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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 November 2016 (17.11.2016)

WIPO | PCT

(10) International Publication Number
WO 2016/180351 A1

(51) International Patent Classification:
H04L 12/741 (2013.01)

(21) International Application Number:
PCT/CN2016/081832

(22) International Filing Date:
12 May 2016 (12.05.2016)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
201510243201.9 13 May 2015 (13.05.2015) CN

(71) Applicant: **HANGZHOU H3C TECHNOLOGIES CO., LTD.** [CN/CN]; 466 Changhe Road, Binjiang District, Hangzhou, Zhejiang 310052 (CN).

(72) Inventors: **PING, Dan**; Room 730, Oriental Electronic BLD., NO.2, Chuangye Road, Shangdi Information Industry Base, Haidian District, Beijing 100085 (CN). **LIAO, Junyun**; Room 730, Oriental Electronic BLD., NO.2, Chuangye Road, Shangdi Information Industry Base, Haidian District, Beijing 100085 (CN). **LUO, Guobing**; Room 730, Oriental Electronic BLD., NO.2, Chuangye Road, Shangdi Information Industry Base, Haidian District, Beijing 100085 (CN). **YU, Chenchen**; Room 730, Oriental Electronic BLD., NO.2, Chuangye Road, Shangdi Information Industry Base, Haidian District, Beijing 100085 (CN). **PENG, Zhang**; Room 730, Oriental Electronic BLD., NO.2, Chuangye Road, Shangdi Information Industry Base, Haidian District, Beijing 100085 (CN).

(74) Agent: **DEQI INTELLECTUAL PROPERTY LAW CORPORATION**; 7/F, Xueyuan International Tower, NO.1 Zhichun Road, Haidian District, Beijing 100083 (CN).

(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, 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, ST, 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, 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))*

(54) **Title**: ENDPOINT MIGRATION DETECTION

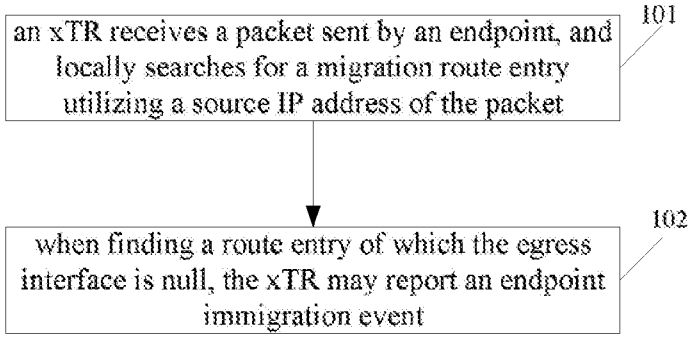

FIG. 1

(57) **Abstract**: An endpoint immigration detection method includes: an xTR receives a packet sent by an endpoint, and searches for a migration route entry using a source IP address of the packet; when finding a route entry of which the egress interface is null, reports an endpoint immigration event.

WO 2016/180351 A1

ENDPOINT MIGRATION DETECTION

BACKGROUND

[0001] The Locator/Identity Separation Protocol (LISP) networking scheme may provide two independent address spaces, namely Endpoint Identifier (EID) address and Routing Locator (RLOC) address.

[0002] The EID address is an address of a host of an endpoint, used to identify the identity of the host. The role of the EID address in the LISP is similar to a Domain Name System (DNS), and the EID address possesses a separate address space. In the LISP network, the EID address may be migrated independently of the RLOC address. During the migration of an endpoint, the EID address of the host of the endpoint is changeless. The RLOC address is an address of a LISP router, and may be routing forwarded in an Internet. The RLOC address may be globally routed, and may be aggregated according to network topologies.

[0003] The endpoint may be a server, a virtual machine connected to a router, or a mobile terminal, such as a mobile phone, an iPAD, a notebook computer.

BRIEF DESCRIPTION OF THE DRAWINGS

[0004] For a better understanding of the present disclosure, reference should be made to the Detailed Description below, in conjunction with the following drawings in which like reference numerals refer to corresponding parts throughout the figures.

[0005] FIG. 1 is a flow diagram illustrating a method for detecting immigration of an endpoint according an example of the present disclosure.

[0006] FIG. 2 is a flow diagram illustrating a method for detecting immigration of an endpoint according another example of the present disclosure.

[0007] FIG. 3 is a schematic diagram illustrating a LISP network in which a virtual machine migrates from one network segment to another network segment according to examples of the present disclosure.

[0008] FIG.4 is a schematic diagram illustrating a LISP network in which a virtual machine migrates in the same network segment according to examples of the present disclosure.

[0009] FIG.5 is a schematic diagram illustrating a device for detecting immigration of an endpoint according an example of the present disclosure.

[0010] FIG. 6 is a schematic diagram illustrating a device for detecting immigration of an endpoint according another example of the present disclosure.

DETAILED DESCRIPTION

[0011] Reference will now be made in detail to examples, which are illustrated in the accompanying drawings. In the following detailed description, numerous specific details are set forth in order to provide a thorough understanding of the present disclosure. Also, the figures are illustrations of an example, in which modules or procedures shown in the figures are not necessarily essential for implementing the present disclosure. In other instances, well-known methods, procedures, components, and circuits have not been described in detail so as not to unnecessarily obscure aspects of the examples.

[0012] At present, the migration detection of an endpoint is usually achieved through a hardware chip of a router. When the hardware chip of the router cannot support the detection function, the immigration of an endpoint cannot be detected by the router. In order to leave the router free from the hardware chip, in examples of the present disclosure, software logic is utilized to perform the migration detection of the endpoint by taking the place of the hardware chip.

[0013] In an example, migration data may be sent to a LISP thread, and then the migration detection of the endpoint may be performed by inquiring the data of the LISP thread. For instance, the migration data may include initial configuration data and running data generated during the running of the LISP thread.

[0014] The configuration data may include at least one of the followings.

[0015] 1) Dynamic-EID strategy configuration: the dynamic-EID strategy is used to specify information of an immigration network segment.

[0016] Since the LISP network allows an endpoint to migrate from one data center to another data center, it is necessary for an xTR to configure a dynamic-EID strategy to specify an immigration network segment. The xTR is a router supporting the functions both of an

Ingress Tunnel Router (ITR) and an Egress Tunnel Router (ETR).In the present disclosure, the number of the network segments may be specified as required. An endpoint matching the immigration network segment may immigrates, namely an endpoint of which the Internet Protocol (IP) address is within the immigration network segment is permitted to immigrate.

[0017] 2) Interface migration configuration: in order to migrate in the same network segment, it is necessary to configure an extend-subnet-mode command on an interface, on which an endpoint immigration event should be detected.

[0018] In the scenario of migration in the same network segment, an extend-subnet-mode command is configured on an interface, on which an endpoint immigration event should be detected. If the extend-subnet-mode command is not configured on the interface, it may be a scenario that an endpoint emigrated from this network segment re-immigrates to this network segment, and an endpoint immigration event will not be reported.

[0019] Furthermore, in order to reduce unnecessary attack performed by illegal packets on an interface, in the example, the dynamic-EID strategy may be enabled on the interface, on which an endpoint immigration event should be detected (namely the interface on which the immigration detection should be performed). Multiple dynamic-EID strategies may be enabled on one interface. It is not necessary to perform endpoint immigration detection on an interface, on which no dynamic-EID strategy is enabled.

[0020] Running data may include at least one of the followings.

[0021] 1) Configuration Null0 route entry, namely a network segment route entry of which the egress interface is null.

[0022] If the network segment of the interface on which the immigration detection should be performed includes the immigration network segment configured by the dynamic-EID strategy, it is determined that there is a direct route. In general, there exists a direct route in a scenario of migration in the same network segment, namely a same-network segment immigration scenario, and there is not a direct route in a scenario of migration from one network segment to another network segment, namely a cross-network segment immigration scenario. When there does not exist a direct route, the xTR will generates a Null0 route entry corresponding to the dynamic-EID strategy, and the Null0 route entry may be called

configuration Null0 route entry. That is to say, a network segment route entry, of which the egress interface is Null, is generated corresponding to the immigration network segment specified by the dynamic-EID strategy. Since there does not exist a direct route in the cross-network segment immigration scenario, the xTR will generates a configuration Null0 route entry for detecting the cross-network segment immigration.

[0023] 2) Immigration host route entry, namely a host route entry of which the egress interface is not null.

[0024] When an xTR reports an endpoint immigration event, the xTR may generate a 32-bit immigration host route entry, of which the egress interface is the interface receiving a packet of the endpoint. The immigration host route entry may be used to indicate that an endpoint immigrates to the site, and when a sequent packet matches the immigration host route entry, the endpoint immigration event will not be reported again. In addition, the xTR will send a map-register packet for the endpoint to a map-server (MS). When a condition for sending a multicast map-notify packet is satisfied, the xTR may also send a multicast map-notify packet to other xTRs in the same multicast group.

[0025] When receiving the map-register packet sent for the endpoint by the xTR, the map-server may determine whether information that the endpoint has been registered on an xTR in another data center is recorded in the map-server, when the information is recorded in the map-server, the map-server may send a map-notify packet to the xTR in the another data center, and update the register information of the endpoint.

[0026] 3) Emigration Null0 route entry, namely a host route entry of which the egress interface is null.

[0027] When an endpoint emigrates, the xTR may generate a 32-bit emigration Null0 route entry to indicate that the endpoint emigrates from the site. That is to say, when receiving a map-notify packet sent by the map-server or a multicast map-notify packet sent by that xTR, the xTR in the another data center may determine whether there exists a immigration host route entry, namely a host route entry of which the egress interface is not null, when there exists the immigration host route entry, delete the immigration host route entry; and determine whether there exists a configuration Null0 route entry, when there exists the

configuration Null0 route entry, ignores the map-notify packet; when there does not exist the configuration Null0 route entry, corresponding to the IP address of the endpoint, generate a host route entry, of which the egress interface is null, namely an emigration Null0 route entry.

[0028] The process of performing endpoint migration detection by inquiring the data of the LISP thread will be described in detail hereinafter.

[0029] FIG. 1 is a flow diagram illustrating a method for detecting immigration of an endpoint according an example of the present disclosure. As shown in FIG.1, the method may include the following processes.

[0030] At block 101, an xTR receives a packet sent by an endpoint, and searches for a migration route entry from the xTR utilizing a source IP address of the packet.

[0031] The migration route entry may be an immigration host route entry, a configuration Null0 route entry, or an emigration Null0 route entry. The configuration Null0 route entry is a network segment route entry of which the egress interface is null; the emigration Null0 route entry is a host route entry of which the egress interface is null. Namely, the configuration Null0 route entry and the emigration Null0 route entry are respectively a route entry of which the egress interface is null.

[0032] At block 102, when finding a route entry of which the egress interface is null（a configuration Null0 route entry or an emigration Null0 route entry）, the xTR may report an endpoint immigration event.

[0033] When the route entry of which the egress interface is null is the emigration Null0 route entry, it may indicate a scenario that an endpoint emigrated from this network segment re-immigrates to this network segment. When the route entry of which the egress interface is null is the configuration Null0 route entry, it may indicate a scenario that an endpoint immigrates to this network segment for the first time, namely a cross-network segment immigration scenario.

[0034] When finding an immigration host route entry, for instance, a route entry with a 32-bit IP address, the xTR may not report the endpoint immigration event.

[0035] When not finding a route entry of which the egress interface is null or the immigration host route entry, the xTR may determine whether the source IP address of the packet and the IP address of the interface receiving the packet belong to the same network segment, when determining that the source IP address of the packet and the IP address of the interface receiving the packet belong to the same network segment, the xTR may further determine whether an extend-subnet-mode command is configured on the interface receiving the packet, and when the extend-subnet-mode command is configured on the interface receiving the packet, report the endpoint immigration event; when determining that the source IP address of the packet and the IP address of the interface receiving the packet do not belong to the same network segment, or when the extend-subnet-mode command is not configured on the interface receiving the packet, not report the endpoint immigration event.

[0036] When determining that the source IP address of the packet and the IP address of the interface receiving the packet do not belong to the same network segment, the xTR may not report the endpoint immigration event.

[0037] FIG. 2 is a flow diagram illustrating a method for detecting immigration of an endpoint according another example of the present disclosure. As shown in FIG.2, the method may include the following processes.

[0038] At block 201, an xTR receives a packet sent by an endpoint.

[0039] At block 202, the xTR determines whether a dynamic-EID strategy is enabled on the interface receiving the packet, when the dynamic-EID strategy is enabled on the interface receiving the packet, block 203 is performed; otherwise, block 208 is performed.

[0040] At block 203, the xTR determines whether a source IP address of the packet matches an immigration network segment specified by the enabled dynamic-EID strategy, when the source IP address of the packet matches the immigration network segment specified by the enabled dynamic-EID strategy, block 204 is performed; otherwise, block 208 is performed.

[0041] In the example, the longest matching principle may be utilized to perform the match of the source IP address of the packet with the immigration network segment specified by the enabled dynamic-EID strategy.

[0042] In the example, the execution sequence of block 202 and block 203 is not limited to sequence shown in FIG.2, for example, block 203 may be executed before block 202, namely, the xTR may determine whether a source IP address of the packet matches an immigration network segment specified by the enabled dynamic-EID strategy first, and when the source IP address of the packet matches the immigration network segment specified by the enabled dynamic-EID strategy, the xTR determines whether a dynamic-EID strategy is enabled on the interface receiving the packet, and when the dynamic-EID strategy is enabled on the interface receiving the packet, block 204 is performed.

[0043] At block 204, the xTR locally searches for a migration route entry utilizing the source IP address of the packet. When finding an immigration host route entry, block 208 is performed; when finding a route entry of which the egress interface is null, block 207 is performed; when not finding a route entry of which the egress interface is null or the immigration host route entry , block 205 is performed.

[0044] The route entry of which the egress interface is null may be a configuration Null0 route entry or an emigration Null0 route entry. When the route entry of which the egress interface is null is the emigration Null0 route entry, it may indicate a scenario that an endpoint emigrated from this network segment re-immigrates to this network segment. When the route entry of which the egress interface is null is the configuration Null0 route entry, it may indicate a scenario that an endpoint immigrates to this network segment from other network segment.

[0045] When there exist simultaneously the configuration Null0 route entry and the immigration host route entry, the immigration host route entry will be found first, and the configuration Null0 route entry will not be found.

[0046] At block 205, the xTR determines whether the source IP address of the packet and the IP address of the interface receiving the packet belong to the same network segment, when the source IP address of the packet and the IP address of the interface receiving the packet belong to the same network segment, block 206 is performed; otherwise, block 208 is performed.

[0047] At block 206, the xTR determines whether an extend-subnet-mode command is configured on the interface receiving the packet, when the extend-subnet-mode command is configured on the interface receiving the packet, block 207 is performed; otherwise, block 208 is performed.

[0048] At block 207, the xTR reports the endpoint immigration event, and generates an immigration host route entry corresponding to the source IP address of the packet, of which the egress interface is the interface receiving the packet. According to the immigration host route entry, the endpoint immigration event will not be reported again when a sequent packet matches the immigration host route entry.

[0049] In the example, when the xTR reports the endpoint immigration event to a CPU of the xTR, and the CPU performs the relevant processing, the xTR may send a map-register packet for the endpoint to a map-server.

[0050] When a condition for sending a multicast map-notify packet is satisfied, the xTR may also send a multicast map-notify packet to other xTRs in the same multicast group. When receiving the multicast map-notify packet, the xTRs in the same multicast group may send a valid forwarding route entry to the forwarding layer of the router, and the xTRs in a different multicast group may send an invalid forwarding route entry to the forwarding layer of the router.

[0051] When receiving the map-register packet sent for the endpoint by the xTR, the map-server may determine whether information that the endpoint has been registered on an xTR in another data center is recorded in the map-server, when the information is recorded in the map-server, the map-server may send a map-notify packet to the xTR in the another data center, and update the register information of the endpoint.

[0052] When receiving a map-notify packet sent by the map-server or a multicast map-notify packet sent by that xTR, the xTR in the another data center may determine whether there exists a immigration host route entry, namely a host route entry of which the egress interface is not null, when there exists the immigration host route entry, delete the immigration host route entry; and determine whether there exists a configuration Null0 route entry, when there exists the configuration Null0 route entry, ignores the map-notify packet; when there does not

exist the configuration Null0 route entry, corresponding to the IP address of the endpoint, generate a host route entry, of which the egress interface is null, namely an emigration Null0 route entry.

[0053] At block 208, the xTR does not report the endpoint immigration event.

[0054] In can be seen from above examples, a dynamic-EID strategy may be configured to specify an immigration network segment, so that an endpoint of which the IP address is within the immigration network segment may immigrate. In addition, the dynamic-EID strategy may be enabled on an interface, on which an endpoint immigration event should be detected, so that endpoint immigration detection may be performed on the interface, namely the endpoint immigration detection may be performed in a limited range. By performing the endpoint immigration detection on a software level, the router may be not limited by the hardware.

[0055] The process of detecting an endpoint migration in one network segment and cross different network segments will be respectively described in detail hereinafter by taking a virtual machine as example.

[0056] FIG. 3 is a schematic diagram illustrating a LISP network in which a virtual machine migrates from one network segment to another network segment according to examples of the present disclosure.

[0057] In FIG.3, xTR1 in data center (DC) 1 and xTR2 in data center (DC) 2 are respectively configured with a dynamic-EID strategy in which an immigration network segment 10.17.1.0/24 is specified. The dynamic-EID strategy is respectively enabled on the interface 1 of xTR1 and the interface 2 of xTR2. The address of the interface 1 is 10.17.1.5/24, and the address of the interface 2 is 10.17.2.9/24. Because there is not a direct route corresponding to the network segment 10.17.1.0/24 on xTR2, xTR2 generates a network segment route entry of which the egress interface is null, namely a configuration Null0 route entry.

[0058] At first, the procedure that virtual machine (VM) B goes online in DC1 will be described hereinafter.

[0059] VM B (of which the IP address is 10.17.1.65/32) goes online in DC1, and sends a gratuitous ARP packet.

[0060] XTR1 receives the gratuitous ARP packet sent by VM B through the interface 1, and determines that the source IP address of the gratuitous ARP packet matches the immigration network segment specified by the dynamic-EID strategy enabled on the interface 1, and searches for a migration route entry utilizing the source IP address of the gratuitous ARP packet. xTR1 does not find a migration route entry, namely not find an immigration host route entry (the host route entry corresponding to the IP address 10.17.1.65/32), or a configuration Null0 route entry (the network segment route entry of which the egress interface is null). XTR1 further determines that the IP address of the interface 1 and the source IP address of the gratuitous ARP packet belong to the same network segment, and no extend-subnet-mode command is configured on the interface 1, xTR1 does not report a VM B immigration event, namely VM B is not deemed as a VM immigrating to DC1.

[0061] Secondly, the procedure that VM B migrates from DC1 to DC2, and sends an IP data packet to xTR2 in DC2 will be described hereinafter.

[0062] XTR2 receives an IP data packet sent by VM B through the interface 2, and determines that the source IP address of the IP data packet matches the immigration network segment specified by the dynamic-EID strategy enabled on the interface 2, searches for a migration route entry utilizing the source IP address of the IP data packet, and finds a configuration Null0 route entry, namely, utilizing the source IP address 10.17.1.65/32, finds a network segment route entry, of which the egress interface is null, corresponding to the network segment 10.17.1.0/24. XTR2 reports a VM B immigration event, and corresponding to the source IP address 10.17.1.65/32 of VM B, generates a host route entry of which the egress interface is the interface 2 receiving the IP data packet, namely an immigration host route entry.

[0063] Subsequently, when receiving a packet sent by the VM B again, and finding the immigration host route entry corresponding to the source IP address 10.17.1.65/32 of the packet, xTR2 will not report the VM B immigration event.

[0064] When xTR2 reports the VM B immigration event to a CPU of the xTR2, and the CPU performs the relevant processing, xTR2 sends a map-register packet for VM B to a map-server.

[0065] When receiving the map-register packet sent for VM B by xTR2, and determining that VM B has been registered on xTR1, the map-server may send a map-notify packet to the xTR1 in DC1, and update the register information of VM B.

[0066] When receiving the map-notify packet sent by the map-server, xTR1 in DC1 determines that there is not an immigration host route entry corresponding to the IP address 10.17.1.65/32, and generates an emigration Null0 route entry corresponding to the IP address, namely a host route entry corresponding to the IP address, of which the egress interface is null,to indicate that the address 10.17.1.65/32 is an IP address of a VM which emigrates from DC1.

[0067] So far, the process that VM B migrates from DC1 to DC2 is terminated.

[0068] When VM B migrates from DC2 to DC1, and sends a data packet to xTR1 in DC1, after receiving the data packet sent by VM B, xTR1 will find the emigration Null0 route entry according to the source IP address 10.17.1.65/32, and will report a VM B immigration event.

[0069] FIG.4 is a schematic diagram illustrating a LISP network in which a virtual machine migrates in the same network segment according to examples of the present disclosure.

[0070] In FIG.4, xTR1 in DC 1 and xTR2 in DC 2 are respectively configured with a dynamic-EID strategy in which an immigration network segment 10.17.1.0/24 is specified. The dynamic-EID strategy is respectively enabled on the interface 1 of xTR1 and the interface 2 of xTR2. The address of the interface 1 is 10.17.1.5/24, and the address of the interface 2 is 10.17.1.9/24. Because the virtual machine immigration is performed in the same network segment, it is necessary to configure an extend-subnet-mode command on both the interface 1 and the interface 2. In the LISP network shown in FIG.4, xTRs in different DCs may communicated with each other via a configured layer-2.

[0071] At first, the procedure that VM B goes online in DC1 will be described hereinafter.

[0072] VM B goes online in DC1, and sends a gratuitous ARP packet to xTR1

[0073] XTR1 receives the gratuitous ARP packet sent by VM B through the interface 1, and does not find a route entry of which the egress interface is null. xTR1 determines that the IP address of the interface 1 and the source IP address of the gratuitous ARP packet belong to the same network segment, and an extend-subnet-mode command is configured on the interface 1, xTR1 reports a VM B immigration event.

[0074] After detecting the immigration of VM B, xTR1 generates an immigration host route entry, namely a host route entry, corresponding to the IP address 10.17.1.65/32, of which the egress interface is the interface 1, and sends a multicast map-notify packet to a multicast group configured on the interface 1.

[0075] XTR1 simultaneously sends a map-register packet to a map-server to register VM B, after receiving the map-register packet sent by xTR1, the map-server records register information of VM B registered on xTR1.

[0076] When receiving the multicast map-notify packet sent by xTR1, xTR2 determines whether there is a host route entry corresponding to the IP address 10.17.1.65/32, when there is not the host route entry corresponding to the IP address 10.17.1.65/32, generates an emigration Null0 route entry, namely a host route entry corresponding to the IP address, of which the egress interface is null; when there is the host route entry corresponding to the IP address 10.17.1.65/32 and the egress interface of the host route entry is null, remain unchanged; when there is the host route entry corresponding to the IP address 10.17.1.65/32 and the egress interface is not null, namely there is an immigration host route entry, deletes the immigration host route entry, and generates an emigration Null0 route entry.

[0077] Secondly, the procedure that VM B migrates from DC1 to DC2 will be described hereinafter.

[0078] VM B sends a data packet to xTR2 in DC2.

[0079] XTR2 receives the data packet sent by VM B, and finds an emigration Null0 route entry corresponding to the source IP address 10.17.1.65/32 of the data packet, namely a host route entry corresponding to the source IP address 10.17.1.65/32, and the egress interface of the host route entry is null, xTR2 reports a VM B immigration event.

[0080] After detecting the immigration of VM B, xTR2 generates an immigration host route entry, namely a host route entry, corresponding to the IP address 10.17.1.65/32, of which the egress interface is the interface 2, and sends a multicast map-notify packet to a multicast group configured on the interface 2; sends a map-register packet to the map-server to register VM B. After updating the register information of VM B, the map-server sends a map-notify packet to xTR1.

[0081] When receiving the multicast map-notify packet sent by xTR2 or the map-notify packet sent by the map-server, xTR1 determines that there is a host route entry corresponding to the IP address 10.17.1.65/32 and the egress interface of the host route entry is the interface 1, namely an immigration host route entry corresponding to the IP address 10.17.1.65/32, xTR1 deletes the immigration host route entry, and generates an emigration Null0 route entry corresponding to the IP address 10.17.1.65/32.

[0082] So far, the process that VM B migrates from DC1 to DC2 is terminated.

[0083] When VM B migrates from DC2 to DC1, the process is similar to above description, and no further descriptions will be provided here.

[0084] Examples in the present disclosure also provide a device for detecting immigration of an endpoint, which may be applied to an xTR in the LISP network. FIG.5 is a schematic diagram illustrating a device for detecting immigration of an endpoint according an example of the present disclosure. As shown in FIG.5, the device may include a configuring and storing unit 501, a receiving unit 502, a matching unit 503 and a processing unit 504.

[0085] The configuring and storing unit 501 is adapted to configure a dynamic-EID strategy to specify an immigration network segment; and generate a configuration Null0 route entry corresponding to the immigration network segment, when determining to perform cross-network segment endpoint immigration detection according to the immigration network segment.

[0086] The receiving unit 502 is adapted to receive a packet sent by an endpoint.

[0087] The matching unit 503 is adapted to, when the receiving unit 502 receives the packet sent by the endpoint, search for a migration route entry from the configuring and storing unit 501 utilizing a source IP address of the packet.

[0088] The processing unit 504 is adapted to, when the matching unit503 finds a route entry of which the egress interface is null, report an endpoint immigration event. The route entry of which the egress interface is null may be a configuration Null0 route entry or an emigration Null0 route entry. When the route entry of which the egress interface is null is the emigration Null0 route entry, it may indicate a scenario that an endpoint emigrated from this network segment re-immigrates to this network segment. When the route entry of which the egress interface is null is the configuration Null0 route entry, it may indicate a scenario that an endpoint immigrates to this network segment from other network segment for the first time, namely a cross-network segment immigration scenario.

[0089] In an example, the processing unit 504 is further adapted to, when the matching unit 503 finds an immigration host route entry, namely a host route entry of which the egress interface is not null, not report the endpoint immigration event.

[0090] In an example, the configuring and storing unit 501 is further adapted to configure an extend-subnet-mode command on an interface on which an endpoint immigration event should be detected when determining to perform same-network segment endpoint immigration detection according to the immigration network segment specified by the dynamic-EID strategy.

[0091] The processing unit 504 is further adapted to, when the matching unit 503 does not find a migration route entry, namely a route entry of which the egress interface is null or an immigration host route entry, determine whether a source IP address of the packet and the IP address of the interface receiving the packet belong to the same network segment, when the source IP address of the packet and the IP address of the interface receiving the packet belong to the same network segment, determine whether an extend-subnet-mode command is configured on the interface receiving the packet, when the extend-subnet-mode command is configured on the interface receiving the packet, report the endpoint immigration event; when the source IP address of the packet and the IP address of the interface receiving the packet do

not belong to the same network segment, or when the extend-subnet-mode command is not configured on the interface receiving the packet, not report the endpoint immigration event.

[0092] In an example, the receiving unit 502 is further adapted to receive a map-notify packet. The map-notify packet may be sent by a map-server or an xTR in another data center for indicating that the endpoint immigrates to that data center.

[0093] The configuring and storing unit 501 is further adapted to, when the receiving unit receives the map-notify packet, determine whether there is an immigration host route entry corresponding to the endpoint, when there is the immigration host route entry, delete the immigration host route entry, and determine whether there is a configuration Null0 route entry, when there is the configuration Null0 route entry, ignore the packet; when there is not the configuration Null0 route entry, generate an emigration Null0 route entry corresponding to the IP address of the endpoint; when the processing unit 504 reports the endpoint immigration event, generate an immigration host route entry corresponding to the IP address of the endpoint, and the egress interface of the immigration host route entry is the interface receiving the packet.

[0094] In an example, the configuring and storing unit 501 is further adapted to enable the dynamic-EID strategy on an interface, on which an endpoint immigration event should be detected.

[0095] The processing unit 504 is further adapted to, when the receiving unit 502 receives the packet sent by the endpoint, and when determining that the dynamic-EID strategy is enabled on the interface receiving the packet, and the source IP address of the packet matches the immigration network segment specified by the enabled dynamic-EID strategy, instruct the matching unit 503 to search for a migration route entry utilizing the source IP address of the packet; when determining that the dynamic-EID strategy is not enabled on the interface receiving the packet, or the source IP address of the packet does not match the immigration network segment specified by the enabled dynamic-EID strategy, not report the endpoint immigration event.

[0096] The units in the device in above examples disclosed herein may be distributed in the device of the examples according to the descriptions of the examples, and may also be varied

to be located in one or more devices different from that of the examples. The units of the above examples may be integrated into one unit or may be further divided into multiple sub-units.

[0097] FIG. 6 is a schematic diagram illustrating a device for detecting immigration of an endpoint according another example of the present disclosure. As shown in FIG.6, the device may include a non-transitory storage medium 610, a processor 620 in communication with the non-transitory storage medium 610 and an interface 630.

[0098] The non-transitory storage medium 610 may be configured to store a group of instructions for detecting immigration of an endpoint which may be executed by the processor 620 to implement the operations of any one of the methods shown in FIG.1 to FIG.4, or the operations of the units in the device shown in FIG.5.

[0099] As can be seen, in examples of the present disclosure, when receiving a packet sent by an endpoint, an xTR may, according to a source IP address of the packet and an IP address of an interface receiving the packet, determine whether an endpoint immigration event should be reported. Thus, the endpoint immigration may be detected without depending on the hardware. In addition, by configuring a dynamic-EID strategy, the immigration detection of an endpoint within a specific network segment may be achieved according to requirements.

[00100] The foregoing description, for purpose of explanation, has been described with reference to specific examples. However, the illustrative discussions above are not intended to be exhaustive or to limit the present disclosure to the precise forms disclosed. Many modifications and variations are possible in view of the above teachings. The examples were chosen and described in order to best explain the principles of the present disclosure and its practical applications, to thereby enable others skilled in the art to best utilize the present disclosure and various examples with various modifications as are suited to the particular use contemplated.

[00101] The above examples may be implemented by hardware, software, firmware, or a combination thereof. For example the various methods, processes and functional modules described herein may be implemented by a processor (the term processor is to be interpreted broadly to include a CPU, processing unit/module, ASIC, logic module, or programmable

gate array, etc.). The processes, methods and functional modules may all be performed by a single processor or split between several processors; reference in this disclosure or the claims to a 'processor' should thus be interpreted to mean 'one or more processors'. The processes, methods and functional modules are implemented as machine readable instructions executable by one or more processors, hardware logic circuitry of the one or more processors or a combination thereof. The modules, if mentioned in the aforesaid examples, may be combined into one module or further divided into a plurality of sub-modules. Further, the examples disclosed herein may be implemented in the form of a software product. The computer software product is stored in a non-transitory storage medium and comprises a plurality of instructions for making an electronic device implement the method recited in the examples of the present disclosure.

CLAIMS

WHAT IS CLAIMED IS:

1. A method for detecting immigration of an endpoint, comprising:

configuring, by an xTR in a Locator/Identity Separation Protocol (LISP) network, a dynamic-Endpoint Identifier (EID) strategy to specify an immigration network segment; and generating a configuration Null0 route entry corresponding to the immigration network segment when determining to perform cross-network segment endpoint immigration detection;

receiving a packet sent by an endpoint, and searching for a route entry utilizing a source Internet Protocol (IP) address of the packet; and

reporting an endpoint immigration event when finding the configuration Null0 route entry.

2. The method according to claim 1, after reporting the endpoint immigration event, further comprising:

generating an immigration host route entry corresponding to the source IP address of the packet, and the egress interface is an interface receiving the packet.

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

not reporting the endpoint immigration event when finding the immigration host route entry.

4. The method according to claim 2, further comprising:

determining whether the source IP address of the packet and an IP address of the interface receiving the packet belong to a same network segment, when not finding the configuration Null0 route entry or the immigration host route entry; and

determining whether an extend-subnet-mode command is configured on the interface receiving the packet when determining that the source IP address of the packet and the IP address of the interface receiving the packet belong to the same network segment; and when the extend-subnet-mode command is configured on the interface receiving the packet, reporting the endpoint immigration event;

when determining that the source IP address of the packet and the IP address of the interface receiving the packet do not belong to the same network segment, or when the extend-subnet-mode command is not configured on the interface receiving the packet, not reporting the endpoint immigration event.

5. The method according to claim 2, further comprising:

receiving a map-notify packet indicating that the endpoint emigrates to another data center sent by a map-server or an xTR in the another data center, determining whether there is an immigration host route entry corresponding to the endpoint, when there is the immigration host route entry corresponding to the endpoint, deleting the an immigration host route entry corresponding to the endpoint, and determining whether there is a configuration Null0 route entry, when there is the configuration Null0 route entry, ignoring the packet; when there is not the configuration Null0 route entry, generating an emigration Null0 route entry corresponding to the IP address of the endpoint.

6. The method according to claim 5, further comprising:

reporting the endpoint immigration event when finding the emigration route entry corresponding to the endpoint.

7. The method according to claim 1, after receiving the packet sent by an endpoint, and before searching for the route entry, further comprising:

determining whether the dynamic-EID strategy is enabled on the interface receiving the packet and whether the source IP address of the packet matches the immigration network segment specified by the enabled dynamic-EID strategy; and

searching for the route entry utilizing the source IP address of the packet, when determining that the dynamic-EID strategy is enabled on the interface receiving the packet and the source IP address of the packet matches the immigration network segment specified by the enabled dynamic-EID strategy.

8. A device for detecting immigration of an endpoint, applied to an xTR in a Locator/Identity Separation Protocol (LISP) network, comprising: a processor and a non-transitory storage medium in communication with the processor;

the non-transitory storage medium stores a group of instructions which may be executed by the processor to:

configure a dynamic- Endpoint Identifier (EID) strategy to specify an immigration network segment; and generate a configuration Null0 route entry corresponding to the immigration network segment, when determining to perform cross-network segment endpoint immigration detection according to the immigration network segment;

receive a packet sent by an endpoint;

search for a migration route entry utilizing a source Internet Protocol (IP) address of the packet;

when finding the configuration Null0 route entry, report an endpoint immigration event.

9. The device according to claim 8, wherein, the processor is further to:

when reporting the endpoint immigration event, generate an immigration host route entry corresponding to the IP address of the endpoint, and the egress interface of the immigration host route entry is the interface receiving the packet.

10. The device according to claim 9, wherein, the processor is further to:

when finding an immigration host route entry, not report the endpoint immigration event.

11. The device according to claim 8, wherein, the processor is further to:

configure an extend-subnet-mode command on an interface on which an endpoint immigration event should be detected when determining to perform same-network segment endpoint immigration detection according to the immigration network segment specified by the dynamic-EID strategy; and

when not finding the configuration Null0 route entry or the immigration host route entry, determine whether a source IP address of the packet and the IP address of the interface receiving the packet belong to the same network segment,

when the source IP address of the packet and the IP address of the interface receiving the packet belong to the same network segment, determine whether an extend-subnet-mode command is configured on the interface receiving the packet, when the extend-subnet-mode command is configured on the interface receiving the packet, report the endpoint immigration event; when the source IP address of the packet and the IP address of the interface receiving the packet do not belong to the same network segment, or when the extend-subnet-mode command is not configured on the interface receiving the packet, not report the endpoint immigration event.

12. The device according to any one of claims 8 to 11, wherein, the processor is further to:

receive a map-notify packet; and

determine whether there is an immigration host route entry corresponding to the endpoint, when there is the immigration host route entry, delete the immigration host route entry, and determine whether there is a configuration Null0 route entry, when there is the configuration Null0 route entry, ignore the packet; when there is not the configuration Null0 route entry, generate an emigration Null0 route entry corresponding to the IP address of the endpoint.

13. The device according to claim 12, wherein, the processor is further to:

when finding an emigration Null0 route entry, report the endpoint immigration event.

14. The device according to any one of claims 8 to 11, wherein, the processor is further to:

enable the dynamic-EID strategy on an interface, on which an endpoint immigration event should be detected;

when receiving the packet sent by the endpoint, and when determining that the dynamic-EID strategy is enabled on the interface receiving the packet, and the source IP address of the packet matches the immigration network segment specified by the enabled dynamic-EID strategy, search for a migration route entry utilizing the source IP address of the packet; when determining that the dynamic-EID strategy is not enabled on the interface receiving the packet, or

the source IP address of the packet does not match the immigration network segment specified by the enabled dynamic-EID strategy, not report the endpoint immigration event.

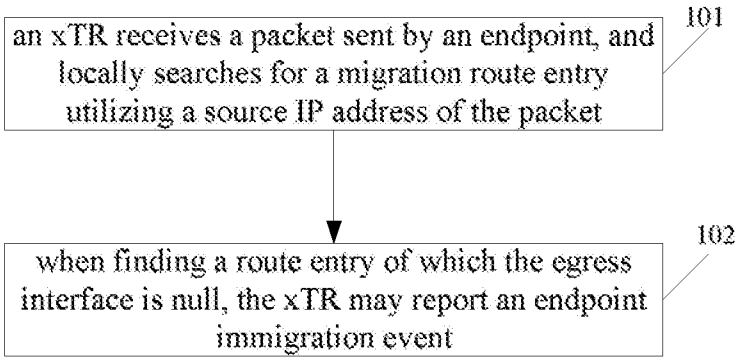
an xTR receives a packet sent by an endpoint, and locally searches for a migration route entry utilizing a source IP address of the packet
101
when finding a route entry of which the egress interface is null, the xTR may report an endpoint immigration event
102

FIG. 1

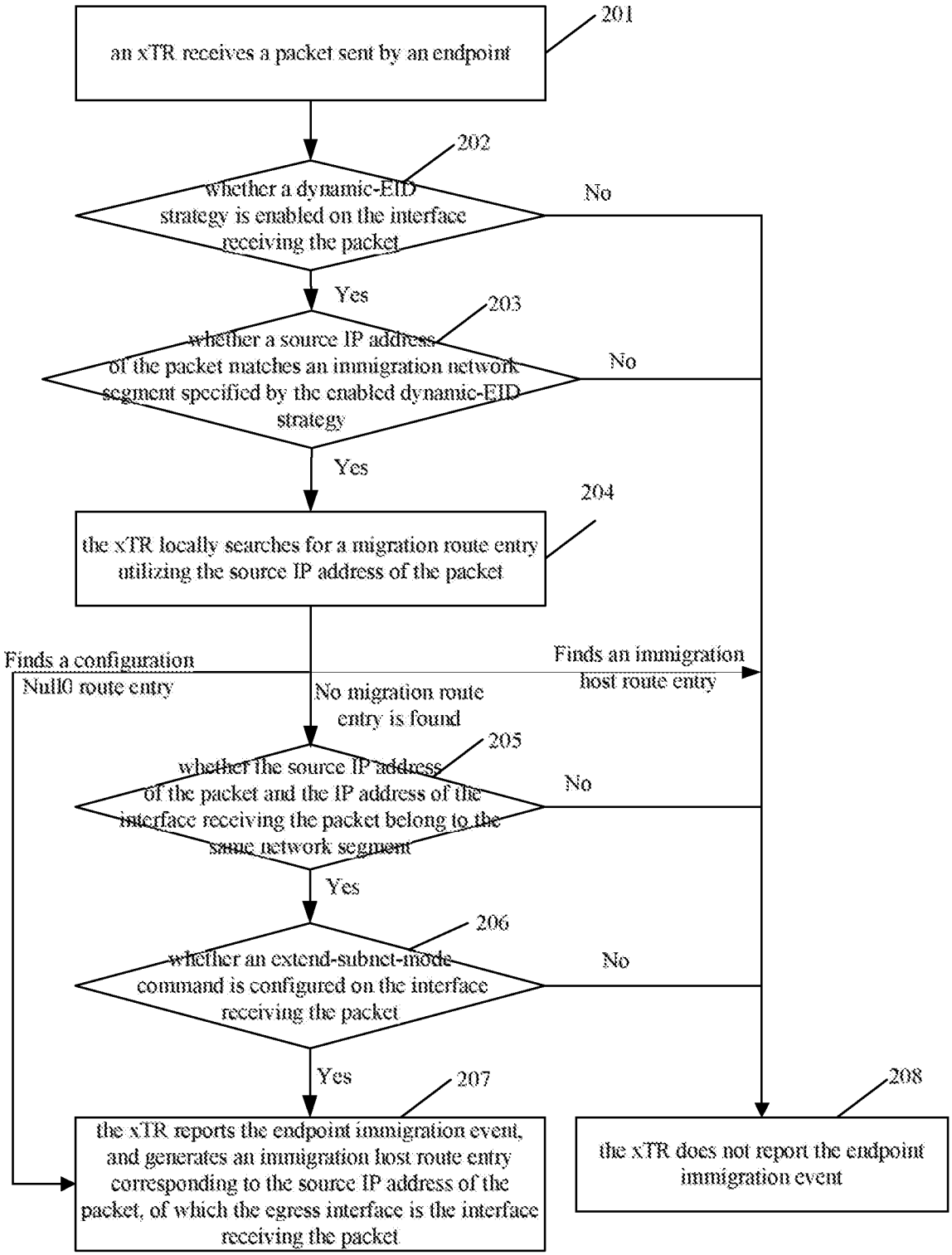
an xTR receives a packet sent by an endpoint
201
whether a dynamic-EID strategy is enabled on the interface receiving the packet
202
No
Yes
whether a source IP address of the packet matches an immigration network segment specified by the enabled dynamic-EID strategy
203
No
Yes
the xTR locally searches for a migration route entry utilizing the source IP address of the packet
204
Finds a configuration Null0 route entry
Finds an immigration host route entry
No migration route entry is found
whether the source IP address of the packet and the IP address of the interface receiving the packet belong to the same network segment
205
No
Yes
whether an extend-subnet-mode command is configured on the interface receiving the packet
206
No
Yes
the xTR reports the endpoint immigration event, and generates an immigration host route entry corresponding to the source IP address of the packet, of which the egress interface is the interface receiving the packet
207
the xTR does not report the endpoint immigration event
208

FIG. 2

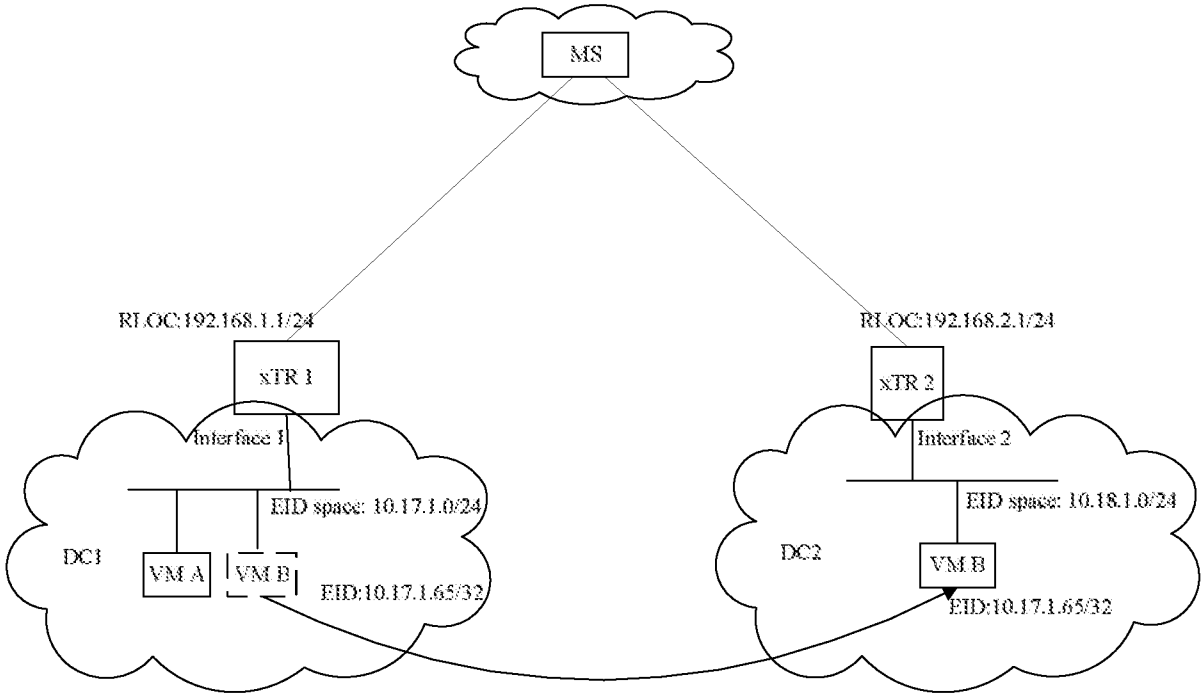
MS
RLOC:192.168.1.1/24
xTR 1
Interface 1
EID space: 10.17.1.0/24
DC1
VM A
VM B
EID:10.17.1.65/32
RLOC:192.168.2.1/24
xTR 2
Interface 2
EID space: 10.18.1.0/24
DC2
VM B
EID:10.17.1.65/32

FIG. 3

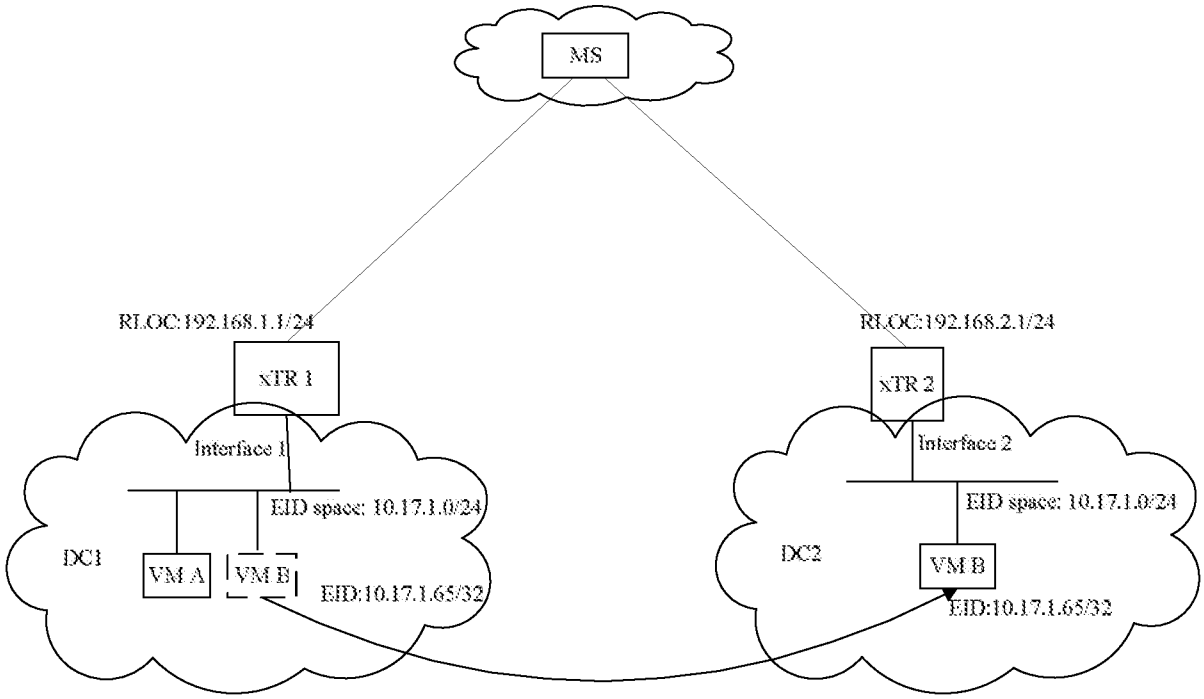
MS
RLOC:192.168.1.1/24
xTR 1
Interface 1
EID space: 10.17.1.0/24
DC1
VM A
VM B
EID:10.17.1.65/32
RLOC:192.168.2.1/24
xTR 2
Interface 2
EID space: 10.17.1.0/24
DC2
VM B
EID:10.17.1.65/32

FIG. 4

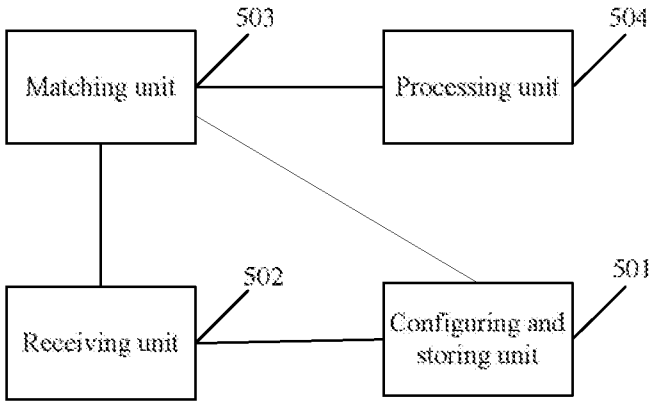
503
504
Matching unit
Processing unit
502
501
Receiving unit
Configuring and storing unit

FIG. 5

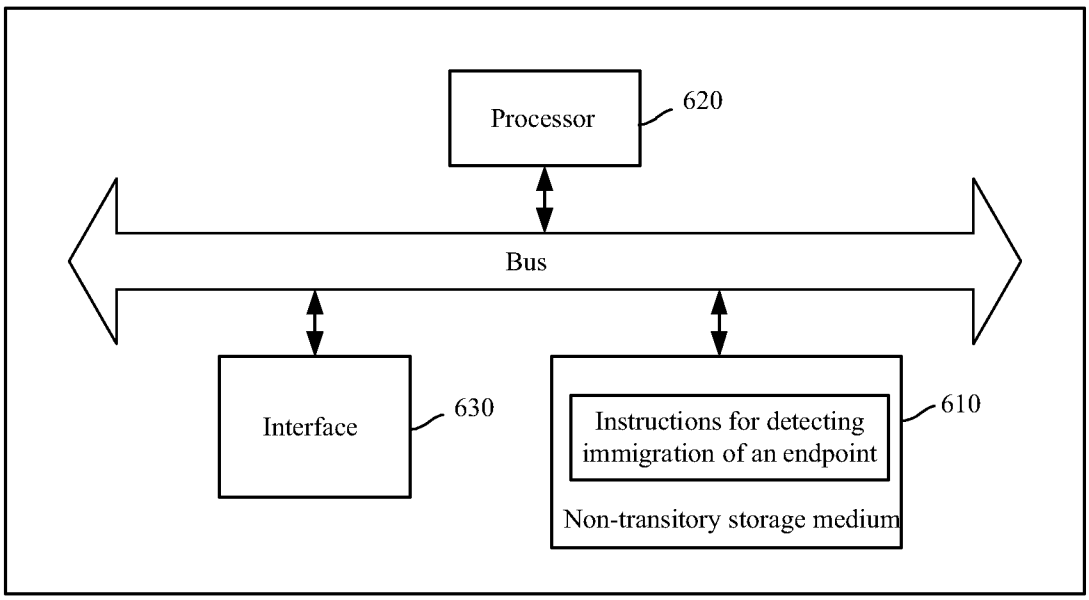
Processor
620
Bus
Interface
630
Instructions for detecting immigration of an endpoint
610
Non-transitory storage medium

FIG. 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/081832

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/741(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)

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)

CNKI,CNPAT,WPI,EPODOC:migrat+, immigrat+, emmigrat+, mov+, switch, detect+, sens+, monitor+, route, entry, IP, LISP, virtual machine, VM, network, segment, assign, specify, TR, tunnel router, interface, null, null0

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 103095722 A (HUAWEI TECHNOLOGIES CO., LTD.) 08 May 2013 (2013-05-08) description, paragraphs [0039]-[0064], [0089]-[0090], and figures 2, 3, 8	1-14
A	CN 102447618 A (HANGZHOU H3C TECHNOLOGIES CO., LTD.) 09 May 2012 (2012-05-09) the whole document	1-14
A	CN 104113459 A (HANGZHOU H3C TECHNOLOGIES CO., LTD.) 22 October 2014 (2014-10-22) the whole document	1-14
A	WO 2008103936 A1 (CHAO TIENWEI ET AL.) 28 August 2008 (2008-08-28) the whole document	1-14
A	US 2010115080 A1 (KAGEYAMA SOSHI ET AL.) 06 May 2010 (2010-05-06) the whole document	1-14

☐ 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	Date of mailing of the international search report
14 July 2016	**26 July 2016**
Name and mailing address of the ISA/CN **STATE INTELLECTUAL PROPERTY OFFICE OF THE P.R.CHINA** **6, Xitucheng Rd., Jimen Bridge, Haidian District, Beijing 100088, China** Facsimile No. **(86-10)62019451**	Authorized officer **DONG,Zhenxing** Telephone No. **(86-10)62413389**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/081832

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 103095722 A	08 May 2013	None	
CN 102447618 A	09 May 2012	None	
CN 104113459 A	22 October 2014	EP 2987282 A1	24 February 2016
		WO 2014169782 A1	23 October 2014
		US 2016028624 A1	28 January 2016
WO 2008103936 A1	28 August 2008	US 2008205377 A1	28 August 2008
US 2010115080 A1	06 May 2010	JP 2010114665 A	20 May 2010