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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
30 December 2015 (30.12.2015)

WIPO | PCT

(10) International Publication Number
WO 2015/197099 A1

(51) International Patent Classification:
H04L 12/46 (2006.01) *H04L 12/751* (2013.01)
H04L 12/715 (2013.01)

(21) International Application Number:
PCT/EP2014/063109

(22) International Filing Date:
23 June 2014 (23.06.2014)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **HUAWEI TECHNOLOGIES CO.,LTD** [CN/CN]; Huawei Administration Building, Bantian Longgang, Shenzhen, Guangdong 518129 (CN).

(72) Inventors; and
(71) Applicants *(for US only)*: **NARKOLAYEV, Shlomo** [IL/DE]; c/o Huawei Technologies Duesseldorf GmbH, Riesstr. 25, 80992 Munich (DE). **PORAT, Hayim** [IL/DE]; c/o Huawei Technologies Duesseldorf GmbH, Riesstr. 25, 80992 Munich (DE).

(74) Agent: **KREUZ, Georg M.**; c/o Huawei Technologies Duesseldorf GmbH, Messerschmittstr. 4, 80992 Munich (DE).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV,

[Continued on next page]

(54) Title: INTER-CARRIER VIRTUAL PRIVATE NETWORKING

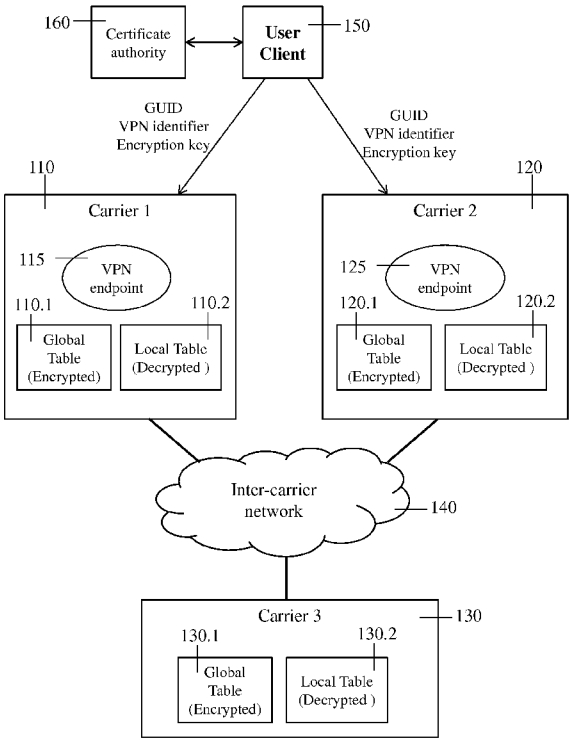

FIGURE 1

(57) Abstract: A method for establishing an endpoint of a multi-carrier virtual private network includes: at the carrier, receiving a request from a user client to host an endpoint of a multi-carrier virtual private network (VPN). The user request includes a VPN identifier identifying the VPN, a universal identifier identifying the user client, and a VPN encryption key. The carrier establishes the requested VPN endpoint and generates a routing entry for the established VPN endpoint. The routing entry includes the VPN ID, the universal identifier and routing information for the VPN endpoint. The carrier encrypts the routing entry with the encryption key and distributes the encrypted routing entry to at least one other carrier. The carrier also identifies other VPN carriers by decrypting routing entries received from the other carriers, and establishes VPN connections with the other carriers over an inter-carrier network.

WO 2015/197099 A1

MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

INTER-CARRIER VIRTUAL PRIVATE NETWORKING

BACKGROUND

The present invention, in some embodiments thereof, relates to establishing a virtual private network over multiple carriers and, more specifically, but not exclusively, to distributing virtual private network routing information between the multiple carriers.

Cloud computing enables business and enterprise customers to deploy their servers and computers as virtual machines (VMs) in data centers all over the world. When deploying different parts of their information technology (IT) servers on differing clouds and data centers, users need to be able to interconnect all of their sites, as was the case when they owned the physical IT infrastructure.

Currently, there are a number of ways to connect multiple endpoints of a virtual private network (VPN) when the endpoints are connected to different autonomous systems. This may occur when the VPN sites are connected to different service providers. These ways include:

A) Virtual routing and forwarding (VRF) to VRF connections at the Autonomous System (AS) border routers;

B) Exterior Border Gateway Protocol (EBGP) redistribution of labeled VPN-Internet Protocol ver. 4 (IPv4) routes from AS to neighboring AS; and

C) Multi-hop EBGP redistribution of labeled VPN-IPv4 routes between source and destination ASs, with EBGP redistribution of labeled IPv4 routes from AS to neighboring AS.

Additional background art includes:

"BGP/MPLS IP Virtual Private Networks (VPNs)"; copyright by The Internet Society (2006).

SUMMARY

In the following, a Global Universal Identifier (also denoted herein a GUID or universal identifier) assigns global meaning to a VPN identifier (VPN ID). Routing information for a VPN identified by a combination of the GUID and VPN ID is encrypted using an encryption key. Optionally, the GUID is provided to the client by an independent authority (such as a CA), and which may also provide the encryption key. The encrypted routing information is distributed to other carriers, for example by extending the MPLS VPN protocol to include distribution of the encrypted routing information (e.g. an encrypted routing entry) as a global resource.

Only authorized carriers which have received the encryption key from the user may be able to decrypt the encrypted routing information and discover the locations of other VPN endpoints.

Coupled with software defined networking (SDN), the aspects of the present invention herein enable automation of VPN establishment as a cloud federation service (i.e. as a service offered by the cloud providers and not as an over-the-cloud task maintained by the user). The establishment of a VPN over multiple carriers, as described herein, enables global, inter-carrier, inter-cloud, VPN and cloud connectivity. AAA mechanisms may be used for end user resource identification, discovery, and advertisement (including scope and access list).

As used herein the term "carrier" means any network entity with the ability to host a VPN endpoint, such as a service provider or autonomous system (AS).

According to a first aspect of of the present invention there is provided a method for establishing an endpoint of a multi-carrier virtual private network. The virtual private network is distributed over multiple carriers communicating over an inter-carrier network. The method includes performing the following:

I) Receiving a request from a user client to host an endpoint of a multi-carrier virtual private network (VPN). The request includes a respective VPN identifier (VPN ID) identifying the VPN, a universal identifier identifying the user client, and a VPN encryption key;

II) Establishing the requested endpoint of the VPN;

III) Generating a routing entry for the established endpoint of the multi-carrier virtual private network. The routing entry includes the respective VPN ID, the respective universal identifier and respective routing information for the VPN endpoint;

IV) Encrypting the routing entry with the respective encryption key;

V) Distributing the encrypted routing entry to at least one other carrier of the inter-carrier network; and

VI) Identifying other carriers of endpoints of the VPN from respective routing entries received from the other carriers, and establishing VPN connections with the other carriers over the inter-carrier network.

All or some of these steps can be performed at a carrier network infrastructure (CNI).

In a first possible implementation form of the first aspect of the invention as such, identifying other carriers includes: maintaining a global routing table which includes encrypted routing entries; receiving an encrypted routing entry from a respective carrier of the inter-carrier network and storing the encrypted routing entry in the global routing table; and classifying the respective carrier as a carrier of an endpoint of the VPN when the received encrypted routing entry is decryptable with the VPN encryption key.

In a possible implementation form of the first implementation form of the first aspect of the invention, the method further includes: decrypting the received encrypted routing entry into a decrypted routing entry and storing the decrypted routing entry in a local routing table. The decrypted routing entry includes a VPN ID, universal identifier and routing information for a respective VPN endpoint.

In a third possible implementation form according to the first aspect as such or according to any of the preceding implementation forms of the first aspect, the method further includes validating with a certificate authority at least one of: the universal identifier and the encryption key.

In a fourth possible implementation form according to the first aspect as such or according to any of the preceding implementation forms of the first aspect, the method further includes

performing at least one of: authenticating the user client, authorizing activities of the user client and accounting transactions with the user client.

In a fifth possible implementation form according to the first aspect as such or according to any of the preceding implementation forms of the first aspect, the carriers communicate over the inter-carrier network according to a Border Gateway protocol (BGP).

According to a second aspect of the present invention there is provided a method for establishing a multi-carrier virtual private network with multiple carriers. The carriers communicate over an inter-carrier network. The method includes performing the following:

A) Sending a request to a certificate authority for a VPN identifier (VPN ID) identifying a respective virtual private network (VPN), and a respective VPN encryption key for the virtual private network;

B) Receiving the respective VPN ID and the respective VPN encryption key from the certificate authority;

C) Sending requests to multiple carriers to host respective endpoints of the multi-carrier virtual private network (VPN). The requests include a universal identifier identifying the user client, the respective VPN ID and the respective encryption key;

D) Receiving acknowledgement from the carriers that the respective VPN endpoints are established, wherein the VPN is identified by the carriers of the VPN endpoints from a combination of the respective VPN ID and the universal identifier.

All or some of these steps can be performed at a user client.

In a first possible implementation form of the second aspect, the method further includes: sending a request to the certificate authority for the universal identifier identifying the user client and receiving the universal identifier from the certificate authority.

In a second possible implementation form of the second aspect as such or according to the first implementation form of the second aspect, the method further includes receiving acknowledgement that respective encrypted routing entries for the VPN endpoints are

distributed to carriers of the inter-carrier network. The encrypted routing entries are decryptable with the encryption key, and each decrypted routing entry includes the VPN ID, the universal identifier and routing information for a respective VPN endpoint.

In a third possible implementation form of the second aspect as such or according any of the preceding implementation forms of the second aspect, the carriers communicate over the inter-carrier network according to a Border Gateway protocol (BGP).

According to a third aspect of the present invention there is provided a system for establishing an endpoint of a multi-carrier virtual private network. The system includes:

I) A carrier network infrastructure (CNI), for hosting an endpoint of a multi-carrier virtual private network (VPN);

II) A network interface for electrical communication with at least one user and with carriers over an inter-carrier network;

III) A hardware processor in electrical communication with the carrier network infrastructure and the network interface; and

IV) A non-transitory memory in electrical communication with the hardware processor. The memory stores: a local table data structure storing unencrypted routing entries, wherein the unencrypted routing entries include routing information for at least one VPN; a global table data structure storing encrypted routing entries, wherein the encrypted routing entries are encrypted with respective encryption keys; and program modules for instruction execution by the hardware processor.

The program modules include:

i) An endpoint establishment module for receiving a request from a user client to host an endpoint of a multi-carrier virtual private network (VPN) and for establishing the requested endpoint of the VPN on the CNI. The request includes a respective VPN identifier (VPN ID) identifying the VPN, a universal identifier identifying the user client, and a respective VPN encryption key;

ii) A routing distribution module for generating a routing entry for the established VPN endpoint, for encrypting the routing entry with a respective encryption key and for distributing the encrypted routing entry to at least one other carrier of the inter-carrier network. A routing entry includes the respective VPN ID, the respective universal identifier and respective routing information for the VPN endpoint; and

iii) An identification module for identifying other carriers of endpoints of the VPN by decrypting respective routing entries received from the other carriers, and establishing VPN connections with the other carriers over an inter-carrier network.

In a first possible implementation form of the third aspect, the identification module is further for: receiving an encrypted routing entry from a respective carrier of the inter-carrier network and classifying the respective carrier as a carrier of an endpoint of the VPN when the received encrypted routing entry is decryptable with the respective encryption key.

In a second possible implementation form of the third aspect as such or according to the first implementation form of the third aspect, the network interface is further for: receiving an encrypted routing entry from a carrier and storing the encrypted routing entry in the global table data structure.

In a third possible implementation form of the third aspect as such or according any of the preceding implementation forms of the third aspect, the non-transitory memory further includes an encryption key data structure for storing respective VPN encryption keys. The identification module decrypts an encrypted routing entry with a key stored in the encryption key data structure, and stores the decrypted routing entry in the local table data structure.

In a fourth possible implementation form of the third aspect as such or according any of the preceding implementation forms of the third aspect, the system further includes an AAA module for performing authentication, authorization and accounting transactions for the VPN endpoint.

According to a fourth aspect of the present invention there is provided a user client system for establishing a virtual private network with a multiple carriers. The user client system includes:

I) A network interface for electrical communication with VPN endpoint carriers and a certificate authority;

II) A hardware processor in electrical communication with the network interface; and

III) A non-transitory memory in electrical communication with the hardware processor. The memory stores: a VPN identifier (VPN ID) identifying a respective virtual private network (VPN); a respective VPN encryption key for the virtual private network; a universal identifier identifying the user client; and program modules for instruction execution by the hardware processor.

The program modules include:

i) A certification request module for sending a request to a certificate authority for a VPN identifier (VPN ID) and a respective VPN encryption key for the virtual private network, and for receiving the respective VPN ID and the respective VPN encryption key from the certificate authority;

ii) An endpoint request module for sending requests to a plurality of carriers to host respective endpoints VPN. The requests include the universal identifier, the respective VPN ID and the respective encryption key; and

iii) An acknowledgement module for receiving acknowledgement from the carriers that the respective VPN endpoints are established, wherein the VPN is identified by the carriers of the VPN endpoints from a combination of the respective VPN ID and the universal identifier.

Unless otherwise defined, all technical and/or scientific terms used herein have the same meaning as commonly understood by one of ordinary skill in the art to which the invention pertains. Although methods and materials similar or equivalent to those described herein can be used in the practice or testing of embodiments of the invention, exemplary methods and/or materials are described below. In case of conflict, the patent specification, including definitions, will control. In addition, the materials, methods, and examples are illustrative only and are not intended to be necessarily limiting.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWINGS

Some embodiments of the invention are herein described, by way of example only, with reference to the accompanying drawings. With specific reference now to the drawings in detail, it is stressed that the particulars shown are by way of example and for purposes of illustrative discussion of embodiments of the invention. In this regard, the description taken with the drawings makes apparent to those skilled in the art how embodiments of the invention may be practiced.

In the drawings:

FIG. 1 is a simplified block diagram of a VPN distributed over multiple carriers, according to embodiments of the present invention;

FIG. 2 is a simplified diagram of a network with VPN endpoints on two carriers, according to embodiments of the present invention;

FIG. 3 is a simplified flowchart of a method for establishing an endpoint of a multi-carrier virtual private network, according to embodiments of the present invention;

FIG. 4 is a simplified flowchart of a method for establishing a VPN with multiple carriers, according to embodiments of the present invention;

FIG. 5 is a simplified flowchart of a method for establishing a VPN over multiple carriers, according to embodiments of the invention;

FIG. 6 is a simplified block diagram of a system for establishing an endpoint of a multi-carrier virtual private network, according to embodiments of the invention; and

FIG. 7 is a simplified block diagram of a user client system for establishing a virtual private network with a plurality of carriers, according to embodiments of the invention.

DETAILED DESCRIPTION

The present invention, in some embodiments thereof, relates to establishing a virtual private network over multiple carriers and, more specifically, but not exclusively, to distributing virtual private network routing information between the multiple carriers.

Virtual private networking extends a private network across a multi-carrier network, such as the Internet. Users establish VPN endpoints on multiple carriers. For routing purposes there is a need to publish and synchronize information about the locations of these VPN endpoints per-user and per-carrier.

If the VPN endpoints have public IP addresses, information about their location may be published using standard Border Gateway Protocol (BGP), but no information is published about the actual cloud or carrier on which they are located. If the VPN endpoints have private IP addresses, VPN (Virtual Private Networking) and VRF (virtual routing and forwarding) may be used to isolate address spaces.

However under BGP, if two sites of a VPN are connected to different Autonomous Systems (AS) a way to use External BGP (EBGP) to distribute VPN-Internet Protocol version 4 (IPv4) or VPN-Internet Protocol version 6 (IPv6) addresses is needed. Such a situation may occur, for example, when the sites are connected to different service providers (SP).

Moreover, BGP has security for the BGP entities only and not for the resources and users. There is no way to perform authentication, authorization and accounting (AAA) with the customer or the private topology information.

Currently, there are a number of different ways of handling this case:

A) VRF-to-VRF connections at the AS (Autonomous System) border routers

With this approach, a Provider Edge (PE) router in one AS connects directly to a PE router in another. The two PE routers are connected by multiple sub-interfaces, at least one sub-interface for each of the VPNs whose routes need to be passed from AS to AS. Each PE router treats the other as if it were a Customer Edge (CE) router. That is, the PE routers associate each such sub-interface with a VRF, and use EBGP to distribute unlabeled IPv4

addresses to each other. This is a procedure that does not require Multiprotocol Label Switching (MPLS) at the border between autonomous systems. However, it does not scale as well as the other approaches discussed below.

B) EBGP redistribution of labeled VPN-IPv4 routes from AS to neighboring AS

In this approach, the PE routers use Internal BGP (IBGP) to redistribute labeled VPN-IPv4 routes either to an Autonomous System Border Router (ASBR) or to a route reflector of which an ASBR is a client. The ASBR then uses EBGP to redistribute those labeled VPN-IPv4 routes to an ASBR in another AS. The other AS in turn distributes the labeled VPN-IPv4 routes to the PE routers in that AS, or perhaps to another ASBR which in turn distributes them further, and so on.

When using this procedure, VPN-IPv4 routes are only accepted on EBGP connections at private peering points, as part of a trusted arrangement between SPs. VPN-IPv4 routes are not distributed to or accepted from the public Internet, or from any BGP peers that are not trusted. An ASBR does not accept a labeled packet from an EBGP peer unless it has actually distributed the top label to that peer. If there are many VPNs with sites attached to different Autonomous Systems, there does not need to be a single ASBR between the ASs that holds all the routes for all the VPNs. There can be multiple ASBRs, each of which holds only the routes for a particular subset of the VPNs. This procedure requires that there be a label switched path leading from a packet's ingress PE to its egress PE. Hence the appropriate trust relationships must exist between and amongst the set of ASs along the path. Also, there must be agreement amongst the set of SPs as to which border routers need to receive routes with which Route Targets.

C) Multi-hop EBGP redistribution of labeled VPN-IPv4 routes between source and destination ASs, with EBGP redistribution of labeled IPv4 routes from AS to neighboring AS

In this approach, VPN-IPv4 routes are neither maintained nor distributed by the ASBRs. An ASBR must maintain labeled IPv4/32 routes to the PE routers within its AS. It uses EBGP to distribute these routes to other ASs. ASBRs in any transit ASs will also have to use EBGP to pass along the labeled /32 routes. This results in the creation of a label switched path from the ingress PE router to the egress PE router.

Once the path is created, PE routers in different ASs are able establish multi-hop EBGP connections to each other and exchange VPN-IPv4 routes over those connections. If the /32 routes for the PE routers are made known to the PE routers of each AS communication within the VPN proceeds normally. If the /32 routes for the PE routers are NOT made known to the PE routers (other than the ASBRs), then this procedure requires a packet's ingress PE to put a three-label stack on it. The bottom label is assigned by the egress PE, corresponding to the packet's destination address in a particular VRF. The middle label is assigned by the ASBR, corresponding to the /32 route to the egress PE. The top label is assigned by the ingress PE's IGP Next Hop, corresponding to the /32 route to the ASBR. To improve scalability, the multi-hop EBGP connections may exist only between a route reflector in one AS and a route reflector in another. (However, when the route reflectors distribute routes over this connection, they do not modify the BGP next hop attribute of the routes.) The actual PE routers then only have IBGP connections to the route reflectors in their own AS. Like the previous procedure, this requires that there be a label switched path leading from a packet's ingress PE to its egress PE.

Additionally, current VRF solutions still necessitate manual configuration of per-user information and only exist within the context of a single network operator, as the route distinguishers are managed independently by each carrier. (IP subnets advertised by the CE routers to the PE routers are augmented with a 64-bit prefix route distinguisher to make them unique.) The resulting 96-bit addresses are then exchanged between the PE routers using a special address family of Multiprotocol BGP (MP-BGP). The redistribution of the per-VPN routing information into MP-BGP is not automatic and must be manually configured on the router for each VRF.

Before explaining at least one embodiment of the invention in detail, it is to be understood that the invention is not necessarily limited in its application to the details of construction and the arrangement of the components and/or methods set forth in the following description and/or illustrated in the drawings and/or the Examples. The invention is capable of other embodiments or of being practiced or carried out in various ways.

The present invention may be a system, a method, and/or a computer program product. The computer program product may include a computer readable storage medium (or media)

having computer readable program instructions thereon for causing a processor to carry out aspects of the present invention.

The computer readable storage medium can be a tangible device that can retain and store instructions for use by an instruction execution device. The computer readable storage medium may be, for example, but is not limited to, an electronic storage device, a magnetic storage device, an optical storage device, an electromagnetic storage device, a semiconductor storage device, or any suitable combination of the foregoing. A non-exhaustive list of more specific examples of the computer readable storage medium includes the following: a portable computer diskette, a hard disk, a random access memory (RAM), a read-only memory (ROM), an erasable programmable read-only memory (EPROM or Flash memory), a static random access memory (SRAM), a portable compact disc read-only memory (CD-ROM), a digital versatile disk (DVD), a memory stick, a floppy disk, a mechanically encoded device such as punch-cards or raised structures in a groove having instructions recorded thereon, and any suitable combination of the foregoing. A computer readable storage medium, as used herein, is not to be construed as being transitory signals per se, such as radio waves or other freely propagating electromagnetic waves, electromagnetic waves propagating through a waveguide or other transmission media (e.g., light pulses passing through a fiber-optic cable), or electrical signals transmitted through a wire.

Computer readable program instructions described herein can be downloaded to respective computing/processing devices from a computer readable storage medium or to an external computer or external storage device via a network, for example, the Internet, a local area network, a wide area network and/or a wireless network. The network may comprise copper transmission cables, optical transmission fibers, wireless transmission, routers, firewalls, switches, gateway computers and/or edge servers. A network adapter card or network interface in each computing/processing device receives computer readable program instructions from the network and forwards the computer readable program instructions for storage in a computer readable storage medium within the respective computing/processing device.

Computer readable program instructions for carrying out operations of the present invention may be assembler instructions, instruction-set-architecture (ISA) instructions, machine

instructions, machine dependent instructions, microcode, firmware instructions, state-setting data, or either source code or object code written in any combination of one or more programming languages, including an object oriented programming language such as Smalltalk, C++ or the like, and conventional procedural programming languages, such as the "C" programming language or similar programming languages. The computer readable program instructions may execute entirely on the user's computer, partly on the user's computer, as a stand-alone software package, partly on the user's computer and partly on a remote computer or entirely on the remote computer or server. In the latter scenario, the remote computer may be connected to the user's computer through any type of network, including a local area network (LAN) or a wide area network (WAN), or the connection may be made to an external computer (for example, through the Internet using an Internet Service Provider). In some embodiments, electronic circuitry including, for example, programmable logic circuitry, field-programmable gate arrays (FPGA), or programmable logic arrays (PLA) may execute the computer readable program instructions by utilizing state information of the computer readable program instructions to personalize the electronic circuitry, in order to perform aspects of the present invention.

Aspects of the present invention are described herein with reference to flowchart illustrations and/or block diagrams of methods, apparatus (systems), and computer program products according to embodiments of the invention. It will be understood that each block of the flowchart illustrations and/or block diagrams, and combinations of blocks in the flowchart illustrations and/or block diagrams, can be implemented by computer readable program instructions.

These computer readable program instructions may be provided to a processor of a general purpose computer, special purpose computer, or other programmable data processing apparatus to produce a machine, such that the instructions, which execute via the processor of the computer or other programmable data processing apparatus, create means for implementing the functions/acts specified in the flowchart and/or block diagram block or blocks. These computer readable program instructions may also be stored in a computer readable storage medium that can direct a computer, a programmable data processing apparatus, and/or other devices to function in a particular manner, such that the computer

readable storage medium having instructions stored therein comprises an article of manufacture including instructions which implement aspects of the function/act specified in the flowchart and/or block diagram block or blocks.

The computer readable program instructions may also be loaded onto a computer, other programmable data processing apparatus, or other device to cause a series of operational steps to be performed on the computer, other programmable apparatus or other device to produce a computer implemented process, such that the instructions which execute on the computer, other programmable apparatus, or other device implement the functions/acts specified in the flowchart and/or block diagram block or blocks.

The flowchart and block diagrams in the Figures illustrate the architecture, functionality, and operation of possible implementations of systems, methods, and computer program products according to various embodiments of the present invention. In this regard, each block in the flowchart or block diagrams may represent a module, segment, or portion of instructions, which comprises one or more executable instructions for implementing the specified logical function(s). In some alternative implementations, the functions noted in the block may occur out of the order noted in the figures. For example, two blocks shown in succession may, in fact, be executed substantially concurrently, or the blocks may sometimes be executed in the reverse order, depending upon the functionality involved. It will also be noted that each block of the block diagrams and/or flowchart illustration, and combinations of blocks in the block diagrams and/or flowchart illustration, can be implemented by special purpose hardware-based systems that perform the specified functions or acts or carry out combinations of special purpose hardware and computer instructions.

Reference is now made to Fig. 1, which is a simplified block diagram of a VPN distributed over multiple carriers, according to embodiments of the present invention. For clarity, Fig. 1 shows two carriers (110 and 120) hosting respective VPN endpoints (115 and 125 respectively) and a single carrier (130) which does not host a VPN endpoint. It is noted that the VPN may be established over additional carriers and further noted that there may be multiple carriers which do not host a VPN endpoint. The carriers communicate over inter-carrier network 140.

In order to establish a VPN endpoint on a carrier, user client 150 sends a request to the carrier. The request includes at least:

A) A universal identifier (GUID) which uniquely identifies the user to the carriers communicating over inter-carrier network 140. The GUID is used to uniquely identify all of the VPNs that belong to the user, as described below;

B) A VPN identifier (VPN ID) identifying the specific VPN instance for which the endpoint is being established. Optionally, the VPN ID is selected by the user; and

C) An encryption key which is unique to the respective VPN, and which is used to encrypt and decrypt VPN routing information as described in more detail below.

Each VPN receives a unique encryption key. Optionally only one GUID is provided to a given user. Optionally user client 150 obtains the GUID and/or encryption key and/or VPN ID from a trusted third party such as certificate authority (CA) 160. Optionally there are multiple certificate authorities that operate in cooperation to ensure that each user gets a unique GUID and encryption key(s).

The GUID and VPN ID together uniquely identify a specific VPN distributed over multiple carriers. Even if two users use the same VPN ID, the two VPNs are distinguished from one another by the GUID.

Optionally, an extended community label is formed from a combination of the GUID, VPN ID and the internal VPN address, as shown in Table 1. The extended community label identifies a specific address within the VPN.

Extended community label		
GUID	VPN ID	Internal VPN address

Table 1

When the user request is received at a carrier, the carrier establishes a VPN endpoint. The carrier creates routing information for the VPN endpoint according to the protocol used in the inter-carrier network. The routing information (denoted herein a routing entry) is encrypted

by the carrier with the encryption key provided by the user. The encrypted routing entry is distributed to the other carriers in the network.

When a carrier receives an encrypted routing entry it attempts to decrypt the encrypted routing entry with the encryption key or keys in its possession. Since a carrier only has keys for VPNs which have been established at that carrier, the carrier is able to decrypt the encrypted routing entry only if it is also hosting an endpoint of the same VPN. The carrier then establishes connections with other carriers of the VPN. Optionally, connections with other VPN carriers are performed automatically when an encrypted routing entry is decrypted by the carrier.

Optionally, if the carrier it is not hosting a VPN endpoint it retains the routing information in encrypted form. If the carrier later receives a user request to establish a VPN endpoint, it attempts to decrypt encrypted routing entries with the respective encryption key provided by the user. The carrier identifies other VPN endpoint carriers from the routing entries which have been decrypted successfully.

Optionally, carriers store encrypted routing entries in a respective global table (e.g. 110.1, 120.1 and 130.1) and decrypted routing entries in a respective local table (e.g. 110.2, 120.2 and 130.2).

Consider the exemplary network shown in Fig. 1. VPN endpoints have been established on Carrier 1 (110) and on Carrier 2 (120). Thus carriers 1 and 2 both have the VPN's encryption key. Using the encryption key, each of the carriers decrypts routing information to the VPN endpoint on the other carrier (e.g. Carrier 1 has routing information to VPN endpoint 125 and Carrier 2 has routing information to VPN endpoint 115). Carrier 3 (130) does not have an encryption key for the VPN, so although it has been sent encrypted routing entries from carriers 1 and 2 it is unable to decrypt them.

In some embodiments the inter-carrier network operates with a BGP protocol. The BGP protocol may be modified to include network-wide distribution of encrypted routing entries amongst carriers.

Reference is now made to Fig. 2, which is a simplified diagram of a network with VPN endpoints on two carriers, according to embodiments of the present invention. For clarity, Fig. 2 shows two carriers hosting VPN endpoints; however the number of carriers hosting endpoints may vary according to the VPN architecture. Other carriers which do not host VPN endpoints (not shown) may also connect via the inter-carrier network.

Each carrier connect to the inter-carrier network 250 (denoted Public internet / Inter carrier MPLS in Fig. 2) using a provider edge (PE) router (230 and 240 respectively).

Each PE router maintains a respective global table (210.1 and 220.1) and local table (210.2 and 220.2).

a) Global Table - stores encrypted BGP route information received from other carriers (e.g. autonomous systems) on the inter-carrier network 250 (denoted Public internet / Inter carrier MPLS in Fig. 2). The information is stored in the global table in cipher text form.

b) Local Table - stores BGP route information that the carrier was able to decrypt from the encrypted entries in the global table using encryption keys provided by users. The information stored is clear text.

In order to set up a VPN on carriers 1 and 2 (210 and 220 respectively), user 260 signs in to certificate authority CA 270 and requests a GUID and encryption key. User 260 then provides the GUID and encryption key to carrier 1 network management 215 and to carrier 2 network management 225, and requests each carrier to set up a VPN endpoint. Each carrier then establishes a VPN endpoint with a virtual customer edge (CE) router (216 and 226) which peers with the respective PE router (230 and 240).

Each carrier generates a respective VPN routing entry, and encrypts the routing entry with the encryption key provided by user 260. The carriers publish the available VPN endpoint destination augmented with the encrypted routing information, optionally using BGP or extended BGP protocol.

All of the carriers on inter-carrier network 250 receive encrypted routing entries for all users and store them in a global table in cipher text. Each carrier may only decrypt the information

for the users that provided them with their certificates. The decrypted information is used to build the clear text local table.

Using the local table routing information, carriers automatically establish connections between user sites across multiple carrier (e.g. AS) domains.

Reference is now made to Fig. 3, which is a simplified flowchart of a method for establishing an endpoint of a multi-carrier virtual private network, according to embodiments of the present invention. Fig. 3 shows operations performed by the carrier network infrastructure (CNI). Optionally the carrier uses a BGP protocol.

In 300 a request is received from a user client (denoted herein a user) to host a VPN endpoint. The request includes a VPN identifier (VPN ID) identifying the VPN, a GUID identifying the user client, and a VPN encryption key. In 310 the requested endpoint of the VPN is established at the carrier, using any protocol and/or architecture known in the art.

In 320 a routing entry is generated at the carrier for the established VPN endpoint. The routing entry includes routing information for the VPN endpoint, along with the VPN ID and GUID. In 330 the routing entry is encrypted with the encryption key received from the user. In 340 the encrypted routing entry is distributed to other carriers in the inter-carrier network.

In 350, the carrier establishes VPN connections with other carriers over the inter-carrier network. The routing to other VPN endpoints is determined by decrypting routing entries received from other carriers using the encryption key.

In some embodiments, the GUID and/or the encryption key are first validated with a certificate authority before the VPN endpoint is established by the carrier.

In some embodiments, authentication, authorization and accounting (AAA) mechanisms are implemented in the VPN by the carrier, possibly in cooperation with other carriers, service provides and/or external servers. The AAA mechanisms may be used for end user resource identification and/or discovery and/or advertisement (including scope and access list).

Reference is now made to Fig. 4, which is a simplified flowchart of a method for establishing a VPN with multiple carriers, according to embodiments of the present invention. Fig. 4 shows user-side operations performed by a user client.

In 400, the user sends a request to a certificate authority for a VPN ID and a respective encryption key.

In 410, the user receives a VPN ID and encryption key from the certificate authority.

Optionally, the user also requests and receives a GUID from the certificate authority.

In 420, the user sends requests to multiple carriers to host VPN endpoints of the multi-carrier virtual private network (VPN). The requests include the user's GUID, the VPN ID and the encryption key.

In 430 the user receives acknowledgement from the carriers that the respective VPN endpoints have been established.

Optionally, the user also receives acknowledgement from one or more carriers that the encrypted routing entries have been distributed throughout the inter-carrier network. This may allow the user to ensure that the VPN is established correctly amongst the hosting carriers and is properly accessible through the inter-carrier network.

Reference is now made to Fig. 5, which is a simplified flowchart of a method for establishing a VPN over multiple carriers, according to embodiments of the invention. Fig. 5 includes both user-side and carrier-side operations.

In 500 the VPN is initialized. In 510 the user contacts the CA and receives an encryption key (denoted a certificate in Fig. 5), a GUID and VPN ID from the CA.

In 520 the user establishes VPN endpoints on multiple carriers. The VPN is identified in the inter-carrier network by a combination of the GUID and VPN ID. The user also supplies the VPN certificate to the carriers.

In 530 the VPN endpoint carriers generate and encrypt routing entries for their respective VPN endpoint. The carriers publish (e.g. distribute) the encrypted routing information to other carriers connected to the inter-carrier network.

In 540 the carriers collect encrypted routing information published by other carriers and store the encrypted routing information in a global table. Optionally, collection of the encrypted routing information is performed continuously.

In 550 the carriers attempt to decrypt encrypted routing information from the global table. The decryption attempts may be performed each time a new encryption key is received from a user, possibly along with a request to establish a new VPN endpoint. Optionally, the encryption key is provided separately by the user.

When a carrier does not succeed in decrypting a routing entry, in 560 the routing entry is saved by the carrier in the global table in encrypted form. No change is made to existing routings.

When a carrier succeeds in decrypting a routing entry, in 570 the decrypted routing entry is saved by the carrier in the local table. Then, in 580, the carrier connects to other relevant carriers and VPN connections are established between the endpoints.

Reference is now made to FIG. 6, which is a simplified block diagram of a system for establishing an endpoint of a multi-carrier virtual private network, according to embodiments of the invention. Carrier 600 has VPN hosting capabilities which are managed by carrier network infrastructure 610.

Network interface 620 is an interface for communicating with other carriers and with users. Network interface 620 receives user requests to host VPN endpoints of a multi-carrier virtual private network (VPN). Each request includes a respective VPN identifier (VPN ID), a respective VPN encryption key and a universal identifier identifying the user.

Processor 630 performs processing operations and connects with carrier network infrastructure 610, network interface 620 and memory 640.

Memory 640 stores data and programming modules which are executed by processor 630.

The data stored in memory 640 includes a local table data structure 680.2 which stores the unencrypted routing entries and a global table data structure 680.1 which stores the encrypted routing entries.

The stored program modules include:

A) Endpoint establishment module 650 which establishes the requested VPN endpoint on the CNI in response to the user request;

B) Routing distribution module 660 which generates a routing entry for the established VPN endpoint. Routing distribution module 660 also encrypts the routing entry with the encryption key and distributes the encrypted routing entry to at least one other carrier; and

C) Identification module 670 which identifies other carriers hosting VPN endpoints by decrypting routing entries received from the other carriers. Identification module 670 establishes VPN connections with the other carriers over the inter-carrier network. Optionally, identification module 670 stores the decrypted routing entries in local table 680.2.

Optionally, memory 640 further includes an encryption key data structure 680.3 which stores the VPN encryption keys. Identification module 670 uses the stored encryption keys, optionally retrieved from encryption key data structure 680.3, when it attempts to decrypt an encrypted routing entry received from another carrier.

Optionally, memory 640 further includes an AAA module executed by processor 630. The AAA module performs authentication, authorization and accounting transactions for the VPN endpoint.

Reference is now made to FIG. 7, which is a simplified block diagram of a user client system for establishing a virtual private network with a plurality of carriers, according to embodiments of the invention.

Network interface 710 is an interface for communicating with VPN endpoint carriers and a certificate authority.

Processor 720 performs processing operations and connects with network interface 710 and memory 730.

Memory 730 stores: at least one VPN ID 740.1 and respective VPN encryption key 740.2, and a universal identifier 740.3.

Memory 730 also stores programming modules which are executed by processor 720. The stored program modules include:

A) Certification request module 750 which sends requests to a certificate authority for a VPN ID and a respective VPN encryption key for the virtual private network, and receives the requested items from the certificate authority. The VPN ID and encryption key are stored in 740.1 and 740.2. Optionally, certification request module 750 also requests and receives a GUID from the certificate authority, however this may not be necessary every time a new VPN is established.;

B) Endpoint request module 760 which sends requests to carriers to host respective VPN endpoints. The requests include the universal identifier, the respective VPN ID and the respective encryption key; and

C) Acknowledgement module 770 which receives acknowledgement from the carriers that the respective VPN endpoints are established.

The embodiments described herein enable users to deploy VPNs across multiple domains and carriers without the need to manually configure the interconnection between the carriers. VPN interconnection between sites may be performed automatically by the carriers. VPNs may become a global routable asset while maintaining layer (L2) private addressing. Information about private networks may only be accessed by authorized carriers so confidentiality is maintained.

The methods as described above are used in the fabrication of integrated circuit chips.

The flowchart and block diagrams in the Figures illustrate the architecture, functionality, and operation of possible implementations of systems, methods and computer program products according to various embodiments of the present invention. In this regard, each block in the

flowchart or block diagrams may represent a module, segment, or portion of code, which comprises one or more executable instructions for implementing the specified logical function(s). It should also be noted that, in some alternative implementations, the functions noted in the block may occur out of the order noted in the figures. For example, two blocks shown in succession may, in fact, be executed substantially concurrently, or the blocks may sometimes be executed in the reverse order, depending upon the functionality involved. It will also be noted that each block of the block diagrams and/or flowchart illustration, and combinations of blocks in the block diagrams and/or flowchart illustration, can be implemented by special purpose hardware-based systems that perform the specified functions or acts, or combinations of special purpose hardware and computer instructions.

The descriptions of the various embodiments of the present invention have been presented for purposes of illustration, but are not intended to be exhaustive or limited to the embodiments disclosed. Many modifications and variations will be apparent to those of ordinary skill in the art without departing from the scope and spirit of the described embodiments. The terminology used herein was chosen to best explain the principles of the embodiments, the practical application or technical improvement over technologies found in the marketplace, or to enable others of ordinary skill in the art to understand the embodiments disclosed herein.

The terms "comprises", "comprising", "includes", "including", “having” and their conjugates mean "including but not limited to". This term encompasses the terms "consisting of" and "consisting essentially of".

It is appreciated that certain features of the invention, which are, for clarity, described in the context of separate embodiments, may also be provided in combination in a single embodiment. Conversely, various features of the invention, which are, for brevity, described in the context of a single embodiment, may also be provided separately or in any suitable subcombination or as suitable in any other described embodiment of the invention. Certain features described in the context of various embodiments are not to be considered essential features of those embodiments, unless the embodiment is inoperative without those elements.

Although the invention has been described in conjunction with specific embodiments thereof, it is evident that many alternatives, modifications and variations will be apparent to those

skilled in the art. Accordingly, it is intended to embrace all such alternatives, modifications and variations that fall within the spirit and broad scope of the appended claims.

CLAIMS

1. A method for establishing an endpoint of a multi-carrier virtual private network, said virtual private network being distributed over a plurality of carriers communicating over an inter-carrier network, said method comprising:

receiving (300) a request from a user client to host an endpoint of a multi-carrier virtual private network (VPN);

establishing (310) said requested endpoint of said VPN;

wherein said request includes a respective VPN identifier (VPN ID) identifying said VPN, a universal identifier identifying said user client, and a VPN encryption key

generating (320) a routing entry for said established endpoint of said multi-carrier virtual private network, said routing entry comprising said respective VPN ID, said respective universal identifier and respective routing information for said VPN endpoint;

encrypting (330) said routing entry with said respective encryption key;

distributing (340) said encrypted routing entry to at least one other carrier of said inter-carrier network; and

identifying (350) other carriers of endpoints of said VPN from respective routing entries received from said other carriers, and establishing VPN connections with said other carriers over said inter-carrier network.

2. A method according to claim 1, wherein said identifying (350) other carriers comprises:

maintaining a global routing table comprising encrypted routing entries;

receiving an encrypted routing entry from a respective carrier of said inter-carrier network and storing said encrypted routing entry in said global routing table; and

classifying said respective carrier as a carrier of an endpoint of said VPN when said

received encrypted routing entry is decryptable with said VPN encryption key.

3. A method according to claim 2, further comprising:

decrypting said received encrypted routing entry into a decrypted routing entry, wherein said decrypted routing entry comprises a VPN ID, universal identifier and routing information for a respective VPN endpoint; and

storing said decrypted routing entry in a local routing table.

4. A method according to any one of claims 1-3, wherein validating with a certificate authority comprises at least one of: said universal identifier and said encryption key.

5. A method according to any one of claims 1-4, further comprising performing at least one of: authenticating said user client, authorizing activities of said user client and accounting transactions with said user client.

6. A method according to any one of claims 1-5, wherein said carriers communicate over said inter-carrier network according to a Border Gateway protocol, BGP.

7. A method for establishing a multi-carrier virtual private network with a plurality of carriers, wherein said carriers communicate over an inter-carrier network, said method comprising:

requesting (400) a certificate authority for a VPN identifier, VPN ID, identifying a respective virtual private network, VPN, and a respective VPN encryption key for said virtual private network;

receiving (410) said respective VPN ID and said respective VPN encryption key from said certificate authority;

sending (420) requests to a plurality of carriers to host respective endpoints of said multi-carrier virtual private network, said requests including a universal identifier identifying said user client, said respective VPN ID and said respective encryption key; and

receiving (430) acknowledgement from said carriers that said respective VPN endpoints are established, wherein said VPN is identified by said carriers of said VPN endpoints from a combination of said respective VPN ID and said universal identifier.

8. A method according to claim 7, further comprising, sending a request to said certificate authority for said universal identifier identifying said user client and receiving said universal identifier from said certificate authority.

9. A method according to claim 7 or 8, further comprising, receiving acknowledgement that respective encrypted routing entries for said VPN endpoints are distributed to carriers of said inter-carrier network, wherein said encrypted routing entries are decryptable with said encryption key, and wherein each decrypted routing entry comprises said VPN ID, said universal identifier and routing information for a respective VPN endpoint.

10. A method according to any one of claims 7-9, wherein said carriers communicate over said inter-carrier network according to a Border Gateway protocol, BGP.

11. A system for establishing an endpoint of a multi-carrier virtual private network, comprising:

a carrier network infrastructure, CNI, (610), configured to host an endpoint of a multi-carrier virtual private network;

a network interface (620) for electrical communication with at least one user and with carriers over an inter-carrier network;

a hardware processor (630) in electrical communication with said CNI (610) and said network interface (620); and

a non-transitory memory (640) in electrical communication with the hardware processor (630),

the memory (640) having stored thereon:

a local table data structure (680.2) configured to store unencrypted routing entries,

wherein said unencrypted routing entries comprise routing information for at least one VPN;

a global table data structure (680.1) configured to store encrypted routing entries, wherein said encrypted routing entries are encrypted with respective encryption keys;

program modules for instruction execution by the hardware processor, comprising:

an endpoint establishment module (650) configured to receive a request from a user client to host an endpoint of a multi-carrier virtual private network, VPN, said request including a respective VPN identifier, VPN ID, identifying said VPN, a universal identifier identifying said user client, and a respective VPN encryption key and for establishing said requested endpoint of said VPN on said CNI (610);

a routing distribution module (660) configured to generate a routing entry for said established VPN endpoint, to encrypt said routing entry with a respective encryption key and to distribute said encrypted routing entry to at least one other carrier of said inter-carrier network, wherein a routing entry comprises said respective VPN ID, said respective universal identifier and respective routing information for said VPN endpoint; and

an identification module (670) configured to identify other carriers of endpoints of said VPN by decrypting respective routing entries received from said other carriers and establishing VPN connections with said other carriers over an inter-carrier network.

12. A system according to claim 11, wherein the identification module (670) is further configured to receive an encrypted routing entry from a respective carrier of said inter-carrier network and classifying said respective carrier as a carrier of an endpoint of said VPN when said received encrypted routing entry is decryptable with said respective encryption key.

13. A system according to claim 11 or 12, wherein said network interface (620) is further

configured to receive an encrypted routing entry from a carrier and storing said encrypted routing entry in said global table data structure.

14. A system according to any one of claims 11-13, wherein said non-transitory memory (640) further comprises an encryption key data structure for storing respective VPN encryption keys, and wherein said identification module is configured to decrypt an encrypted routing entry with a key stored in said encryption key data structure, and to store said decrypted routing entry in said local table data structure.

15. A system according to any one of claims 11-14, further comprising an AAA module configured to perform authentication, authorization and accounting transactions for said VPN endpoint.

16. A user client system (700) for establishing a virtual private network with a plurality of carriers, comprising:

a network interface (710) for electrical communication with VPN endpoint carriers and a certificate authority;

a hardware processor (720) in electrical communication with said network interface (710); and

a non-transitory memory (730) in electrical communication with the hardware processor,

the memory (730) having stored thereon:

a VPN identifier, VPN ID, (740.1) identifying a respective virtual private network, VPN;

a respective VPN encryption key (740.2) for said virtual private network;

a universal identifier (740.3) identifying said user client; and

program modules for instruction execution by the hardware processor (720), comprising:

a certification request module (750) configured to send a request to a certificate authority for a VPN identifier, VPN ID, (740.1) and a respective VPN encryption key (740.2) for said virtual private network, and to receive said respective VPN ID (740.1) and said respective VPN encryption key (740.2) from said certificate authority;

an endpoint request module configured to send requests to a plurality of carriers to host respective endpoints VPN, said requests including said universal identifier (740.3), said respective VPN ID (740.1) and said respective encryption key (740.2); and

an acknowledgement module configured to receive acknowledgement from said carriers that said respective VPN endpoints are established, wherein said VPN is identified by said carriers of said VPN endpoints from a combination of said respective VPN ID (740.1) and said universal identifier (740.3).

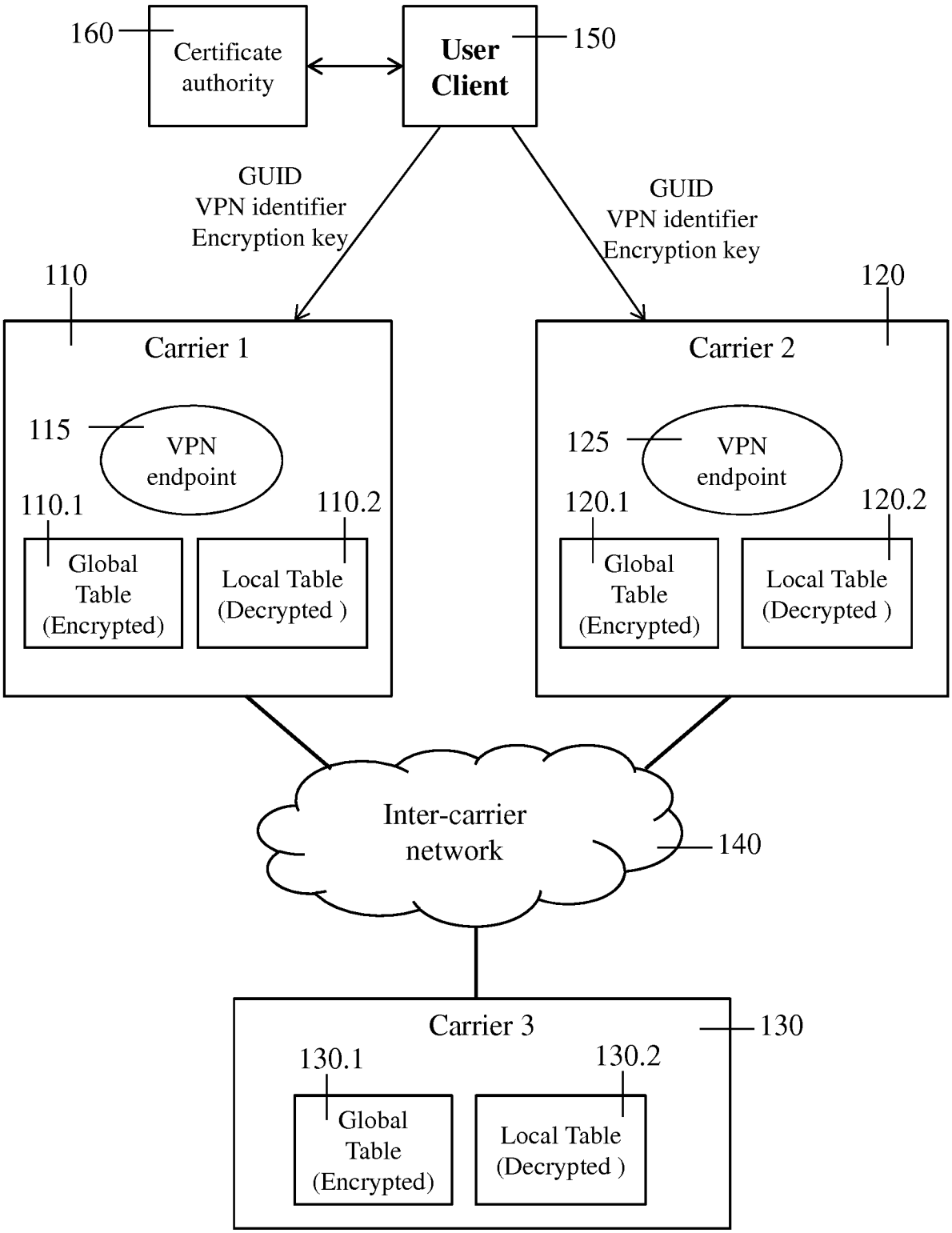
160
Certificate authority
User Client
150
GUID
VPN identifier
Encryption key
GUID
VPN identifier
Encryption key
110
Carrier 1
120
Carrier 2
115
VPN endpoint
125
VPN endpoint
110.1
Global Table (Encrypted)
110.2
Local Table (Decrypted)
120.1
Global Table (Encrypted)
120.2
Local Table (Decrypted)
Inter-carrier network
140
Carrier 3
130
130.1
Global Table (Encrypted)
130.2
Local Table (Decrypted)

FIGURE 1

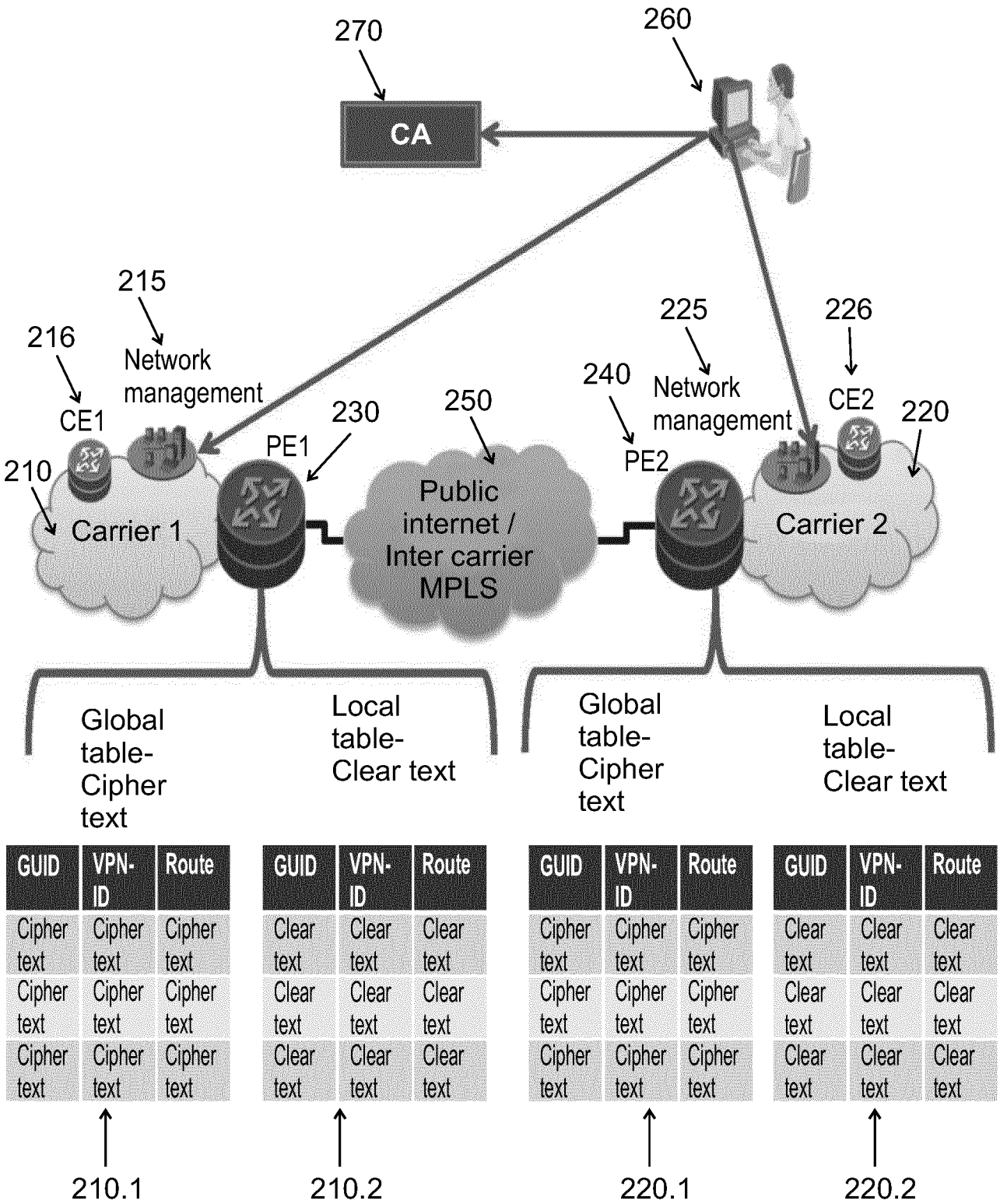
270
CA
260
215
216
Network management
CE1
210
Carrier 1
PE1
230
250
Public internet / Inter carrier MPLS
240
PE2
225
Network management
226
CE2
220
Carrier 2
Global table- Cipher text
Local table- Clear text
Global table- Cipher text
Local table- Clear text
GUID
VPN-ID
Route
Cipher text
Clear text
210.1
210.2
220.1
220.2

FIGURE 2

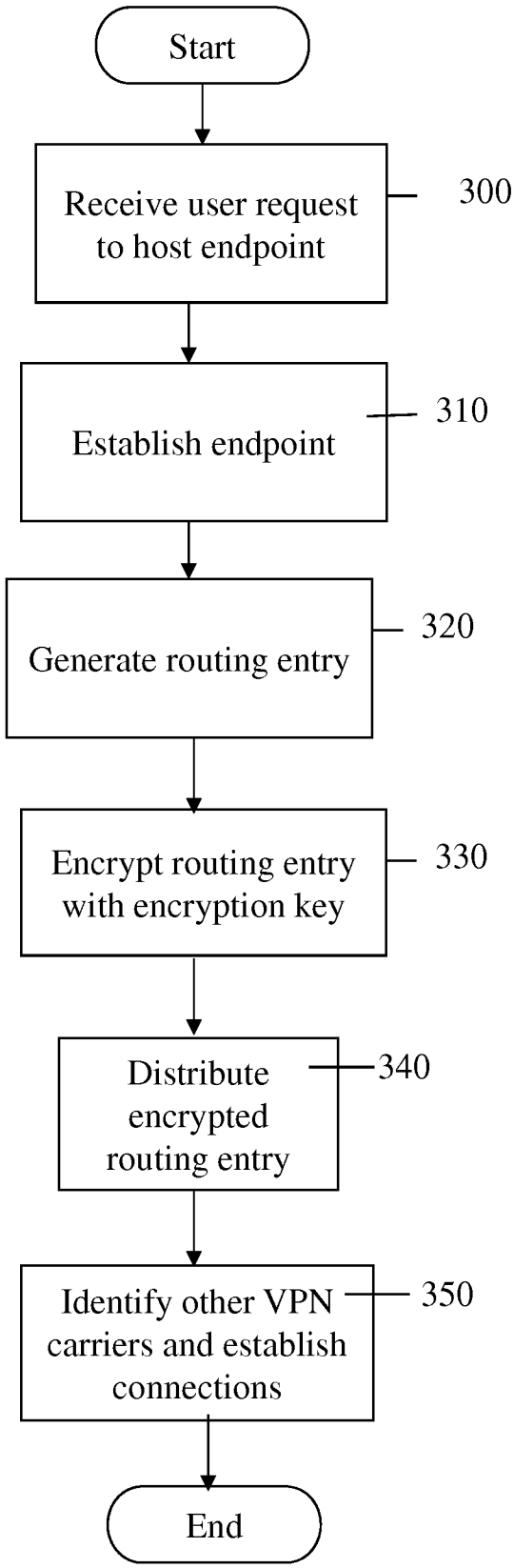
Start
Receive user request to host endpoint
300
Establish endpoint
310
Generate routing entry
320
Encrypt routing entry with encryption key
330
Distribute encrypted routing entry
340
Identify other VPN carriers and establish connections
350
End

FIGURE 3

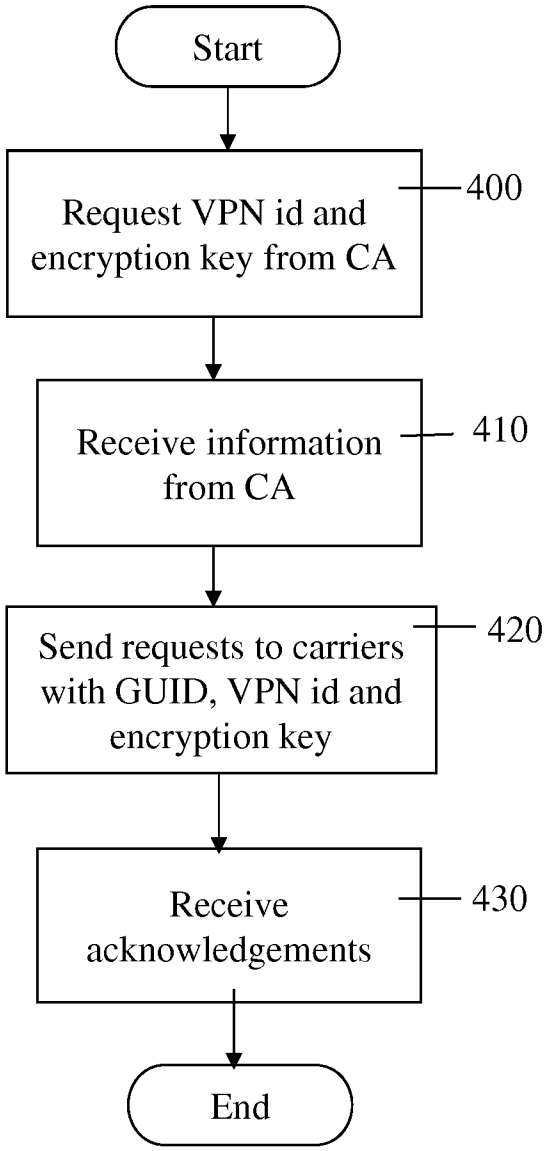
Start
Request VPN id and encryption key from CA
400
Receive information from CA
410
Send requests to carriers with GUID, VPN id and encryption key
420
Receive acknowledgements
430
End

FIGURE 4

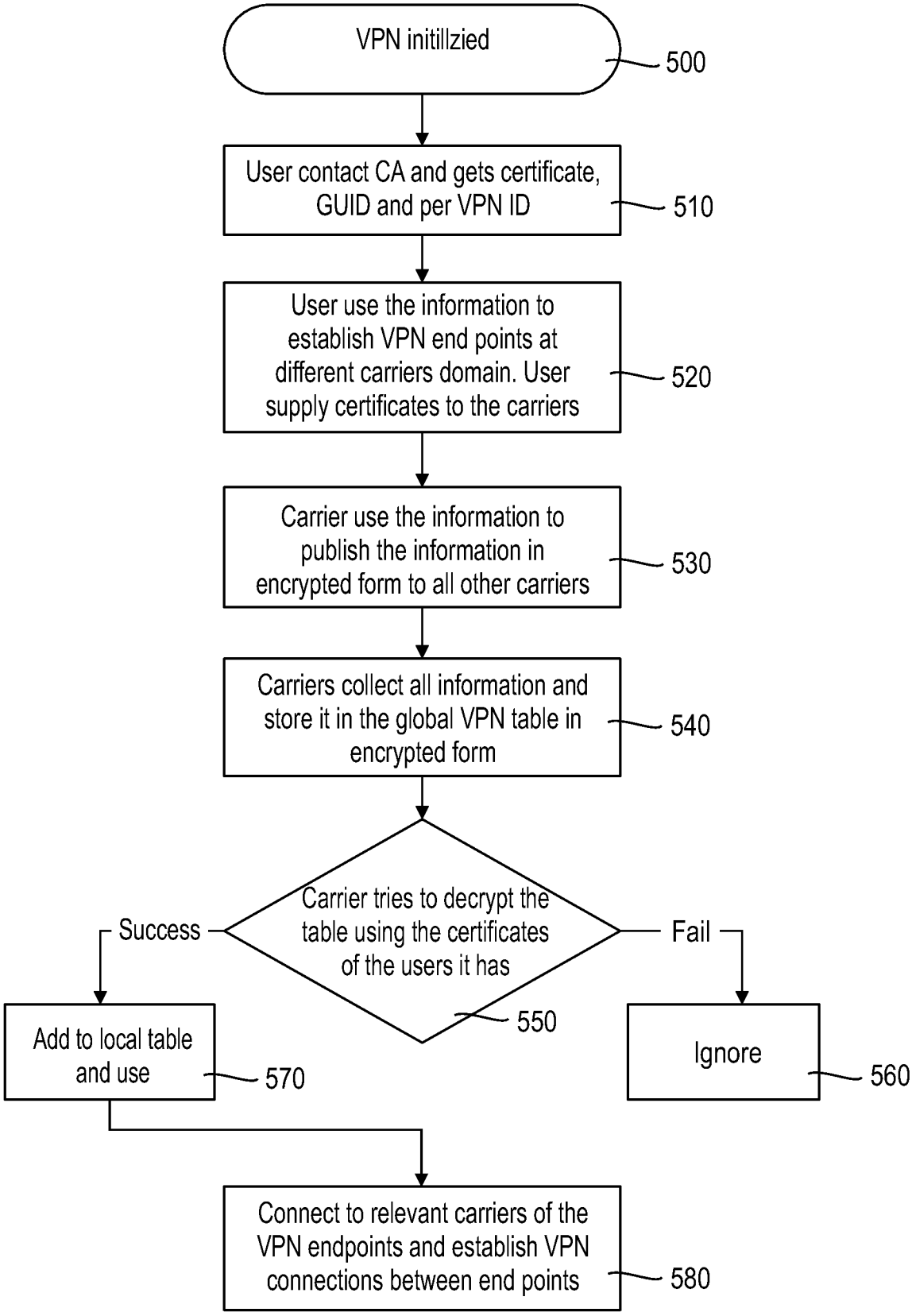
VPN initillzied
500
User contact CA and gets certificate, GUID and per VPN ID
510
User use the information to establish VPN end points at different carriers domain. User supply certificates to the carriers
520
Carrier use the information to publish the information in encrypted form to all other carriers
530
Carriers collect all information and store it in the global VPN table in encrypted form
540
Carrier tries to decrypt the table using the certificates of the users it has
550
Success
Fail
Add to local table and use
570
Ignore
560
Connect to relevant carriers of the VPN endpoints and establish VPN connections between end points
580

FIGURE 5

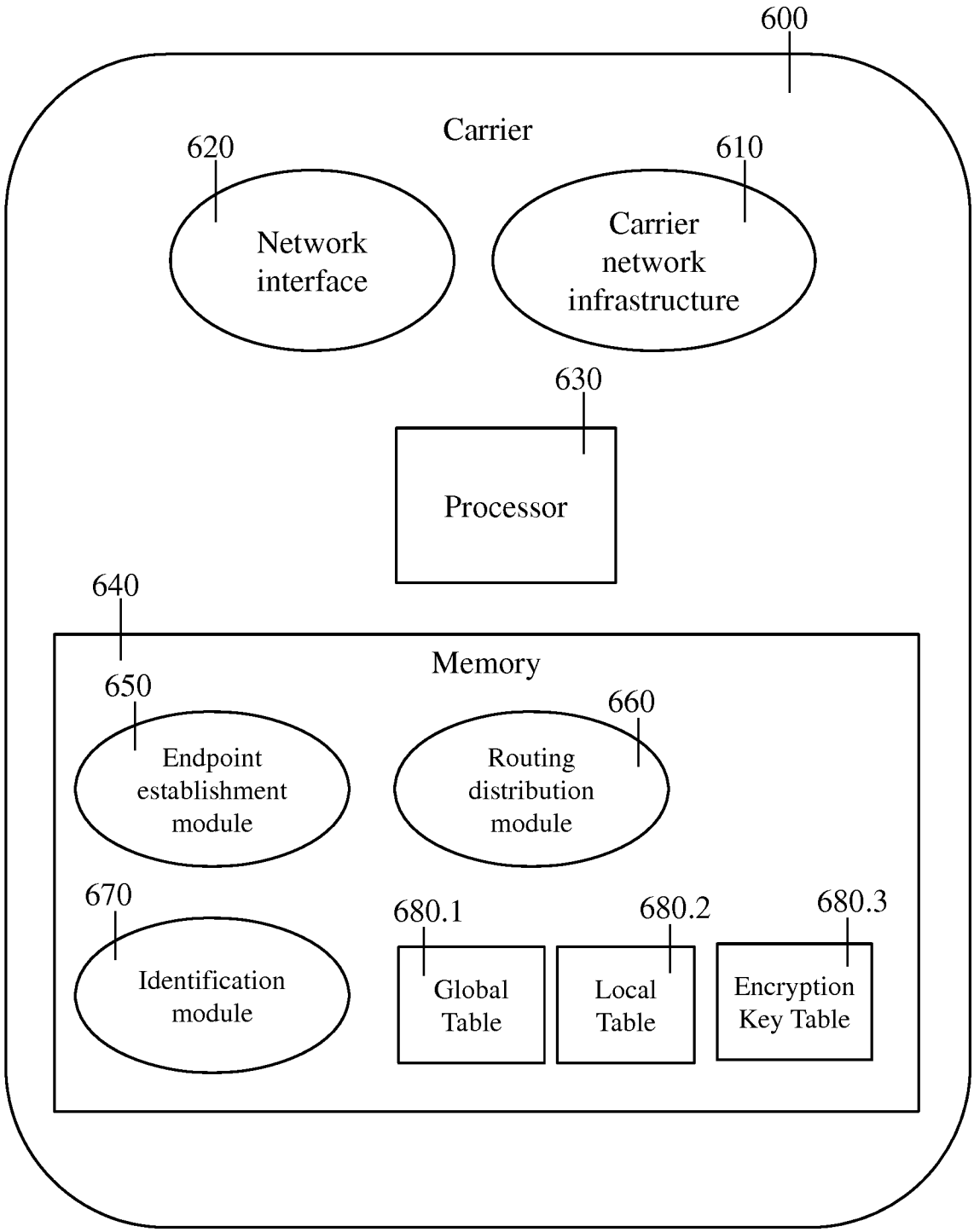
600
Carrier
620
Network interface
610
Carrier network infrastructure
630
Processor
640
Memory
650
Endpoint establishment module
660
Routing distribution module
670
Identification module
680.1
Global Table
680.2
Local Table
680.3
Encryption Key Table

FIGURE 6

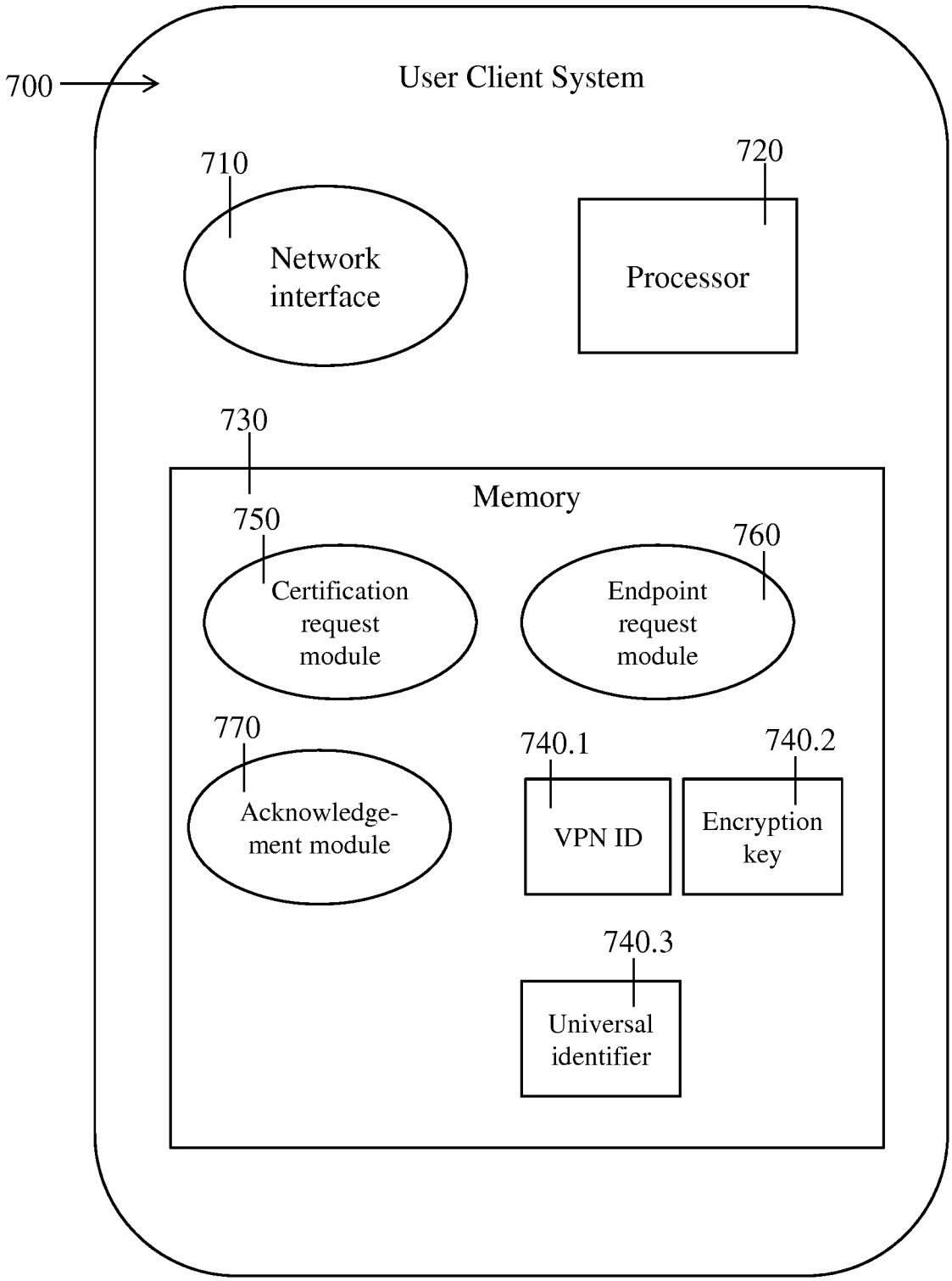
700
User Client System
710
Network interface
720
Processor
730
Memory
750
Certification request module
760
Endpoint request module
770
Acknowledge-ment module
740.1
VPN ID
740.2
Encryption key
740.3
Universal identifier

FIGURE 7

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2014/063109

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L12/46
ADD. H04L12/715 H04L12/751

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	ROSEN CISCO SYSTEMS E ET AL: "BGP/MPLS IP Virtual Private Networks (VPNs); rfc4364.txt", 20060201, 1 February 2006 (2006-02-01), XP015044797, ISSN: 0000-0003	1,4-11, 15,16
A	sections 4, 4.3.2, 9 and 10	2,3, 12-14

Y	CALLON JUNIPER NETWORKS M SUZUKI NTT CORPORATION R: "A Framework for Layer 3 Provider-Provisioned Virtual Private Networks (PPVPNs); rfc4110.txt", 20050701, 1 July 2005 (2005-07-01), XP015041891, ISSN: 0000-0003	1,4-11, 15,16
A	sections 3.1.1.2, 4.1, 4.2.1.4, 4.4.4.2, 4.7.2 and 6.7	2,3, 12-14

	-/--	

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 February 2015	09/03/2015

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Ramenzoni, Stefano

1

Form PCT/ISA/210 (second sheet) (April 2005)

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 2 720 415 A1 (HUAWEI TECH CO LTD [CN]) 16 April 2014 (2014-04-16) paragraphs [0023] - [0028], [0047] - [0074]	1-16
A	MICHAEL ROSSBERG ET AL: "A survey on automatic configuration of virtual private networks", COMPUTER NETWORKS, ELSEVIER SCIENCE PUBLISHERS B.V., AMSTERDAM, NL, vol. 55, no. 8, 5 January 2011 (2011-01-05), pages 1684-1699, XP028203871, ISSN: 1389-1286, DOI: 10.1016/J.COMNET.2011.01.003 [retrieved on 2011-01-09] the whole document	1-16

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2014/063109

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 2720415 A1	16-04-2014	CN 102449964 A	09-05-2012
		EP 2720415 A1	16-04-2014
		WO 2012106919 A1	16-08-2012