



**(19) 대한민국특허청(KR)**  
**(12) 공개특허공보(A)**

(11) 공개번호 10-2022-0098152  
(43) 공개일자 2022년07월11일

- |  |   |
|--|---|
| <p>(51) 국제특허분류(Int. Cl.)<br/>H04L 45/17 (2022.01) H04L 12/46 (2006.01)<br/>H04L 45/00 (2022.01) H04L 45/121 (2022.01)<br/>H04L 45/16 (2022.01)</p> <p>(52) CPC특허분류<br/>H04L 45/17 (2022.05)<br/>H04L 12/4641 (2022.05)</p> <p>(21) 출원번호 10-2022-7017354</p> <p>(22) 출원일자(국제) 2022년09월23일<br/>심사청구일자 2022년06월10일</p> <p>(85) 번역문제출일자 2022년05월23일</p> <p>(86) 국제출원번호 PCT/CN2020/117139</p> <p>(87) 국제공개번호 WO 2021/077971<br/>국제공개일자 2021년04월29일</p> <p>(30) 우선권주장<br/>201911008408.2 2019년10월22일 중국(CN)<br/>(뒷면에 계속)</p> | <p>(71) 출원인<br/>후아웨이 테크놀로지 컴퍼니 리미티드<br/>중국 518129 광둥성 셴젠 롱강 디스트릭트 반티안 후아웨이 어드미니스트레이션 빌딩</p> <p>(72) 발명자<br/>등 자자<br/>중국 518129 광둥 셴젠 롱강 디스트릭트 반티안 후아웨이 어드미니스트레이션 빌딩</p> <p>후 즈보<br/>중국 518129 광둥 셴젠 롱강 디스트릭트 반티안 후아웨이 어드미니스트레이션 빌딩</p> <p>(74) 대리인<br/>유미특허법인</p> |
|--|---|

전체 청구항 수 : 총 26 항

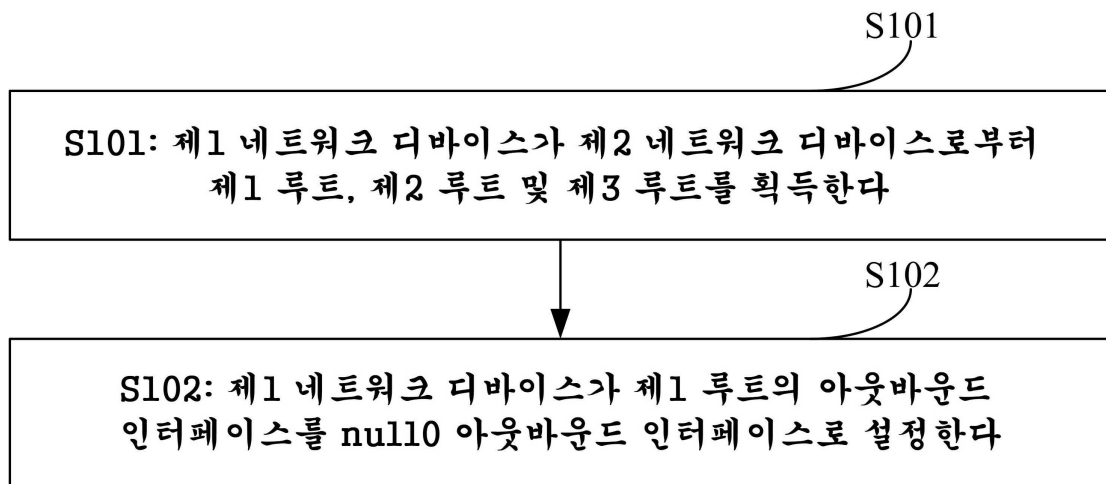
(54) 발명의 명칭 **통신 방법 및 장치**

**(57) 요약**

본 출원의 실시예는 통신 방법을 개시하며, 이 방법은: 제1 네트워크 디바이스가 제2 네트워크 디바이스로부터 제1 루트, 제2 루트 및 제3 루트를 획득하는 것을 포함한다. 제3 루트는 세그먼트 라우팅 인터넷 프로토콜 버전 6의 세그먼트 식별자(SRv6 SID)에 대응하는 네트워크 세그먼트 루트를 포함하고, 제3 루트에 대응하는 네트워크

(뒷면에 계속)

**대표도** - 도2



세그먼트는 제1 루트에 대응하는 네트워크 세그먼트의 서브넷 세그먼트이며, 제3 루트에 대응하는 네트워크 세그먼트는 제2 루트에 대응하는 네트워크 세그먼트의 서브넷 세그먼트이고, 제1 루트에 대응하는 네트워크 세그먼트는 제2 루트에 대응하는 네트워크 세그먼트의 서브넷 세그먼트이다. 제1 네트워크 디바이스는 제1 루트의 아웃바운드 인터페이스를 null0 아웃바운드 인터페이스로 설정한다. 대안으로, 제1 네트워크 디바이스는 제2 네트워크 디바이스로부터 제3 루트를 획득한다. 제3 루트는 SRv6 SID에 대응하는 네트워크 세그먼트 루트를 포함한다. 제3 루트에 도달할 수 없다고 결정하면, 제1 네트워크 디바이스는 제3 루트의 아웃바운드 인터페이스를 null0 아웃바운드 인터페이스로 설정한다. 제1 네트워크 디바이스는 미리 설정된 시간을 대기한 후 제3 루트를 삭제한다. 이 방법에 의해, 패킷 포워딩의 패킷 손실률이 낮아질 수 있다.

(52) CPC특허분류

*H04L 45/04* (2022.05)  
*H04L 45/121* (2022.05)  
*H04L 45/16* (2022.05)

(30) 우선권주장

201911046892.8 2019년10월30일 중국(CN)  
 201911137412.9 2019년11월19일 중국(CN)

## 명세서

### 청구범위

#### 청구항 1

통신 방법으로서,

제1 네트워크 디바이스에 의해, 제2 네트워크 디바이스로부터 제1 루트(route), 제2 루트 및 제3 루트를 획득하는 단계 - 상기 제3 루트는 세그먼트 라우팅 인터넷 프로토콜 버전 6(segment routing Internet protocol version 6)의 세그먼트 식별자(SRv6 SID)에 대응하는 네트워크 세그먼트 루트를 포함하고, 상기 제3 루트에 대응하는 네트워크 세그먼트는 상기 제1 루트에 대응하는 네트워크 세그먼트의 서브넷(subnet) 세그먼트이며, 상기 제3 루트에 대응하는 네트워크 세그먼트는 상기 제2 루트에 대응하는 네트워크 세그먼트의 서브넷 세그먼트이고, 상기 제1 루트에 대응하는 네트워크 세그먼트는 상기 제2 루트에 대응하는 네트워크 세그먼트의 서브넷 세그먼트임 -; 및

상기 제1 네트워크 디바이스에 의해, 상기 제1 루트의 아웃바운드 인터페이스(outbound interface)를 null0 아웃바운드 인터페이스로 설정하는 단계를 포함하는,

통신 방법.

#### 청구항 2

제1항에 있어서,

상기 제3 루트는 루프백(loopback) 인터페이스 어드레스 루트를 더 포함하는,

통신 방법.

#### 청구항 3

제1항에 있어서,

상기 방법은:

상기 제1 네트워크 디바이스에 의해, 상기 제2 네트워크 디바이스로부터 제1 식별자를 수신하는 단계를 더 포함하고; 그리고

상기 제1 네트워크 디바이스에 의해, 상기 제1 루트의 아웃바운드 인터페이스를 null0 아웃바운드 인터페이스로 설정하는 단계는:

상기 제1 네트워크 디바이스에 의해, 상기 제1 식별자를 기초로 상기 제1 루트의 아웃바운드 인터페이스를 상기 null0 아웃바운드 인터페이스로 설정하는 단계를 포함하는,

통신 방법.

#### 청구항 4

제1항에 있어서,

상기 제1 네트워크 디바이스와 상기 제2 네트워크 디바이스 모두에 가상 사설 네트워크(VPN: virtual private network) 인스턴스가 구성되고,

상기 제1 네트워크 디바이스와 상기 제2 네트워크 디바이스 간에 경계 게이트웨이 프로토콜(BGP: border gateway protocol) 피어(peer) 관계가 미리 설정되며,

상기 제1 네트워크 디바이스와 상기 제2 네트워크 디바이스 모두 상기 세그먼트 라우팅 인터넷 프로토콜 버전 6(SRv6)을 지원하는,

통신 방법.

**청구항 5**

제1항에 있어서,

상기 제1 네트워크 디바이스 및 상기 제2 네트워크 디바이스는 제1 내부 게이트웨이 프로토콜(IGP: interior gateway protocol) 도메인에 위치되고,

제2 IGP 도메인은 상기 제1 IGP 도메인의 네트워크 디바이스를 포함하지 않으며,

상기 제1 루트는 상기 제2 IGP 도메인에 위치된 특정 루트를 포함하지 않는,

통신 방법.

**청구항 6**

제1항에 있어서,

상기 제1 네트워크 디바이스에 의해, 제2 네트워크 디바이스로부터 제1 루트, 제2 루트 및 제3 루트를 획득하는 단계는:

상기 제1 네트워크 디바이스에 의해, 중간 시스템 간(IS-IS: intermediate system-to-intermediate system) 프로토콜 또는 개방형 최단 경로 우선(OSPF: open shortest path first) 프로토콜을 사용함으로써 상기 제2 네트워크 디바이스에 의해 송신되는 상기 제1 루트, 상기 제2 루트 및 상기 제3 루트를 수신하는 단계를 포함하는,

통신 방법.

**청구항 7**

제1항 내지 제6항 중 어느 한 항에 있어서,

상기 방법은:

상기 제1 네트워크 디바이스에 의해, 제3 네트워크 디바이스로부터 제4 루트를 수신하는 단계를 더 포함하며,

액세스 측 디바이스는 상기 제3 네트워크 디바이스와 상기 제2 네트워크 디바이스로 듀얼 호밍(dual-home)되거나, 상기 제4 루트는 고속 재라우트(FRR: fast reroute) 방법을 사용함으로써 결정된, 상기 제3 루트의 백업 루트(backup)인,

통신 방법.

**청구항 8**

통신 방법으로서,

제1 네트워크 디바이스에 의해, 제2 네트워크 디바이스로부터 제3 루트를 획득하는 단계 - 상기 제3 루트는 세그먼트 라우팅 인터넷 프로토콜 버전 6의 세그먼트 식별자(SRv6 SID)에 대응하는 네트워크 세그먼트 루트를 포함함 -;

상기 제3 루트에 도달할 수 없다고 결정하면, 상기 제1 네트워크 디바이스에 의해, 상기 제3 루트의 아웃바운드 인터페이스를 null0 아웃바운드 인터페이스로 설정하는 단계; 및

상기 제1 네트워크 디바이스에 의해, 미리 설정된 시간을 대기한 후 상기 제3 루트를 삭제하는 단계를 포함하는,

통신 방법.

**청구항 9**

제8항에 있어서,

상기 제3 루트는 루프백(loopback) 인터페이스 어드레스 루트를 더 포함하는,

통신 방법.

**청구항 10**

제8항에 있어서,

상기 방법은:

상기 제1 네트워크 디바이스에 의해, 상기 제2 네트워크 디바이스로부터 제2 루트를 획득하는 단계를 더 포함하며,

상기 제3 루트에 대응하는 네트워크 세그먼트는 상기 제2 루트에 대응하는 네트워크 세그먼트의 서브넷 세그먼트인,

통신 방법.

**청구항 11**

제8항 내지 제10항 중 어느 한 항에 있어서,

상기 제1 네트워크 디바이스와 상기 제2 네트워크 디바이스 모두에 가상 사설 네트워크(VPN) 인스턴스가 구성되고,

상기 제1 네트워크 디바이스와 상기 제2 네트워크 디바이스 간에 경계 게이트웨이 프로토콜(BGP) 피어 관계가 미리 설정되며,

상기 제1 네트워크 디바이스와 상기 제2 네트워크 디바이스 모두 상기 세그먼트 라우팅 인터넷 프로토콜 버전 6(SRv6)을 지원하는,

통신 방법.

**청구항 12**

제8항 내지 제11항 중 어느 한 항에 있어서,

상기 방법은:

상기 제1 네트워크 디바이스에 의해, 제3 네트워크 디바이스로부터 제4 루트를 수신하는 단계를 더 포함하며,

액세스 측 디바이스는 상기 제3 네트워크 디바이스와 상기 제2 네트워크 디바이스로 듀얼 호밍되거나, 상기 제4 루트는 고속 재라우트(FRR) 방법을 사용함으로써 결정된, 상기 제3 루트의 백업 루트인,

통신 방법.

**청구항 13**

통신 장치로서,

제2 네트워크 디바이스로부터 제1 루트, 제2 루트 및 제3 루트를 획득하도록 구성된 획득 유닛 - 상기 제3 루트는 세그먼트 라우팅 인터넷 프로토콜 버전 6의 세그먼트 식별자(SRv6 SID)에 대응하는 네트워크 세그먼트 루트를 포함하고, 상기 제3 루트에 대응하는 네트워크 세그먼트는 상기 제1 루트에 대응하는 네트워크 세그먼트의 서브넷 세그먼트이며, 상기 제3 루트에 대응하는 네트워크 세그먼트는 상기 제2 루트에 대응하는 네트워크 세그먼트의 서브넷 세그먼트이고, 상기 제1 루트에 대응하는 네트워크 세그먼트는 상기 제2 루트에 대응하는 네트워크 세그먼트의 서브넷 세그먼트임 -; 및

상기 제1 루트의 아웃바운드 인터페이스를 null0 아웃바운드 인터페이스로 설정하도록 구성된 설정 유닛을 포함하는,

통신 장치.

**청구항 14**

제13항에 있어서,

상기 제3 루트는 루프백(loopback) 인터페이스 어드레스 루트를 더 포함하는,

통신 장치.

**청구항 15**

제13항에 있어서,

상기 장치는:

상기 제2 네트워크 디바이스로부터 제1 식별자를 수신하도록 구성된 제1 수신 유닛을 더 포함하고; 그리고

상기 설정 유닛은 구체적으로:

상기 제1 식별자를 기초로 상기 제1 루트의 아웃바운드 인터페이스를 상기 null0 아웃바운드 인터페이스로 설정하도록 구성되는,

통신 장치.

**청구항 16**

제13항에 있어서,

상기 통신 장치는 제1 네트워크 디바이스에 적용되고; 그리고

상기 제1 네트워크 디바이스와 상기 제2 네트워크 디바이스 모두에 가상 사설 네트워크(VPN) 인스턴스가 구성되고,

상기 제1 네트워크 디바이스와 상기 제2 네트워크 디바이스 간에 경계 게이트웨이 프로토콜(BGP) 피어 관계가 미리 설정되며,

상기 제1 네트워크 디바이스와 상기 제2 네트워크 디바이스 모두 상기 세그먼트 라우팅 인터넷 프로토콜 버전 6(SRv6)을 지원하는,

통신 장치.

**청구항 17**

제13항에 있어서,

상기 통신 장치는 제1 네트워크 디바이스에 적용되며,

상기 제1 네트워크 디바이스 및 상기 제2 네트워크 디바이스는 제1 내부 게이트웨이 프로토콜(IGP) 도메인에 위치되고,

제2 IGP 도메인은 상기 제1 IGP 도메인의 네트워크 디바이스를 포함하지 않으며,

상기 제1 루트는 상기 제2 IGP 도메인에 위치한 특정 루트를 포함하지 않는,

통신 장치.

**청구항 18**

제13항에 있어서,

상기 획득 유닛은 구체적으로:

중간 시스템 간(IS-IS) 프로토콜 또는 개방형 최단 경로 우선(OSPF) 프로토콜을 사용함으로써 상기 제2 네트워크 디바이스에 의해 송신되는 상기 제1 루트, 상기 제2 루트 및 상기 제3 루트를 수신하도록 구성되는,

통신 장치.

**청구항 19**

제13항 내지 제18항 중 어느 한 항에 있어서,

상기 장치는:

제3 네트워크 디바이스로부터 제4 루트를 수신하도록 구성된 제2 수신 유닛을 더 포함하며,  
 액세스 측 디바이스는 상기 제3 네트워크 디바이스와 상기 제2 네트워크 디바이스로 듀얼 호밍되거나, 상기 제4 루트는 고속 재라우트(FRR) 방법을 사용함으로써 결정된, 상기 제3 루트의 백업 루트인,  
 통신 장치.

**청구항 20**

통신 장치로서,  
 제2 네트워크 디바이스로부터 제3 루트를 획득하도록 구성된 제1 획득 유닛 - 상기 제3 루트는 세그먼트 라우팅 인터넷 프로토콜 버전 6의 세그먼트 식별자(SRv6 SID)에 대응하는 네트워크 세그먼트 루트를 포함함 -;  
 상기 제3 루트에 도달할 수 없다고 결정되면, 상기 제3 루트의 아웃바운드 인터페이스를 null0 아웃바운드 인터페이스로 설정하도록 구성된 설정 유닛; 및  
 미리 설정된 시간을 대기한 후 상기 제3 루트를 삭제하도록 구성된 삭제 유닛을 포함하는,  
 통신 장치.

**청구항 21**

제20항에 있어서,  
 상기 제3 루트는 루프백(loopback) 인터페이스 어드레스 루트를 더 포함하는,  
 통신 장치.

**청구항 22**

제20항에 있어서,  
 상기 장치는:  
 상기 제2 네트워크 디바이스로부터 제2 루트를 획득하도록 구성된 제2 획득 유닛을 더 포함하며,  
 상기 제3 루트에 대응하는 네트워크 세그먼트는 상기 제2 루트에 대응하는 네트워크 세그먼트의 서브넷 세그먼트인,  
 통신 장치.

**청구항 23**

제20항 내지 제22항 중 어느 한 항에 있어서,  
 상기 통신 장치는 제1 네트워크 디바이스에 적용되며,  
 상기 제1 네트워크 디바이스와 상기 제2 네트워크 디바이스 모두에 가상 사설 네트워크(VPN) 인스턴스가 구성되고,  
 상기 제1 네트워크 디바이스와 상기 제2 네트워크 디바이스 간에 경계 게이트웨이 프로토콜(BGP) 피어 관계가 미리 설정되며,  
 상기 제1 네트워크 디바이스와 상기 제2 네트워크 디바이스 모두 상기 세그먼트 라우팅 인터넷 프로토콜 버전 6(SRv6)을 지원하는,  
 통신 장치.

**청구항 24**

제20항 내지 제23항 중 어느 한 항에 있어서,  
 상기 장치는:  
 제3 네트워크 디바이스로부터 제4 루트를 수신하도록 구성된 수신 유닛을 더 포함하며,

액세스 측 디바이스는 상기 제3 네트워크 디바이스와 상기 제2 네트워크 디바이스로 듀얼 호밍되거나, 상기 제4 루트는 고속 재라우트(FRR) 장치를 사용함으로써 결정된, 제3 루트의 백업 루트인, 통신 장치.

**청구항 25**

프로세서 및 메모리를 포함하는 통신 디바이스로서,  
 상기 메모리는 프로그램을 저장하도록 구성되고; 그리고  
 상기 프로세서는 상기 메모리의 프로그램을 실행하여, 제1항 내지 제12항 중 어느 한 항에 따른 방법을 수행하도록 구성되는,  
 통신 디바이스.

**청구항 26**

컴퓨터 판독 가능 저장 매체로서,  
 프로그램을 포함하며,  
 컴퓨터 상에서 상기 프로그램이 실행될 때, 상기 컴퓨터는 제1항 내지 제12항 중 어느 한 항에 따른 방법을 수행하는 것이 가능해지는,  
 컴퓨터 판독 가능 저장 매체.

**발명의 설명**

**기술 분야**

[0001] 본 출원은 "ROUTING INFORMATION GENERATION METHOD, DEVICE, AND SYSTEM"이라는 명칭으로 중국 국가지식산권국에 2019년 10월 22일자 출원된 중국 특허출원 제201911008408.2호, "COMMUNICATION METHOD AND APPARATUS"라는 명칭으로 중국 국가지식산권국에 2019년 10월 30일자 출원된 중국 특허출원 제201911046892.8호, 및 "COMMUNICATION METHOD AND APPARATUS"라는 명칭으로 중국 국가지식산권국에 2019년 11월 19일자 출원된 중국 특허출원 제201911137412.9호에 대한 우선권을 주장하며, 이들은 그 전체가 인용에 의해 본 명세서에 포함된다.

[0002] 본 출원은 통신 분야에 관한 것으로, 특히 통신 방법 및 장치에 관한 것이다.

**배경 기술**

[0003] 통신 기술의 발전에 따라, 통신 네트워크는 증가하는 규모를 가지며, 이는 네트워크 디바이스에 저장된 라우팅 정보 베이스(RIB: routing information base)의 데이터 양의 증가로 이어진다. RIB의 데이터 양을 줄이기 위해, 축약 루트(aggreated route)가 나타난다. 복수의 특정 루트가 하나의 축약 루트로 축약되므로, 하나의 축약 루트는 네트워크 디바이스가 아닌 네트워크 세그먼트에 대응할 수 있다. 이는 RIB의 데이터 양을 효과적으로 감소시킨다.

[0004] 그러나 축약 루트가 도입된 후, 일부 시나리오에서는 데이터 패킷 포워딩 프로세스에서 비교적 심각한 패킷 손실이 발생할 수 있다. 따라서 이 문제를 해결하기 위한 솔루션이 시급하다.

**발명의 내용**

[0005] 본 출원의 실시예는 축약 루트의 도입으로 야기되는 비교적 높은 패킷 손실률의 문제를 해결하기 위한 통신 방법을 제공한다.

[0006] 본 출원의 실시예의 제1 양상에 따르면, 통신 방법이 제공되며, 이 방법은: 제1 네트워크 디바이스가 제2 네트워크 디바이스로부터 제1 루트, 제2 루트 및 제3 루트를 획득하는 것을 포함한다. 제3 루트는 세그먼트 라우팅 인터넷 프로토콜 버전 6(segment routing Internet protocol version 6)의 세그먼트 식별자(SRv6 SID)에 대응하는 네트워크 세그먼트 루트를 포함하고, 제3 루트에 대응하는 네트워크 세그먼트는 제1 루트에 대응하는 네트워크 세그먼트의 서브넷(subnet) 세그먼트이며, 제3 루트에 대응하는 네트워크 세그먼트는 제2 루트에 대응하는 네트워크 세그먼트의 서브넷 세그먼트이고, 제1 루트에 대응하는 네트워크 세그먼트는 제2 루트에 대응하는 네



트위크 세그먼트의 서브넷 세그먼트이다. 제1 네트워크 디바이스는 제1 루트의 아웃바운드 인터페이스(outbound interface)를 null0 아웃바운드 인터페이스로 설정한다.

[0007] 이 방법에서, 제3 루트의 마스크(mask) 길이는 제1 루트의 마스크 길이보다 길고, 제1 루트의 마스크 길이는 제2 루트의 마스크 길이보다 길다. 따라서 루트 반복을 수행할 때, 제1 네트워크 디바이스는 최장 마스크 매칭 규칙에 기반한 매칭을 통해 먼저 제3 루트를 획득할 수 있다. 종래 기술에서는, 제3 루트에 도달할 수 없으면, 예를 들어, 제2 네트워크 디바이스가 결함이 있고 제3 루트에 도달할 수 없게 되면, 제3 루트가 삭제된다. 그러나 제2 루트는 제3 루트와 함께 삭제되지 않는다. 따라서 최장 마스크 매칭 규칙에 기반하여, 제1 네트워크 디바이스는 매칭을 통해 제2 루트를 획득한다. 본 출원의 이 실시예에서는, 제1 루트가 도입되고, 제1 루트의 마스크 길이가 제2 루트의 마스크 길이보다 길어, 제3 루트에 도달할 수 없을 때, 제1 네트워크 디바이스가 매칭을 통해 제1 루트를 획득할 수 있다. 제1 루트의 아웃바운드 인터페이스는 null0 아웃바운드 인터페이스이기 때문에, 제1 루트에 대한 루트 반복 후, 제1 네트워크 디바이스는 다음 홉(hop)에 도달할 수 없음을 신속하게 결정할 수 있고, 제1 네트워크 디바이스는 다른 동작, 예를 들어 루트 반복을 위한 백업(backup) 다음 홉으로의 전환을 수행할 수 있어, 패킷이 포워딩될 때, 다른 루트에 의해 지시된 경로를 사용함으로써 패킷이 포워딩될 수 있다. 이것은 패킷 손실률을 낮춘다.

[0008] 가능한 구현에서, 제1 네트워크 디바이스가 루프백 인터페이스 어드레스 루트를 사용함으로써 BGP VPNv4 루트 반복을 수행하고, 루프백 인터페이스 어드레스 루트에 기초하여 아웃바운드 인터페이스 및 다음 홉을 결정하도록 구성된다면, 제3 루트는 로케이터(locator) 루트 외에도 루프백 인터페이스 어드레스 루트를 포함할 수 있다. 이런 식으로, 본 출원의 이 실시예의 솔루션을 이용하면, 제1 네트워크 디바이스가 루프백 인터페이스 어드레스 루트를 사용함으로써 BGP VPNv4 루트 반복을 수행하도록 구성되더라도, 패킷 포워딩 경로의 빠른 전환이 구현되어, 패킷 손실률 효과적으로 낮출 수 있다.

[0009] 가능한 구현에서, 제1 네트워크 디바이스가 구체적으로 제1 루트의 아웃바운드 인터페이스를 null0 아웃바운드 인터페이스로 설정할 때, 예를 들어, 제1 네트워크 디바이스는 제1 식별자에 기초하여 제1 루트의 아웃바운드 인터페이스를 null0 아웃바운드 인터페이스로 설정할 수 있고, 제1 식별자는 제2 네트워크 디바이스에 의해 제1 네트워크 디바이스로 송신될 수 있다. 제1 식별자는 제1 루트와 독립적인 다른 메시지를 사용함으로써 제2 네트워크 디바이스에 의해 제1 네트워크 디바이스로 송신될 수 있거나, 제1 루트에 추가되어 제2 네트워크 디바이스에 의해 제1 네트워크 디바이스로 송신될 수 있다. 이는 본 출원의 이 실시예에서 구체적으로 제한되지 않는다.

[0010] 가능한 구현에서는, SRv6을 통한 L3VPN 시나리오에서, SRv6 LSP가 먼저 설정될 필요가 있고, VPN 인스턴스(instance)를 사용함으로써 사설 네트워크 루트가 학습될 필요가 있다. 따라서 VPN 인스턴스는 제1 네트워크 디바이스와 제2 네트워크 디바이스 모두에 구성되고, 제1 네트워크 디바이스와 제2 네트워크 디바이스 간에 BGP 피어(peer) 관계가 미리 설정되며, 제1 네트워크 디바이스와 제2 네트워크 디바이스 모두 SRv6을 지원한다.

[0011] 가능한 구현에서, 제1 루트의 아웃바운드 인터페이스가 null0 아웃바운드 인터페이스인 것을 고려하여, 매칭을 통해 제1 루트가 획득되면, 제1 루트에 대응하는 네트워크 세그먼트에 도달할 수 없는 것으로 간주된다. 제1 루트가 다른 관리 도메인의 특정 루트를 포함한다면, 다른 관리 도메인의 특정 루트도 또한 도달할 수 없게 된다. 이 문제를 피하기 위해, 제1 루트는 다른 관리 도메인의 특정 루트를 포함하지 않는다. 즉, 제1 루트는 제2 IGP 도메인의 특정 루트를 포함하지 않는다. 제2 IGP 도메인은 제1 네트워크 디바이스 및 제2 네트워크 디바이스가 위치되는 제1 IGP 도메인과는 다른 관리 도메인인데, 즉 제2 IGP 도메인은 제1 IGP 도메인의 네트워크 디바이스를 포함하지 않는다.

[0012] 가능한 구현에서, 제1 루트, 제2 루트 및 제3 루트는 IS-IS 프로토콜 또는 OSPF 프로토콜을 사용함으로써 제2 네트워크 디바이스에 의해 제1 네트워크 디바이스로 송신될 수 있다.

[0013] 가능한 구현에서, 제1 네트워크 디바이스는 제3 네트워크 디바이스로부터 제4 루트를 추가로 수신할 수 있다. SRv6을 통한 L3VPN 듀얼 호밍(dual-homing) 시나리오에서, 액세스 측 디바이스는 제3 네트워크 디바이스와 제2 네트워크 디바이스로 듀얼 호밍될 수 있다. SR-TE FRR 시나리오에서, 제4 루트는 FRR 방법을 사용함으로써 결정된, 제3 루트의 백업 경로일 수 있다. 이런 식으로, 매칭을 통해 null0 아웃바운드 인터페이스를 획득한 후, 제1 네트워크 디바이스는 루트 다음 홉 전환을 추가로 수행할 수 있는데, 예를 들어 제3 네트워크 디바이스로의 루트 다음 홉 전환을 트리거할 수 있어, 패킷 포워딩 프로세스에서는, 제4 루트와 같은 다른 루트가 패킷 포워딩 경로를 결정하는 데 사용될 수 있으며, 이로써 패킷 포워딩 경로의 빠른 전환을 구현하여 패킷 손실률을 효과적으로 낮출 수 있다.

- [0014] 본 출원의 실시예의 제2 양상에 따르면, 통신 방법이 제공된다. 구체적으로, 제1 네트워크 디바이스는 제2 네트워크 디바이스로부터 제3 루트를 획득한다. 제3 루트는 SRv6 SID에 대응하는 네트워크 세그먼트 루트를 포함한다. 제3 루트에 도달할 수 없다고 결정하면, 제1 네트워크 디바이스는 제3 루트의 아웃바운드 인터페이스를 null0 아웃바운드 인터페이스로 설정한다. 제1 네트워크 디바이스는 미리 설정된 시간을 대기한 후 제3 루트를 삭제한다.
- [0015] 이 방법으로, 루트 반복을 수행할 때, 제1 네트워크 디바이스는 최장 마스크 매칭 규칙에 기반한 매칭을 통해 먼저 제3 루트를 획득할 수 있다. 종래 기술에서는, 제3 루트에 도달할 수 없으면, 예를 들어, 제2 네트워크 디바이스가 결함이 있고 제3 루트에 도달할 수 없게 되면, 제3 루트가 삭제된다. 본 출원의 이 실시예에서, 제3 루트에 도달할 수 없다고 결정하면, 제1 네트워크 디바이스는 제3 루트의 아웃바운드 인터페이스를 null0 아웃바운드 인터페이스로 설정하고, 미리 설정된 시간을 대기한 후 제3 루트를 삭제한다. 이런 식으로, 제3 루트에 도달할 수 없더라도, 제1 네트워크 디바이스는 여전히 매칭을 통해 제3 루트를 획득한다. 추가로, 제1 루트의 아웃바운드 인터페이스는 null0 아웃바운드 인터페이스이기 때문에, 매칭을 통해 제3 루트를 획득한 후, 제1 네트워크 디바이스는 다음 홉에 실제로 도달할 수 없음을 신속하게 결정할 수 있고, 제1 네트워크 디바이스는 다른 동작, 예를 들어 루트 반복을 위한 백업 다음 홉으로의 전환을 수행할 수 있어, 패킷이 포워딩될 때, 다른 루트에 의해 지시된 경로를 사용함으로써 패킷이 포워딩된다. 이것은 패킷 손실률을 낮춘다.
- [0016] 가능한 구현에서, 제1 네트워크 디바이스가 루프백 인터페이스 어드레스 루트를 사용함으로써 BGP VPNv4 루트 반복을 수행하고, 루프백 인터페이스 어드레스 루트에 기초하여 아웃바운드 인터페이스 및 다음 홉을 결정하도록 구성된다면, 제3 루트는 로케이터 루트 외에도 루프백 인터페이스 어드레스 루트를 포함할 수 있다. 이런 식으로, 본 출원의 이 실시예의 솔루션을 이용하면, 제1 네트워크 디바이스가 루프백 인터페이스 어드레스 루트를 사용함으로써 BGP VPNv4 루트 반복을 수행하도록 구성되더라도, 패킷 포워딩 경로의 빠른 전환이 구현되어, 패킷 손실률 효과적으로 낮출 수 있다.
- [0017] 가능한 구현에서, 제1 네트워크 디바이스는 제2 네트워크 디바이스로부터 제2 경로를 획득할 수 있다. 제3 루트에 대응하는 네트워크 세그먼트는 제2 루트에 대응하는 네트워크 세그먼트의 서브넷 세그먼트이다. 여기서 언급된 제2 루트는 축약 루트일 수 있다.
- [0018] 가능한 구현에서, 제3 루트에 도달할 수 없다고 결정하면, 제1 네트워크 디바이스는 제2 식별자에 기초하여 제3 루트의 아웃바운드 인터페이스를 null0 아웃바운드 인터페이스로 설정할 수 있다. 제2 식별자는 제2 네트워크 디바이스에 의해 제1 네트워크 디바이스로 송신될 수 있다. 구체적으로, 제2 식별자는 제3 루트와 독립적인 다른 메시지를 사용함으로써 제2 네트워크 디바이스에 의해 제1 네트워크 디바이스로 송신될 수 있거나, 제3 루트에 추가되어 제2 네트워크 디바이스에 의해 제1 네트워크 디바이스로 송신될 수 있다. 이는 본 출원의 이 실시예에서 구체적으로 제한되지 않는다.
- [0019] 가능한 구현에서, 제2 네트워크 디바이스가 IS-IS 프로토콜 또는 OSPF 프로토콜을 사용함으로써 제1 네트워크 디바이스에 제3 루트를 송신할 때, 제2 네트워크 디바이스는 IS-IS 패킷 또는 OSPF 패킷의 필드에 제2 식별자를 추가할 수 있다.
- [0020] 가능한 구현에서는, SRv6을 통한 L3VPN 시나리오에서, SRv6 LSP가 먼저 설정될 필요가 있고, VPN 인스턴스를 사용함으로써 사설 네트워크 루트가 학습될 필요가 있다. 따라서 VPN 인스턴스는 제1 네트워크 디바이스와 제2 네트워크 디바이스 모두에 구성되고, 제1 네트워크 디바이스와 제2 네트워크 디바이스 간에 BGP 피어 관계가 미리 설정되며, 제1 네트워크 디바이스와 제2 네트워크 디바이스 모두 SRv6을 지원한다.
- [0021] 가능한 구현에서, 제1 네트워크 디바이스는 제3 네트워크 디바이스로부터 제4 루트를 추가로 수신할 수 있다. SRv6을 통한 L3VPN 듀얼 호밍 시나리오에서, 액세스 측 디바이스는 제3 네트워크 디바이스와 제2 네트워크 디바이스로 듀얼 호밍될 수 있다. SR-TE FRR 시나리오에서, 제4 루트는 FRR 방법을 사용함으로써 결정된, 제3 루트의 백업 경로일 수 있다. 이런 식으로, 매칭을 통해 null0 아웃바운드 인터페이스를 획득한 후, 제1 네트워크 디바이스는 루트 다음 홉 전환을 추가로 수행할 수 있는데, 예를 들어 제3 네트워크 디바이스로의 루트 다음 홉 전환을 트리거할 수 있어, 패킷 포워딩 프로세스에서는, 제4 루트와 같은 다른 루트가 패킷 포워딩 경로를 결정하는 데 사용될 수 있으며, 이로써 패킷 포워딩 경로의 빠른 전환을 구현하여 패킷 손실률을 효과적으로 낮출 수 있다.
- [0022] 제3 양상에 따르면, 본 출원의 일 실시예는 통신 장치를 제공한다. 이 장치는: 제2 네트워크 디바이스로부터 제1 루트, 제2 루트 및 제3 루트를 획득하도록 구성된 획득 유닛 - 제3 루트는 세그먼트 라우팅 인터넷 프로토

콜 버전 6의 세그먼트 식별자(SRv6 SID)에 대응하는 네트워크 세그먼트 루트를 포함하고, 제3 루트에 대응하는 네트워크 세그먼트는 제1 루트에 대응하는 네트워크 세그먼트의 서브넷 세그먼트이며, 제3 루트에 대응하는 네트워크 세그먼트는 제2 루트에 대응하는 네트워크 세그먼트의 서브넷 세그먼트이고, 제1 루트에 대응하는 네트워크 세그먼트는 제2 루트에 대응하는 네트워크 세그먼트의 서브넷 세그먼트임 -; 및 제1 루트의 아웃바운드 인터페이스를 null0 아웃바운드 인터페이스로 설정하도록 구성된 설정 유닛을 포함한다.

- [0023] 가능한 구현에서, 제3 루트는 루프백(loopback) 인터페이스 어드레스 루트를 더 포함한다.
- [0024] 가능한 구현에서, 이 장치는: 제2 네트워크 디바이스로부터 제1 식별자를 수신하도록 구성된 제1 수신 유닛을 더 포함하며; 설정 유닛은 구체적으로: 제1 식별자에 기초하여 제1 루트의 아웃바운드 인터페이스를 null0 아웃바운드 인터페이스로 설정하도록 구성된다.
- [0025] 가능한 구현에서, 통신 장치는 제1 네트워크 디바이스에 적용되며, 제1 네트워크 디바이스와 제2 네트워크 디바이스 모두에 가상 사설 네트워크(VPN: virtual private network) 인스턴스가 구성되고, 제1 네트워크 디바이스와 제2 네트워크 디바이스 간에 경계 게이트웨이 프로토콜(BGP: border gateway protocol) 피어 관계가 미리 설정되며, 제1 네트워크 디바이스와 제2 네트워크 디바이스 모두 세그먼트 라우팅 인터넷 프로토콜 버전 6(SRv6: segment routing Internet protocol version 6)을 지원한다.
- [0026] 가능한 구현에서, 통신 장치는 제1 네트워크 디바이스에 적용되며, 제1 네트워크 디바이스 및 제2 네트워크 디바이스는 제1 내부 게이트웨이 프로토콜(IGP: interior gateway protocol) 도메인에 위치되고, 제2 IGP 도메인은 제1 IGP 도메인의 네트워크 디바이스를 포함하지 않으며, 제1 루트는 제2 IGP 도메인에 위치된 특정 루트를 포함하지 않는다.
- [0027] 가능한 구현에서, 획득 유닛은 구체적으로: 중간 시스템 간(IS-IS: intermediate system-to-intermediate system) 프로토콜 또는 개방형 최단 경로 우선(OSPF: open shortest path first) 프로토콜을 사용함으로써 제2 네트워크 디바이스에 의해 송신되는 제1 루트, 제2 루트 및 제3 루트를 수신하도록 구성된다.
- [0028] 가능한 구현에서, 이 장치는: 제3 네트워크 디바이스로부터 제4 루트를 수신하도록 구성된 제2 수신 유닛을 더 포함하며, 여기서 액세스 측 디바이스는 제3 네트워크 디바이스와 제2 네트워크 디바이스로 듀얼 호밍되거나, 제4 루트는 고속 재라우트(FRR: fast reroute) 장치를 사용함으로써 결정된, 제3 루트의 백업 루트이다.
- [0029] 제4 양상에 따르면, 본 출원의 일 실시예는 통신 장치를 제공한다. 이 장치는: 제2 네트워크 디바이스로부터 제3 루트를 획득하도록 구성된 제1 획득 유닛 - 제3 루트는 세그먼트 라우팅 인터넷 프로토콜 버전 6의 세그먼트 식별자(SRv6 SID)에 대응하는 네트워크 세그먼트 루트를 포함함 -; 제3 루트에 도달할 수 없다고 결정되면, 제3 루트의 아웃바운드 인터페이스를 null0 아웃바운드 인터페이스로 설정하도록 구성된 설정 유닛; 및 미리 설정된 시간을 대기한 후 제3 루트를 삭제하도록 구성된 삭제 유닛을 포함한다.
- [0030] 가능한 구현에서, 제3 루트는 루프백(loopback) 인터페이스 어드레스 루트를 더 포함한다.
- [0031] 가능한 구현에서, 이 장치는: 제2 네트워크 디바이스로부터 제2 루트를 획득하도록 구성된 제2 획득 유닛을 더 포함하며, 여기서 제3 루트에 대응하는 네트워크 세그먼트는 제2 루트에 대응하는 네트워크 세그먼트의 서브넷 세그먼트이다.
- [0032] 가능한 구현에서, 통신 장치는 제1 네트워크 디바이스에 적용되며, 제1 네트워크 디바이스와 제2 네트워크 디바이스 모두에 가상 사설 네트워크(VPN) 인스턴스가 구성되고, 제1 네트워크 디바이스와 제2 네트워크 디바이스 간에 경계 게이트웨이 프로토콜(BGP) 피어 관계가 미리 설정되며, 제1 네트워크 디바이스와 제2 네트워크 디바이스 모두 세그먼트 라우팅 인터넷 프로토콜 버전 6(SRv6)을 지원한다.
- [0033] 가능한 구현에서, 이 장치는: 제3 네트워크 디바이스로부터 제4 루트를 수신하도록 구성된 수신 유닛을 더 포함하며, 여기서 액세스 측 디바이스는 제3 네트워크 디바이스와 제2 네트워크 디바이스로 듀얼 호밍되거나, 제4 루트는 고속 재라우트(FRR) 장치를 사용함으로써 결정된, 제3 루트의 백업 루트이다.
- [0034] 제5 양상에 따르면, 본 출원의 일 실시예는 프로세서 및 메모리를 포함하는 통신 디바이스를 제공한다. 메모리는 프로그램을 저장하도록 구성된다. 프로세서는 메모리 내의 프로그램을 실행하거나, 제1 양상에 따른 방법을 수행하거나, 제2 양상에 따른 방법을 수행하도록 구성된다.
- [0035] 제6 양상에 따르면, 본 출원의 일 실시예는 프로그램을 포함하는 컴퓨터 판독 가능 저장 매체를 제공한다. 컴퓨터 상에서 프로그램이 실행될 때, 컴퓨터는 제1 양상에 따른 방법을 수행하거나 제2 양상에 따른 방법을 수행

하는 것이 가능해진다.

[0036] 제7 양상에 따르면, 본 출원의 일 실시예는 프로그램을 포함하는 컴퓨터 프로그램 제품을 제공한다. 컴퓨터 상에서 프로그램이 실행될 때, 컴퓨터는 제1 양상에 따른 방법을 수행하거나 제2 양상에 따른 방법을 수행하는 것이 가능해진다.

**도면의 간단한 설명**

[0037] 본 출원의 실시예의 또는 종래 기술의 기술적 솔루션을 보다 명확하게 설명하기 위해, 다음은 실시예 또는 종래 기술을 설명하기 위한 첨부 도면을 간략하게 설명한다. 다음 설명의 첨부 도면은 본 출원의 일부 실시예를 도시하고, 당해 기술분야에서 통상의 지식을 가진 자는 창의적인 노력 없이 여전히 이러한 첨부 도면으로부터 다른 도면을 도출할 수 있다는 것이 명백하다.

- 도 1은 본 출원의 일 실시예에 따른 적용 시나리오의 개략도이다.
- 도 2는 본 출원의 일 실시예에 따른 통신 방법의 개략적인 흐름도이다.
- 도 3은 본 출원의 일 실시예에 따른 통신 방법의 개략적인 흐름도이다.
- 도 4는 본 출원의 일 실시예에 따른 통신 장치의 구조의 개략도이다.
- 도 5는 본 출원의 일 실시예에 따른 통신 장치의 구조의 개략도이다.
- 도 6은 본 출원의 일 실시예에 따른 통신 디바이스의 구조의 개략도이다.

**발명을 실시하기 위한 구체적인 내용**

[0038] 본 출원의 실시예는 축약 루트의 도입으로 야기되는 비교적 높은 패킷 손실률의 문제를 해결하기 위한 통신 방법을 제공한다.

[0039] 이해의 편의상, 본 출원의 실시예의 가능한 적용 시나리오가 먼저 설명된다.

[0040] 도 1은 본 출원의 일 실시예에 따른 적용 시나리오의 개략도이다. 도 1에 도시된 시나리오는 세그먼트 라우팅 인터넷 프로토콜 버전 6(SRv6: segment routing internet protocol version 6)을 기반으로 하는 계층 3 가상 사설 네트워크(L3VPN: layer 3 virtual private network)의 시나리오이며, 이는 줄여서 SRv6을 통한 L3VPN으로 지칭된다. 도 1에 도시된 시나리오에서, 제공자 에지(PE: provider edge) 디바이스(101)와 PE 디바이스(102) 둘 다 고객 에지(CE: customer edge) 디바이스(105)에 접속되고, PE 디바이스(101)는 PE 디바이스(102)에 접속된다. PE 디바이스(101)는 네트워크 디바이스(107)를 사용함으로써 PE 디바이스(103)에 접속된다. PE 디바이스(102)는 네트워크 디바이스(108)를 사용함으로써 PE 디바이스(104)에 접속된다. 네트워크 디바이스(107)는 네트워크 디바이스(108)에 접속되고, PE 디바이스(103)는 PE 디바이스(104)에 접속되고, PE 디바이스(103)와 PE 디바이스(104)는 모두 CE 디바이스(106)에 접속된다. PE 디바이스(101), PE 디바이스(102), PE 디바이스(103), PE 디바이스(104), 네트워크 디바이스(107) 및 네트워크 디바이스(108)는 하나의 관리 도메인에 위치된다. 추가로, 도 1은 이해의 편의상 도시된 것일 뿐, 본 출원의 실시예에 대한 제한을 구성하지 않는다. 실제로, PE 디바이스(101)와 PE 디바이스(103) 사이의 네트워크 디바이스는 네트워크 디바이스(107) 외에도 다른 네트워크 디바이스를 포함할 수 있다. 마찬가지로, PE 디바이스(102)와 PE 디바이스(104) 사이의 네트워크 디바이스는 네트워크 디바이스(108) 외에도 다른 네트워크 디바이스를 포함할 수 있다.

[0041] SRv6을 통한 L3VPN은 인터넷 프로토콜 버전 4(IPv4: Internet protocol version 4) 또는 IPv6 VPN 사설 네트워크 데이터를 전달하기 위해 공용 네트워크의 SRv6 라벨 교환 경로(LSP: label switched path)를 사용하는 것을 의미한다. SRv6 LSP를 사용하여 IPv4 VPN 사설 네트워크 데이터 또는 IPv6 VPN 사설 네트워크 데이터를 운반하려면, 먼저 SRv6 LSP가 설정될 필요가 있고, VPN 인스턴스를 사용함으로써 사설 네트워크 루트가 학습될 필요가 있다고 이해될 수 있다. 도 1을 참조하여 다음의 설명이 제공된다.

[0042] 다음은 PE 디바이스(101)와 PE 디바이스(103) 사이의 루트 전달 프로세스를 설명한다. PE 디바이스(102)와 PE 디바이스(104) 사이의 루트 전달 프로세스는 이와 유사하다. 구체적으로, PE 디바이스(101)와 PE 디바이스(103) 모두 SRv6을 지원한다. PE 디바이스(103)와 PE 디바이스(101) 사이에 경계 게이트웨이 프로토콜(BGP: border gateway protocol) 피어 관계가 설정되고, PE 디바이스(103) 및 PE 디바이스(101)에 VPN 인스턴스가 구성된다. 구체적으로, SRv6 LSP를 사용하여 IPv4 VPN 사설 네트워크 데이터를 전달하려면, PE 디바이스(103) 및 PE 디바이스(101)에 VPNv4 인스턴스가 구성될 수 있다. SRv6 LSP를 사용하여 IPv6 VPN 사설 네트워크 데이터를

전달하려면, PE 디바이스(103) 및 PE 디바이스(101)에 VPNv6 인스턴스가 구성될 수 있다. 이것은 여기에 제한되지 않는다. 다음은 VPNv4 인스턴스를 설명에 대한 일례로 사용한다.

[0043] CE 디바이스(106)가 사실 네트워크 루트, 예를 들어 10.1.1.0/24를 통지한다면, PE 디바이스(103)는 BGP를 사용함으로써 먼저 VPN 인스턴스 사실 네트워크 루트 10.1.1.0/24를 도입할 수 있다. 그 다음, PE 디바이스(103)는 VPN 인스턴스 사실 네트워크 루트를 BGP VPNv4 루트로 변환하고, BGP 피어 관계를 사용함으로써 PE 디바이스(101)에 루트를 통지한다. 즉, PE 디바이스(101)는 BGP를 사용함으로써 루트 10.1.1.0/24를 학습하고, 다음 홉이 PE 디바이스(103)의 루프백(loopback) 인터페이스 어드레스라고 결정한다. 예를 들어, 루프백 어드레스는 A1:1:13::3이다. 대응하여, PE 디바이스(101) 상의 VPN 인스턴스는 또한 루트를 학습할 수 있다. 그러나 PE 디바이스(103)에는 VPN 세그먼트 식별자(SID: segment ID)가 설정되므로, PE(101) 상에서 VPN 인스턴스에 의해 학습된 루트의 다음 홉은 VPN SID이다. 예를 들어, VPN SID는 A1:1:3::B100이다. 즉, PE 디바이스(101)는 하기 표 1에 도시된 바와 같이, PE 디바이스(103)로부터 2개의 루트를 학습할 수 있다.

표 1

시퀀스 번호	루트 타입	어드레스 프리픽스	다음 홉
1	BGP VPNv4 루트	10.1.1.0/24	A1:1:13::3
2	VPN 루트	10.1.1.0/24	A1:1:3::B100

[0045] 표 1의 BGP VPNv4 루트는 BGP를 사용함으로써 PE 디바이스(101)에 의해 PE 디바이스(103)로부터 학습된 루트이고, VPN 루트는 PE 디바이스(101) 상의 VPN 인스턴스에 의해 PE 디바이스(103)로부터 학습된 루트이다. VPNv4 루트를 학습한 후, PE 디바이스(101)는 해당 VPN 인스턴스 라우팅 표로 루트를 가로지른 다음, 루트를 공통 IPv4 루트로 변환하고, 루트를 CE 디바이스(105)에 통지할 수 있다. 이런 식으로, CE 디바이스(105)와 CE 디바이스(106) 사이에 도달 가능한 루트가 구현된다. 추가로, PE 디바이스(101)와 PE 디바이스(103) 모두 SRv6을 지원하기 때문에, PE 디바이스(103)는 PE 디바이스(103)의 SRv6 SID에 대응하는 네트워크 세그먼트 루트를 PE 디바이스(101)에 추가로 송신할 수 있다. 이 루트는 또한 로케이터 루트로도 지칭된다. 로케이터 루트를 사용함으로써 PE 디바이스(101)와 PE 디바이스(103) 사이에서 패킷이 또한 포워딩될 수 있다. 예를 들어, PE 디바이스(103)의 로케이터 루트는 A1:1:3::/64이다. 로케이터 루트는 표 2에 도시될 수 있다.

표 2

루트 타입	목적지 어드레스	다음 홉
로케이터 루트	A1:1:3::/64	A1:1:13::7

[0047] 예를 들어, A1:1:13::7은 도 1에 도시된 네트워크 디바이스(107)의 루프백 인터페이스 어드레스일 수 있는데, 즉 이는 다음 홉이 네트워크 디바이스(107)임을 지시할 수 있다.

[0048] CE 디바이스(105)가 CE 디바이스(106)로 패킷을 송신할 때, CE 디바이스(105)는 목적지 어드레스가 CE 디바이스(106)인 공통 IPv4 패킷을 PE 디바이스(101)에 송신하는데, 즉 IPv4 패킷의 목적지 어드레스는 10.1.1.0/24이다. VPN 인스턴스에 바인딩(bind)된 인터페이스로부터 공통 IPv4 패킷을 수신한 후, PE 디바이스(101)는 추가 포워딩을 위해 표 1의 BGP VPNv4 루트 또는 VPN 루트를 사용함으로써 IPv4 패킷을 SRv6 패킷으로 캡슐화할 수 있다. VPN 루트가 일례로 사용된다. PE 디바이스(101)는 해당 VPN 인스턴스의 라우팅 및 포워딩 표를 검색하고, 목적지 IPv4 프리픽스 매칭을 수행하여, 연관된 VPN SID 및 다음 홉 정보를 찾는다. 그런 다음, VPN SID A1:1:3::B100이 패킷의 목적지 어드레스로서 직접 사용되어, 패킷을 SRv6 패킷으로 캡슐화한다. PE 디바이스(101)는 최장 매칭 규칙에 기반하여 목적지 어드레스와의 매칭을 통해 로케이터 루트 A1:1:3::/64를 획득하고, 최단 경로를 따라 패킷을 네트워크 디바이스(107)로 포워딩한다. 네트워크 디바이스(107)는 최장 매칭 규칙에 기반한 매칭을 통해 로케이터 루트 A1:1:3::/64를 획득하고, 최단 경로를 따라 패킷을 PE 디바이스(103)로 포워딩한다. PE 디바이스(103)는 VPN SID A1:1:3::B100을 기반으로 해당 포워딩 동작을 결정하고, SRv6 패킷의 캡슐화를 해제하고, 패킷을 공통 IPv4 패킷으로 복원한 다음, VPN SID A1:1:3::B100과의 매칭을 통해 VPN 인스턴스를 획득하고, VPN 인스턴스의 라우팅 표를 검색하고, 복원된 공통 IPv4 패킷을 CE 디바이스(106)로 송신하여 패킷 포워딩을 완료한다.

[0049] PE 디바이스(101)가 BGP VPNv4 루트를 사용함으로써 IPv4 패킷을 SRv6 패킷으로 캡슐화하고 추가로 SRv6 패킷을

포워딩하는 특정 프로세스는 앞서 말한 설명과 유사하며, 세부사항들은 여기서 다시 설명되지 않는다.

[0050] 도 1에 도시된 적용 시나리오를 참조하면, CE 디바이스(105)는 PE 디바이스(101) 및 PE 디바이스(102)에 접속되고, CE 디바이스(106)는 PE 디바이스(103) 및 PE 디바이스(104)에 접속된다. PE 디바이스(101)와 PE 디바이스(102)는 L3VPN 듀얼 호밍 액세스를 구현하는 2개의 디바이스일 수 있는데, 즉 CE 디바이스(105)는 PE 디바이스(101)와 PE 디바이스(102)로 듀얼 호밍된다. PE 디바이스(103) 및 PE 디바이스(104)는 또한 L3VPN 듀얼 호밍 액세스를 구현하는 디바이스일 수 있는데, 즉 CE 디바이스(106)는 PE 디바이스(103)와 PE 디바이스(104)에 듀얼 호밍된다. 대안으로, PE 디바이스(101)와 PE 디바이스(102)는 고속 재라우트(FRR: fast reroute)를 구현하는 2개의 디바이스일 수 있다. 예를 들어, PE 디바이스(102)를 포함하는 패킷 포워딩 경로는 PE 디바이스(101)의 패킷 포워딩 경로를 포함하는 FRR 경로이다. 대안으로, PE 디바이스(103)와 PE 디바이스(104)는 FRR을 구현하는 2개의 디바이스일 수 있다. 예를 들어, PE 디바이스(104)를 포함하는 패킷 포워딩 경로는 PE 디바이스(103)의 패킷 포워딩 경로를 포함하는 FRR 경로이다.

[0051] 앞서 말한 시나리오에서는, PE 디바이스(103)로의 루트 외에도, PE 디바이스(101)는 PE 디바이스(104)로의 루트, 예를 들어 PE 디바이스(104)로의 BGP VPNv4 루트, VPN 루트 및 로케이터 루트를 추가로 가지며, 이러한 루트는 표 3 및 표 4에 도시된다. PE 디바이스(103)와 PE 디바이스(104) 간의 듀얼 호밍 액세스 프로토콜 또는 FRR 프로토콜에 따르면, PE 디바이스(103)가 도달할 수 없는 경우, PE 디바이스(101)는 PE 디바이스(103)로의 루트를 추가 패킷 포워딩을 위해 PE 디바이스(104)로의 루트로 대체할 수 있다.

표 3

시퀀스 번호	루트 타입	어드레스 프리픽스	다음 홉
1	BGP VPNv4 루트	10.1.1.0/24	A1:1:14::4
2	VPN 루트	10.1.1.0/24	A1:1:4::B100

표 4

루트 타입	목적지 어드레스	다음 홉
로케이터 루트	A1:1:4::/64	A1:1:13::8

[0054] 예를 들어, A1:1:13::8은 도 1에 도시된 네트워크 디바이스(108)의 루프백 인터페이스 어드레스일 수 있는데, 즉 이는 다음 홉이 네트워크 디바이스(108)임을 지시한다.

[0055] PE 디바이스(103)와 PE 디바이스(104)는 둘 다 축약 루트, 예를 들어 A1::/32를 도입할 수 있다. 로케이터 루트에 대응하는 네트워크 세그먼트는 축약 루트에 대응하는 네트워크 세그먼트의 서브넷 세그먼트이다. 로케이터 루트 A1:1:3::/64에 도달할 수 없는 경우, 예를 들어 PE 디바이스(103)가 결함이 있고 로케이터 루트 A1:1:3::/64를 도달할 수 없게 하는 경우, PE 디바이스(101)는 내부 게이트웨이 프로토콜(IGP: internal gateway protocol)을 사용함으로써, 로케이터 루트에 도달할 수 없음을 신속하게 검출할 수 있는데, 즉 PE 디바이스(101)는 로케이터 루트가 실제로 존재하지 않는다고 결정할 수 있다. 따라서 PE 디바이스(101)는 로케이터 루트를 즉시 삭제할 수 있다. 그러나 PE 디바이스(104)가 또한 축약 루트를 도입하기 때문에 축약 루트는 삭제되지 않는다. 추가로, PE 디바이스(101)는 PE 디바이스(101)와 PE 디바이스(103) 사이의 BGP 접속이 중단된 것을 검출하지 못했는데, 이는 BGP를 사용함으로써 접속 중단 검출을 수행하는 데 어느 정도 시간이 걸리기 때문이다. 따라서 표 1에 도시된 BGP VPNv4 루트와 VPN 루트의 경우, VPN 루트의 다음 홉 VPN SID A1:1:3::B100 또는 BGP VPNv4 루트의 다음 홉 루프백 인터페이스 어드레스 A1:1:13::3을 사용함으로써 루트 반복이 수행될 때, 최장 마스크 매칭 규칙에 기반한 매칭을 통해 축약 루트 A1::/32가 획득되는데, 즉 사설 네트워크 루트 10.1.1.0/24의 다음 홉(PE 디바이스(103))으로 인해 루트 반복이 성공한다. PE 디바이스(101)는 PE 디바이스(101)와 PE 디바이스(103) 사이의 SRv6 터널에 여전히 도달할 수 있다고 간주하고, PE 디바이스(104)로의 루트 다음 홉 전환을 트리거하지 않는다. 그 결과, 패킷 포워딩 중에, 패킷(예를 들어, CE 디바이스(105)로부터의 공통 IPv4 패킷)은 여전히 목적지 어드레스로서 PE(103)에 대응하는 VPN SID A1:1:3::B100을 갖는 SRv6 패킷으로 캡슐화되며, 이는 심각한 패킷 손실로 이어진다.

[0056] 여기서, 도 1에 도시된 PE 디바이스(101)와 같은 각각의 네트워크 디바이스는 미리 설정된 주기를 기초로 루트 반복을 수행하여, 루트에 도달할 수 있는지 여부를 결정하고, 루트 반복 결과에 기초하여 RIB를 업데이트하고, 업데이트된 RIB에 기초하여, 패킷 포워딩을 안내하기 위한 포워딩 정보 베이스(FIB: forwarding information

base)를 대응하게 업데이트한다는 점이 주목되어야 한다. 패킷 포워딩 프로세스에서, PE 디바이스(101)는 최신 FIB를 기반으로 패킷을 포워딩한다. 앞서 말한 시나리오에서, 루트 반복을 수행할 때, PE 디바이스(101)는 시간상 VPN 루트 다음 홉 전환을 트리거하지 않으므로, 실제로 도달할 수 없는 루트가 FIB에 존재한다. 그 결과, 패킷을 포워딩할 때, 패킷은 실제로 도달할 수 없는 루트를 따라 포워딩되어, 심각한 패킷 손실로 이어진다.

[0057] 앞서 말한 문제를 해결하기 위해, 본 출원의 실시예는 통신 방법을 제공한다. 다음은 첨부 도면을 참조하여 방법을 설명한다.

[0058] 도 2는 본 출원의 일 실시예에 따른 통신 방법의 개략적인 흐름도이다. 본 출원의 이 실시예에서 제공되는 통신 방법은 예를 들어, 다음의 S101 및 S102를 수행함으로써 구현될 수 있다.

[0059] S101: 제1 네트워크 디바이스가 제2 네트워크 디바이스로부터 제1 루트, 제2 루트 및 제3 루트를 획득한다.

[0060] 본 출원의 이 실시예에서, 제1 네트워크 디바이스는 라우터일 수 있거나 스위치일 수 있다. 대응하게, 제2 네트워크 디바이스는 또한 라우터 또는 스위치일 수 있다. SRv6을 통한 L3VPN 시나리오에서, 제1 네트워크 디바이스 및 제2 네트워크 디바이스는 PE 디바이스일 수 있다. 예를 들어, 제1 네트워크 디바이스는 도 1에 도시된 PE 디바이스(101)에 대응할 수 있고, 제2 네트워크 디바이스는 도 1에 도시된 PE 디바이스(103)에 대응할 수 있다. SR-TE FRR 시나리오에서, 제1 네트워크 디바이스 및 제2 네트워크 디바이스는 PE 디바이스일 수 있는 것이 아니라, 네트워크 내의 임의의 네트워크 노드일 수 있다.

[0061] SRv6을 통한 L3VPN 시나리오에서는, SRv6 LSP가 먼저 설정될 필요가 있고, VPN 인스턴스를 사용함으로써 사실 네트워크 루트가 학습될 필요가 있다고 이해될 수 있다. 따라서 VPN 인스턴스는 제1 네트워크 디바이스와 제2 네트워크 디바이스 모두에 구성되고, 제1 네트워크 디바이스와 제2 네트워크 디바이스 간에 BGP 피어 관계가 미리 설정되며, 제1 네트워크 디바이스와 제2 네트워크 디바이스 모두 SRv6을 지원한다.

[0062] 본 출원의 이 실시예에서, 제3 루트는 SRv6 SID에 대응하는 네트워크 세그먼트 루트, 즉 로케이터 루트를 포함할 수 있고, 제3 루트는 공용 네트워크 루트로 간주될 수 있다. 제2 네트워크 디바이스가 SRv6을 지원하는 경우, 제2 네트워크 디바이스는 SRv6 SID에 대응하는 네트워크 세그먼트 루트를 갖는다. 가능한 구현에서, 제1 네트워크 디바이스가 루프백 인터페이스 어드레스 루트를 사용함으로써 BGP VPNv4 루트 반복을 수행하고, 루프백 인터페이스 어드레스 루트에 기초하여 아웃바운드 인터페이스 및 다음 홉을 결정하도록 구성된다면, 제3 루트는 로케이터 루트 외에도 루프백 인터페이스 어드레스 루트를 포함할 수 있다. 본 출원의 이 실시예에서, 제1 네트워크 디바이스와 제2 네트워크 디바이스는 동일한 IGP 도메인에 위치된다. 따라서 제1 네트워크 디바이스는 IGP를 사용함으로써 제3 루트를 학습할 수 있는데, 즉 제2 네트워크 디바이스는 IGP를 사용함으로써 제3 루트를 제1 네트워크 디바이스에 통지할 수 있다. 예를 들어, 제2 네트워크 디바이스는 중간 시스템 간(IS-IS: intermediate system-to-intermediate system) 프로토콜을 사용함으로써 제3 루트를 제1 네트워크 디바이스로 송신할 수 있다. 다른 예를 들면, 제2 네트워크 디바이스는 개방형 최단 경로 우선(OSPF: open shortest path first) 프로토콜을 사용함으로써 제3 루트를 제1 네트워크 디바이스로 송신할 수 있다. 본 출원의 이 실시예에서, 제2 루트는 제2 네트워크 디바이스에 도입된 축약 루트이고, 제2 루트에 대응하는 네트워크 세그먼트는 제3 루트에 대응하는 네트워크 세그먼트를 포함한다. 즉, 제3 루트에 대응하는 네트워크 세그먼트는 제2 루트에 대응하는 네트워크 세그먼트의 서브넷 세그먼트이다.

[0063] 실제 적용에서, 제1 네트워크 디바이스와 제2 네트워크 디바이스가 동일한 IGP 도메인에 위치되기 때문에, 제1 네트워크 디바이스는 IGP를 사용함으로써, 제3 루트에 도달할 수 있는지 여부를 결정할 수 있다고 이해될 수 있다. 제1 네트워크 디바이스가 제3 루트에 도달할 수 없다고 결정하는 경우, 제1 네트워크 디바이스는 제3 루트를 삭제할 수 있다. 그러나 실제 적용에서, 제1 네트워크 디바이스는 제1 네트워크 디바이스와 제2 네트워크 디바이스 간의 BGP 접속이 중단되었는지 여부를 결정할 수 없는데, 이는 BGP 접속이 중단되었는지 여부를 검출하는 데 어느 정도 시간이 걸리기 때문이다. 따라서 제1 네트워크 디바이스가 제3 루트에 도달할 수 없다고 결정했다더라도, 제1 네트워크 디바이스는 표 1에 도시되는 BGP VPNv4 루트와 VPN 루트를 삭제하지 않는다. 따라서 루트 다음 홉 반복을 수행할 때, 제1 네트워크 디바이스는 최장 마스크 매칭 방식의 매칭을 통해 제2 루트를 획득할 수 있고 루트 다음 홉 반복이 성공하고 루트 다음 홉 전환을 트리거하지 않는 것으로 간주할 수 있다. 그 결과, 라우팅 및 포워딩 표는 실제로 도달할 수 없는 루트를 포함하여, 비교적 심각한 패킷 손실로 이어진다. 도 1을 참조하면, VPN 루트의 다음 홉 VPN SID A1:1:3::B100을 사용함으로써 루트 다음 홉 반복이 수행될 때, 최장 마스크 매칭 규칙에 기반한 매칭을 통해 제2 루트 A1::/32가 획득된다고 이해된다. 다음 홉 PE 디바이스(103)에 도달할 수 있고, PE 디바이스(104)로의 다음 홉 전환이 트리거되지 않는 것으로 간주된다.

- [0064] 이를 고려하여, 본 출원의 이 실시예에서, 제2 루트를 제1 네트워크 디바이스에 통지할 때, 제2 네트워크 디바이스는 블랙홀(blackhole) 루트를 추가로 통지할 수 있다. 블랙홀 루트는 아웃바운드 인터페이스가 null0 아웃바운드 인터페이스인 루트를 의미한다. 일단 루트 반복 중 매칭을 통해 블랙홀 루트가 획득되면 다음 홉에 도달할 수 없다고 결정될 수 있다. 본 출원의 이 실시예에서 언급된 제1 루트는 블랙홀 루트이다. 구체적으로, 제2 네트워크 디바이스는 IGP를 사용함으로써 제1 루트 및 제2 루트를 제1 네트워크 디바이스에 통지할 수 있다. 본 출원의 이 실시예에서, 제1 루트 및 제2 루트를 제1 네트워크 디바이스에 통지하기 위해 제2 네트워크 디바이스에 의해 사용되는 IGP 프로토콜은 구체적으로 제한되지 않는다. 일례로, 제2 네트워크 디바이스는 IS-IS 프로토콜을 사용함으로써 제1 루트 및 제2 루트를 제1 네트워크 디바이스에 통지할 수 있다. 다른 예에서, 제2 네트워크 디바이스는 OSPF를 사용함으로써 제1 루트 및 제2 루트를 제1 네트워크 디바이스에 통지할 수 있다.
- [0065] 본 출원의 이 실시예에서, 제2 루트에 대응하는 네트워크 세그먼트는 제1 루트에 대응하는 네트워크 세그먼트를 포함하고, 제1 루트에 대응하는 네트워크 세그먼트는 제3 루트에 대응하는 네트워크 세그먼트를 포함한다. 즉, 제3 루트의 마스크 길이는 제1 루트의 마스크 길이보다 길고, 제1 루트의 마스크 길이는 제2 루트의 마스크 길이보다 길다.
- [0066] S102: 제1 네트워크 디바이스는 제1 루트의 아웃바운드 인터페이스를 null0 아웃바운드 인터페이스로 설정한다.
- [0067] 본 출원의 이 실시예에서, 제1 루트를 수신한 후, 제1 네트워크 디바이스는 제1 루트의 아웃바운드 인터페이스를 null0 아웃바운드 인터페이스로 설정할 수 있다. 구체적으로, 본 출원의 이 실시예의 구현에서, 제1 네트워크 디바이스는 제1 식별자에 기초하여 제1 루트의 아웃바운드 인터페이스를 null0 아웃바운드 인터페이스로 설정할 수 있고, 제1 식별자는 제2 네트워크 디바이스에 의해 제1 네트워크 디바이스로 송신될 수 있다. 제1 식별자의 경우, 제1 식별자는 제1 루트와 독립적인 다른 메시지를 사용함으로써 제2 네트워크 디바이스에 의해 제1 네트워크 디바이스로 송신될 수 있거나, 제1 루트에 추가되어 제2 네트워크 디바이스에 의해 제1 네트워크 디바이스로 송신될 수 있다는 점이 주목되어야 한다. 이는 본 출원의 이 실시예에서 구체적으로 제한되지 않는다. 제2 네트워크 디바이스가 IS-IS 프로토콜 또는 OSPF 프로토콜을 사용함으로써 제1 네트워크 디바이스에 제1 루트를 송신할 때, 제2 네트워크 디바이스는 IS-IS 패킷 또는 OSPF 패킷의 필드에 제1 식별자를 추가할 수 있다.
- [0068] 제3 루트가 삭제된다면, 제1 루트가 도입되고 제1 루트의 마스크 길이가 제2 루트의 마스크 길이보다 길기 때문에, 제1 네트워크 디바이스가 루트 다음 홉 반복을 수행할 때 최장 마스크 매칭 규칙을 기반으로 한 매칭을 통해 제1 루트를 획득될 수 있다고 이해될 수 있다. 제1 루트의 아웃바운드 인터페이스가 null0 아웃바운드 인터페이스이기 때문에, 매칭을 통해 제1 루트를 획득한 후, 제1 네트워크 디바이스는 다음 홉에 도달할 수 없음을 신속하게 결정할 수 있고, 제1 네트워크 디바이스는 다른 동작, 예를 들어 루트 반복을 위한 백업 다음 홉으로의 전환을 수행할 수 있어, 패킷 포워딩 중에, 백업 루트와 같은 다른 루트를 사용함으로써 패킷 포워딩 경로가 결정될 수 있다. 이것은 패킷 손실률을 낮춘다. 예를 들어, 도 1을 참조하면, VPN 루트의 다음 홉 VPN SID A1:1:3::B100을 사용함으로써 루트 다음 홉 반복이 수행될 때, 최장 마스크 매칭 규칙에 기반한 매칭을 통해 제1 루트, 예를 들어 A1:1::/48이 획득된다고 이해될 수 있다. 제1 루트의 아웃바운드 인터페이스는 null0 아웃바운드 인터페이스이다. 따라서 PE 디바이스(101)는 다음 홉 PE 디바이스(103)가 도달할 수 없는 것으로 간주하고, PE 디바이스(104)로의 다음 홉 전환을 트리거한다. 즉, PE 디바이스(104)의 VPN SID, 예를 들어 A1:1:4::B100을 사용함으로써 루트 다음 홉 반복이 수행된다. 반복이 성공한다면, 패킷이 포워딩될 때, 패킷, 예를 들어 CE 디바이스(105)로부터의 공통 IPv4 패킷이 목적지 어드레스로서 PE 디바이스(104)에 대응하는 VPN SID A1:1:4::B100을 갖는 SRv6 패킷으로 캡슐화된다. 이것은 패킷 손실을 피한다.
- [0069] 앞서 말한 설명으로부터, 제1 루트의 아웃바운드 인터페이스는 null0 아웃바운드 인터페이스이고, 매칭을 통해 제1 루트가 획득되면, 제1 루트에 대응하는 네트워크 세그먼트에 도달할 수 없다고 학습될 수 있다. 그러나 제1 루트는 해당 네트워크 세그먼트를 가지며, 제1 루트가 다른 관리 도메인의 특정 루트를 포함한다면, 다른 관리 도메인의 특정 루트도 또한 도달할 수 없게 된다. 이 문제를 피하기 위해, 본 출원의 이 실시예의 구현에서, 제1 루트는 다른 관리 도메인의 특정 루트를 포함하지 않는다. 즉, 제1 루트는 제2 IGP 도메인의 특정 루트를 포함하지 않는다. 제2 IGP 도메인은 제1 네트워크 디바이스 및 제2 네트워크 디바이스가 위치되는 제1 IGP 도메인과는 다른 관리 도메인인데, 즉 제2 IGP 도메인은 제1 IGP 도메인의 네트워크 디바이스를 포함하지 않는다.
- [0070] 본 출원의 이 실시예의 구현에서, 제1 네트워크 디바이스는 제3 네트워크 디바이스로부터 제4 루트를 추가로 수



신할 수 있다. 위에서 설명된 SRv6을 통한 L3VPN 듀얼 호밍 시나리오에서, CE 디바이스(106)와 같은 액세스 측 디바이스는 PE 디바이스(104)와 같은 제3 네트워크 디바이스와 PE 디바이스(103)와 같은 제2 네트워크 디바이스에 듀얼 호밍될 수 있다. 위에 도시된 FRR 시나리오에서, 제4 루트는 FRR 방법을 사용함으로써 결정된, 제3 루트의 백업 경로일 수 있다. 이런 식으로, 매칭을 통해 null0 아웃바운드 인터페이스를 획득한 후, 제1 네트워크 디바이스는 루트 다음 홉 전환을 추가로 수행할 수 있는데, 예를 들어 제3 네트워크 디바이스로의 루트 다음 홉 전환을 트리거할 수 있어, 패킷 포워딩 프로세스에서는, 제4 루트와 같은 다른 루트가 패킷 포워딩 경로를 결정하는 데 사용될 수 있으며, 이로써 패킷 포워딩 경로의 빠른 전환을 구현하여 패킷 손실률을 효과적으로 낮출 수 있다.

- [0071] 추가 블랙홀 루트를 통지하는 방식에 추가하여, 본 출원의 이 실시예에서, 미리 설정된 기간 내에 제3 루트를 블랙홀 루트로 변경하는 방식이 또한, 축약 루트의 도입으로 야기되는 비교적 높은 패킷 손실률의 문제를 해결하는 데 사용될 수 있다. 다음은 첨부 도면을 참조하여 통신 방법을 설명한다.
- [0072] 도 3은 본 출원의 일 실시예에 따른 통신 방법의 개략적인 흐름도이다. 본 출원의 이 실시예에서 제공되는 통신 방법은 예를 들어, 다음의 S201 내지 S203를 수행함으로써 구현될 수 있다.
- [0073] S201: 제1 네트워크 디바이스는 제2 네트워크 디바이스로부터 제3 루트를 획득한다.
- [0074] 제3 루트는 SRv6 SID에 대응하는 네트워크 세그먼트 루트, 즉 로케이터 루트를 포함할 수 있고, 제3 루트는 공용 네트워크 루트로 간주될 수 있다.
- [0075] 제3 루트에 대해서는, 도 2에 도시된 통신 방법에서 제3 루트의 설명 부분을 참조한다. 세부사항은 여기서 다시 설명되지 않는다. 제1 네트워크 디바이스 및 제2 네트워크 디바이스에 대해서는, 도 2에 도시된 통신 방법의 관련 설명 부분을 참조한다. 세부사항은 여기서 다시 설명되지 않는다.
- [0076] 앞서 설명된 바와 같이, SRv6을 통한 L3VPN 시나리오에서, SRv6 LSP가 먼저 설정될 필요가 있고, VPN 인스턴스를 사용함으로써 사설 네트워크 루트가 학습될 필요가 있다. 따라서 VPN 인스턴스는 제1 네트워크 디바이스와 제2 네트워크 디바이스 모두에 구성되고, 제1 네트워크 디바이스와 제2 네트워크 디바이스 간에 BGP 피어 관계가 미리 설정되며, 제1 네트워크 디바이스와 제2 네트워크 디바이스 모두 SRv6을 지원한다.
- [0077] S202: 제3 루트에 도달할 수 없다고 결정하면, 제1 네트워크 디바이스는 제3 루트의 아웃바운드 인터페이스를 null0 아웃바운드 인터페이스로 설정한다.
- [0078] S203: 제1 네트워크 디바이스는 미리 설정된 시간을 대기한 후 제3 루트를 삭제한다.
- [0079] 위에서 설명된 바와 같이, 종래 기술에서는 제1 네트워크 디바이스가 제3 루트에 도달할 수 없다고 결정하면, 즉 제3 루트가 제1 IGP 도메인에 더 이상 존재하지 않는다고 결정하면, 제3 루트가 삭제된다. 그 결과, 제1 네트워크 디바이스는 최장 마스크 매칭 규칙에 기반한 매칭을 통해 제2 루트를 획득한다. 제2 루트는 제2 네트워크 디바이스에 도입된 축약 루트이다. 제1 네트워크 디바이스는 제2 네트워크 디바이스로부터 제2 루트를 수신할 수 있고, 제2 루트에 대응하는 네트워크 세그먼트는 제3 루트에 대응하는 네트워크 세그먼트를 포함한다. 제2 루트에 대해서는, 앞서 말한 관련 내용의 설명 부분을 참조한다. 세부사항은 여기서 다시 설명되지 않는다.
- [0080] 이 문제를 해결하기 위해, 제3 루트에 도달할 수 없다고 결정하면, 제1 네트워크 디바이스는 제3 루트를 즉시 삭제하는 것이 아니라, 먼저 제3 루트의 아웃바운드 인터페이스를 null0 아웃바운드 인터페이스로 설정하고, 미리 설정된 시간, 예를 들어 10초를 대기한 후 제3 루트를 삭제한다. 이런 식으로, 미리 설정된 시간 내에 제3 루트가 삭제되지 않기 때문에, 패킷이 축약 루트와 매칭될 때 야기된 패킷 손실이 방지될 수 있고, 제1 네트워크 디바이스는 null0 인터페이스인 제3 루트의 아웃바운드 인터페이스를 사용함으로써, 다음 홉에 도달할 수 없음을 인지하고, 제3 루트를 듀얼 호밍 액세스 또는 FRR을 구현하는 다른 백업 루트로 교체할 수 있다. 미리 설정된 시간 후에, 제1 네트워크 디바이스는 BGP를 사용함으로써 이미 접속 중단 검출을 수행할 수 있으며, 제2 네트워크 디바이스로의 BGP 루트와 VPN 루트 모두에 도달할 수 없음을 인지할 수 있어, 축약 루트에 의해 야기된 패킷 손실의 문제가 존재하지 않는다.
- [0081] 구체적으로, 본 출원의 이 실시예의 구현에서, 제3 루트에 도달할 수 없다고 결정하면, 제1 네트워크 디바이스는 제2 식별자에 기초하여 제3 루트의 아웃바운드 인터페이스를 null0 아웃바운드 인터페이스로 설정할 수 있다. 제2 식별자는 제2 네트워크 디바이스에 의해 제1 네트워크 디바이스로 송신될 수 있다. 제2 식별자의 경우, 제2 식별자는 제3 루트와 독립적인 다른 메시지를 사용함으로써 제2 네트워크 디바이스에 의해 제1 네트

워크 디바이스로 송신될 수 있거나, 제3 루트에 추가되어 제2 네트워크 디바이스에 의해 제1 네트워크 디바이스로 송신될 수 있다는 점이 주목되어야 한다. 이는 본 출원의 이 실시예에서 구체적으로 제한되지 않는다. 제2 네트워크 디바이스가 IS-IS 프로토콜 또는 OSPF 프로토콜을 사용함으로써 제1 네트워크 디바이스에 제3 루트를 송신할 때, 제2 네트워크 디바이스는 IS-IS 패킷 또는 OSPF 패킷의 필드에 제2 식별자를 추가할 수 있다. 본 출원의 이 실시예의 다른 가능한 구현에서, 제1 네트워크 디바이스는 구성 정보를 획득할 수 있고, 구성 정보에 기초하여 제3 루트에 도달할 수 없다고 결정할 때 제3 루트의 아웃바운드 인터페이스를 null0 아웃바운드 인터페이스로 설정할 수 있다. 구성 정보는 관리 담당자에 의해 구성될 수 있거나, 다른 디바이스에 의해 전달될 수 있다. 이는 본 출원의 이 실시예에서 구체적으로 제한되지 않는다.

[0082] 미리 설정된 시간은 예를 들어, 제2 식별자에서 전달될 수 있거나, 다른 방식으로 결정될 수 있는데, 예를 들어 제1 네트워크 디바이스에 대해 미리 구성될 수 있다는 점이 주목되어야 한다. 미리 설정된 시간의 특정 값은 실제 상황에 기초하여 결정될 수 있다. 이는 본 출원의 이 실시예에서 구체적으로 제한되지 않는다.

[0083] 앞서 말한 설명으로부터, 제1 네트워크 디바이스가 패킷을 포워딩할 때, 제3 루트가 실제로 존재하지 않더라도, 제1 네트워크 디바이스는 여전히 매칭을 통해 제3 루트를 획득한다는 것이 학습될 수 있다. 추가로, 제3 루트의 아웃바운드 인터페이스는 null0 아웃바운드 인터페이스이므로, 제3 루트는 기본적으로 로케이터 루트 또는 루프백 인터페이스 어드레스 루트에서 블랙홀 루트로 변경된다. 대응하게, 매칭을 통해 제3 루트를 획득한 후, 제1 네트워크 디바이스는 다음 홉에 도달할 수 없음을 신속하게 결정할 수 있고, 제1 네트워크 디바이스는 다른 동작, 예를 들어 루트 반복을 위한 백업 다음 홉으로의 전환을 수행할 수 있어, 패킷 포워딩 스테이지에서, 제1 네트워크 디바이스는 백업 루트와 같은 다른 루트를 사용함으로써 패킷 포워딩 경로를 결정할 수 있다. 이것은 패킷 손실률을 낮춘다. 예를 들어, 도 1을 참조하면, 제3 루트, 예를 들어 로케이터 루트 A1:1:3::/64가 도달할 수 없다고 결정한 후, 제1 네트워크 디바이스가 로케이터 루트의 아웃바운드 인터페이스를 null0 아웃바운드 인터페이스로 설정하는데, 즉 로케이터 루트를 블랙홀 루트로 변경하고, 미리 설정된 시간, 예를 들어 10초 대기한 후 로케이터 루트를 삭제한다고 이해될 수 있다. 이런 식으로, VPN 루트의 다음 홉 VPN SID A1:1:3::B100을 사용함으로써 루트 다음 홉 반복이 수행될 때, 최장 마스크 매칭 규칙에 기반한 매칭을 통해 제3 루트, 예를 들어 A1:1:3::/64가 획득된다. 제3 루트의 아웃바운드 인터페이스는 null0 아웃바운드 인터페이스이다. 따라서 PE 디바이스(101)는 다음 홉 PE 디바이스(103)가 도달할 수 없는 것으로 간주하고, PE 디바이스(104)로의 다음 홉 전환을 트리거한다. 즉, PE 디바이스(104)의 VPN SID, 예를 들어 A1:1:4::B100을 사용함으로써 루트 다음 홉 반복이 수행된다. 반복이 성공한다면, 패킷이 포워딩될 때, 패킷, 예를 들어 CE 디바이스(105)로부터의 공통 IPv4 패킷이 목적지 어드레스로서 PE 디바이스(104)에 대응하는 VPN SID A1:1:4::B100을 갖는 SRv6 패킷으로 캡슐화된다. 이것은 패킷 손실률을 낮춘다.

[0084] 본 출원의 이 실시예의 구현에서, 제1 네트워크 디바이스는 제3 네트워크 디바이스로부터 제4 루트를 추가로 수신할 수 있다. 위에서 설명된 SRv6을 통한 L3VPN 듀얼 호밍 시나리오에서, CE 디바이스(106)와 같은 액세스 측 디바이스는 PE 디바이스(104)와 같은 제3 네트워크 디바이스와 PE 디바이스(103)와 같은 제2 네트워크 디바이스에 듀얼 호밍될 수 있다. 위에 도시된 FRR 시나리오에서, 제4 루트는 FRR 방법을 사용함으로써 결정된, 제3 루트의 백업 경로일 수 있다. 이런 식으로, 매칭을 통해 null0 아웃바운드 인터페이스를 획득한 후, 제1 네트워크 디바이스는 루트 다음 홉 전환을 추가로 수행할 수 있는데, 예를 들어 제3 네트워크 디바이스로의 루트 다음 홉 전환을 트리거할 수 있어, 패킷 포워딩 프로세스에서는, 제4 루트와 같은 다른 루트가 패킷 포워딩 경로를 결정하는 데 사용될 수 있으며, 이로써 패킷 포워딩 경로의 빠른 전환을 구현하여 패킷 손실률을 효과적으로 낮출 수 있다.

[0085] 앞서 말한 실시예에서 제공된 방법에 기초하여, 본 출원의 일 실시예는 대응하는 통신 장치를 추가로 제공한다. 다음은 첨부 도면을 참조하여 통신 장치를 설명한다.

[0086] 도 4는 본 출원의 일 실시예에 따른 통신 장치의 구조의 개략도이다.

[0087] 도 4에 도시된 통신 장치(400)는 앞서 말한 방법 실시예에서 제1 네트워크 디바이스에 의해 수행되는, 도 2에 도시된 통신 방법을 수행하도록 구성된다. 구체적으로, 통신 장치(400)는 예를 들어, 획득 유닛(401) 및 설정 유닛(402)을 포함할 수 있다.

[0088] 획득 유닛(401)은 제2 네트워크 디바이스로부터 제1 루트, 제2 루트 및 제3 루트를 획득하도록 구성된다. 제3 루트는 세그먼트 라우팅 인터넷 프로토콜 버전 6의 세그먼트 식별자(SRv6 SID)에 대응하는 네트워크 세그먼트 루트를 포함하고, 제3 루트에 대응하는 네트워크 세그먼트는 제1 루트에 대응하는 네트워크 세그먼트의 서브넷 세그먼트이며, 제3 루트에 대응하는 네트워크 세그먼트는 제2 루트에 대응하는 네트워크 세그먼트의 서브넷 세

그먼트이고, 제1 루트에 대응하는 네트워크 세그먼트는 제2 루트에 대응하는 네트워크 세그먼트의 서브넷 세그먼트이다.

- [0089] 설정 유닛(402)은 제1 루트의 아웃바운드 인터페이스를 null0 아웃바운드 인터페이스로 설정하도록 구성된다.
- [0090] 일 구현에서, 제3 루트는 루프백(loopback) 인터페이스 어드레스 루트를 더 포함한다.
- [0091] 일 구현에서, 장치(400)는:
- [0092] 제2 네트워크 디바이스로부터 제1 식별자를 수신하도록 구성된 제1 수신 유닛을 더 포함하고; 그리고
- [0093] 설정 유닛(402)은 구체적으로:
- [0094] 제1 식별자를 기초로 제1 루트의 아웃바운드 인터페이스를 null0 아웃바운드 인터페이스로 설정하도록 구성된다.
- [0095] 일 구현에서, 통신 장치(400)는 제1 네트워크 디바이스에 적용되며, 제1 네트워크 디바이스는 예를 들어, 도 2에 도시된 통신 방법을 수행하는 제1 네트워크 디바이스일 수 있다.
- [0096] 제1 네트워크 디바이스와 제2 네트워크 디바이스 모두에 가상 사설 네트워크(VPN) 인스턴스가 구성되고, 제1 네트워크 디바이스와 제2 네트워크 디바이스 간에 경계 게이트웨이 프로토콜(BGP) 피어 관계가 미리 설정되며, 제1 네트워크 디바이스와 제2 네트워크 디바이스 모두 세그먼트 라우팅 인터넷 프로토콜 버전 6(SRv6)을 지원한다.
- [0097] 일 구현에서, 통신 장치는 제1 네트워크 디바이스에 적용되며, 제1 네트워크 디바이스 및 제2 네트워크 디바이스는 제1 내부 게이트웨이 프로토콜(IGP) 도메인에 위치되고, 제2 IGP 도메인은 제1 IGP 도메인의 네트워크 디바이스를 포함하지 않으며, 제1 루트는 제2 IGP 도메인에 위치된 특정 루트를 포함하지 않는다.
- [0098] 일 구현에서, 획득 유닛(401)은 구체적으로:
- [0099] 중간 시스템 간(IS-IS) 프로토콜 또는 개방형 최단 경로 우선(OSPF) 프로토콜을 사용함으로써 제2 네트워크 디바이스에 의해 송신되는 제1 루트, 제2 루트 및 제3 루트를 수신하도록 구성된다.
- [0100] 일 구현에서, 장치(400)는:
- [0101] 제3 네트워크 디바이스로부터 제4 루트를 수신하도록 구성된 제2 수신 유닛을 더 포함하며,
- [0102] 액세스 측 디바이스는 제3 네트워크 디바이스와 제2 네트워크 디바이스로 듀얼 호밍되거나, 제4 루트는 고속 재라우트(FRR) 장치를 사용함으로써 결정된, 제3 루트의 백업 루트이다.
- [0103] 장치(400)는 앞서 말한 방법 실시예에서 제공되는, 도 2에 도시된 통신 방법에 대응하는 장치이므로, 장치(400)의 각각의 유닛의 특정 구현은 앞서 말한 방법 실시예의 개념과 동일한 개념에 속한다. 따라서 장치(400)의 각각의 유닛의 특정 구현에 대해서는, 앞서 말한 방법 실시예에서 도 2에 도시된 통신 방법의 설명 부분을 참조한다. 세부사항은 여기서 다시 설명되지 않는다.
- [0104] 도 5는 본 출원의 일 실시예에 따른 통신 장치의 구조의 개략도이다.
- [0105] 도 5에 도시된 통신 장치(500)는 앞서 말한 방법 실시예에서 제1 네트워크 디바이스에 의해 수행되는, 도 3에 도시된 통신 방법을 수행하도록 구성된다. 구체적으로, 통신 장치(500)는 예를 들어, 제1 획득 유닛(501), 설정 유닛(502) 및 삭제 유닛(503)을 포함할 수 있다.
- [0106] 제1 획득 유닛(501)은 제2 네트워크 디바이스로부터 제3 루트를 획득하도록 구성된다. 제3 루트는 세그먼트 라우팅 인터넷 프로토콜 버전 6의 세그먼트 식별자(SRv6 SID)에 대응하는 네트워크 세그먼트 루트를 포함한다.
- [0107] 설정 유닛(502)은: 제3 루트에 도달할 수 없다고 결정되면, 제3 루트의 아웃바운드 인터페이스를 null0 아웃바운드 인터페이스로 설정하도록 구성된다.
- [0108] 삭제 유닛(503)은 미리 설정된 시간을 대기한 후 제3 루트를 삭제하도록 구성된다.
- [0109] 일 구현에서, 제3 루트는 루프백(loopback) 인터페이스 어드레스 루트를 더 포함한다.
- [0110] 일 구현에서, 장치(500)는:
- [0111] 제2 네트워크 디바이스로부터 제2 루트를 획득하도록 구성된 제2 획득 유닛을 더 포함하며, 여기서 제3 루트에

대응하는 네트워크 세그먼트는 제2 루트에 대응하는 네트워크 세그먼트의 서브넷 세그먼트이다.

- [0112] 일 구현에서, 통신 장치는 제1 네트워크 디바이스에 적용되며, 제1 네트워크 디바이스는 예를 들어, 도 3에 도시된 통신 방법을 수행하는 제1 네트워크 디바이스일 수 있다. 제1 네트워크 디바이스와 제2 네트워크 디바이스 모두에 가상 사설 네트워크(VPN) 인스턴스가 구성되고, 제1 네트워크 디바이스와 제2 네트워크 디바이스 간에 경계 게이트웨이 프로토콜(BGP) 피어 관계가 미리 설정되며, 제1 네트워크 디바이스와 제2 네트워크 디바이스 모두 세그먼트 라우팅 인터넷 프로토콜 버전 6(SRv6)을 지원한다.
- [0113] 일 구현에서, 장치(500)는:
- [0114] 제3 네트워크 디바이스로부터 제4 루트를 수신하도록 구성된 수신 유닛을 더 포함하며,
- [0115] 액세스 측 디바이스는 제3 네트워크 디바이스와 제2 네트워크 디바이스로 듀얼 호밍되거나, 제4 루트는 고속 재라우트(FRR) 장치를 사용함으로써 결정된, 제3 루트의 백업 루트이다.
- [0116] 장치(500)는 앞서 말한 방법 실시예에서 제공되는, 도 3에 도시된 통신 방법에 대응하는 장치이므로, 장치(500)의 각각의 유닛의 특정 구현은 앞서 말한 방법 실시예의 개념과 동일한 개념에 속한다. 따라서 장치(500)의 각각의 유닛의 특정 구현에 대해서는, 앞서 말한 방법 실시예에서 도 3에 도시된 통신 방법의 설명 부분을 참조한다. 세부사항은 여기서 다시 설명되지 않는다.
- [0117] 본 출원의 일 실시예는 통신 디바이스를 추가로 제공한다. 이 디바이스는 프로세서 및 메모리를 포함한다. 메모리는 프로그램을 저장하도록 구성된다. 도 4 또는 도 5에 도시된 실시예가 구현되고, 도 4 또는 도 5에 도시된 실시예에서 설명된 유닛이 소프트웨어에 의해 구현될 때, 도 4 또는 도 5의 유닛의 기능을 수행하는데 필요한 소프트웨어 또는 프로그램 코드가 메모리에 저장된다. 프로세서는 메모리의 프로그램을 실행하여, 앞서 말한 방법 실시예에서 제공되고 제1 네트워크 디바이스에 의해 수행되는 통신 방법을 수행하도록, 예를 들어 앞서 말한 방법 실시예에서 제공되며 제1 네트워크 디바이스에 의해 수행되는, 도 2에 대응하는 통신 방법을 수행하거나, 다른 예의 경우, 앞서 말한 방법 실시예에서 제공되며 제1 네트워크 디바이스에 의해 수행되는, 도 3에 대응하는 통신 방법을 수행하도록 구성된다. 일부 실시예에서, 통신 디바이스는 도 1의 PE 디바이스(101)일 수 있다.
- [0118] 통신 디바이스의 하드웨어 구조는 도 6에 도시된 구조일 수 있다는 점이 주목되어야 한다. 도 6은 본 출원의 일 실시예에 따른 통신 디바이스의 개략적인 구조도이다.
- [0119] 도 6을 참조하면, 통신 디바이스(600)는 프로세서(610), 통신 인터페이스(620) 및 메모리(630)를 포함한다. 통신 디바이스(600)에는 하나 이상의 프로세서(610)가 있을 수 있다. 도 6에서는 하나의 프로세서가 일례로 사용된다. 본 출원의 이 실시예에서, 프로세서(610), 통신 인터페이스(620) 및 메모리(630)는 버스 시스템을 통해 또는 다른 방식으로 접속될 수 있다. 도 6에서는 프로세서(610), 통신 인터페이스(620) 및 메모리(630)가 버스 시스템(640)을 통해 접속되는 예가 사용된다.
- [0120] 프로세서(610)는 중앙 프로세싱 유닛(CPU: central processing unit), 네트워크 프로세서(NP: network processor), 또는 CPU와 NP의 조합일 수 있다. 프로세서(610)는 하드웨어 칩을 더 포함할 수 있다. 하드웨어 칩은 주문형 집적 회로(ASIC: application-specific integrated circuit), 프로그래밍 가능 로직 디바이스(PLD: programmable logic device), 또는 이들의 조합일 수 있다. PLD는 복합 프로그램 가능 로직 디바이스(CPLD: complex programmable logic device), 필드 프로그램 가능 게이트 어레이(FPGA: field-programmable gate array), 일반 어레이 로직(GAL: generic array logic), 또는 이들의 임의의 조합일 수 있다.
- [0121] 메모리(630)는 휘발성 메모리(volatile memory), 예를 들어 랜덤 액세스 메모리(RAM: random-access memory)를 포함할 수 있다. 메모리(630)는 대안으로 비휘발성 메모리(non-volatile memory), 예를 들어 플래시 메모리(flash memory), 하드 디스크 드라이브(HDD: hard disk drive) 또는 솔리드 스테이트 드라이브(SSD: solid-state drive)를 포함할 수 있다. 메모리(630)는 앞서 말한 타입의 메모리의 조합을 더 포함할 수 있다. 메모리(630)는 제1 루트, 제2 루트, 제3 루트 및 제4 루트를 저장하도록 구성될 수 있다.
- [0122] 선택적으로, 메모리(630)는 운영 체제 및 프로그램, 실행 가능 모듈, 또는 데이터 구조, 또는 이들의 서브세트, 또는 이들의 확장된 세트를 저장한다. 프로그램은 다양한 동작을 구현하는 데 사용되는 다양한 동작 프로그램을 포함할 수 있다. 운영 체제는 다양한 기본 서비스를 구현하고 하드웨어 기반 동작을 처리하기 위한 다양한 시스템 프로그램을 포함할 수 있다. 프로세서(610)는 본 출원의 앞서 말한 실시예에서 제공되는 통신 방법을 구현하도록 메모리(630)에서 프로그램을 관독할 수 있다.

- [0123] 버스 시스템(640)은 주변 컴포넌트 상호 접속(PCI: peripheral component interconnect) 버스, 확장된 산업 표준 아키텍처(EISA: extended industry standard architecture) 버스 등일 수 있다. 버스 시스템(640)은 어드레스 버스, 데이터 버스, 제어 버스 등으로 분류될 수 있다. 표현의 편의상, 도 6에서 버스를 표현하기 위해 굵은 선이 하나만 사용되지만, 이것이 단 하나의 버스만이 존재하거나 버스의 타입이 단 하나뿐임을 의미하는 것은 아니다.
- [0124] 특정 실시예에서, 프로세서(602)는 제2 네트워크 디바이스로부터 제1 루트, 제2 루트 및 제3 루트를 획득하고 - 제3 루트는 세그먼트 라우팅 인터넷 프로토콜 버전 6의 세그먼트 식별자(SRv6 SID)에 대응하는 네트워크 세그먼트 루트를 포함하고, 제3 루트에 대응하는 네트워크 세그먼트는 제1 루트에 대응하는 네트워크 세그먼트의 서브넷 세그먼트이며, 제3 루트에 대응하는 네트워크 세그먼트는 제2 루트에 대응하는 네트워크 세그먼트의 서브넷 세그먼트이고, 제1 루트에 대응하는 네트워크 세그먼트는 제2 루트에 대응하는 네트워크 세그먼트의 서브넷 세그먼트임 -; 그리고 제1 루트의 아웃바운드 인터페이스를 null0 아웃바운드 인터페이스로 설정하도록 구성된다. 프로세서(602)의 상세한 처리 프로세스에 대해서는, 도 2에 도시된 실시예의 상세한 설명을 참조한다. 세부사항은 여기서 다시 설명되지 않는다.
- [0125] 특정 실시예에서, 프로세서(602)는 제2 네트워크 디바이스로부터 제3 루트를 획득하고 - 제3 루트는 세그먼트 라우팅 인터넷 프로토콜 버전 6의 세그먼트 식별자(SRv6 SID)에 대응하는 네트워크 세그먼트 루트를 포함함 -; 제3 루트에 도달할 수 없다고 결정되면, 제3 루트의 아웃바운드 인터페이스를 null0 아웃바운드 인터페이스로 설정하고; 그리고 미리 설정된 시간을 대기한 후 제3 루트를 삭제하도록 구성된다. 프로세서(602)의 상세한 처리 프로세스에 대해서는, 도 3에 도시된 실시예의 상세한 설명을 참조한다. 세부사항은 여기서 다시 설명되지 않는다.
- [0126] 본 출원의 일 실시예는 프로그램을 포함하는 컴퓨터 판독 가능 저장 매체를 추가로 제공한다. 컴퓨터 상에서 프로그램이 실행될 때, 컴퓨터는 앞서 말한 방법 실시예에서 제공되고 제1 네트워크 디바이스에 의해 수행되는 통신 방법을 수행하는, 예를 들어 앞서 말한 방법 실시예에서 제공되는, 도 2에 대응하는 통신 방법을 수행하거나, 다른 예의 경우, 앞서 말한 방법 실시예에서 제공되는, 도 3에 대응하는 통신 방법을 수행하는 것이 가능해진다.
- [0127] 본 출원의 일 실시예는 프로그램을 포함하는 컴퓨터 프로그램 제품을 추가로 제공한다. 컴퓨터 상에서 프로그램이 실행될 때, 컴퓨터는 앞서 말한 방법 실시예에서 제공되고 제1 네트워크 디바이스에 의해 수행되는 통신 방법을 수행하는, 예를 들어 앞서 말한 방법 실시예에서 제공되는, 도 2에 대응하는 통신 방법을 수행하거나, 다른 예의 경우, 앞서 말한 방법 실시예에서 제공되는, 도 3에 대응하는 통신 방법을 수행하는 것이 가능해진다.
- [0128] 본 출원의 명세서, 청구항들 및 첨부 도면들에서, "제1", "제2", "제3", "제4" 등(존재한다면)의 용어는 유사한 객체들 간에 구별하는 것으로 의도되지만, 반드시 특정 순서 또는 시퀀스를 지시하는 것은 아니다. 그러한 방식으로 지칭되는 데이터는, 본 명세서에서 설명되는 실시예가 본 명세서에서 예시 또는 설명되는 순서 이외의 다른 순서로 구현될 수 있도록, 적절한 상황에서 교환 가능하다고 이해되어야 한다. 더욱이, "포함하다", "함유하다"라는 용어 및 임의의 다른 변형은 배타적이지 않은 포함을 커버하는 것을 의미하는데, 예를 들어 단계 또는 유닛의 리스트를 포함하는 프로세스, 방법, 시스템, 제품 또는 디바이스가 반드시 그러한 명백하게 나열된 단계 또는 유닛으로 제한되는 것이 아니라, 그러한 프로세스, 방법, 시스템, 제품 또는 디바이스에 고유하거나 명백하게 나열되지 않은 다른 단계 또는 유닛을 포함할 수 있다.
- [0129] 편리하고 간단한 설명의 목적으로, 앞서 언급한 시스템, 장치 및 유닛의 상세한 작동 프로세스를 위해, 앞서 언급한 방법 실시예의 대응하는 프로세서를 참조하며, 세부사항은 본 명세서에서 다시 설명되지 않는다고 당해 기술분야에서 통상의 지식을 가진 자에 의해 명백히 이해될 수 있다.
- [0130] 본 출원에서 제공되는 여러 실시예에서, 개시된 시스템, 장치 및 방법은 다른 방식으로 구현될 수 있다고 이해되어야 한다. 예를 들어, 설명된 장치 실시예는 단지 예일 뿐이다. 예를 들어, 유닛으로의 분할은 단지 논리적 서비스 분할일 뿐이며, 실제 구현에서는 다른 분할일 수 있다. 예를 들어, 복수의 유닛 또는 컴포넌트가 다른 시스템에 조합 또는 통합될 수 있거나, 일부 특징이 무시되거나 수행되지 않을 수 있다. 추가로, 표시 또는 논의된 상호 결합 또는 직접 결합 또는 통신 접속은 일부 인터페이스를 통해 구현될 수 있다. 장치 또는 유닛 간의 간접 결합 또는 통신 접속은 전기, 기계 또는 다른 형태로 구현될 수 있다.
- [0131] 개별 부분으로서 설명된 유닛은 물리적으로 분리될 수 있거나 분리되지 않을 수 있고, 유닛으로서 디스플레이된

부분은 물리적 유닛일 수 있거나 물리적 유닛이 아닐 수 있는데, 즉 하나의 위치에 위치될 수 있거나, 복수의 네트워크 유닛 상에 분배될 수 있다. 유닛 중 일부 또는 전부는 실시예의 솔루션의 목적을 달성하도록 실제 요건에 기초하여 선택될 수 있다.

[0132] 추가로, 본 출원의 실시예의 서비스 유닛이 하나의 프로세싱 유닛에 통합될 수 있거나, 유닛 각각이 물리적으로 단독으로 존재할 수 있거나, 2개 이상의 유닛이 하나의 유닛으로 통합될 수 있다. 통합 유닛은 하드웨어 형태로 구현될 수 있거나, 소프트웨어 서비스 유닛 형태로 구현될 수 있다.

[0133] 통합 유닛이 소프트웨어 서비스 유닛 형태로 구현되어 독립 제품으로서 판매되거나 사용될 때, 통합 유닛은 컴퓨터 판독 가능 저장 매체에 저장될 수 있다. 이러한 이해를 바탕으로, 본질적으로 본 출원의 기술적 솔루션, 또는 종래 기술에 기여하는 부분, 또는 기술적 솔루션의 전부 또는 일부는 소프트웨어 제품의 형태로 구현될 수 있다. 컴퓨터 소프트웨어 제품은 저장 매체에 저장되고, 본 출원의 실시예에서 설명되는 방법의 단계의 전부 또는 일부를 수행하도록 (개인용 컴퓨터, 서버, 네트워크 디바이스 등일 수 있는) 컴퓨터 디바이스에 명령하기 위한 여러 명령을 포함한다. 앞서 언급한 저장 매체는: USB 플래시 드라이브, 착탈식 하드 디스크, 판독 전용 메모리(ROM: Read-Only Memory), 랜덤 액세스 메모리(RAM: Random Access Memory), 자기 디스크 또는 광 디스크와 같이 프로그램 코드를 저장할 수 있는 임의의 매체를 포함한다.

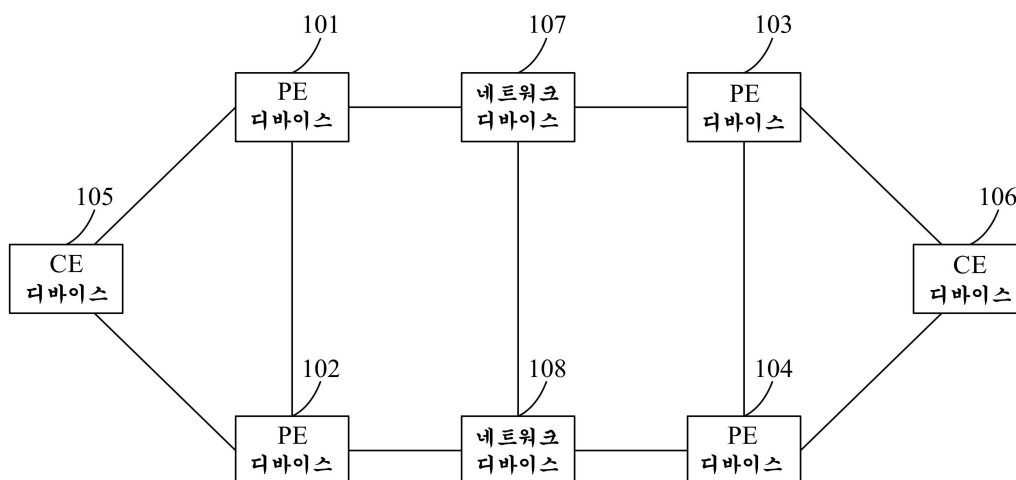
[0134] 당해 기술분야에서 통상의 지식을 가진 자는 앞서 말한 하나 이상의 예에서, 본 발명에서 설명된 서비스가 하드웨어, 소프트웨어, 펌웨어, 또는 이들의 임의의 조합에 의해 구현될 수 있다고 인식할 것이다. 서비스가 소프트웨어에 의해 구현되는 경우, 서비스는 컴퓨터 판독 가능 매체에 저장되거나 컴퓨터 판독 가능 매체에서 하나 이상의 프로그램 또는 코드로서 전송될 수 있다. 컴퓨터 판독 가능 매체는 컴퓨터 저장 매체 및 통신 매체를 포함하며, 여기서 통신 매체는 컴퓨터 프로그램이 한 장소에서 다른 장소로 전송될 수 있게 하는 임의의 매체를 포함한다. 저장 매체는 범용 또는 특수 목적 컴퓨터에 액세스 가능한 임의의 이용 가능한 매체일 수 있다.

[0135] 앞서 말한 특정 구현에서, 본 발명의 목적, 기술적 솔루션 및 이점이 추가로 상세히 설명된다. 앞서 말한 설명은 단지 본 발명의 특정 구현이라고 이해되어야 한다.

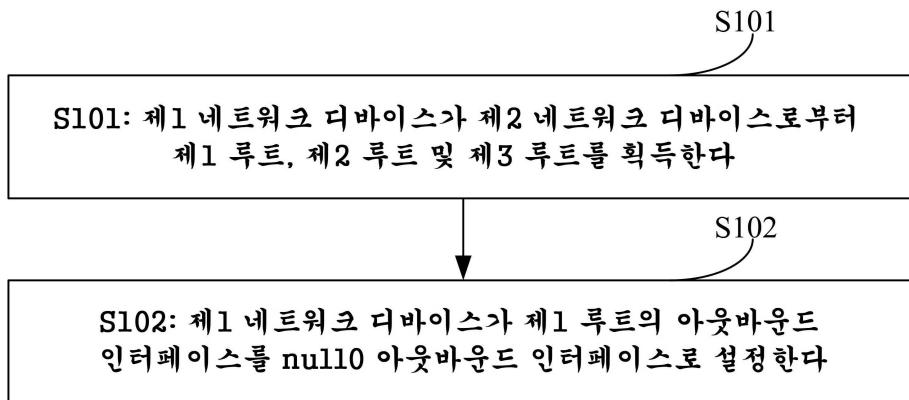
[0136] 앞서 말한 실시예는 단지 본 출원의 기술적 솔루션을 설명하기 위한 것일 뿐, 본 출원을 제한하는 것으로 의도되는 것은 아니다. 본 출원은 앞서 말한 실시예를 참조하여 상세히 설명되지만, 당해 기술분야에서 통상의 지식을 가진 자는 본 출원의 실시예의 기술적 솔루션의 범위를 벗어나지 않으면서, 이들이 여전히 앞서 말한 실시예에서 설명된 기술적 솔루션을 수정하거나 이들의 일부 기술적 특징에 대해 동등한 대체를 행할 수 있다고 이해해야 한다.

**도면**

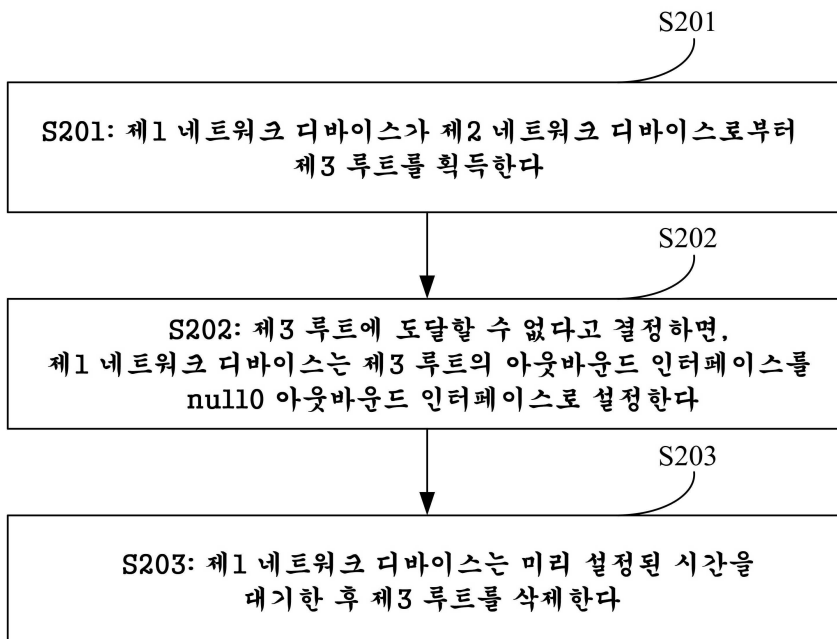
**도면1**



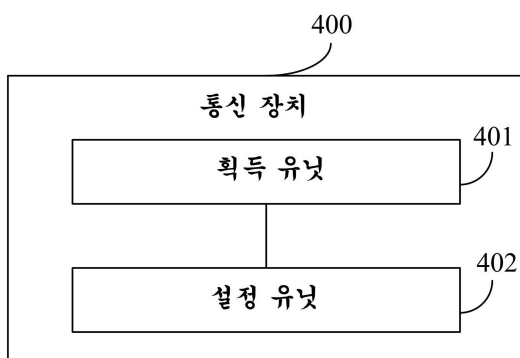
도면2



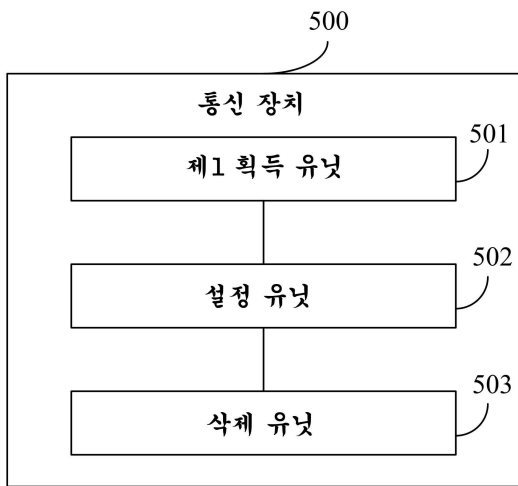
도면3



도면4



도면5



도면6

