NETWORK LABEL DISTRIBUTION METHOD, DEVICE AND SYSTEM

(57) Embodiments of the present invention relate to the communications field, and provide a network label allocation method, a device, and a system, which enable a local PE to distinguish packets from different remote PEs, thereby laying a foundation for fault management and performance measurement of an L3VPN. The network label allocation method includes: generating, by a local provider edge PE, a VPN label route for each remote PE, where VPN labels in VPN label routes of different remote PEs are different, and the remote PE and the local PE at least belong to a same VPN; and sending, by the local PE, the VPN label route to the remote PE, so that the remote PE separately matches an IP address of the remote PE with a target device IP address in the VPN label route, and matches an import route target RT of each virtual routing forwarding VRF of the remote PE with a route target RT in the VPN label route, so as to make the remote PE carry the VPN label when the remote PE sends, to the local PE, a packet related to a successfully matched VRF. The network label allocation method, the device, and the system provided in the embodiments of the present invention are used for network label allocation.

A local provider edge generates a virtual private network label route for each remote provider edge, where virtual private network labels in virtual private network label routes of different remote provider edges are different, and the remote provider edge and the local provider edge belong to a same virtual private network.

The local provider edge sends the virtual private network label route to the remote provider edge.

FIG. 1
This application claims priority to Chinese Patent Application No. 201210184163.0, filed with the Chinese Patent Office on June 6, 2012 and entitled “NETWORK LABEL ALLOCATION METHOD, DEVICE, AND SYSTEM”, which is incorporated herein by reference in its entirety.

The present invention relates to the communications field, and in particular, to a network label allocation method, a device, and a system.

A BGP (Border Gateway Protocol, border gateway protocol) is an exterior gateway protocol for communication between different autonomous systems. A BGP-based MPLS (Multi Protocol Label Switching, multi protocol label switching) IP (Internet Protocol, Internet Protocol) VPN (Virtual Private Network, virtual private network) is generally called an L3VPN (Level3 VPN, Level 3 virtual private network). In the L3VPN, a RD (Route Distinguisher, route distinguisher RD) is generally used to distinguish overlapping VPN route prefixes in different VPNs, and an RT (Route Target) is used to identify a VPN membership.

In an existing L3VPN, when publishing VPN routing information by using the BGP, a local PE (Provider Edge, provider edge) allocates a specific VPN label to a VPN route prefix belonging to a specific VPN and publishes the VPN label to all remote PEs belonging to a same VPN. In this way, when forwarding packets to the local PE, the remote PEs belonging to the same VPN all carry a same VPN label. A BGP/MPLS L3VPN needs to use an MPLS tunnel for bearing. When an LSP (Label Switching Path, label switching path) established by using an LDP (Label Distribution Protocol, label distribution protocol) is used to bear the L3VPN, because the LDP LSP belongs to a multi-point to point type, that is, an egress node (Egress) of the LSP cannot determine a source of a packet according to an LSP tunnel label, and packets sent by different remote PEs carry a same VPN label, consequently the local PE cannot distinguish the packets from the different remote PEs. For fault management and performance measurement of the L3VPN, two ends for sending and receiving a packet need to be determined; therefore, in this case, fault management and performance measurement of the L3VPN cannot be implemented.

Embodiments of the present invention provide a network label allocation method, a device, and a system, which enable a local PE to distinguish packets from different remote PEs, thereby laying a foundation for fault management and performance measurement of an L3VPN.

According to one aspect, a network label allocation method is provided and includes:

- generating, by a local provider edge PE, a VPN label route for each remote PE, where VPN labels in VPN label routes of different remote PEs are different, and the remote PE and the local PE at least belong to a same VPN; and
- sending, by the local PE, the VPN label route to the remote PE, so that the remote PE separately matches an IP address of the remote PE with a target device IP address in the VPN label route, and matches an import route target RT of each virtual routing forwarding VRF of the remote PE with a route target RT in the VPN label route, so as to make the remote PE carry the VPN label when sending a packet related to a successfully matched VRF.

According to one aspect, a network label allocation method is provided and includes:

- receiving, by a remote PE, a VPN label route sent by a local PE, where the local PE and the remote PE at least belong to a same VPN, and the VPN label route includes a VPN label different from that of another remote PE; matching, by the remote PE separately, an IP address of the remote PE with a target device IP address in the VPN label route, and matching an import route target RT of each virtual routing forwarding VRF of the remote PE with a route target RT in the VPN label route, so as to make the remote PE carry the VPN label when sending a packet related to a successfully matched VRF, so that the local PE distinguishes the packet sent by the remote PE from a packet sent by the another remote PE.
According to one aspect, a local provider edge is provided and includes:

- a first generating unit, configured to generate a VPN label route for each remote PE, where VPN labels in VPN label routes of different remote PEs are different, and the remote PE and the local PE at least belong to a same VPN; and
- a first sending unit, configured to send the VPN label route to the remote PE, so that the remote PE separately matches an IP address of the remote PE with a target device IP address in the VPN label route, and matches an import route target RT of each virtual routing forwarding VRF of the remote PE with a route target RT in the VPN label route, so as to make the remote PE carry the VPN label when the remote PE sends, to the local PE, a packet related to a successfully matched VRF.

According to one aspect, a remote provider edge is provided and includes:

- a second receiving unit, configured to receive a VPN label route sent by a local PE, where the local PE and the remote PE at least belong to a same VPN, and the VPN label route includes a VPN label different from that of another remote PE;
- a second matching unit, configured to separately match an IP address of the remote PE with a target device IP address in the VPN label route, and match an import route target RT of each virtual routing forwarding VRF of the remote PE with a route target RT in the VPN label route; and
- a second sending unit, configured to carry the VPN label when the remote PE sends, to the local PE, a packet related to a successfully matched VRF, so that the local PE distinguishes the packet sent by the remote PE from a packet sent by the another remote PE.

According to one aspect, a communications system is provided and includes:

- any one of the foregoing local provider edges;
- and
- any one of the foregoing remote provider edges.

The embodiments of the present invention provide the network label allocation method, the device, and the system. The network label allocation method includes: generating, by a local provider edge PE, a VPN label route for each remote PE, where VPN labels in VPN label routes of different remote PEs are different, and the remote PE and the local PE at least belong to a same VPN; and sending, by the local PE, the VPN label route to the remote PE, so that the remote PE separately matches an IP address of the remote PE with a target device IP address in the VPN label route, and matches an import route target RT of each virtual routing forwarding VRF of the remote PE with a route target RT in the VPN label route, so as to make the remote PE carry the VPN label when the remote PE sends, to the local PE, a packet related to a successfully matched VRF. In this way, because the local PE sends a different VPN label route to each remote PE, when each remote PE sends a packet of a corresponding VPN to the local PE, the local PE can distinguish the sending end PE of the packet according to a different VPN label carried in the packet. Therefore, the local PE can distinguish packets from different remote PEs, and a foundation is laid for fault management and performance measurement of an L3VPN.

BRIEF DESCRIPTION OF DRAWINGS

To describe the technical solutions in the embodiments of the present invention or in the prior art more clearly, the following briefly introduces the accompanying drawings required for describing the embodiments or the prior art. Apparently, the accompanying drawings in the following description show merely some embodiments of the present invention, and a person of ordinary skill in the art may still derive other drawings from these accompanying drawings without creative efforts.

FIG. 1 is a flowchart of a network label allocation method according to an embodiment of the present invention; FIG. 2 is a flowchart of another network label allocation method according to an embodiment of the present invention; FIG. 3 is a flowchart of still another network label allocation method according to an embodiment of the present invention; FIG 4 is a schematic structural diagram of a local provider edge according to an embodiment of the present invention; FIG 5 is a schematic structural diagram of another local provider edge according to an embodiment of the present invention; FIG 6 is a schematic structural diagram of a remote provider edge according to an embodiment of the present invention;
The following clearly and completely describes the technical solutions in the embodiments of the present invention with reference to the accompanying drawings in the embodiments of the present invention. Apparently, the described embodiments are merely a part rather than all of the embodiments of the present invention. All other embodiments obtained by a person of ordinary skill in the art based on the embodiments of the present invention without creative efforts shall fall within the protection scope of the present invention.

An embodiment of the present invention provides a network label allocation method. As shown in FIG. 1, the method includes:

S101: A local PE generates a VPN label route for each remote PE, where VPN labels in VPN label routes of different remote PEs are different, and the remote PE and the local PE at least belong to a same VPN.

The VPN label route may include: an IP address of the local PE, an RT (Route Target, route target), a target device IP address, and a VPN label. As shown in Table 1:

- The length field of the IP address of the local PE is used to indicate the length of the IP address of the local PE. Because there may be multiple types of IP addresses, such as, IPV4 and IPV6, lengths of the IP addresses thereof are different. The field of the IP address of the local PE is used to indicate an IP address of the PE, and the number of bytes of the field is related to the length field of the IP address of the local PE. Exemplarily, when it is indicated that the length of the IP address of the local PE is 4 bytes, a length of the field of the IP address of the local PE is four bytes, and an IP address type in the field is IPV4. Similarly, the length field of the target device IP address is used to indicate a length of an IP address of a target PE, and a field of the target device IP address is used to indicate the IP address of the target PE. The RT field carries information about an Export (export) RT, of the local PE, matched with an Import (import) RT in a member discovery route of a target device, and the information may also be carried by using a BGP extended community attribute. The field of the VPN label is used to indicate the VPN label, and in a VPN label route sent by the local PE for each remote PE, a VPN label in the field is different. Particularly, relative to the local PE, the target device may be considered as a remote PE; therefore, in an actual application, the target device in the VPN label route is generally considered as a remote PE by default.

S102: The local PE sends the VPN label route to the remote PE, so that the remote PE separately matches an IP address of the remote PE with a target device IP address in the VPN label route, and matches an import route target RT of each VRF (Virtual Routing Forwarding, virtual routing and forwarding) of the remote PE with a route target RT in the VPN label route, so as to make the remote PE carry the VPN label when the remote PE sends, to the local PE, a packet related to a successfully matched VRF.

In this way, because the local PE sends a different VPN label route to each remote PE, when each remote PE sends a packet of a corresponding VPN to the local PE, the local PE can distinguish the sending end PE of the packet according to a different VPN label carried in the packet. Therefore, the local PE can distinguish packets from different remote PEs, and a foundation is laid for fault management and performance measurement of an L3VPN.

Particularly, before step S101, the network label allocation method provided in the embodiment of the present invention may further include: receiving, by the local PE, a VPN member discovery route sent by the remote PE; and matching, by the local PE, an Export RT of each VRF of the local PE with an Import RT in the VPN member discovery route.
route, and if the matching succeeds, determining that successfully matched VRFs in the remote PE and the local PE belong to a same VPN.

[0022] The VPN member discovery route includes: an IP address of the remote PE and the Import RT. When an Export RT, of the VRF same as the Import RT in the VPN member discovery route, exists in the local PE, step S101 specifically includes: setting the target device IP address in the VPN label route to be the same as the IP address of the remote PE in the VPN member discovery route; and making the RT in the VPN label route include an Export RT of the successfully matched VRF in the local PE.

[0023] An embodiment of the present invention provides a network label allocation method. As shown in FIG. 2, the method includes:

[0024] S201: A remote PE receives a VPN label route sent by a local PE, where the local PE and the remote PE at least belong to a same VPN, and the VPN label route includes a VPN label different from that of another remote PE.

[0025] Exemplarily, the VPN label route includes: an IP address of the local PE, an RT, a target device IP address, and the VPN label. Particularly, the VPN label route may further include a RD, of the local PE, for identifying a VRF generating the VPN label route.

[0026] S202: The remote PE separately matches an IP address of the remote PE with a target device IP address in the VPN label route, and matches an import route target RT of each virtual routing forwarding VRF of the remote PE with a route target RT in the VPN label route.

[0027] S203: The remote PE carries the VPN label when sending, to the local PE, a packet related to a successfully matched VRF, so that the local PE distinguishes the packet sent by the remote PE from a packet sent by the another remote PE.

[0028] In this way, because the VPN label route, for the remote PE, received by the remote PE, is different from a VPN label route of another PE, when the remote PE sends a packet, namely, a packet related to the successfully matched VRF, of a corresponding VPN to the local PE after the remote PE matches the successfully obtained VPN label route for the remote PE, the remote PE carries the VPN label in the VPN label route. Therefore, the local PE can distinguish packets from different remote PEs, and a foundation is laid for fault management and performance measurement of an L3VPN.

[0029] Particularly, before step S201, the method may further include: generating, by the remote PE, a VPN member discovery route; and sending, by the remote PE, the VPN member discovery route to the local PE, so that the local PE determines whether the remote PE and the local PE belong to a same VPN. The VPN member discovery route includes: an IP address of the remote PE and an Import RT. As shown in Table 2:

<table>
<thead>
<tr>
<th>Table 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Length of the IP address of the remote PE (1 byte)</td>
</tr>
<tr>
<td>Length of the IP address of the remote PE (a variable length)</td>
</tr>
<tr>
<td>Import RT-1 (8 bytes)</td>
</tr>
<tr>
<td>...</td>
</tr>
<tr>
<td>Import RT-n (8 bytes)</td>
</tr>
</tbody>
</table>

[0030] The length field of the IP address of the remote PE is used to indicate a length of the IP address of the remote PE, and the field of the IP address of the remote PE is used to indicate the IP address of the remote PE. Reference may be made to a related explanation in Table 1 for a detailed explanation. The Import RT field indicates the Import RT, and multiple fields may exist. Exemplarily, the Import RT field may carry all Import RTs on the PE.

[0031] Further, after step S202, the method may further include:

when the IP address of the remote PE and the target device IP address in the VPN label route are the same, and an Import RT, of the VRF, same as the RT in the VPN label route, exists, determining that the matching succeeds, and importing (Import) the VPN label route in the successfully matched VRF in the remote PE, where "importing" may also be referred to as "introducing", and represents an action of adding a new route to a VRF table.

[0032] Further, step S203 specifically includes: recording, by the remote PE, the successfully matched VRF and routing information in the successfully matched VRF; and sending, by the remote PE, the packet in a VPN to which the successfully matched VRF belongs, and when a next hop of a VPN route of the packet is the same as an IP address, of the local PE, recorded in label routing information in the VRF, carrying the VPN label in the packet according to label routing information in the successfully matched VRF.

[0033] Exemplarily, an embodiment of the present invention provides a network label allocation method. As shown in
FIG. 3, the method includes:

S301: A remote PE generates a VPN member discovery route.

S302: The remote PE sends the VPN member discovery route to the local PE.

S303: The local PE matches an Export RT of a VRF with the Import RT in the VPN member discovery route.

S304: The local PE generates, for each remote PE, a VPN label route including a different VPN label. Step S305 is performed.

S305: The local PE sends the VPN label route to the remote PE. Step S306 is performed.

S306: The remote PE sends the VPN label route to the remote PE. Step S307 is performed.

S307: The local PE matches an Export RT of a VRF with the Import RT in the VPN member discovery route.

S308: The local PE matches an Export RT of each VRF of the local PE with the Import RT in the VPN member discovery route; and if the matching succeeds, determines that successfully matched VRFs in the remote PE and the local PE belong to a same VPN. If no Export RT that is the same as the Import RT in the VPN member discovery route exists in the local PE, it is determined that the remote PE and the local PE do not belong to a same VPN. Particularly, there may be multiple VRFs whose export route targets Export RT in the local PE match with the import route target Import RT in the VPN member discovery route.

S309: In the embodiment of the present invention, if the remote PE and the local PE belong to a same VPN, and step S304 is performed.

S310: The local PE generates, for each remote PE, a VPN label route including a different VPN label. Step S311 is performed.

S311: The local PE sends the VPN label route to the remote PE. Step S312 is performed.

S312: The remote PE sends the VPN label route to the remote PE. Step S313 is performed.

S313: The local PE matches an Export RT of a VRF with the Import RT in the VPN member discovery route.

S314: The local PE matches an Export RT of each VRF of the local PE with the Import RT in the VPN member discovery route; and if the matching succeeds, determines that successfully matched VRFs in the remote PE and the local PE belong to a same VPN. If no Export RT that is the same as the Import RT in the VPN member discovery route exists in the local PE, it is determined that the remote PE and the local PE do not belong to a same VPN. Particularly, there may be multiple VRFs whose export route targets Export RT in the local PE match with the import route target Import RT in the VPN member discovery route.

S315: In the embodiment of the present invention, if the remote PE and the local PE belong to a same VPN, and step S310 is performed.

S316: The local PE generates, for each remote PE, a VPN label route including a different VPN label. Step S317 is performed.

S317: The local PE sends the VPN label route to the remote PE. Step S318 is performed.

S318: The remote PE sends the VPN label route to the remote PE. Step S319 is performed.

S319: The local PE matches an Export RT of a VRF with the Import RT in the VPN member discovery route.

S320: The local PE matches an Export RT of each VRF of the local PE with the Import RT in the VPN member discovery route; and if the matching succeeds, determines that successfully matched VRFs in the remote PE and the local PE belong to a same VPN. If no Export RT that is the same as the Import RT in the VPN member discovery route exists in the local PE, it is determined that the remote PE and the local PE do not belong to a same VPN. Particularly, there may be multiple VRFs whose export route targets Export RT in the local PE match with the import route target Import RT in the VPN member discovery route.
label routes of different remote PEs are different, and the remote PE and the local PE at least belong to a same VPN, where the VPN label route may include: an Internet Protocol IP address of the local PE, an RT, a target device IP address, and a VPN label; and

a first sending unit 402, configured to send the VPN label route to the remote PE, so that the remote PE separately matches an IP address of the remote PE with a target device IP address in the VPN label route, and matches an import route target RT of each virtual routing forwarding VRF of the remote PE with a route target RT in the VPN label route, so as to make the remote PE carry the VPN label when the remote PE sends, to the local PE, a packet related to a successfully matched VRF.

[0052] In this way, because the first generating unit generates, for each remote PE, a VPN label route including a different virtual private network VPN label, the first sending unit sends a different VPN label route to each remote PE, and when each remote PE sends a packet of a corresponding VPN to the local PE, the local PE can distinguish the sending PE of the packet according to a different VPN label carried in the packet. Therefore, the local PE can distinguish packets from different remote PEs, and a foundation is laid for fault management and performance measurement of an L3VPN.

[0053] Particularly, as shown in FIG. 5, the local provider edge 40 may further include:

- a first receiving unit 403, configured to receive a VPN member discovery route sent by the remote PE; and
- a first matching unit 404, configured to match an Export RT of each VRF of the local PE with an Import RT in the VPN member discovery route; and if the matching succeeds, determine that successfully matched VRFs in the remote PE and the local PE belong to a same VPN.

[0054] The VPN member discovery route includes: an IP address of the remote PE and the Import RT.

[0055] Particularly, when the matching succeeds, the first generating unit 401 is further configured to:

- set the target device IP address in the VPN label route to be the same as the IP address of the remote PE in the VPN member discovery route; and
- make the RT in the VPN label route include an Export RT of the successfully matched VRF in the local PE.

[0056] An embodiment of the present invention provides a remote provider edge 60, as shown in FIG. 6, including:

- a second receiving unit 601, configured to receive a VPN label route sent by a local PE, where the local PE and the remote PE at least belong to a same VPN, and the VPN label route includes a VPN label different from that of another remote PE;
- a second matching unit 602, configured to separately match an IP address of the remote PE with a target device IP address in the VPN label route, and match an import route target RT of each virtual routing forwarding VRF of the remote PE with a route target RT in the VPN label route, where the VPN label route includes: an IP address of the local PE, an RT, a target device IP address, and a VPN label; and
- a second sending unit 603, configured to carry the VPN label when the remote PE sends, to the local PE, a packet related to a successfully matched VRF, so that the local PE distinguishes the packet sent by the remote PE from a packet sent by the another remote PE.

[0057] In this way, because the VPN label route, for the remote PE, received by the second receiving unit is different from a VPN label route of another PE, when the second sending unit sends a packet of a corresponding VPN to the local PE after the second matching unit matches the successfully obtained VPN label route for the remote PE, the second sending unit carries the VPN label in the VPN label route. Therefore, the local PE can distinguish packets from different remote PEs, and a foundation is laid for fault management and performance measurement of an L3VPN.

[0058] Particularly, as shown in FIG. 7, the device may further include:

- a second generating unit 604, configured to generate a VPN member discovery route, where the VPN member discovery route may include: an IP address of the remote PE and the import route target RT; a third sending unit 605, configured to send the VPN member discovery route to the local PE, so that the local PE determines whether the remote PE and the local PE belong to a same VPN; and
- an importing unit 606, configured to: when the IP address of the remote PE and the target device IP address in the VPN label route are the same, and an import route target RT, of a VRF, same as the route target RT in the VPN label route exists, determine that the matching succeeds, and import the VPN label route in the successfully matched VRF in the remote PE.
Further, as shown in FIG. 8, the third sending unit 605 is specifically configured to:

- a recording subunit 6051, configured to record the successfully matched VRF and routing information in the successfully matched VRF; and
- a sending subunit 6052, configured to send the packet in a VPN to which the successfully matched VRF belongs, and when a next hop of a VPN route of the packet is the same as an IP address, of the local PE, recorded in label routing information in the VRF, carry the VPN label in the packet according to label routing information in the successfully matched VRF.

An embodiment of the present invention provides a communications system, including any one of the foregoing local provider edges and any one of the foregoing remote provider edges.

It should be noted that, in an actual application, for convenient use, the communications system may integrate, into a same PE, functions of the local provider edge and the remote provider edge that are provided in the embodiments of the present invention. Exemplarily, as shown in FIG. 9, a communications system 90 includes multiple PEs: a PEX, a PE1, a PE2, to a PEN. In the communications system 90, a local PE and a remote PE are relative, for example, from a perspective of the PEX, the PEX is a local PE, and the PE1, the PE2, to the PEN are remote PEs; and from a perspective of the PE1, the PE1 is a local PE, and the PEX, the PE2, to the PEN are remote PEs. In the embodiment of the present invention, the PEX being a local PE is used as an example. The PEX may belong to multiple VPNs, and if the PEX belongs to a VPN-P and a VPN-Q, the PE1, the PE2, to the PEN respectively generate VPN member discovery routes 1, 2, ..., N and send the routes to PEs in the communications system 90. If the PE1, the PE2, to the PEN all belong to the VPN-P and the VPN-Q, export route targets, of at least two VRFs, matched with Import RTs in the VPN member discovery routes of the PE1, the PE2, to the PEN, exist in the PEX. The PEX generates, for each remote PE, a VPN label route including a different VPN label. Exemplarily, in the VPN-P, the PEX allocates VPN labels 11, 21, to N1 respectively to the PE1, the PE2, to the PEN; and in the VPN-Q, the PEX allocates VPN labels 12, 22, to N2 respectively to the PE1, the PE2, to the PEN, so that when specific information in the remote PE is the same as specific information in the VPN label route, the remote PE carries the VPN label in the VPN label route when sending a packet to the PEX, and the PEX distinguishes the sending end PE of the VPN label according to the received VPN label.

The embodiment of the present invention provides the communications system. Because a local PE sends a different VPN label route to each remote PE, when each remote PE sends a packet of a corresponding VPN to the local PE, the local PE can distinguish the sending end PE of the packet according to a different VPN label carried in the packet. Therefore, the local PE can distinguish packets from different remote PEs, and a foundation is laid for fault management and performance measurement of an L3VPN.

It may be clearly understood by a person skilled in the art that, for the purpose of ease and brevity of description, for a detailed working process of the foregoing system, apparatus, and unit, reference may be made to a corresponding process in the foregoing method embodiments, and details are not repeatedly described herein.

In the several embodiments provided in the present application, it should be understood that the disclosed system, apparatus, and method may be implemented in other manners. For example, the described apparatus embodiment is merely exemplary. For example, the unit division is merely logical function division and may be other division in actual implementation. For example, a plurality of units or components may be combined or integrated into another system, or some features may be ignored or not performed. In addition, insertion or discussed direct couplings or communication connections may be implemented through some interfaces. The indirect couplings or communication connections between the apparatuses or units may be implemented in electronic, mechanical, or other forms.

The units described as separate parts may or may not be physically separate, and parts displayed as units may or may not be physical units, may be located in one position, or may be distributed on a plurality of network units. A part or all of the units may be selected according to actual needs to achieve the objectives of the solutions of the embodiments.

In addition, functional units in the embodiments of the present invention may be integrated into one processing unit, or each of the units may exist alone physically, or two or more units are integrated into one unit. The integrated unit may be implemented in a form of hardware, or may be implemented in a form of hardware in addition to a software functional unit.

A person of ordinary skill in the art may understand that all or a part of the steps of the method embodiments may be implemented by a program instructing relevant hardware. The program may be stored in a computer readable storage medium. When the program runs, the steps of the method embodiments are performed. The foregoing storage medium includes: any medium that can store program code, such as a ROM, a RAM, a magnetic disk, or an optical disc.

The foregoing descriptions are merely specific implementation manners of the present invention, but are not intended to limit the protection scope of the present invention. Any variation or replacement readily figured out by a person skilled in the art within the technical scope disclosed in the present invention shall fall within the protection scope.
of the present invention. Therefore, the protection scope of the present invention shall be subject to the protection scope of the claims.

Claims

1. A network label allocation method, comprising:

   generating, by a local provider edge PE, a virtual private network VPN label route for each remote PE, wherein VPN labels in VPN label routes of different remote PEs are different, and the remote PE and the local PE at least belong to a same VPN; and

   sending, by the local PE, the VPN label route to the remote PE, so that the remote PE separately matches an IP address of the remote PE with a target device IP address in the VPN label route, and matches an import route target RT of each virtual routing forwarding VRF of the remote PE with a route target RT in the VPN label route, so as to make the remote PE carry the VPN label when the remote PE sends, to the local PE, a packet related to a successfully matched VRF.

2. The method according to claim 1, wherein the VPN label route comprises: an IP address of the local PE, the route target RT, the target device IP address, and the VPN label.

3. The method according to claim 1 or 2, wherein before the generating, by a local provider edge PE, a VPN label route for each remote PE, the method further comprises:

   receiving, by the local PE, a VPN member discovery route sent by the remote PE; and

   matching, by the local PE, an export route target RT of each VRF of the local PE with an import route target RT in the VPN member discovery route; and if the matching succeeds, determining that successfully matched VRFs in the remote PE and the local PE belong to a same VPN.

4. The method according to claim 3, wherein the VPN member discovery route comprises: the IP address of the remote PE and the import route target RT.

5. The method according to claim 3 or 4, wherein when the matching succeeds, the generating, by a local PE, a VPN label route for each remote PE comprises:

   setting the target device IP address in the VPN label route to be the same as the IP address of the remote PE in the VPN member discovery route; and

   making the route target RT in the VPN label route comprise an export route target RT of the successfully matched VRF in the local PE.

6. A network label allocation method, comprising:

   receiving, by a remote PE, a VPN label route sent by a local PE, wherein the local PE and the remote PE at least belong to a same VPN, and the VPN label route comprises a VPN label different from that of another remote PE;

   matching, by the remote PE separately, an IP address of the remote PE with a target device IP address in the VPN label route, and matching an import route target RT of each virtual routing forwarding VRF of the remote PE with a route target RT in the VPN label route; and

   carrying, by the remote PE, the VPN label when sending, to the local PE, a packet related to a successfully matched VRF, so that the local PE distinguishes the packet sent by the remote PE from a packet sent by the another remote PE.

7. The method according to claim 6, wherein the VPN label route comprises: an IP address of the local PE, the route target RT, the target device IP address, and the VPN label.

8. The method according to claim 6 or 7, wherein before the receiving, by a remote PE, a VPN label route sent by a local PE, the method further comprises:
generating, by the remote PE, a VPN member discovery route; and

sending, by the remote PE, the VPN member discovery route to the local PE, so that the local PE determines

whether the remote PE and the local PE belong to a same VPN.

9. The method according to claim 8, wherein the VPN member discovery route comprises: the IP address of the remote PE and an import route target RT.

10. The method according to any one of claims 6 to 9, wherein

after the matching, by the remote PE separately, an IP address of the remote PE with a target device IP address in the VPN label route, and matching an import route target RT of each virtual routing forwarding VRF of the remote PE with a route target RT in the VPN label route, the method further comprises:

when the IP address of the remote PE and the target device IP address in the VPN label route are the same, and an import route target RT, of a VRF, same as the route target RT in the VPN label route exists, determining that the matching succeeds, and importing the VPN label route in the successfully matched VRF in the remote PE.

11. The method according to any one of claims 6 to 10, wherein

the carrying, by the remote PE, the VPN label when sending, to the local PE, a packet related to a successfully matched VRF specifically comprises:

recording, by the remote PE, the successfully matched VRF and routing information in the successfully matched VRF; and

sending, by the remote PE, the packet in a VPN to which the successfully matched VRF belongs, and when a next hop of a VPN route of the packet is the same as an IP address, of the local PE, recorded in label routing information in the VRF, carrying the VPN label in the packet according to label routing information in the successfully matched VRF.

12. A local provider edge, comprising:

a first generating unit, configured to generate a VPN label route for each remote PE, wherein VPN labels in VPN label routes of different remote PEs are different, and the remote PE and the local PE at least belong to a same VPN; and

a first sending unit, configured to send the VPN label route to the remote PE, so that the remote PE separately matches an IP address of the remote PE with a target device IP address in the VPN label route, and matches an import route target RT of each virtual routing forwarding VRF of the remote PE with a route target RT in the VPN label route, so as to make the remote PE carry the VPN label when the remote PE sends, to the local PE, a packet related to a successfully matched VRF.

13. The device according to claim 12, wherein the VPN label route comprises: an Internet Protocol IP address of the local PE, the route target RT, the target device IP address, and the VPN label.

14. The device according to claim 12 or 13, wherein the device further comprises:

a first receiving unit, configured to receive a VPN member discovery route sent by the remote PE; and

a first matching unit, configured to match an export route target RT of each VRF of the local PE with an import route target RT in the VPN member discovery route; and if the matching succeeds, determine that successfully matched VRFs in the remote PE and the local PE belong to a same VPN.

15. The device according to claim 14, wherein the VPN member discovery route comprises: the IP address of the remote PE and the import route target RT.

16. The device according to claim 14 or 15, wherein when the matching succeeds, the first generating unit is further configured to:

set the target device IP address in the VPN label route to be the same as the IP address of the remote PE in the VPN member discovery route; and

make the route target RT in the VPN label route comprise an export route target RT of the successfully matched VRF in the local PE.
17. A remote provider edge, comprising:

- a second receiving unit, configured to receive a VPN label route sent by a local PE, wherein the local PE and the remote PE at least belong to a same VPN, and the VPN label route comprises a VPN label different from that of another remote PE;
- a second matching unit, configured to separately match an IP address of the remote PE with a target device IP address in the VPN label route, and match an import route target RT of each virtual routing forwarding VRF of the remote PE with a route target RT in the VPN label route; and
- a second sending unit, configured to carry the VPN label when the remote PE sends, to the local PE, a packet related to a successfully matched VRF, so that the local PE distinguishes the packet sent by the remote PE from a packet sent by the another remote PE.

18. The device according to claim 17, wherein the VPN label route comprises: an IP address of the local PE, the route target RT, the target device IP address, and the VPN label.

19. The device according to claim 17 or 18, wherein the device further comprises:

- a second generating unit, configured to generate a VPN member discovery route; and
- a third sending unit, configured to send the VPN member discovery route to the local PE, so that the local PE determines whether the remote PE and the local PE belong to a same VPN.

20. The method according to claim 19, wherein the VPN member discovery route comprises: the IP address of the remote PE and an import route target RT.

21. The device according to any one of claims 17 to 20, wherein the device further comprises:

- an importing unit, configured to: when the IP address of the remote PE and the target device IP address in the VPN label route are the same, and an import route target RT, of a VRF, same as the route target RT in the VPN label route exists, determine that the matching succeeds, and import the VPN label route in the successfully matched VRF in the remote PE.

22. The device according to any one of claims 17 to 21, wherein the third sending unit is specifically configured to:

- a recording subunit, configured to record the successfully matched VRF and routing information in the successfully matched VRF; and
- a sending subunit, configured to send the packet in a VPN to which the successfully matched VRF belongs, and when a next hop of a VPN route of the packet is the same as an IP address, of the local PE, recorded in label routing information in the VRF, carry the VPN label in the packet according to label routing information in the successfully matched VRF.

23. A communications system, comprising:

- the local provider edge according to any one of claims 12 to 16, and
- the remote provider edge according to any one of claims 17 to 22.
A local provider edge generates a virtual private network label route for each remote provider edge, where virtual private network labels in virtual private network label routes of different remote provider edges are different, and the remote provider edge and the local provider edge belong to the same virtual private network.

The local provider edge sends the virtual private network label route to the remote provider edge.

FIG. 1

A remote provider edge receives a virtual private network label route sent by a local provider edge, where the local provider edge and the remote provider edge at least belong to the same virtual private network, and the virtual private network label route includes a virtual private network label different from that of another remote provider edge.

The remote provider edge separately matches an Internet Protocol address of the remote provider edge with a target device Internet Protocol address in the virtual private network label route, and matches an import route target route target of each virtual routing forwarding of the remote provider edge with a route target in the virtual private network label route.

The remote provider carries the virtual private network label when sending to the local provider edge, a data packet related to a successfully matched virtual routing and forwarding table, so that the local provider edge distinguishes the packet sent by the remote PE from a packet sent by the another remote PE.

FIG. 2
Local provider edge

Remote provider edge

S301 Generate a virtual private network member discovery route

S302 Send the virtual private network member discovery route

S303 Match an export route target of a virtual routing and forwarding table with an import route target in the virtual private network member discovery route

S304 Generate a virtual private network label route including a different virtual private network label

S305 Send the virtual private network label route

S306 Match specific information of the remote provider edge with specific information in the virtual private network label route

FIG. 3
FIG. 8

Third sending unit

Recording subunit

Sending subunit

605

6051

6052
FIG. 9

Provider edge 1

Provider edge X

Provider edge 2

Provider edge N

Virtual private network member N1 in a virtual private network Q

Virtual private network member N2 in a virtual private network Q

Virtual private network member P in a virtual private network Q

Virtual private network label L1 in a virtual private network Q

Virtual private network label L2 in a virtual private network Q

Virtual private network label O in a virtual private network Q

Virtual private network label 2 in a virtual private network Q

Virtual private network label 1 in a virtual private network Q

Virtual private network label 0 in a virtual private network Q

Virtual network member P in a virtual private network Q

Virtual network member 2 in a virtual private network Q

Virtual network member 1 in a virtual private network Q

Virtual network member 0 in a virtual private network Q

Virtual network discovery route 1

Virtual network discovery route 2

...
INTERNATIONAL SEARCH REPORT

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/723 (2013.01) i

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)

IPC: H04L; H04W; H04B; H04M

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)

WPI; EPDOC; CNKI; IEEE; CNPAT: local, remote, virtual private network, label, route, route target, virtual routing forwarding, VPN, RT, VRF

C. DOCUMENTS CONSIDERED TO BE RELEVANT

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>CN 102449964 A (HUAWEI TECHNOLOGIES CO., LTD.), 09 May 2012 (09.05.2012), description, paragraphs [0019]-[0020] and [0084]-[0092], and figures 3-4</td>
<td>1-23</td>
</tr>
<tr>
<td>A</td>
<td>CN 101927740 A (HANGZHOU E3C TECHNOLOGIES CO., LTD.), 09 September 2009 (09.09.2009), the whole document</td>
<td>1-23</td>
</tr>
<tr>
<td>A</td>
<td>US 2010/0110928 A1 (ELIAS, M. et al.), 06 May 2010 (06.05.2010), the whole document</td>
<td>1-23</td>
</tr>
</tbody>
</table>

☐ Further documents are listed in the continuation of Box C. ☒ 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

20 August 2013 (20.08.2013)

Date of mailing of the international search report

12 September 2013 (12.09.2013)

Name and mailing address of the ISA/CN:
State Intellectual Property Office of the P. R. China
No. 6, Xitucheng Road, Jimingqiao
Haidian District, Beijing 100088, China
Facsimile No.: (86-10) 62019451

Authorized officer
SUN, Guohui

Telephone No.: (86-10) 61648242

Form PCT/ISA/210 (second sheet) (July 2009)
## INTERNATIONAL SEARCH REPORT
Information on patent family members

<table>
<thead>
<tr>
<th>Patent Documents referred in the Report</th>
<th>Publication Date</th>
<th>Patent Family</th>
<th>Publication Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>CN 10249964 A</td>
<td>09.05.2012</td>
<td>WO 2012106919 A1</td>
<td>16.08.2012</td>
</tr>
<tr>
<td>CN 101527740 A</td>
<td>09.09.2009</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>US 2010/0110928 A1</td>
<td>06.05.2010</td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

Form PCT/ISA/210 (patent family annex) (July 2009)
REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader’s convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

• WO 201210184163 A [0001]