provide similar services, the workload is typically distributed across many nodes rather than centralized at a single location in the peer-to-peer network. Therefore peer-to-peer networks distinguish themselves from infrastructure networks where one or more nodes offer a superset of the functionality of the rest of the network. Infrastructure nodes in these networks typically can handle Dynamic Host Configuration Protocol (DHCP), Address Resolution Protocol (ARP), as well as other services that depend on broadcast traffic. Dynamic Host Configuration Protocol is defined by IETF RFC 2131 and 2132, which are incorporated herein by reference, and is used by a client node to automatically obtain network settings from a central server. These network settings include the client's IP address, the address of Domain Name Servers (DNS), the IP address of default gateways, and many other network settings. Address Resolution Protocol is defined by STD 0037 and RFC 0826, which are incorporated herein by reference, and is used by a network node to map IP addresses to MAC addresses so IP traffic can be delivered to specific hardware. Such infrastructure nodes are normally discovered by broadcast traffic advertisements from their client nodes in a network.

[0005] As can be appreciated by one skilled in the art, traffic in such networks includes direct and indirect communications, in which nodes can be used as routers while both stationary or mobile. A mobile node typically includes a host, such as a personal computer (PC) or personal digital assistant (PDA), with an attached transceiver and a controller. A mobile node can further include a network interface device coupled to a host device, which allows the host device communication access with the network. The transceiver of the mobile node receives data packets, such as voice, data or multimedia data packets, from other nodes, and the controller determines which data packets are intended for it's associated host. If a data packet is intended for the associated host, the host is notified to retrieve the packet.

If the packet is not intended for the associated host, the controller determines the next node to which the data packet should be sent based on routing table or similar information, and controls the transceiver of the mobile node to send the data packet to the next node.

[0006] In traditional networks where the user nodes do not re-route traffic, the network interface device will inspect an incoming packet header and store packet data only if it is destined for the host device associated with the network interface device. Therefore, the host never has the opportunity to examine data which is intended for other devices. However, once a device is required to reroute packets to a destination device other than the associated host as in an ad-hoc network, all packets must be captured and evaluated by the routing device. Once a packet is captured by a network interface device, it then may become susceptible to unauthorized access by the associated host device.

[0007] However, the ability to selectively share data between a routing device and an associated host, such as a personal computer, is necessary in a wireless ad-hoc network. This allows a subscriber to have an access point for extracting or sending data through the network. Because the vast majority of routing resources or nodes that exist in a multihopping, ad-hoc network each route data that is not intended for its associated host, precautions must be taken to insure that only data intended for the node's associated host can be extracted from the routing device in the node. However, many of the methods for achieving this are either inefficient in their ability to route data, require use of multiple memories, or are insecure.

[0008] Accordingly, a need exists for a system and method for protecting data traveling through a network by ensuring that a host device may only access data that was intended for access by that host device.

SUMMARY OF THE INVENTION

[0009] An object of the present invention is to provide a system and method for restricting a host device from accessing network data which is not intended for host access.

[0010] Another object of the present invention is to provide a hardware implemented firewall internal to a routing device in a communication network, such as an ad-hoc network, to prevent unauthorized access by a host device to data stored in shared memory on the routing device.

[0011] A further object of the present invention is to restrict host access to the shared memory such that there may be no access, access to a single area, or access to multiple areas in the shared memory when required.

[0012] Another objective of the present invention is to disallow host access to the shared memory once the host has retrieved the data it is permitted to retrieve.

[0013] These and other objects are substantially achieved by providing a system and method to securely share data between a routing device and an associated host by utilizing a hardware firewall which restricts the host's access to a shared memory area on the routing device. The system and method employs a hardware firewall in the routing device which restricts the host such that it can only access areas in shared memory which contains data destined for the host. The routing device CPU notifies the host of pending data and the location of that data in the shared memory. The hardware firewall is also notified of the location in shared memory which the host may access. When the host attempts to read the data, the firewall ensures that only the stated memory area or areas are accessed by the host. Once the data has been read by the host, the firewall is notified to cancel the host's ability to access the shared memory until such time as a new packet destined for the host arrives in the routing device.

BRIEF DESCRIPTION OF THE DRAWINGS

[0014] These and other objects, advantages and novel features of the invention will be more readily appreciated from the following detailed description when read in conjunction with the accompanying drawings, in which:

[0015] Figure 1 is a conceptual block diagram of an example of an ad-hoc wireless communications network including a plurality of nodes employing an embodiment of the present invention;

[0016] Figure 2 is a conceptual block diagram of an example of components of a wireless node as shown in Figure 1, including firewall hardware elements in accordance with an embodiment of the present invention; and

[0017] Figure 3 is a flow diagram illustrating an example of the logic of a secure data transaction from the routing device of a node as shown in Figures 1 and 2 to the host associated with that routing device in accordance with an embodiment of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0018] Figure 1 is a block diagram illustrating an example of an ad-hoc packet-switched wireless communications network 10 employing an embodiment of the present invention. Specifically, the network 10 includes a plurality of mobile wireless user terminals 102-1 through 102-n (referred to generally as nodes or mobile nodes 102), and a fixed network 104 having a plurality of access points 106-1, 106-2, ...106-n (referred to generally as nodes or access points 106), for providing the nodes 102 with access to the fixed network 104. The fixed network 104 includes, for example, a core local access network (LAN), and a plurality of servers and gateway routers, to provide the nodes 102 with access to other networks, such as other ad-hoc networks, the public switched telephone network (PSTN) and the Internet.

[0019] The network 10 further includes a plurality of fixed routers 107-1 through 107-n (referred to generally as nodes or fixed routers 107) for routing data packets between other nodes 102, 106 or 107. As can be appreciated by one skilled in the art, the nodes 102, 106 and 107 are capable of communicating directly with each other, or via one or more other nodes operating as routers for data packets being sent between nodes, as described in U.S. Patent No. 5,943,322 to Mayor and in U.S. Patent Application Serial Nos. 09/897,790 and 09/815,157, referenced above. The data packets can include voice, data or multimedia.

[0020] Specifically, as shown in Figure 2, any of the nodes 102, 106 or 107 and, in particular, each mobile node 102, includes a routing device 1000 and a host device 100. The host 100 is typically a personal computer (PC) or personal digital assistant (PDA), used by a subscriber to gain access to the network 10 shown in Figure 1, but can be any number of devices, such as a notebook computer terminal, mobile telephone unit, mobile data unit, or any other suitable device. In this example, routing device 1000 includes two external interfaces. The host interface 200 allows a host device 100 and the routing device 1000 to communicate. The radio frequency (RF) interface 910 allows the RF signal 920 to be either received by or transmitted from the routing device 1000. The embodiment shown in Figure 2 utilizes an RF signal as the medium in the physical layer, as defined in the OSI model, ISO/IEC 7498-1 (1994), the entire contents being incorporated herein by reference. However, any type of medium, such as infrared, fiber optics, or wire, could be used by the physical layer to send the data packets between the nodes 102, 106 and 107.

[0021] As further shown in Figure 3, the routing device 1000 of Figure 3 includes an internal hardware firewall 300, a mailbox 400, a packet buffer 500, a routing device CPU 600, a modem interconnect bus 700, a baseband modem 800 and an RF section 900. The hardware firewall 300 provides selective read and write access to the packet buffer 500 by the host 100. The configuration and control of the hardware firewall 300 is controlled solely by the routing device CPU 600 in this example.

[0022] The mailbox 400 of the routing device 1000 in Figure 3 provides a common set of registers, shared by the host 100 and routing device CPU 600, which are used to exchange small amounts of data and messages. The packet buffer 500 of the routing device 1000 is a memory device also shared by the routing device CPU 600 and the host 100. The routing device CPU 600 includes a processor capable of executing instructions that control the functions of the modem 800, execute routing algorithms, and perform data movement transactions. The CPU 600 and modem 800 also include the appropriate hardware and software to provide IP, ARP, admission control (AC), traffic control (TC), ad-hoc routing (AHR), logic link control (LLC) and media access control (MAC). The transceiver 110 further includes the appropriate hardware and software for IAP association (IA), UDP, simple network management protocol (SNMP), data link (DL) protocol and dynamic host configuration protocol (DHCP) relaying.

[0023] The modem interconnect bus 700 of the routing device 1000 in Figure 3 is used to interconnect the elements of the modem transceiver. Further details of an example of this type of bus are described in U.S. Patent Application Serial No. 09/948,159 entitled "Multi-Master Bus Architecture for System-On-Chip Designs" filed on September 6, 2001, the entire content being incorporated herein by reference.

[0024] The baseband modem 800 of the routing device 1000 in Figure 3 modulates the outgoing signals to analog format, and demodulates incoming signals to digital format. The RF section 900 upconverts the modulated baseband signal for RF propagation and downconverts the received RF signal for demodulation by the modem 800, and the RF signal 920 provides the physical layer for communicating between routing devices in the nodes 102, 106 and 107.

[0025] In Figure 3, a flow diagram illustrating an example of the logic of a secure data transaction from the routing device 1000 to the host 100 in accordance with an embodiment of the present invention is shown. In step 1010 shown in Figure 3, data received at the routing device 1000 is transferred from the physical layer, such as an RF signal sent from another node 102, 106 or 107, to the modem 800 where it is converted to digital format. In the embodiment shown in Figure 3, an RF signal is used as the medium in the physical layer, however as pointed out above, any type of medium could be used by the physical layer, such as infrared, fiber optics, or wire.

[0026] In step 1020, the digital format packet is transferred from the baseband modem 800 to the packet buffer 500 by the routing device CPU 600. In step 1030, the routing device CPU 600 determines if the local host 100 needs access to the data, and then notifies the hardware firewall 300 of the specific packet buffer 500 area which the host 100 is to be allowed access. If the packet is not destined for the associated host 100, the host is not notified of the new packet.

[0027] In step 1040, the routing device CPU 600 places the address range of the data to be delivered to the host 100 in the mailbox 400 and then signals the host 100 to retrieve the message from the mailbox. In step 1050, the host 100 reads the message in the mailbox 400 and discovers what part of the packet buffer 500 it is to access, and in step 1060, the host 100 reads the data in the designated area of the packet buffer 500.

[0028] The hardware firewall 300 ensures that only the designated area is accessed by the host 100. In Block 1070 the host 100 writes a message to the mailbox 400 indicating that the read action has been completed and signals the routing device CPU 600. Finally, in Block 1080, the routing device CPU 600 notifies the hardware firewall 300 that the host 100 no longer has access to the designated area of the packet buffer 500.

[0029] The embodiment of the present invention described provides a single memory resource that is utilized by the routing device and the associated host. Since each routing device in the network must temporarily store data in a memory for either access by the host or retransmission to another routing resource or destination, a common memory is used. The use of a shared memory resource, such as a "packet buffer" 500, has the advantage of reducing the number of separate memories required to store data and reduces the number of transactions that a processor must perform in order to transfer data to it's intended destination.

[0030] The embodiment described above provides selective access by the host to the shared memory or "packet buffer" 500 on the routing device 1000. The selective access by the host is implemented solely by hardware in the routing device such that no security protocol or encryption is required to protect data not intended to be accessed by the host. Host access to the packet buffer can be configured to allow multiple windows of different memory ranges, or alternatively, host access to the packet buffer can be eliminated entirely. Additionally, the embodiment includes a mechanism to communicate to the host which areas it is allowed to access in the packet buffer.

[0031] Furthermore, data movement is minimized between memories because the host 100 and routing device CPU 600 have direct access to the shared packet buffer 500. By securely using a single shared memory, cost is minimized and data transfer efficiency is maximized in the routing device while maintaining the integrity of the network data. Furthermore, by implementing the firewall 300 in the routing device hardware, it is not susceptible to hacking from the host computer 100.

[0032] Although network routers and bridges reroute network traffic, they typically do not have associated hosts. While security issue addressed by the embodiment of the present invention described above could potentially apply to any communications device with an associated host, they specifically apply to devices which support multi-hopping. The embodiment of the present invention described above restricts a host from reading data not intended for it, however it does not deal with restrictions on the ability of the host to write data to the routing device.

[0033] Although only a few exemplary embodiments of the present invention have been described in detail above, those skilled in the art will readily appreciate that many modifications are possible in the exemplary embodiments without materially departing from the novel teachings and advantages of this invention. Accordingly, all such modifications are intended to be included within the scope of this invention as defined.

What is claimed is:

1. A node, for use in a wireless ad-hoc communications network, and being adapted to transmit and receive data packets to and from other nodes in said wireless ad-hoc network and to restrict access by an associated host device to said data packets destined for other nodes in said wireless ad-hoc network, said node comprising:

an internal hardware firewall, adapted provide selective read and write access by an associated host device to at least one of a packet buffer and a register mailbox; and

a controller, adapted to configure said internal hardware firewall to provide said selective read and write access.

2. A node as claimed in claim 1, further comprising:

a memory, including said register mailbox and said packet buffer which has a plurality of addresses, and being adapted to provide a common set of registers to said associated host device and said controller.

3. A node as claimed in claim 1, further comprising:

a modem, adapted to modulate an outgoing signal into an analog format, and demodulate an incoming signal into a digital format packet; and

wherein said controller is further adapted to direct modem control functions to demodulate an incoming signal into a digital format packet.

4. A node as claimed in claim 1, wherein:

said controller is further adapted to direct routing functions to transfer a digital format packet from said modem to an address range of said packet buffer.

5. A node as claimed in claim 1, wherein:

said controller is further adapted to determine if said associated host device requires access to said incoming signal digital format packet and in response, to configure said internal hardware firewall to allow said associated host device access to said register mailbox via a host interface.

6. A node as claimed in claim 1, wherein:

said controller is further adapted to determine an address range in said packet buffer which contains said digital format packet and to place a message containing said address range in said register mailbox, and to signal said associated host device to access said register mailbox to retrieve said message.

7. A node as claimed in claim 1, wherein:

said controller is further adapted to configure said internal hardware firewall to allow said associated host device to access said address range of said packet buffer.

8. A node as claimed in claim 1, wherein:

said controller is further adapted to retrieve a completion reply from said associated host device and in response, to configure said internal hardware firewall to prohibit said associated host device to access said register mailbox and said packet buffer.

9. A method of transmitting and receiving data packets to and from a node in a wireless ad-hoc network and restricting access by an associated host device to received data packets destined for other nodes in said wireless ad-hoc network, the method comprising:

controlling an internal hardware firewall at said node to provide selective read and write access by an associated host device to at least one of a packet buffer and a register mailbox; and

controlling a router device central processing unit (CPU) to configure said internal hardware firewall to provide said selective read and write access.

10. A method as claimed in claim 9, further comprising:

controlling said CPU to control a memory, including said register mailbox and said packet buffer which has a plurality of addresses, to provide a common set of registers to said associated host device and said controller.

11. A method as claimed in claim 9, further comprising:

controlling said CPU to control a modem to modulate an outgoing signal into an analog format, and to demodulate an incoming signal into a digital format packet; and controlling said CPU to direct modem control functions to demodulate an incoming signal into a digital format packet.

12. A method as claimed in claim 9, further comprising:

controlling said CPU to direct routing functions to transfer a digital format packet from said modem to an address range of said packet buffer.

13. A method as claimed in claim 9, further comprising:

controlling said CPU to determine if said associated host device requires access to said incoming signal digital format packet and in response, to configure said internal hardware firewall to allow said associated host device access to said register mailbox via a host interface.

14. A method as claimed in claim 9, further comprising:

controlling said CPU to determine an address range in said packet buffer which contains said digital format packet and to place a message containing said address range in said register mailbox, and to signal said associated host device to access said register mailbox to retrieve said message.

15. A method as claimed in claim 9, further comprising:

controlling said CPU to configure said internal hardware firewall to allow said associated host device to access said address range of said packet buffer.

16. A method as claimed in claim 9, further comprising:

controlling said CPU to retrieve a completion reply from said associated host device and in response, to configure said internal hardware firewall to prohibit said associated host device to access said register mailbox and said packet buffer.

17. A computer-readable medium of instructions for controlling a node in a wireless ad-hoc communications network to perform access restriction of an associated host device to data packets destined for other nodes, said node being adapted to transmit and receive data

packets to and from other nodes in said wireless ad-hoc network, said computer-readable medium of instructions comprising:

a first set of instructions, adapted to control an internal hardware firewall at said node to provide selective read and write access by an associated host device to at least one of a packet buffer and a register mailbox; and

a second set of instructions, adapted to control a router device central processing unit (CPU) to controller to configure said internal hardware firewall to provide said selective read and write access.

18. A computer-readable medium of instructions as claimed in claim 17, wherein:

said second set of instructions is adapted to control a memory, including said register mailbox and said packet buffer which has a plurality of addresses, to provide a common set of registers to said associated host device and said controller.

19. A computer-readable medium of instructions as claimed in claim 17, wherein:

said second set of instructions is adapted to control a modem to modulate an outgoing signal into an analog format, and to demodulate an incoming signal into a digital format packet; and

wherein said second set of instructions is further adapted to direct modem control functions to demodulate an incoming signal into a digital format packet.

20. A computer-readable medium of instructions as claimed in claim 17, wherein:

said second set of instructions is adapted to direct routing functions to transfer a digital format packet from said modem to an address range of said packet buffer.

21. A computer-readable medium of instructions as claimed in claim 17, wherein:

said second set of instructions is adapted to determine if said associated host device requires access to said incoming signal digital format packet and in response, to configure said internal hardware firewall to allow said associated host device access to said register mailbox via a host interface.

22. A computer-readable medium of instructions as claimed in claim 17, wherein:

said second set of instructions is adapted to determine an address range in said packet buffer which contains said digital format packet and to place a message containing said address range in said register mailbox, and to signal said associated host device to access said register mailbox to retrieve said message.

23. A computer-readable medium of instructions as claimed in claim 17, wherein:

said second set of instructions is adapted to configure said internal hardware firewall to allow said associated host device to access said address range of said packet buffer.

24. A computer-readable medium of instructions as claimed in claim 17, wherein:

said second set of instructions is adapted to retrieve a completion reply from said associated host device and in response, to configure said internal hardware firewall to prohibit said associated host device to access said register mailbox and said packet buffer.

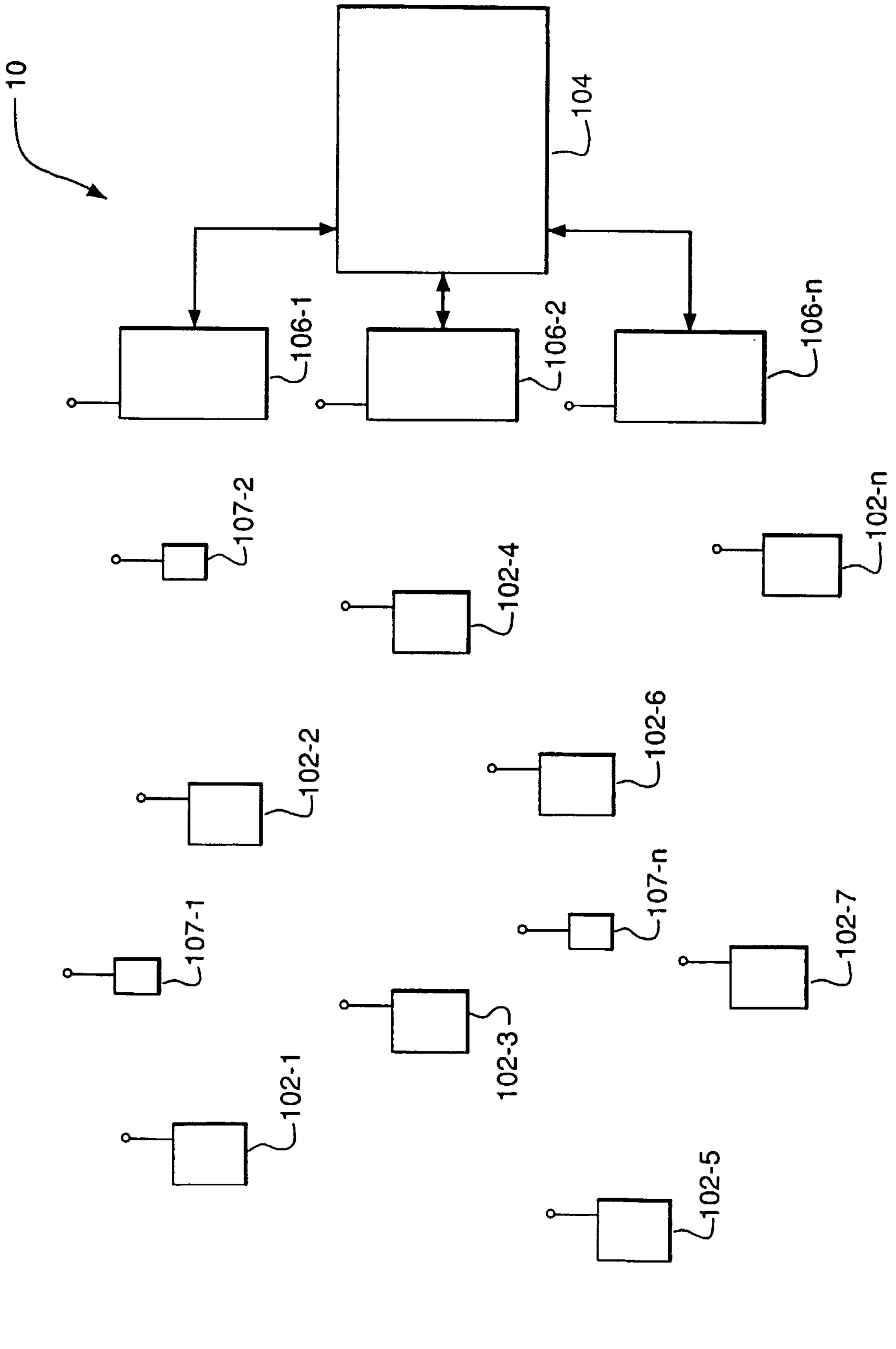

10
104
106-1
106-2
106-n
107-2
102-4
102-n
102-2
102-6
107-1
107-n
102-7
102-3
102-1
102-5

FIGURE 1

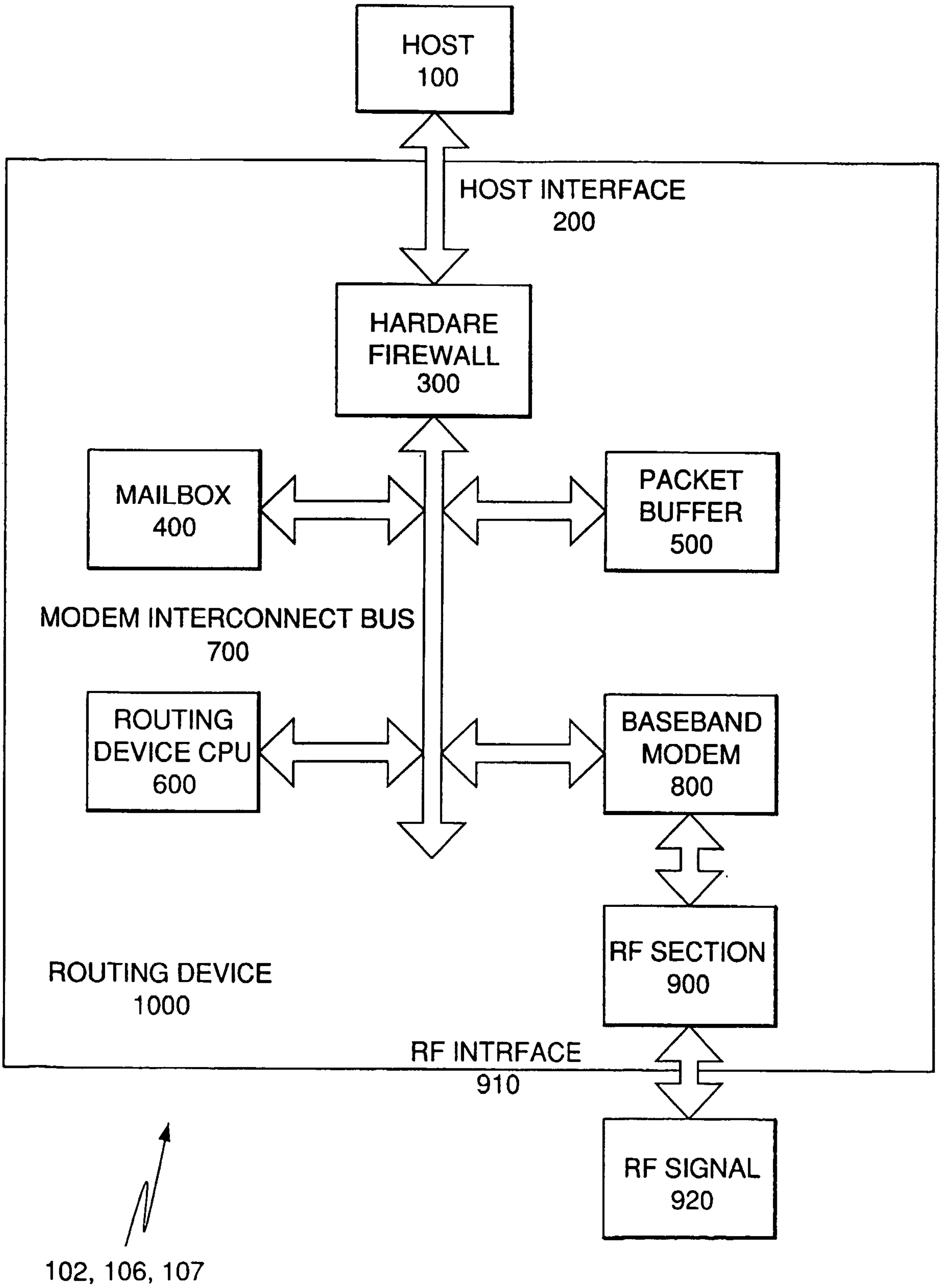

HOST
100
HOST INTERFACE
200
HARDARE
FIREWALL
300
MAILBOX
400
PACKET
BUFFER
500
MODEM INTERCONNECT BUS
700
ROUTING
DEVICE CPU
600
BASEBAND
MODEM
800
RF SECTION
900
ROUTING DEVICE
1000
RF INTRFACE
910
RF SIGNAL
920
102, 106, 107

FIGURE 2

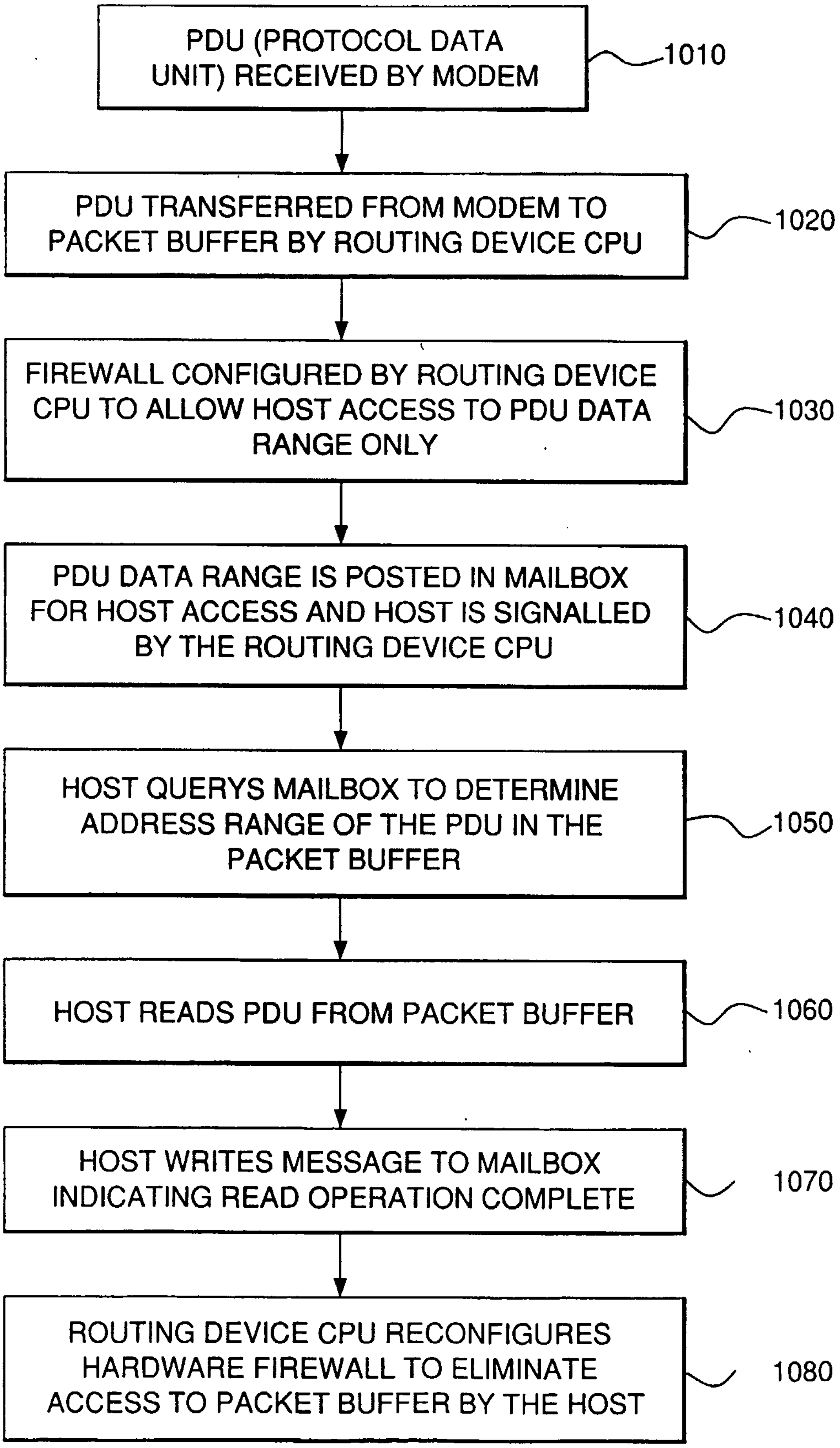

PDU (PROTOCOL DATA UNIT) RECEIVED BY MODEM
1010
PDU TRANSFERRED FROM MODEM TO PACKET BUFFER BY ROUTING DEVICE CPU
1020
FIREWALL CONFIGURED BY ROUTING DEVICE CPU TO ALLOW HOST ACCESS TO PDU DATA RANGE ONLY
1030
PDU DATA RANGE IS POSTED IN MAILBOX FOR HOST ACCESS AND HOST IS SIGNALLED BY THE ROUTING DEVICE CPU
1040
HOST QUERYS MAILBOX TO DETERMINE ADDRESS RANGE OF THE PDU IN THE PACKET BUFFER
1050
HOST READS PDU FROM PACKET BUFFER
1060
HOST WRITES MESSAGE TO MAILBOX INDICATING READ OPERATION COMPLETE
1070
ROUTING DEVICE CPU RECONFIGURES HARDWARE FIREWALL TO ELIMINATE ACCESS TO PACKET BUFFER BY THE HOST
1080

FIGURE 3