Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2456282 C 2010/03/30

(11)(21) 2 456 282

(12) BREVET CANADIEN
CANADIAN PATENT

(13) C

(86) Date de dépôt PCT/PCT Filing Date: 2002/07/23
(87) Date publication PCT/PCT Publication Date: 2003/03/13
(45) Date de délivrance/Issue Date: 2010/03/30
(85) Entrée phase nationale/National Entry: 2004/02/03
(86) N° demande PCT/PCT Application No.: US 2002/023571
(87) N° publication PCT/PCT Publication No.: 2003/021866
(30) Priorité/Priority: 2001/08/31 (US09/945,352)

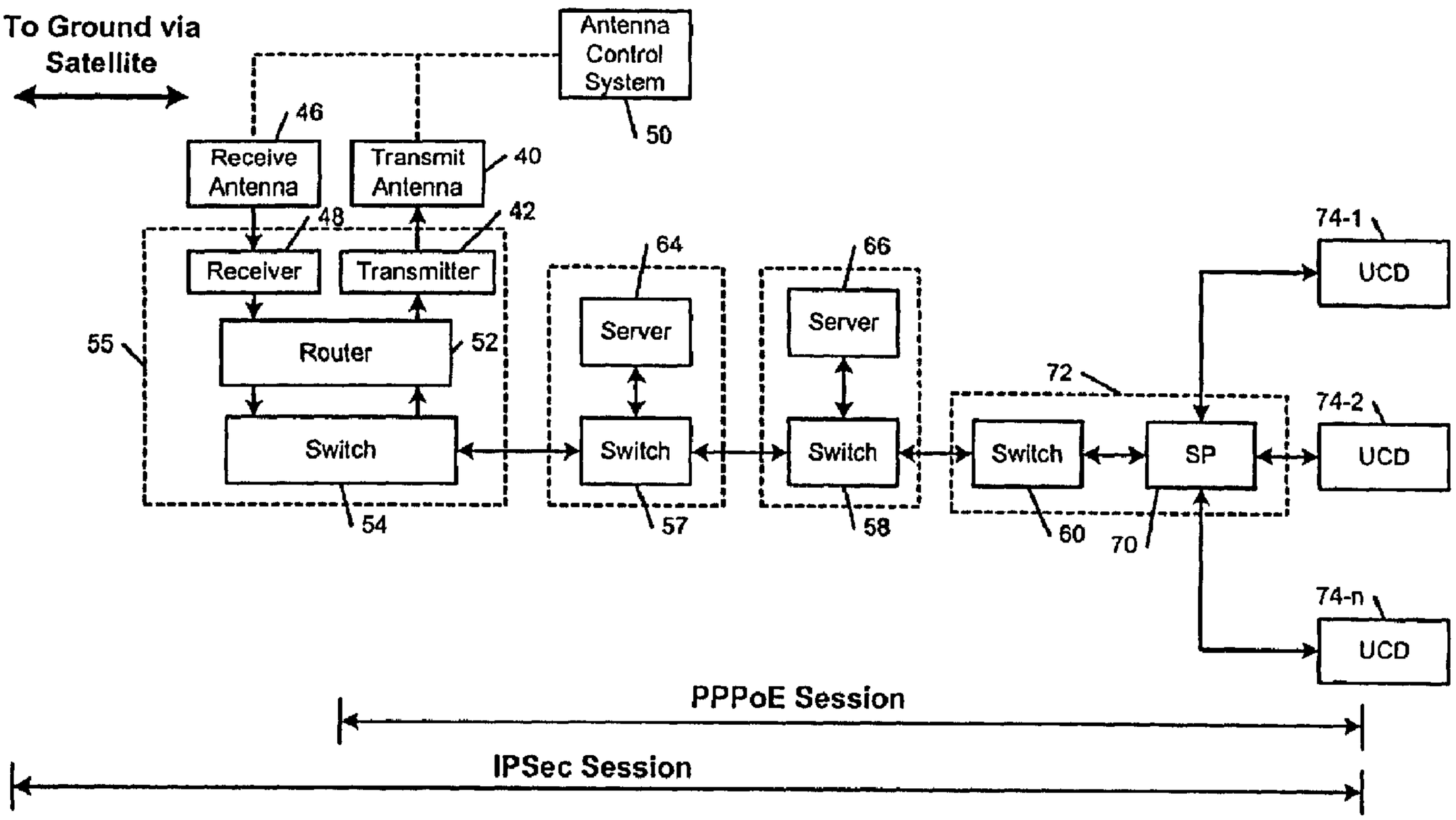
(51) Cl.Int./Int.Cl. *H04W 4/00* (2009.01), *B64D 11/00* (2006.01), *H04B 7/185* (2006.01), *H04W 84/02* (2009.01)

(72) Inventeurs/Inventors:
D'ANNUNZIO, MICHAEL A., US;
SKAHAN, VINCENT D., JR., US;
DEVEREAUX, EUGENE E., US

(73) Propriétaire/Owner:
THE BOEING COMPANY, US

(74) Agent: SMART & BIGGAR

(54) Titre : PROTOCOLE DE POINT A POINT SUR L'ETHERNET POUR PLATES-FORMES MOBILES
(54) Title: POINT-TO-POINT PROTOCOL OVER ETHERNET FOR MOBILE PLATFORMS



(57) Abrégé/Abstract:
A communications system that provides broadband access to passengers of mobile platforms includes a router located on the mobile platform. A network is connected to the router. User communication decives (UCDs)connected to the network, wherein in the UCDs establish point-to-point over Ethernet (PPPoE) sessions with the router. A transmitter and a receiver are connected to the router. A satelite and aground station are in communication with the transmitter and the receiver. A distributed communications system includes virtual private networks (VPN) and is connected to the ground station. A first address manager assigns the public Ip addresses to UCDs when the UCDs request access to the VPNs and private IP addresses for other network service. The UCDs employ IPSec protocol when accessing the VPNs.

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 March 2003 (13.03.2003)

PCT

(10) International Publication Number
WO 03/021866 A3

(51) International Patent Classification[7]: H04L 29/06, 12/28, 29/12, B64D 11/00

(21) International Application Number: PCT/US02/23571

(22) International Filing Date: 23 July 2002 (23.07.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/945,352 31 August 2001 (31.08.2001) US

(71) Applicant: **THE BOEING COMPANY** [US/US]; P.O. Box 3707, M.S. 13-08, Seattle, WA 98124-2207 (US).

(72) Inventors: **D'ANNUNZIO, Michael, A.**; 20530 N.E., 68th Street, Redmond, WA 98053 (US). **SKAHAN, Vincent, D., Jr.**; 32517 20th Court SW, Federal Way, WA 98023 (US). **DEVEREAUX, Eugene, E.**; 4 Pone DeLeon Creek SW, Lakewood, WA 98499 (US).

(74) Agent: **GALBRAITH, Ann, K.**; The Boeing Company, P.O. Box 3707, M/S 13-08, Seattle, WA 98124-2207 (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.

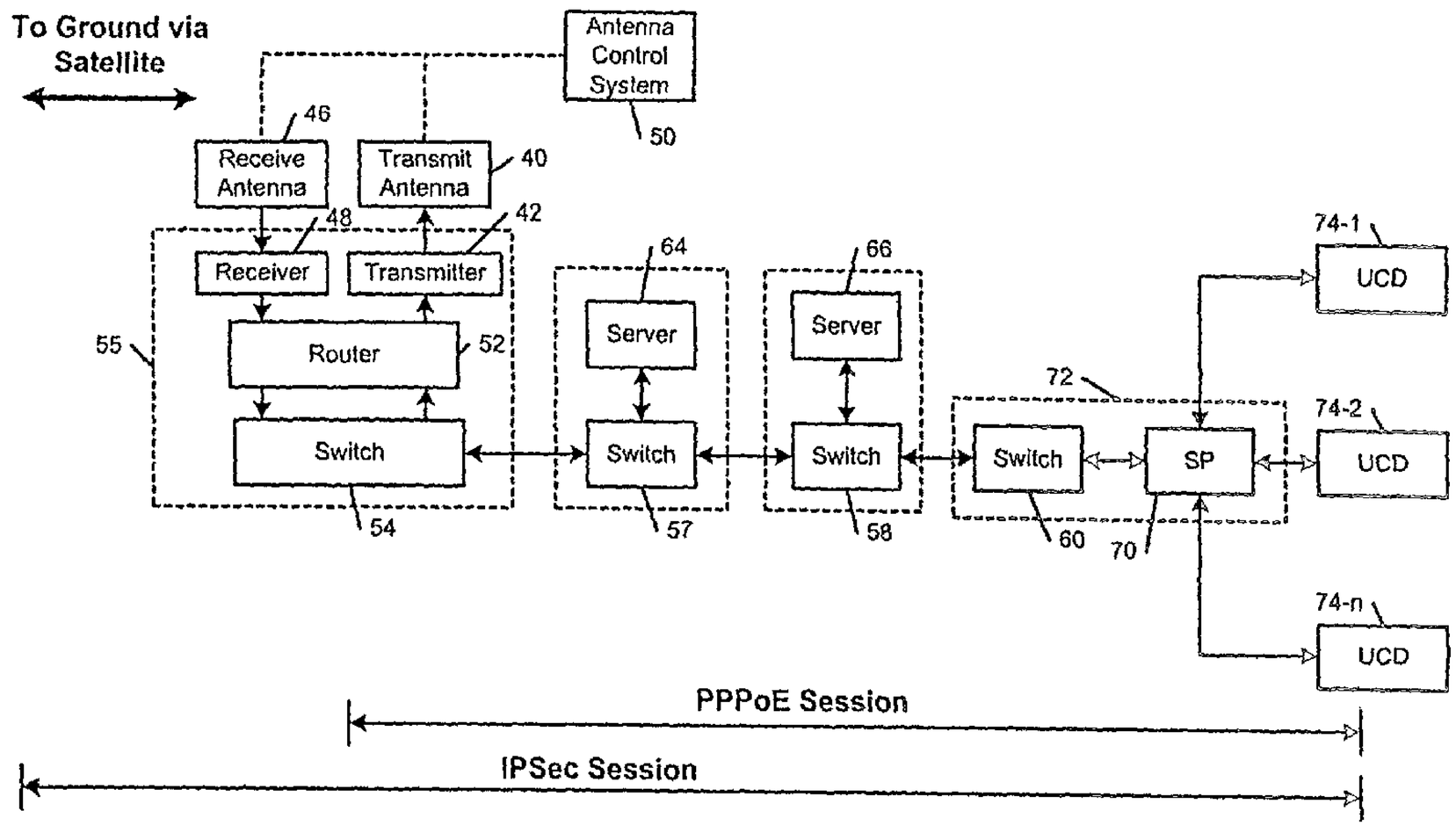
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ,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

Published:
— *with international search report*

(88) Date of publication of the international search report:
16 October 2003

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: POINT-TO-POINT PROTOCOL OVER ETHERNET FOR MOBILE PLATFORMS



(57) Abstract: A communications system that provides broadband access to passengers of mobile platforms includes a router located on the mobile platform. A network is connected to the router. User communication decives (UCDs)connected to the network, wherein in the UCDs establish point-to-point over Ethernet (PPPoE) sessions with the router. A transmitter and a receiver are connected to the router. A satelite and aground station are in communication with the transmitter and the receiver. A distributed communications system includes virtual private networks (VPN) and is connected to the ground station. A first address manager assigns the public Ip addresses to UCDs when the UCDs request access to the VPNs and private IP addresses for other network service. The UCDs employ IPSec protocol when accessing the VPNs.

WO 03/021866 A3

POINT-TO-POINT PROTOCOL OVER ETHERNET FOR MOBILE PLATFORMS

FIELD OF THE INVENTION

The present invention relates to broadband communications systems for mobile platforms, and more particularly to a broadband communication system employing point protocol over Ethernet (PPPoE).

BACKGROUND OF THE INVENTION

Broadband communications access, on which our society and economy is growing increasingly dependent, is not readily available to users on board mobile platforms such as aircraft, ships, and trains. While the technology exists to deliver the broadband communications services to mobile platforms, conventional solutions are commercially unfeasible due to the high costs for service or due to low data rates. The conventional solutions have typically only been available to government/military users and/or to high-end maritime markets such as cruise ships.

Passengers of aircraft are often business users who require access to their corporate network. To attract business users, the broadband communication services must provide acceptable data rates at a reasonable price and allow access to virtual private networks (VPNs). There are two basic modes of operation of VPNs. In a first mode, the VPN provides secure remote access from the client to corporate gateway across the Internet. In a second mode, the VPN provides secure gateway to gateway connections across the Internet. The first mode of operation applies when a passenger's laptop runs VPN client software and communicates with the passenger's corporate VPN gateway.

There are many different security protocols that are currently being used on the Internet. Layer 2 Forwarding (L2F) is a security protocol created by Cisco Systems. Point-to-Point Tunneling Protocol (PPTP), created by the PPTP industry forum, is currently the most widely used VPN protocol. There are several security weaknesses that make PPTP undesirable for future use. Layer 2 Tunneling Protocol (L2TP) evolved through the IETF standards process and is a security protocol that is a combination of PPTP and L2F. Internet protocol security (IPSec) is an architecture and related Internet key exchange (IKE) protocol that is described by IETF RFCs 2401-2409, which are hereby incorporated by reference. IPSec provides robust security and is a preferred protocol for future use.

IPSec provides integrity protection, authentication, privacy and replay protection services for IP level traffic. IPSec packets are of two types. A first type, IP protocol 50 (Encapsulated Security Payload (ESP)), provides privacy, authenticity and integrity. A second type, IP protocol 51 (Authentication Header (AH) format), provides integrity and authenticity for packets but not privacy.

IPSec can be used in two modes. A transport mode secures an existing IP packet from source to destination. A tunneling mode puts an existing IP packet inside a new IP packet that is sent to a tunnel end point in the IPSec format. Both transport and tunnel modes can be encapsulated in ESP or AH headers.

Internet web sites are identified by a public address. Routers and switches use the public address to route IP packets. Public addresses are considered a scarce resource. Requests for public address space from American Registry for Internet Numbers (ARIN) are scrutinized for efficient usage. Permanently assigning even a small number of public addresses to each mobile platform requires a large number of

public addresses. When the mobile platform is not in use, the address(es) allocated to the mobile platform are not used. If a significant percentage of mobile platforms are not in use at a given time, ARIN will conclude that the public addresses are inefficiently used and deny the request.

To efficiently use IP addresses, some broadband communications systems employ Network Address Translation (NAT). NAT allows many hosts to share a single IP address by multiplexing streams based on transmission control protocol/user datagram protocol (TCP/UDP) port numbers as well as IP addresses. NAT was developed as an interim solution to combat IP address depletion. NAT maps IP addresses from one address domain to another, most often by mapping private IP addresses to public IP addresses. In a static NAT, a one-to-one mapping is defined between public and private IP addresses. In a dynamic NAT, a pool of public IP addresses is shared by an entire private IP subnet.

For example, private hosts 192.168.0.1 and 192.168.0.2 both send packets from source port 2000. A NAT device translates these to a single public IP address 207.29.194.28 with two different source ports, for example 2998 and 2999. Response traffic that is received for port 2998 is readdressed and routed to 192.168.0.1. Response traffic that is received for port 2999 is readdressed and routed to 192.168.0.2. As can be appreciated, the NAT gateway is directional.

When IPSec systems employ AH, the entire IP packet including invariant header fields (like source and destination address) is run through a message digest algorithm to produce a keyed hash. The recipient uses the keyed hash to authenticate the IP packet. If any field in the original IP packet is modified, authentication will fail and the recipient will discard the IP packet. AH is intended to prevent unauthorized

modification, source spoofing, and man-in-the-middle attacks. NAT, however, by definition modifies IP packets. NAT modifies the packet header by replacing the packet's source address. As a result, systems employing NAT cannot employ IPSec if the remote system is configured to employ AH or gateway.

Therefore, a broadband communications system for mobile platforms that allows users to access VPNs, that conserves IP address space, that provides sufficiently high data rates and/or that conforms with the IPSec protocol would be desirable.

SUMMARY OF THE INVENTION

In accordance with one aspect of the invention there is provided a communications system for providing broadband access to passengers of a mobile platform. The system includes a communications network located on the mobile platform, the network comprising a router and at least one seat processor, the seat processor being operably configured to facilitate communications between a user communication device and the router. The system further includes a first public address manager client running on the router or other device connected to the network, the first public address manager client being operably configured to communicate with a first public address manager server that is not on the mobile platform, to request and receive address blocks for lease from the first public address manager server. The system further includes an address pool on the mobile platform operably configured to store address blocks received from the first public address manager server. The system further includes a PPoE access server on the mobile platform operably configured to control the use of public addresses stored in the

address pool. The system further includes a second address manager running on the router or other device connected to the network, the second address manager being configured to cause the router or other device on the network to communicate with the address pool and the PPoE access server to assign a public address to the user communication device in response to receiving a virtual private network (VPN) request from the user communication device, and to cause the router or the other device on the network to assign a private address to the user communication device in response to receiving a configuration request frame from the user communication device.

In accordance with another aspect of the invention, there is provided a method for providing broadband access to passengers of mobile platforms. The method involves facilitating communications between a user communication device on the mobile platform and a router on the mobile platform, through a communications network on the mobile platform. The method further involves executing a first public address manager client on the router or other device on the network, to request and receive address blocks for lease from a first public address manager server that is not on the mobile platform. The method further involves executing an address block store on the router or other device on the network for storing address blocks received from the first public address manager server in an address pool on the mobile platform. The method further involves establishing a PPoE access server on the router or other device on the network to control the use of public addresses stored in the address pool by user communication devices. The method further involves executing a second address manager on the router or other device on the network to cause the router or other device on the network to communicate with the PPoE access server and the

address pool and assign a public address to the user communication device, in response to receiving a virtual private network (VPN) request from the user communication device, and cause the router or the other device on the network to assign a private address to the user communication device, in response to receiving a configuration request frame from the user communication device.

In accordance with another aspect of the invention, there is provided a communications system for providing broadband access to passengers of mobile platforms. The system includes a router located on the mobile platform, a network connected to the router, user communication devices (UCDs) connected to the network, the UCDs establishing point-to-point over Ethernet (PPPoE) sessions with the router, a transmitter on the mobile platform, the transmitter being connected to the router, a receiver on the mobile platform, the receiver being connected to the router, a satellite in communication with the transmitter and the receiver of the mobile platform, a ground station in communication with the satellite, a distributed communications system connected to the ground station, a virtual private network (VPN) connected to the distributed communications system, a first address manager connected to the ground station, the first address manager leasing use of public Internet Protocol (IP) addresses by the mobile platform, the router including a second address manager communicating with the first address manager to lease the public IP addresses for the mobile platform.

In accordance with another aspect of the invention, there is provided a communications system for allowing passengers of mobile platforms to access virtual private networks (VPNs). The system includes a network on the mobile platform communicating with a ground station via a satellite, the ground station being

connected to a virtual private network (VPN), user communication devices (UCDs) connected to the network, and a first address manager connected to the network, the first address manager being operable to enable public internet protocol (IP) addresses to be assigned when the UCDs request a connection to the VPN, the first address manager enabling assigning private IP addresses for at least one other network service, the first address manager assigning the public and private addresses without requiring the UCDs to reboot.

In accordance with another aspect of the invention, there is provided a public address manager for a broadband communications system for mobile platforms. The public address manager includes a network on the mobile platform that communicates with a ground station via a satellite, user communication devices (UCDs) connected to the network, a first address manager associated with the mobile platform that requests a public address block for the mobile platform, and a second public address manager associated with the ground station that leases the public address block to the first address manager.

In accordance with another aspect of the invention, there is provided a method for operating a communications system that provides broadband access to passengers of mobile platforms. The method involves locating a router on the mobile platform, connecting a network to the router, connecting user communication devices (UCDs) to the network, establishing point-to-point over Ethernet (PPPoE) sessions between the UCDs and the router, connecting a transmitter to the router, connecting a receiver to the router, communicating with a satellite and a ground station that is connected to a distributed communications system using the transmitter and the receiver of the mobile platform, the distributed communications system connecting to a virtual

private network (VPN), managing use of public address blocks using a first address manager, and requesting the public address blocks using a second address manager associated with the mobile platform.

In accordance with another aspect of the invention, there is provided a method for allowing passengers of mobile platforms to access virtual private networks (VPNs). The method involves providing a network on the mobile platform, connecting user communication devices (UCDs) to the network, providing a first address manager on the network that assigns public internet protocol (IP) addresses to the UCDs when the UCDs request access to the VPNs, and using the first address manager to assign private IP addresses for a service provided by the network, the public and private addresses being assigned without requiring the UCDs to reboot.

In accordance with another aspect of the invention, there is provided a communications system for providing broadband access to passengers of mobile platforms. The system includes a router located on the mobile platform, a network connected to the router, user communication devices (UCDs) connected to the network, a ground station in communication with the mobile platform, and a first address manager connected to the ground station that leases use of public Internet Protocol (IP) addresses by the mobile platform, the router including a second address manager enabling communication with the first address manager to lease public IP addresses for the mobile platform.

In accordance with another aspect of the invention, there is provided a communications system for providing broadband access to passengers of mobile platforms. The system includes a network, user communication devices, UCDs, connected to the network, and a ground station in communication with the mobile

platform via a satellite, wherein a distributed communications system is connected to the ground station. The ground station is characterized by a router located on the mobile platform and being connected to the network, a virtual private network, VPN, connected to the distributed communications system, an address manager connected to the ground station for leasing use of public Internet Protocol, (IP), addresses by the mobile platform, wherein the router includes another address manager for communicating with the address manager to lease the public IP addresses for the mobile platform, the other address manager is being adapted for assigning the public IP addresses, when the UCDs request access to the VPN, and assigning private IP addresses to the UCDs for at least one network service provided by the mobile platform, wherein the UCDs establish point-to-point over Ethernet, PPPoE, sessions with the router.

In accordance with another aspect of the invention, there is provided a method for operating a communications system that provides broadband access to passengers of mobile platforms. The method involves locating a router on the mobile platform, connecting a network to the router, connecting user communication devices, UCDs, to the network, and establishing point-to-point over Ethernet, PPPoE, sessions between the UCDs and the router, providing an address manager connected to a ground station for leasing use of public Internet Protocol, IP, addresses by the mobile platform, communicating with a satellite and the ground station that is connected to a distributed communications system via the router, providing an other address manager on the network for assigning the public IP addresses to the UCDs, the other address manager on the network assigning public Internet Protocol, IP, addresses to the UCDs

when the UCDs request access to virtual private networks, VPNs, and the other address manager assigning private IP addresses for a service provided by the network.

Further areas of applicability of the present invention will become apparent from the detailed description provided hereinafter. It should be understood that the detailed description and specific examples, while indicating the preferred embodiment of the invention, are intended for purposes of illustration only and are not intended to limit the scope of the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will become more fully understood from the detailed description and the accompanying drawings, wherein:

Fig. **1** is a functional block diagram illustrating a broadband communications system including mobile platforms, satellites, ground stations and the Internet;

Fig. **2** is a functional block diagram illustrating the mobile platform communications system that employs a Point-to-Point over Ethernet (PPPoE) protocol on the mobile platform;

Fig. **3** illustrates the protocols employed by the ground-based distributed communications system and by the mobile platform communications system;

Fig. **4** illustrates an address manager;

Fig. **5** illustrates the connectivity between a passenger services network, an air-to-ground network and a command and control network;

Fig. **6** illustrates steps for initiating a PPPoE session by a user communication device (UCD) on the mobile platform;

Fig. **7** illustrates steps employed by the mobile platform for assigning public addresses to allow the UCD to access a VPN;

Fig. **8** illustrates steps employed by the mobile platform for leasing public address blocks from a public address manager server and for assigning the public address to UCDs; and

Fig. **9** illustrates steps employed by the public address manager to manage the public addresses.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The following description of the preferred embodiment(s) is merely exemplary in nature and is in no way intended to limit the invention, its application, or uses.

The present invention provides a broadband communications system for mobile platforms that allows users to access VPNs, that conserves IP address space and that conforms with the IPSec protocol. When users located on the mobile

platform initially request access, the communications system assigns a private address. When the user requests access to a VPN, the communications system assigns a public address to the user from a pool of public addresses that are preferably leased. Switching from the private address to the public address is performed without requiring the user to reboot. Access to other resources such as non-VPN web sites and multimedia services are preferably prevented while the user is assigned the public address to optimize the use of the public address pool. When the user finishes using the VPN, the public address is returned to the pool and the user is reassigned a private address. The reassignment to a private address is also preferably performed without rebooting the user's computer. When accessing a VPN site that employs IPSec with AH, proper authentication is performed and the IP packets are not discarded. Furthermore, the use of public IP address space is conserved in accordance with IANA requirements.

Referring now to Fig. **1**, a mobile platform communications system **10** for mobile platforms **12-1**, **12-2**, ..., **12**-n is shown. The mobile platforms **12** communicate via one or more satellites **16-1**, **16-2**, ..., **16**-n and with one or more ground-based receiving stations **18-1**, **18-2**, ..., **18**-n. The ground-based receiving stations **18** are connected to a distributed communications system **22** via a router **24-1**, **24-2**, ..., **24**-n. A public address manager (PAM) server **28** is connected to the distributed communications system **22**, the router **24** or to the ground-based receiving stations **18**. The PAM server **28** manages the leasing of public addresses that are stored in a public address pool **29** to the mobile platforms **12** as will be described more fully below.

One or more web servers **30-1**, **30-2**, ..., **30**-n are connected to the distributed communications system **22**. Likewise, one or more virtual private networks (VPNs) **32-1**, **32-2**, ..., **32**-n are connected to the distributed communications system **22**. The distributed communications system **22** is preferably the Internet. Users located on the mobile platform **12** access the web servers **30** and/or the VPN's **32** via the mobile platform communications system **10**. As can be appreciated, the mobile platform establishes an air-to-ground network via the satellites **16** and the ground stations **18**.

Referring now to Figs. **2** and **3**, the mobile platform **12** includes a transmit antenna **40** that is connected to a transmitter **42** and a receive antenna **46** that is connected to a receiver **48**. The transmit and receive antennas **40** and **46** are controlled by antenna control system **50** in a conventional manner. The receiver **48**, transmitter **42**, the router **52** and the switch **54** are collectively referred to as a data transceiver router (DTR) **55**. The transmit and receive antennas **40** and **46** are connected to a router **52** and a switch **54**.

The switch **54** is connected to one or more switches **57**, **58**, and **60**. The switches **57** and **58** are connected to servers **64** and **66**. The servers **64** and **66** provide web services, an aircraft interface unit (AIU), flight specific websites such as car rental companies located at the destination, popular web sites such as CNN, MSN, etc. that are stored in cache, targeted advertising, and other content. The switch **60** is connected to one or more seat processors **70** that are connected to one or more user communication devices UCD **74-1**, **74-2**, ..., **74**-n. The switch **60** and seat processor **70** are collectively referred to as a seat electronic box **72**. The UCD **74** is a laptop computer, a personal digital assistant PDA, or any other electronic device that communicates via the Internet. The UCDs **74** preferably include a microprocessor,

memory (such as random access memory, read-only memory, and/or flash memory), and input/output devices such as a keyboard, a mouse, and/or a voice operated interface. The mobile platform communication system **10** establishes a PPPoE session between the UCD **74** and the DTR **55**. From the viewpoint of the distributed communications system, the protocols employed by the mobile platform communication system **10** are transparent as can be seen in Fig. **3**.

Referring now to Fig. **4**, the DTR **55**, the server **64** or the server **66** preferably include an address manager **90** including an address pool **92**, an access server **94** and a PAM client **96**. The PAM client **96** requests address blocks from the PAM server **28** based on need. The PAM client **96** also transmits periodic lease maintenance messages to the PAM server **28** to maintain the leases on the address block(s). The address pool **92** stores the address blocks and the PPPoE Access Server **94** controls the use of the public addresses by the UCDs **74**.

Referring now to Fig. **5**, there are three or more logical subnets: a passenger services network **100**, an air-to-ground network **102** and a command and control network **104**. For example, the servers **64** and **66** that provide web or media services are multi-homed in that they have multiple physical interfaces. The UCDs **74** are connected to the passenger services network **100**. IP aliasing allows multiple IP addresses to be configured on the same physical interface. The IP addresses can be from the same or different subnets. Multiple logical subnets can be created on the same physical network. Since only a router can forward traffic between subnets, logical subnets simplify router and host-based packet filtering to control inter-subnet access. Logical subnets allow access to actual application ports to be restricted to specific subnets. Logical subnets allow maximum uses of private address ranges and

reuse of address ranges between module platforms. Logical subnets minimize the number of subnets that must be advertised to the ground.

The command and control network **104** is an onboard network that supports local command and control functions such as configuration, initialization, data load, and other similar functions. None of the UCD **74** are assigned addresses from the address range of the command and control network **104**. In a preferred embodiment, the command and control network **104** uses a class B private address range that is reused on each aircraft, for example **172.16.0.0/16**. Devices that are attached to the command and control network **104** do not communicate directly to the ground using addresses for the command and control network **104**. The command and control network **104** subnet is not advertised to the ground. Command and control addresses are not altered using NAT.

The air-to-ground network **102** includes devices that need to communicate directly with the ground. These devices are assigned addresses from the air-to-ground network **102** address range. The air-to-ground network **102** is the only subnet that is advertised to the ground as reachable from the aircraft. The air-to-ground network **102** address range is not reused. The air-to-ground network **102** addresses uniquely identify each airborne network. Preferably, the air-to-ground network **102** uses a private class A subnet, for example **10.0.0.0/8** with subnetting to uniquely identify each airborne network.

The passenger services network **100** is a network that provides direct services to UCDs **74** that are assigned addresses from the passenger services network **100**. The servers **64** and **66**, the airborne router **52**, and the SEB **72** are assigned addresses from the passenger services network **100**. The passenger services network preferably

employs a class B private address range, for example **172.17.0.0/16**. The address range is reused on each aircraft. Addresses from the passenger services network **100** are translated into an AGN address by a NAT function in the DTR **55** for offboard access.

Referring now to Fig. **6**, steps for initiating communications by the UCD **74** are illustrated. Control begins with step **150**. In step **152**, control determines whether the UCD **74** transmits a configuration request frame. If not, control loops back to step **152**. The configuration request frame is a broadcast Ethernet frame that employs PPPoE control type code. If the configuration request frame is sent, the SEB **72** and/or the seat processor **70** forwards the configuration request frame to the router **52** in step **154**. In step **156**, control messages are unicast by the router **52**. In step **158**, control determines whether the client is in the data transfer stage. If not, control loops back to step **156**. Otherwise, control continues with step **162** where the router **52** assigns a private address to the client. In step **164**, a PPPoE session is established and data transfer is enabled. Control ends at step **166**.

Referring now to Fig. **7**, steps for establishing a VPN session are shown. Control begins with step **170**. In step **172**, control determines whether one of the UCDs **74** has requested the VPN session. If not, control loops to step **172**. If the UCD **74** has requested a VPN session, control determines whether a PPPoE session has been established by the UCD **74** requesting VPN access in step **174**. If not, a PPPoE session is established between the router **52** and the requesting UCD **74** in step **176** (by executing steps **150-166**). Control continues from steps **174** and **176** to step **178** where the UCD **74** is reassigned the public address from the public address block. In step **180**, the routing tables are set up to support packet forwarding. In step **184**,

control determines whether the UCD **74** terminated the VPN session. If not, control loops back to step **184**. If the VPN session has been terminated, control continues with step **186**. The public address is returned to the public address block in step **188**. Control ends with step **190**.

Fig. **8** illustrates steps performed by the PAM client on the mobile platform to provide public addresses to the UCDs **74** for use with VPNs. Control begins with step **200**. In step **202**, the PAM client **96** requests a public address block from the ground PAM server **28**. In step **204**, control determines whether the public address block has been received. If not, control waits for the timeout period in step **206** and then continues with step **202**. If the public address block has been received, control continues with step **208** where a lease timer is reset. In step **212**, control determines whether the UCD **74** has launched the VPN module. If not, control continues with step **216**. Otherwise, control assigns a public address from the public address block in step **220**. In step **224**, control optionally disables other services such as access to non-VPN web sites or other multimedia services and continues with step **216**. The other services are optionally disabled to optimize the use of the public addresses.

In step **216**, control determines whether the lease timer has timed out. If not, control continues with step **228**. If the lease timer has timed out, control continues with step **230** where the PAM client **96** refreshes the public address block lease with the ground PAM server. In step **234**, control resets the lease timer and continues with step **228**. In step **228**, control determines whether the public address pool **92** on the mobile platform is empty. If not, control continues with step **238**. If the public address pool **92** is empty, the PAM client **96** on the mobile platform requests

additional public addresses from the ground PAM server **28** in step **240** and control continues with step **238**.

In step **238**, control determines whether the client terminated the VPN session by closing the VPN module. If not, control continues with step **246**. If the client terminated the VPN session, control returns the public address to the public address block and assigns the private address to the UCD **74** in step **248**. In step **250**, other services such as access to non-VPN web sites and multimedia services are enabled and control continues with step **246**.

In step **246**, control determines whether the public address block for the mobile platform is still needed. If not, control returns the public address block to the PAM server **28** in step **252** and control ends in step **254**. If the public address block is still needed, control loops back to step **212**. If multiple public address blocks are requested from the PAM server **28**, the mobile platform can return one or more of the public address blocks or simply allow the lease to time out and end.

Referring now to Fig. **9**, steps performed by the ground PAM server **28** are shown. Control begins with step **300**. In step **302**, control determines whether a mobile platform is requesting a public address block. If not, control continues with step **306**. If a mobile platform is requesting a public address block, the ground PAM server **28** assigns a public address block to the mobile platform in step **308**. In step **310**, a lease timer for the public address block that is requested by the mobile platform is started and continues with step **306**. In step **306**, control determines whether the lease timer of any address block of any mobile platform has timed out. If not, control continues with step **314**. If the lease timer has timed out, the ground PAM server **28** returns the public address block to the public address pool (so that the public

addresses can be effectively utilized by another mobile platform) in step **316**. In step **314**, control determines whether a mobile platform returned a public address block. If not, control loops to step **302**. If the mobile platform returns the public access block, the ground PAM server **28** returns the public address block to the public address pool in step **318** and control continues with step **302**.

Those skilled in the art can now appreciate from the foregoing description that the broad teachings of the present invention can be implemented in a variety of forms. Therefore, while this invention has been described in connection with particular examples thereof, the true scope of the invention should not be so limited since other modifications will become apparent to the skilled practitioner upon a study of the drawings, specification, and following claims.

THE EMBODIMENTS OF THE INVENTION IN WHICH AN EXCLUSIVE PROPERTY OR PRIVILEGE IS CLAIMED ARE DEFINED AS FOLLOWS:

1. A communications system for providing broadband access to passengers of a mobile platform, the system comprising:

a communications network located on the mobile platform, said network comprising a router and at least one seat processor, said seat processor being operably configured to facilitate communications between a user communication device and said router;

a first public address manager client running on said router or other device connected to said network, said first public address manager client being operably configured to communicate with a first public address manager server that is not on the mobile platform, to request and receive address blocks for lease from the first public address manager server;

an address pool on the mobile platform operably configured to store address blocks received from the first public address manager server;

a PPoE access server on the mobile platform operably configured to control the use of public addresses stored in the address pool; and

a second address manager running on said router or other device connected to said network, said second address manager being configured to:

cause said router or other device on said network to communicate with said address pool and said PPoE access server to assign a public address to the user communication

device in response to receiving a virtual private network (VPN) request from said user communication device; and

to cause said router or said other device on said network to assign a private address to the user communication device in response to receiving a configuration request frame from said user communication device.

2. The system of claim **1** further comprising logical subnets on said computer network.

3. The system of claim **2** wherein said logical subnets include a passenger services subnetwork and at least part of an air-to-ground-subnetwork, wherein said addresses in said pool are addresses on said passenger services network, and wherein said air-to-ground-subnetwork is operably configured to support communications between said first public address manager client and the first public address manager server.

4. The system of claim **3** wherein said air-to-ground subnetwork includes a private class A network, said passenger subnetwork includes a class B private address network.

5. A method for providing broadband access to passengers of mobile platforms, the method comprising:

facilitating communications between a user communication device on the mobile platform and a router on the mobile platform, through a communications network on the mobile platform;

executing a first public address manager client on said router or other device on said network, to request and receive address blocks for lease

from a first public address manager server that is not on the mobile platform;

executing an address block store on said router or other device on said network for storing address blocks received from the first public address manager server in an address pool on the mobile platform;

establish a PPoE access server on said router or other device on said network to control the use of public addresses stored in the address pool by user communication devices;

executing a second address manager on said router or other device on said network to:

cause said router or other device on the network to communicate with said PPoE access server and said address pool and assign a public address to the user communication device, in response to receiving a virtual private network (VPN) request from said user communication device; and

cause said router or said other device on said network to assign a private address to the user communication device, in response to receiving a configuration request frame from said user communication device.

6. The method of claim 5 further comprising communicating said public address or said private address to said user communication device.

7. The method of claim 5 or 6 further comprising establishing logical subnets on said computer network.

8. The method of claim 7 wherein establishing said logical subnets include establishing a passenger services subnetwork and at least part of an air-to-ground-subnetwork, wherein said addresses in said pool are addresses on said passenger services network, and wherein said air-to-ground-subnetwork is operably configured to support communications between said first public address manager client and said first public address manager server.

9. The method of claim 8 wherein said air-to-ground subnetwork includes a private class A network and said passenger subnetwork includes a class B private address network.

10. A communications system for providing broadband access to passengers of mobile platforms, comprising:

a router located on said mobile platform;

a network connected to said router;

user communication devices (UCDs) connected to said network, said UCDs establishing point-to-point over Ethernet (PPPoE) sessions with said router;

a transmitter on said mobile platform, said transmitter being connected to said router;

a receiver on said mobile platform, said receiver being connected to said router;

a satellite in communication with said transmitter and said receiver of said mobile platform;

a ground station in communication with said satellite;

a distributed communications system connected to said ground station;

a virtual private network (VPN) connected to said distributed communications system;

a first address manager connected to said ground station, said first address manager leasing use of public Internet Protocol (IP) addresses by said mobile platform;

said router including a second address manager communicating with said first address manager to lease said public IP addresses for said mobile platform.

11. The communications system of claim **10** wherein said distributed communications system is the Internet.

12. The communications system of claim **10**, said second address manager assigning said public IP addresses when said UCDs request access to said VPN.

13. The communications system of claim **12**, said second address manager assigning private IP addresses to said UCDs for at least one network service provided by said mobile platform.

14. The communications system of claim **10**, said UCDs employing IPSec security protocol when communicating with said VPN.

15. A communications system for allowing passengers of mobile platforms to access virtual private networks (VPNs), comprising:

a network on said mobile platform communicating with a ground station via a satellite, said ground station being connected to a virtual private network (VPN);

user communication devices (UCDs) connected to said network; and

a first address manager connected to said network, said first address manager being operable to enable public internet protocol (IP) addresses to be assigned when said UCDs request a connection to said VPN, said first address manager enabling assigning private IP addresses for at least one other network service, said first address manager assigning said public and private addresses without requiring said UCDs to reboot.

16. The communications system of claim **15** further comprising:

a router connected to said UCDs and to enable said first address manager, said UCDs establishing point-to-point over Ethernet (PPPoE) sessions with said router.

17. The communications system of claim **15** further comprising:

a second address manager, connected to said ground station and a distributed communications system, for enabling a leasing of use of said public IP addresses to said mobile platform.

18. A public address manager for a broadband communications system for mobile platforms, comprising:

a network on said mobile platform that communicates with a ground station via a satellite;

user communication devices (UCDs) connected to said network;

a first address manager associated with said mobile platform that requests a public address block for said mobile platform; and

a second public address manager associated with said ground station that leases said public address block to said first address manager.

19. The public address manager of claim **18**, said first address manager enabling periodic transmission of a lease maintenance message to said second address manager.

20. The public address manager of claim **19**, said second address manager including a lease timer, enabling termination of said lease if said lease timer expires before said lease maintenance message is received.

21. A method for operating a communications system that provides broadband access to passengers of mobile platforms, comprising:

locating a router on said mobile platform;

connecting a network to said router;

connecting user communication devices (UCDs) to said network;

establishing point-to-point over Ethernet (PPPoE) sessions between said UCDs and said router;

connecting a transmitter to said router;

connecting a receiver to said router;

communicating with a satellite and a ground station that is connected to a distributed communications system using said transmitter and said receiver of said mobile platform, said distributed communications system connecting to a virtual private network (VPN);

managing use of public address blocks using a first address manager; and

requesting said public address blocks using a second address manager associated with said mobile platform.

22. The method of claim **21** wherein said distributed communications system is the Internet.

23. The method of claim **21** further comprising:

assigning public IP addresses to said UCDs when said UCDs request access to said VPN.

24. The method of claim **23** further comprising:

assigning private IP addresses to said UCDs for a network service.

25. The method of claim **21** wherein said UCD employs IPSec security protocol when communicating with said VPN.

26. A method for allowing passengers of mobile platforms to access virtual private networks (VPNs), comprising:

providing a network on said mobile platform;

connecting user communication devices (UCDs) to said network;

providing a first address manager on said network that assigns public internet protocol (IP) addresses to said UCDs when said UCDs request access to said VPNs; and

using said first address manager to assign private IP addresses for a service provided by said network, said public and private addresses being assigned without requiring said UCDs to reboot.

27. The method of claim **26** further comprising:

connecting a router to said UCDs and to said first address manager; and establishing point-to-point over Ethernet (PPPoE) sessions between said UCDs and said router.

28. The method of claim **27** further comprising:

connecting a second address manager (PAM) to a ground station; and

leasing use of said public IP addresses to said first address manager using said second address manager.

29. A communications system for providing broadband access to passengers of mobile platforms, comprising:

a router located on said mobile platform;

a network connected to said router;

user communication devices (UCDs) connected to said network;

a ground station in communication with said mobile platform; and

a first address manager connected to said ground station that leases use of public Internet Protocol (IP) addresses by said mobile platform, said router including a second address manager enabling communication with said first address manager to lease public IP addresses for said mobile platform.

30. The communications system of claim **29**, wherein said UCDs are connected to said router by point-to-point over Ethernet (PPPoE) sessions.

31. The communications system of claim **29** further comprising:

a transmitter on said mobile platform that is connected to said router; and

a receiver on said mobile platform that is connected to said router.

32. The communications system of claim **29** further comprising:

a satellite in communication with said mobile platform; and

a distributed communications system connected to said ground station.

33. The communications system of claim **32**, said distributed communications system comprising a wide area network.

34. The communications system of claim **32**, further comprising:

a virtual private network (VPN) connected to said distributed communications system.

35. The communications system of claim 34, said second address manager enabling the assignment of said public IP addresses if said UCDs request access to said VPN.

36. The communications system of claim 35, said second address manager enabling assignment of private IP addresses to said UCDs for at least one network service provided by said mobile platform.

37. The communications system of claim 34, said UCDs comprising IPSec security protocol when communicating with said VPN.

38. A communications system for providing broadband access to passengers of mobile platforms, comprising:

a network;

user communication devices, UCDs, connected to said network; and

a ground station in communication with said mobile platform via a satellite, wherein a distributed communications system is connected to said ground station;

characterized by a router located on said mobile platform and being connected to said network;

a virtual private network, VPN, connected to said distributed communications system;

an address manager connected to said ground station for leasing use of public Internet Protocol, IP, addresses by said mobile platform, wherein said router includes another address manager for communicating with said address manager to lease said public IP

addresses for said mobile platform, said other address manager being adapted for assigning said public IP addresses, when said UCDs request access to said VPN, and assigning private IP addresses to said UCDs for at least one network service provided by said mobile platform, wherein said UCDs establish point-to-point over Ethernet, PPPoE, sessions with said router.

39. A method for operating a communications system that provides broadband access to passengers of mobile platforms , comprising the steps of:

locating a router on said mobile platform;

connecting a network to said router;

connecting user communication devices, UCDs, to said network; and

establishing point-to-point over Ethernet, PPPoE, sessions between said UCDs and said router, providing an address manager connected to a ground station for leasing use of public Internet Protocol, IP, addresses by said mobile platform, communicating with a satellite and said ground station that is connected to a distributed communications system via said router, providing an other address manager on said network for assigning said public IP addresses to said UCDs, said other address manager on said network assigning public Internet Protocol, IP, addresses to said UCDs when said UCDs request access to virtual private networks, VPNs, and said other address manager assigning private IP addresses for a service provided by said network.

FIG. 1

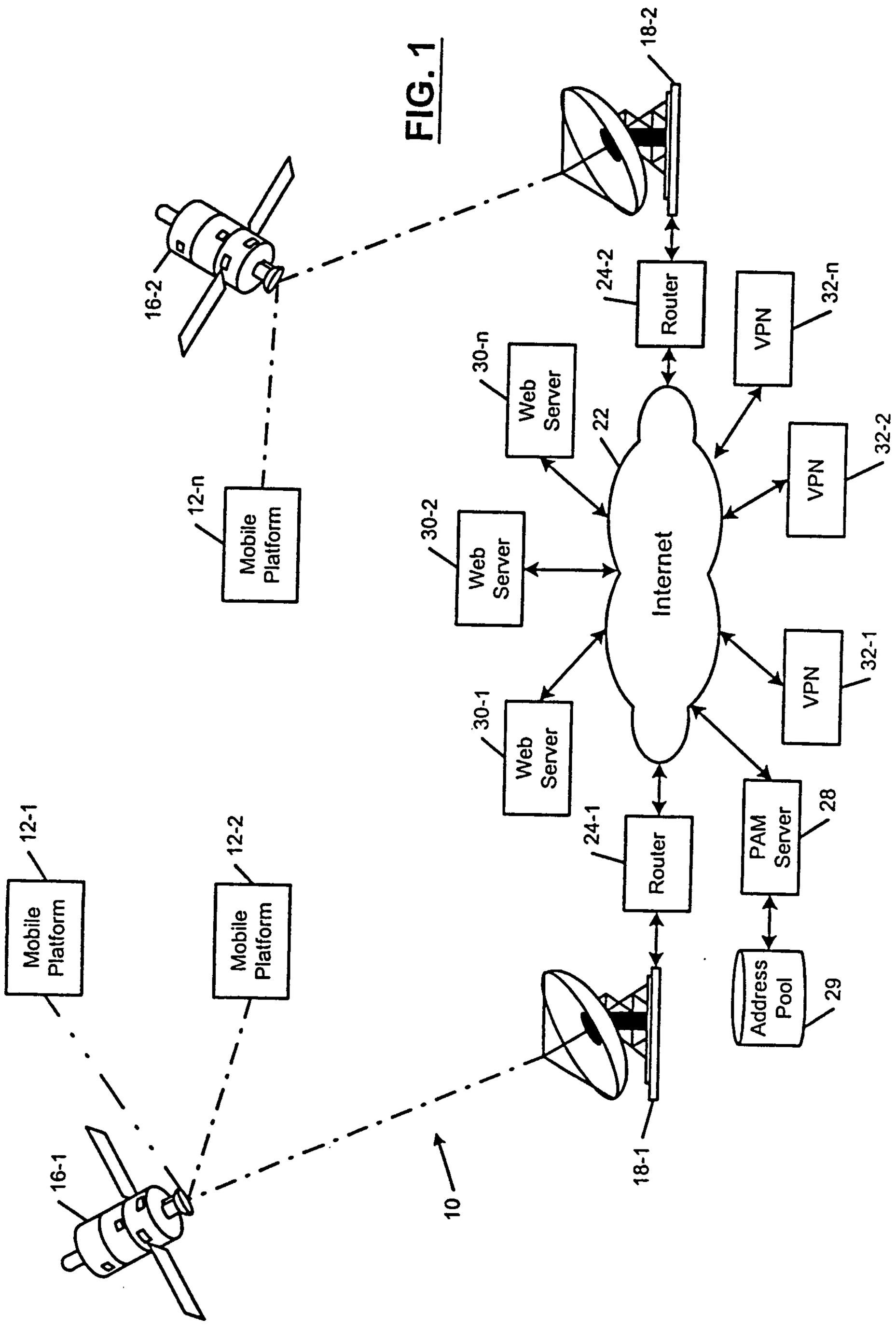

18-2
16-2
12-n
Mobile Platform
24-2
Router
30-n
Web Server
30-2
Web Server
22
Internet
VPN
32-n
VPN
32-2
VPN
32-1
30-1
Web Server
12-1
Mobile Platform
12-2
Mobile Platform
24-1
Router
PAM Server
28
Address Pool
29
16-1
10
18-1

FIG. 2

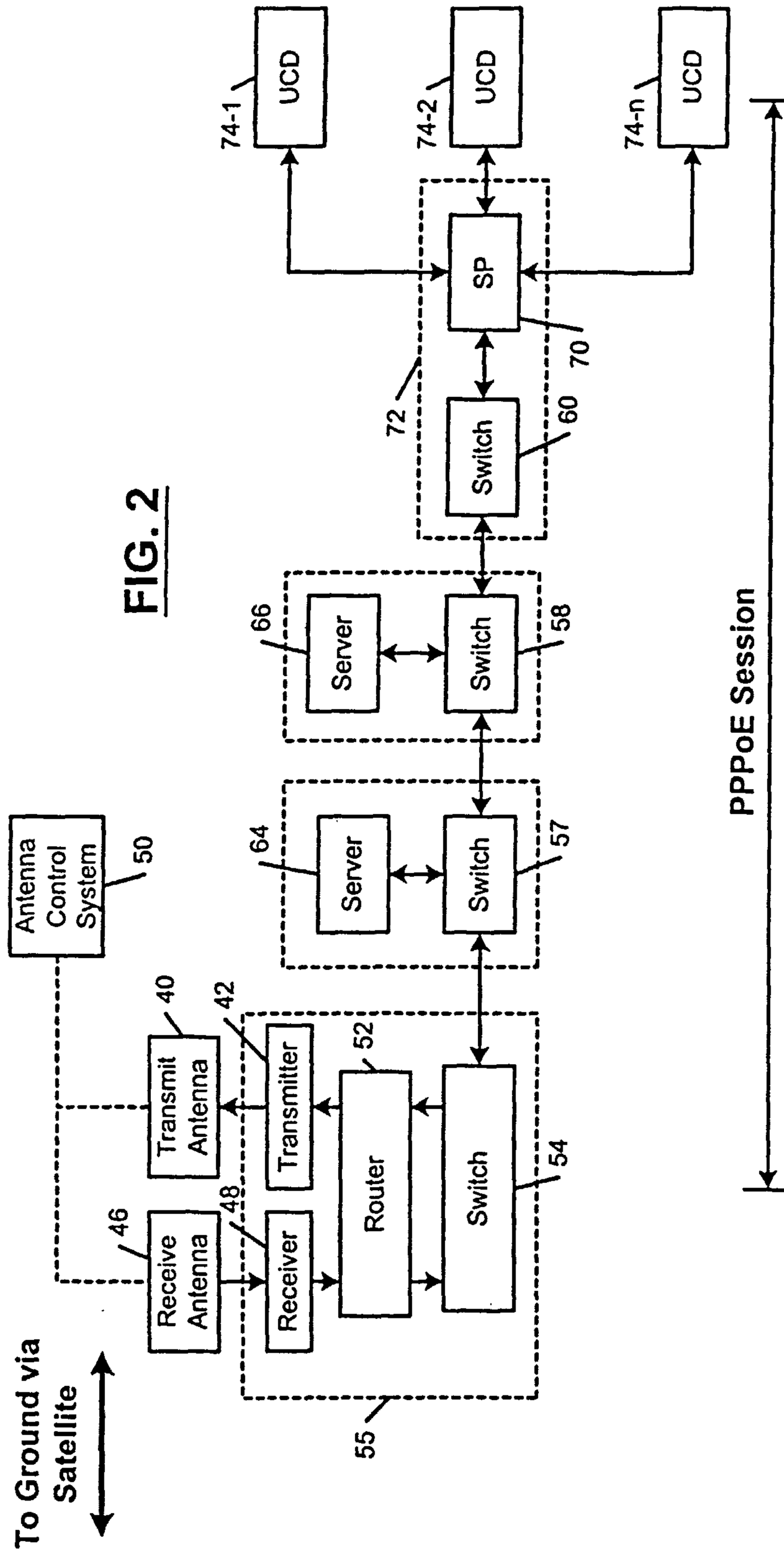

To Ground via Satellite
Antenna Control System
50
Receive Antenna
46
Transmit Antenna
40
Receiver
48
Transmitter
42
Router
52
Switch
54
55
Server
66
Switch
58
Server
64
Switch
57
Switch
60
SP
70
72
74-1
74-2
74-n
UCD
PPP Session
IPSec Session
App (e.g. http)
TCP or UDP
IP
PPP
Ethernet
App (e.g. http)
TCP or UDP
IP
Ethernet

FIG. 3

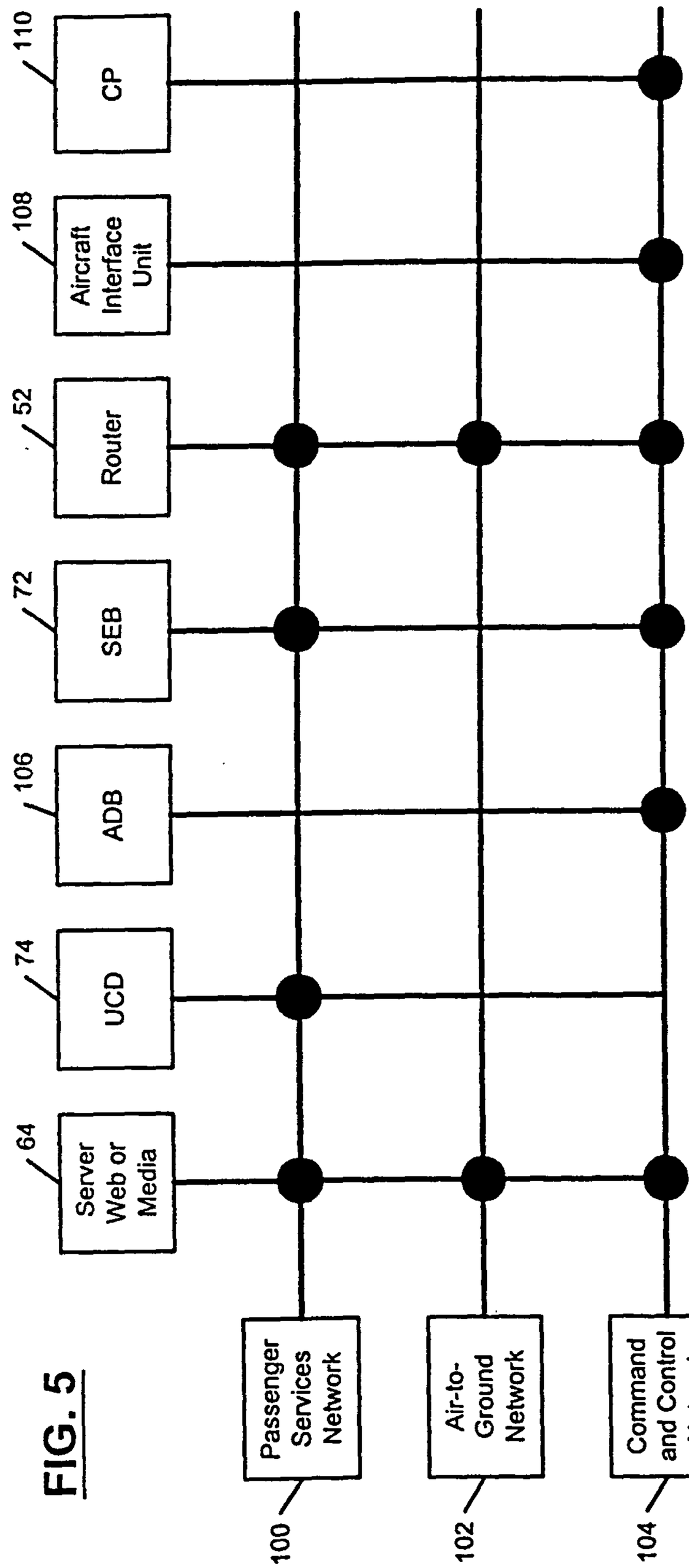

110
CP
108
Aircraft Interface Unit
52
Router
72
SEB
106
ADB
74
UCD
64
Server Web or Media
100
Passenger Services Network
102
Air-to-Ground Network
104
Command and Control Network

FIG. 5

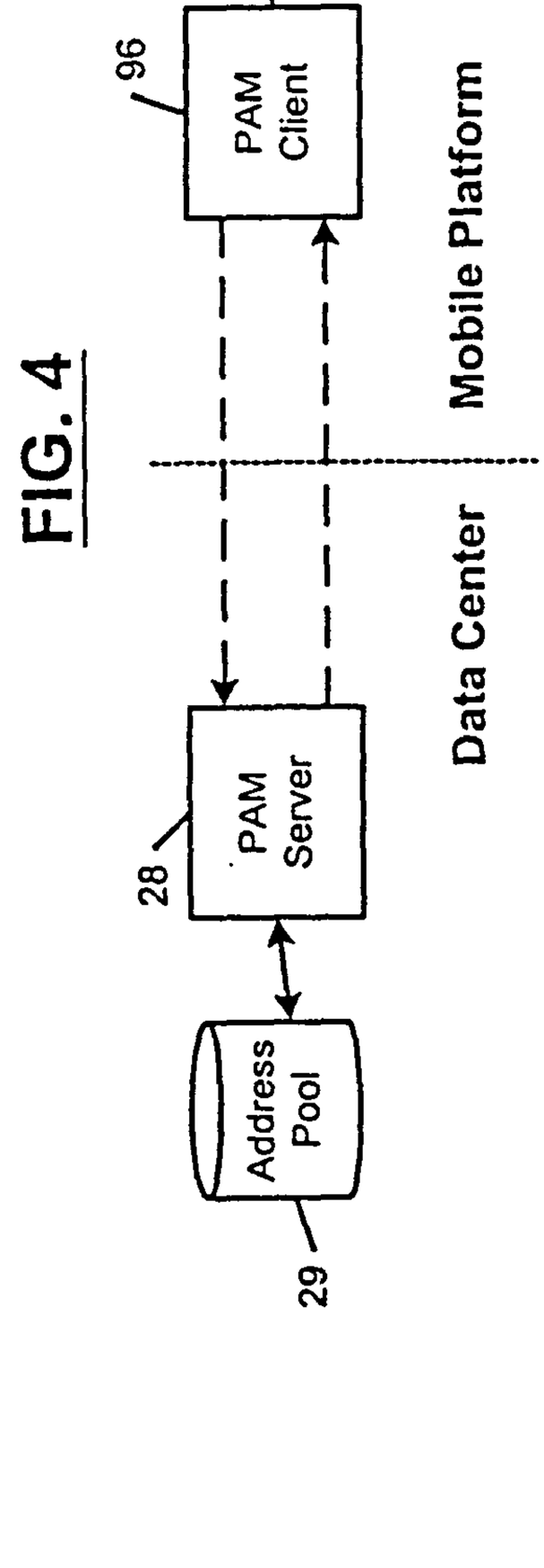

90
94
PPPoE Access Server
92
Address Pool
96
PAM Client
Mobile Platform
Data Center
28
PAM Server
Address Pool
29

FIG. 4

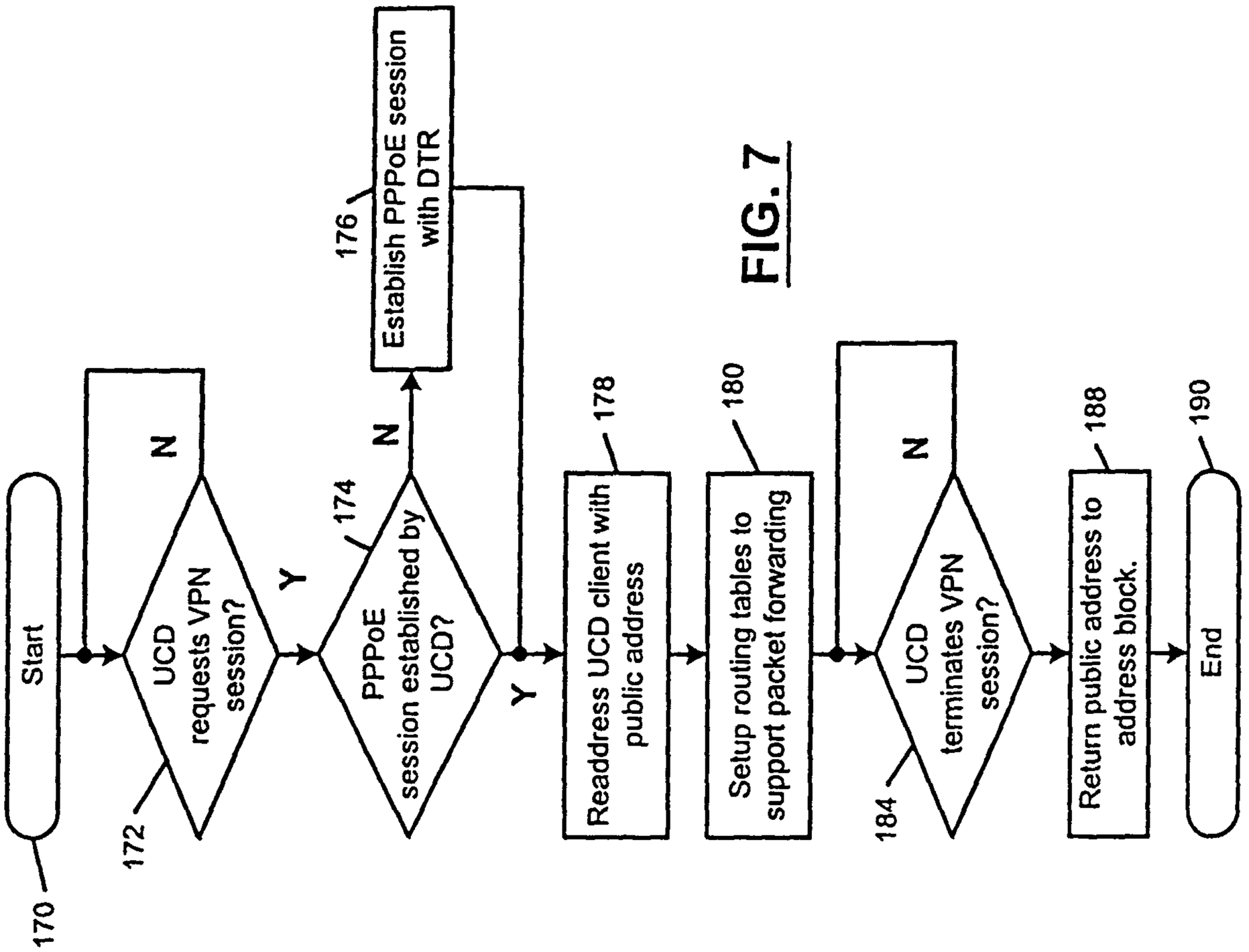

Start
170
UCD requests VPN session?
172
N
Y
PPPoE session established by UCD?
174
N
Establish PPPoE session with DTR
176
Y
Readdress UCD client with public address
178
Setup routing tables to support packet forwarding
180
UCD terminates VPN session?
184
N
Return public address to address block.
188
End
190

FIG. 7

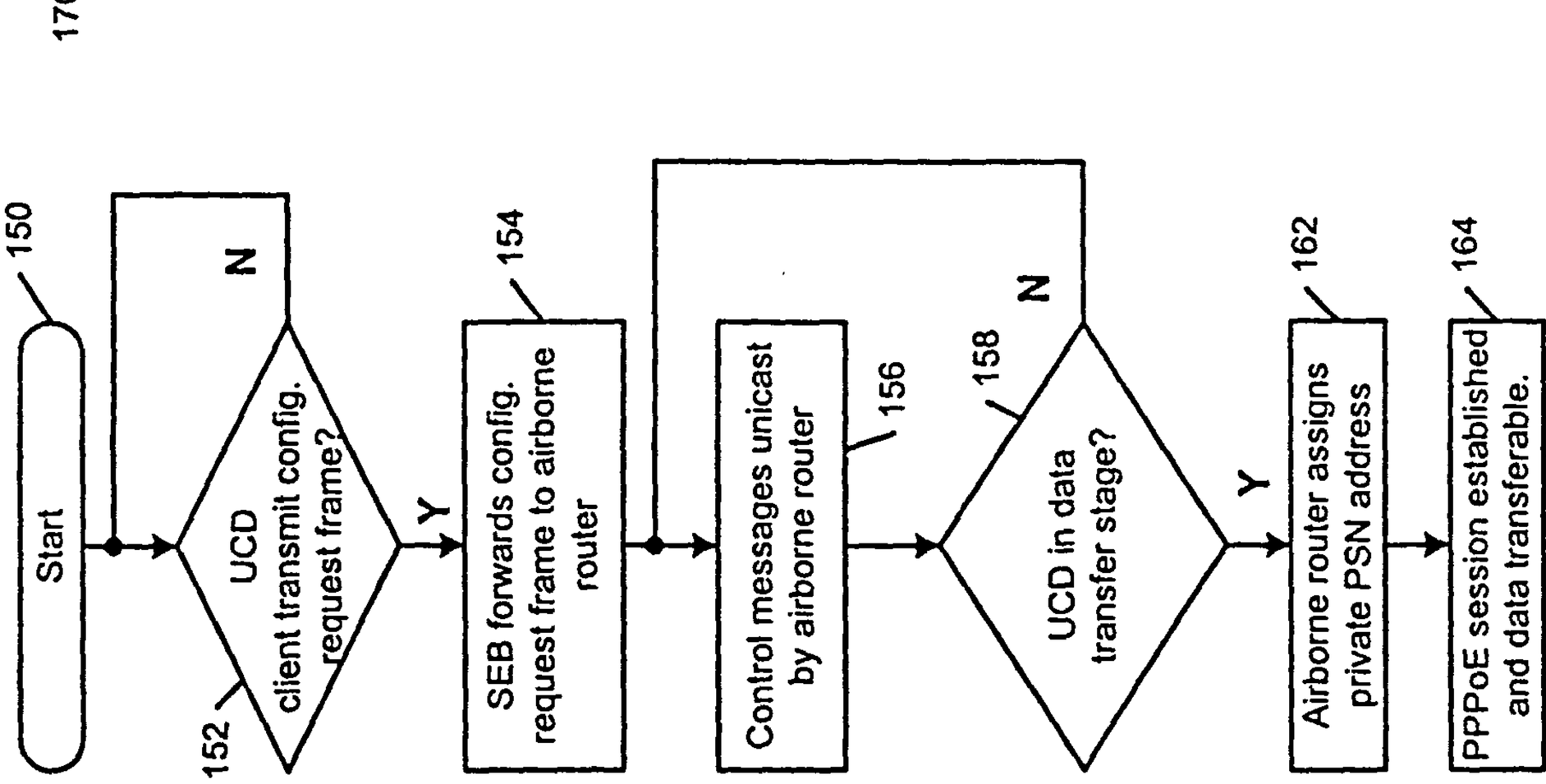

Start
150
UCD client transmit config. request frame?
152
N
Y
SEB forwards config. request frame to airborne router
154
Control messages unicast by airborne router
156
UCD in data transfer stage?
158
N
Y
Airborne router assigns private PSN address
162
PPPoE session established and data transferable.
164
End
166

FIG. 6

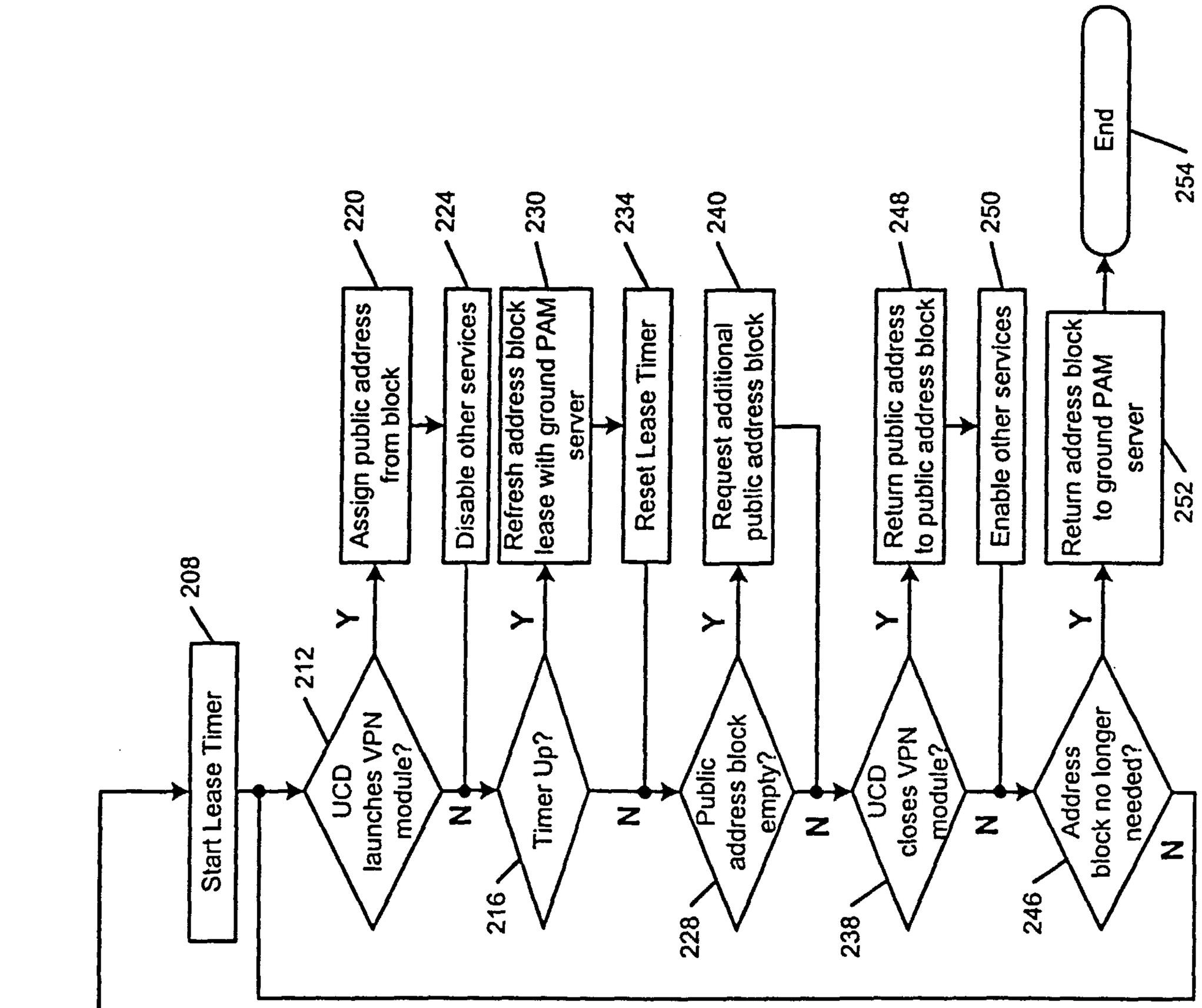

Start
200
Request public address block from ground PAM server
202
Address block received?
204
N
Wait timeout
206
Y
Start Lease Timer
208
UCD launches VPN module?
212
N
Timer Up?
216
N
Public address block empty?
228
N
UCD closes VPN module?
238
N
Address block no longer needed?
246
N
Assign public address from block
220
Disable other services
224
Refresh address block lease with ground PAM server
230
Reset Lease Timer
234
Request additional public address block
240
Return public address to public address block
248
Enable other services
250
Return address block to ground PAM server
252
End
254
Y
Y
Y
Y
Y

FIG. 8

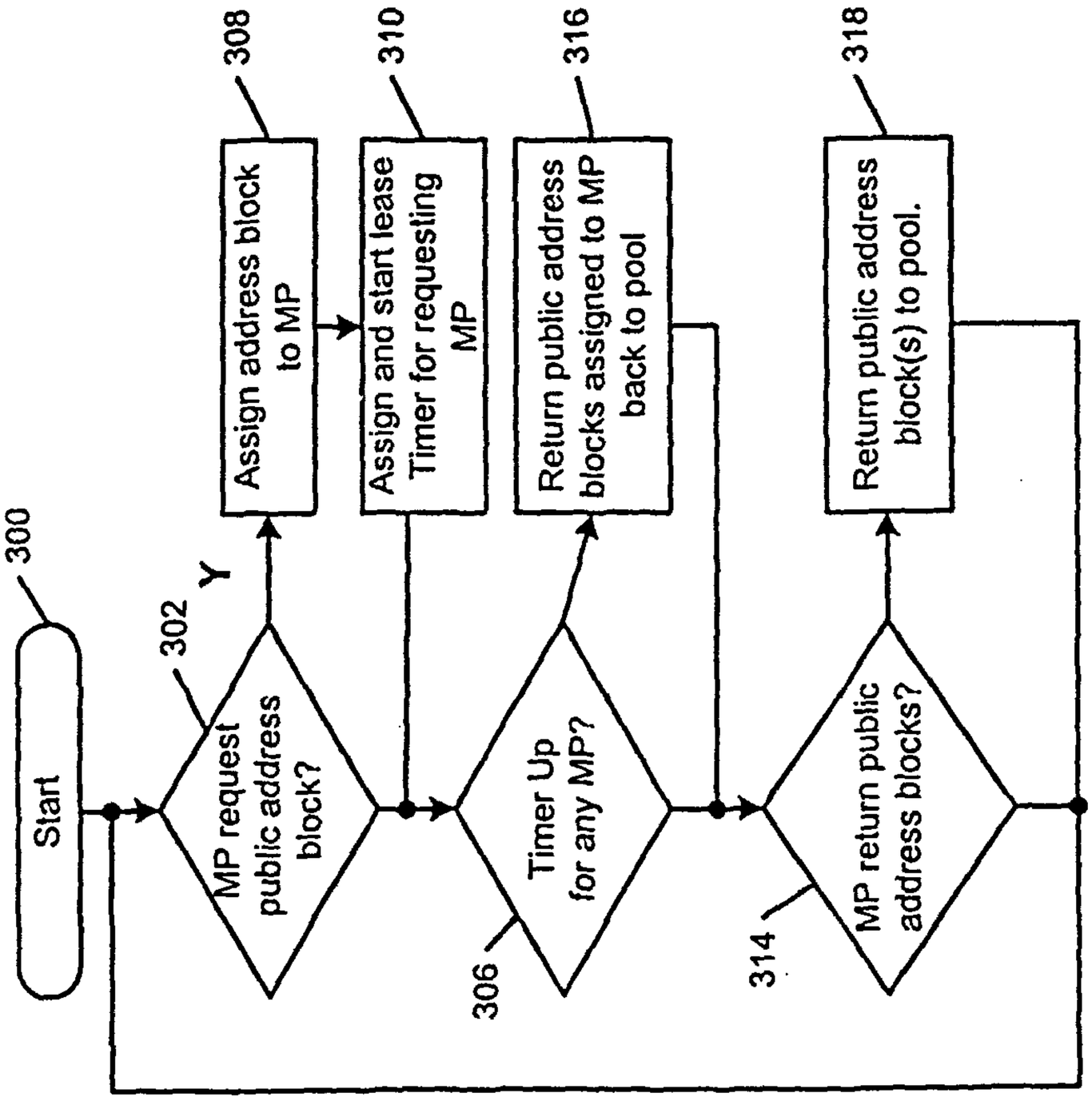
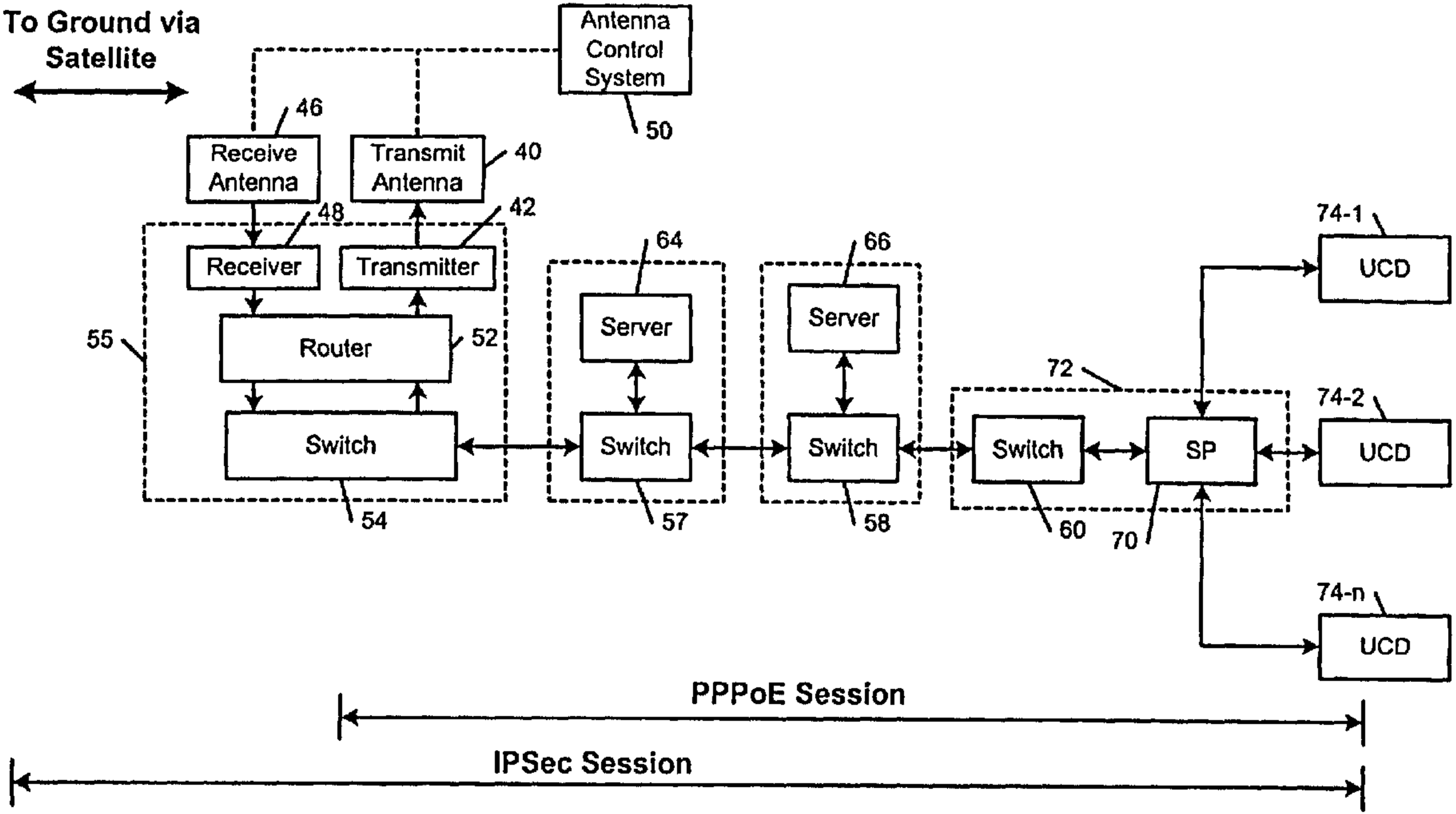

300
Start
302
MP request public address block?
Y
308
Assign address block to MP
310
Assign and start lease Timer for requesting MP
306
Timer Up for any MP?
316
Return public address blocks assigned to MP back to pool
314
MP return public address blocks?
318
Return public address block(s) to pool.

FIG. 9


To Ground via Satellite
Antenna Control System
50
46
Receive Antenna
Transmit Antenna
40
48
42
Receiver
Transmitter
55
Router
52
Switch
54
64
Server
Switch
57
66
Server
Switch
58
72
Switch
SP
60
70
74-1
UCD
74-2
UCD
74-n
UCD
PPPoE Session
IPSec Session