(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2022-0142524
(43) 공개일자 2022년10월21일

(51) 국제특허분류(Int. Cl.)
H04L 45/00 (2022.01) *H04L 43/0811* (2022.01)
H04L 43/10 (2022.01) *H04L 45/28* (2022.01)
(52) CPC특허분류
H04L 45/22 (2022.05)
H04L 43/0811 (2022.05)
(21) 출원번호 10-2022-7032798
(22) 출원일자(국제) 2021년02월26일
심사청구일자 2022년09월21일
(85) 번역문제출일자 2022년09월21일
(86) 국제출원번호 PCT/CN2021/078184
(87) 국제공개번호 WO 2021/170092
국제공개일자 2021년09월02일
(30) 우선권주장
202010119485.1 2020년02월26일 중국(CN)

(71) 출원인
후아웨이 테크놀러지 컴퍼니 리미티드
중국 518129 광동성 센젠 롱강 디스트릭트 반티안 후아웨이 어드미니스트레이션 빌딩
(72) 발명자
시아오 야쿤
중국 518129 광동성 센젠 롱강 디스트릭트 반티안 후아웨이 어드미니스트레이션 빌딩
판 리
중국 518129 광동성 센젠 롱강 디스트릭트 반티안 후아웨이 어드미니스트레이션 빌딩
(74) 대리인
제일특허법인(유)

전체 청구항 수 : 총 28 항

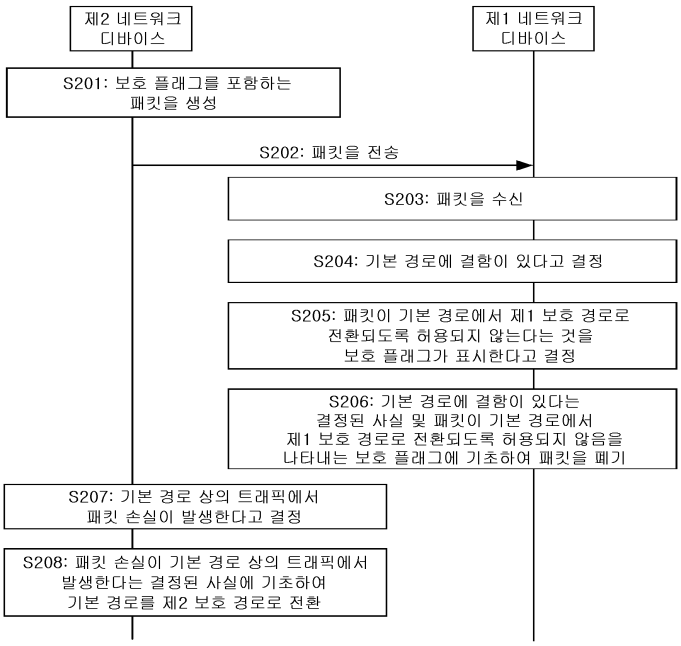
(54) 발명의 명칭 **패킷 처리 방법 및 장치, 네트워크 디바이스 및 저장 매체**

(57) 요 약

통신 기술 분야에 속하는 메시지 처리 방법 및 장치, 네트워크 디바이스 및 저장 매체가 제공된다. 본 출원에서, 로컬 보호가 허용되는지 여부를 나타낼 수 있는 식별자가 메시지에 추가되고, 보호 식별자를 전달하는 메시지가 주 경로를 따라 전송되는 과정 동안, 경로를 따른 노드가 주 경로에 결함이 있다고 결정하고, 보호 식별자가 지

(뒷면에 계속)

대 표 도 - 도7



역성이 보호 경로로 전환되도록 허용되지 않음을 나타내는 경우, 경로를 따른 노드는 로컬 보호를 수행하지 않으므로, 메시지는 경로를 따른 노드에서 보호 경로로 전환되지 않아서, 메시지가 주 경로에 결함이 있을 때 입구로서 경로를 따른 노드를 이용하는 보호 경로로 이동하지 않는 효과를 달성하며, 이는 주 경로 상의 스트림을 적시에 종단 간 보호 경로로 전환하는 것을 용이하게 하고, 메시지의 송신 측이 주 경로 상의 스트림을 적시에 종단 간 보호 경로로 전환하는 것을 용이하게 하며, 메시지의 송신 측이 서비스에 대한 손상과 주 경로의 결함 원인을 적시에 찾는 것을 용이하게 한다.

(52) CPC특허분류
H04L 43/10 (2022.05)
H04L 45/28 (2022.05)

명 세 서

청구범위

청구항 1

패킷 처리 방법으로서,

제1 네트워크 디바이스에 의해, 패킷을 수신하는 단계 - 상기 패킷은 보호 플래그를 포함하고, 상기 보호 플래그는 상기 제1 네트워크 디바이스가 상기 패킷을 기본 경로에서 제1 보호 경로로 전환하도록 허용되는지 여부를 나타내는 데 사용되며, 상기 제1 보호 경로는 상기 기본 경로를 보호하는 데 사용되고, 상기 제1 보호 경로 상의 인그레스 노드(ingress node)는 상기 제1 네트워크 디바이스임 - 와,

상기 제1 네트워크 디바이스에 의해, 상기 기본 경로에 결함이 있다고 결정하는 단계와,

상기 보호 플래그가 상기 패킷이 상기 기본 경로에서 상기 제1 보호 경로로 전환되도록 허용되지 않음을 나타내는 경우, 상기 제1 네트워크 디바이스에 의해, 상기 기본 경로에 결함이 있다는 결정된 사실 및 상기 패킷이 상기 기본 경로에서 상기 제1 보호 경로로 전환되도록 허용되지 않음을 나타내는 상기 보호 플래그에 기초하여 상기 패킷을 폐기하는 단계를 포함하는

패킷 처리 방법.

청구항 2

제1항에 있어서,

상기 기본 경로에서 제2 보호 경로로 전환하기 위한 트리거 조건은 상기 기본 경로 상의 트래픽에서 패킷 손실이 검출되는 것이고, 상기 제2 보호 경로는 상기 기본 경로를 보호하기 위한 백업 경로이며, 상기 제2 보호 경로는 상기 기본 경로와 동일한 인그레스 노드를 갖는

패킷 처리 방법.

청구항 3

제1항 또는 제2항에 있어서,

상기 패킷은 세그먼트 라우팅(SR) 패킷이고, 상기 제1 네트워크 디바이스에 의해, 상기 기본 경로에 결함이 있다고 결정하는 단계는,

상기 패킷의 세그먼트 식별자(SID)에 기초하여 상기 제1 네트워크 디바이스에 의해, 상기 SID에 대응하는 아웃바운드 인터페이스 또는 다음 홉을 결정하는 단계와,

상기 아웃바운드 인터페이스 또는 상기 다음 홉에 결함이 있는 경우, 상기 제1 네트워크 디바이스에 의해, 상기 기본 경로에 결함이 있다고 결정하는 단계를 포함하는

패킷 처리 방법.

청구항 4

제1항 내지 제3항 중 어느 한 항에 있어서,

상기 패킷은 세그먼트 라우팅 오버 인터넷 프로토콜 버전 6(SRv6) 패킷이고, 상기 SRv6 패킷은 세그먼트 라우팅 헤더(SRH)를 포함하며, 상기 보호 플래그는 상기 SRH에 있는

패킷 처리 방법.

청구항 5

제4항에 있어서,

상기 보호 플래그가 상기 SRH에 있는 것은,

상기 보호 플래그가 상기 SRH의 플래그 필드에 있거나, 또는

상기 보호 플래그가 상기 SRH의 유형-길이-값(TLV)에 있는 것을 포함하는

패킷 처리 방법.

청구항 6

제1항 내지 제5항 중 어느 한 항에 있어서,

상기 방법은, 상기 보호 플래그가 상기 패킷이 상기 기본 경로에서 상기 제1 보호 경로로 전환되도록 허용됨을 나타내는 경우 상기 제1 네트워크 디바이스에 의해, 상기 기본 경로에 결함이 있다는 결정된 사실 및 상기 패킷이 상기 기본 경로에서 상기 제1 보호 경로로 전환되도록 허용됨을 나타내는 상기 보호 플래그에 기초하여 상기 제1 보호 경로를 통해 상기 패킷을 전송하는 단계를 더 포함하는

패킷 처리 방법.

청구항 7

제6항에 있어서,

상기 보호 플래그가 상기 패킷이 상기 기본 경로에서 상기 제1 보호 경로로 전환되도록 허용됨을 나타내는 경우 상기 제1 네트워크 디바이스에 의해, 상기 기본 경로에 결함이 있다는 결정된 사실 및 상기 패킷이 상기 기본 경로에서 상기 제1 보호 경로로 전환되도록 허용됨을 나타내는 상기 보호 플래그에 기초하여 상기 제1 보호 경로를 통해 상기 패킷을 전송하는 단계는,

상기 보호 플래그가 상기 패킷이 중간점(Midpoint) TI-LFA 경로로 전환되도록 허용되지만 토폴로지 독립 루프 프리 대체 고속 리라우트(TI-LFA FRR) 경로로 전환되도록 허용되지 않음을 나타내는 경우, 상기 제1 네트워크 디바이스에 의해, 상기 기본 경로에 결함이 있다는 결정된 사실 및 상기 패킷이 상기 중간점 TI-LFA 경로로 전환되도록 허용되지만 상기 TI-LFA FRR 경로로 전환되도록 허용되지 않음을 나타내는 상기 보호 플래그에 기초하여 상기 중간점 TI-LFA 경로를 통해 상기 패킷을 전송하는 단계를 포함하는

패킷 처리 방법.

청구항 8

제6항에 있어서,

상기 보호 플래그가 상기 패킷이 상기 기본 경로에서 상기 제1 보호 경로로 전환되도록 허용됨을 나타내는 경우 상기 제1 네트워크 디바이스에 의해, 상기 기본 경로에 결함이 있다는 결정된 사실 및 상기 패킷이 상기 기본 경로에서 상기 제1 보호 경로로 전환되도록 허용됨을 나타내는 상기 보호 플래그에 기초하여 상기 제1 보호 경로를 통해 상기 패킷을 전송하는 단계는,

상기 보호 플래그가 상기 패킷이 TI-LFA FRR 경로로 전환되도록 허용되지만 중간점 TI-LFA 경로로 전환되도록 허용되지 않음을 나타내는 경우, 상기 제1 네트워크 디바이스에 의해, 상기 기본 경로에 결함이 있다는 결정된 사실 및 상기 패킷이 상기 TI-LFA FRR 경로로 전환되도록 허용되지만 상기 중간점 TI-LFA 경로로 전환되도록 허용되지 않음을 나타내는 상기 보호 플래그에 기초하여 상기 TI-LFA FRR 경로를 통해 상기 패킷을 전송하는 단계

를 포함하는

패킷 처리 방법.

청구항 9

제1항 내지 제6항 중 어느 한 항에 있어서,

상기 보호 플래그는 상기 패킷의 제1 비트를 점유하고, 상기 제1 비트가 설정되면, 상기 패킷이 상기 기본 경로에서 상기 제1 보호 경로로 전환되도록 허용되지 않음을 나타내거나, 또는 상기 제1 비트가 설정되지 않으면, 상기 패킷이 상기 기본 경로에서 상기 제1 보호 경로로 전환되도록 허용됨을 나타내는

패킷 처리 방법.

청구항 10

제7항 또는 제8항에 있어서,

상기 보호 플래그는 상기 패킷의 제2 비트 및 제3 비트를 점유하고, 상기 제2 비트와 상기 제3 비트가 모두 설정되면, 상기 패킷이 상기 기본 경로에서 상기 중간점 TI-LFA 경로 또는 상기 TI-LFA FRR 경로로 전환되도록 허용되지 않음을 나타내거나, 상기 제2 비트가 설정되고 상기 제3 비트가 설정되지 않으면, 상기 패킷이 상기 중간점 TI-LFA 경로로 전환되도록 허용되지 않지만 상기 TI-LFA FRR 경로로 전환되도록 허용됨을 나타내거나, 상기 제2 비트가 설정되지 않고 상기 제3 비트가 설정되면, 상기 패킷이 상기 중간점 TI-LFA 경로로 전환되도록 허용되지만 상기 TI-LFA FRR 경로로 전환되도록 허용되지 않음을 나타내거나, 또는 상기 제2 비트도 상기 제3 비트도 설정되지 않으면, 상기 패킷이 상기 기본 경로에서 상기 중간점 TI-LFA 경로 또는 상기 TI-LFA FRR 경로로 전환되도록 허용됨을 나타내는

패킷 처리 방법.

청구항 11

제1항 내지 제10항 중 어느 한 항에 있어서,

상기 패킷은 데이터 패킷을 포함하고, 상기 데이터 패킷은 상기 기본 경로의 서비스 데이터를 전달하는 데 사용되거나, 또는

상기 패킷은 검출 패킷을 포함하고, 상기 검출 패킷은 상기 기본 경로의 연결성 또는 전송 성능 파라미터 중 적어도 하나를 검출하는 데 사용되는

패킷 처리 방법.

청구항 12

제11항에 있어서,

상기 패킷이 검출 패킷을 포함하는 경우,

상기 검출 패킷은 양방향 포워딩 검출(BFD) 패킷이거나, 또는

상기 검출 패킷은 패킷 인터넷 그로퍼(PING) 검출 패킷이거나, 또는

상기 검출 패킷은 운영, 관리 및 유지보수(OAM) 검출 패킷이거나, 또는

상기 검출 패킷은 양방향 능동 측정 프로토콜(TWAMP) 검출 패킷이거나, 또는

상기 검출 패킷은 인터넷 프로토콜 데이터 흐름 기반 채널 관련 OAM 성능 측정(IFIT) 패킷인

패킷 처리 방법.

청구항 13

패킷 처리 방법으로서,

제2 네트워크 디바이스에 의해, 패킷을 생성하는 단계 - 상기 패킷은 보호 플래그를 포함하고, 상기 보호 플래그는 상기 제1 네트워크 디바이스가 상기 패킷을 기본 경로에서 제1 보호 경로로 전환하도록 허용되는지 여부를 나타내는 데 사용되며, 상기 제1 보호 경로는 상기 기본 경로를 보호하는 데 사용되고, 상기 제1 보호 경로 상의 인그레스 노드는 상기 제1 네트워크 디바이스임 - 와,

상기 제2 네트워크 디바이스에 의해, 상기 패킷을 상기 제1 네트워크 디바이스로 전송하는 단계를 포함하는

패킷 처리 방법.

청구항 14

제13항에 있어서,

상기 제2 네트워크 디바이스에 의해, 상기 패킷을 상기 제1 네트워크 디바이스로 전송하는 단계 이후에, 상기 방법은,

상기 제2 네트워크 디바이스에 의해, 상기 기본 경로 상의 트래픽에서 패킷 손실이 발생한다고 결정하는 단계와,

상기 제2 네트워크 디바이스에 의해, 상기 기본 경로 상의 트래픽에서 상기 패킷 손실이 발생한다는 결정된 사실에 기초하여 상기 기본 경로를 제2 보호 경로로 전환하는 단계 - 상기 제2 보호 경로는 상기 기본 경로를 보호하기 위한 백업 경로이고, 상기 제2 보호 경로는 상기 기본 경로와 동일한 인그레스 노드를 가짐 - 를 더 포함하는

패킷 처리 방법.

청구항 15

제13항 또는 제14항에 있어서,

상기 패킷은 세그먼트 라우팅 오버 인터넷 프로토콜 버전 6(SRv6) 패킷이고, 상기 SRv6 패킷은 세그먼트 라우팅 헤더(SRH)를 포함하며, 상기 보호 플래그는 상기 SRH에 있는

패킷 처리 방법.

청구항 16

제15항에 있어서,

상기 보호 플래그가 상기 SRH에 있는 것은,

상기 보호 플래그가 상기 SRH의 플래그 필드에 있거나, 또는

상기 보호 플래그가 상기 SRH의 유형-길이-값(TLV)에 있는 것을 포함하는

패킷 처리 방법.

청구항 17

제13항 내지 제16항 중 어느 한 항에 있어서,

상기 보호 플래그는 상기 패킷의 제1 비트를 점유하고, 상기 제1 비트가 설정되면, 상기 패킷이 상기 기본 경로에서 상기 제1 보호 경로로 전환되도록 허용되지 않음을 나타내거나, 또는 상기 제1 비트가 설정되지 않으면, 상기 패킷이 상기 기본 경로에서 상기 제1 보호 경로로 전환되도록 허용됨을 나타내거나, 또는

상기 보호 플래그는 상기 패킷의 제2 비트 및 제3 비트를 점유하고, 상기 제2 비트와 상기 제3 비트가 모두 설정되면, 상기 패킷이 상기 기본 경로에서 중간점 TI-LFA 경로 및 TI-LFA FRR 경로로 전환되도록 허용되지 않음을 나타내거나, 상기 제2 비트가 설정되고 상기 제3 비트가 설정되지 않으면, 상기 패킷이 중간점 TI-LFA 경로로 전환되도록 허용되지 않지만 TI-LFA FRR 경로로 전환되도록 허용됨을 나타내거나, 상기 제2 비트가 설정되지 않고 상기 제3 비트가 설정되면, 상기 패킷이 중간점 TI-LFA 경로로 전환되도록 허용되지만 TI-LFA FRR 경로로 전환되도록 허용되지 않음을 나타내거나, 또는 상기 제2 비트도 상기 제3 비트도 설정되지 않으면, 상기 패킷이 상기 기본 경로에서 중간점 TI-LFA 경로 또는 TI-LFA FRR 경로로 전환되도록 허용됨을 나타내는

패킷 처리 방법.

청구항 18

제13항 내지 제17항 중 어느 한 항에 있어서,

상기 패킷은 데이터 패킷을 포함하고, 상기 데이터 패킷은 상기 기본 경로의 서비스 데이터를 전달하는 데 사용되거나, 또는

상기 패킷은 검출 패킷을 포함하고, 상기 검출 패킷은 상기 기본 경로의 연결성 또는 전송 성능 파라미터 중 적어도 하나를 검출하는 데 사용되는

패킷 처리 방법.

청구항 19

제18항에 있어서,

상기 패킷이 검출 패킷을 포함하는 경우,

상기 검출 패킷은 양방향 포워딩 검출(BFD) 패킷이거나, 또는

상기 검출 패킷은 패킷 인터넷 그로퍼(PING) 검출 패킷이거나, 또는

상기 검출 패킷은 운영, 관리 및 유지보수(OAM) 검출 패킷이거나, 또는

상기 검출 패킷은 양방향 능동 측정 프로토콜(TWAMP) 검출 패킷이거나, 또는

상기 검출 패킷은 인터넷 프로토콜 데이터 흐름 기반 채널 관련 OAM 성능 측정(IFIT) 패킷인

패킷 처리 방법.

청구항 20

패킷 처리 장치로서,

패킷을 수신하도록 구성된 수신 모듈 - 상기 패킷은 보호 플래그를 포함하고, 상기 보호 플래그는 제1 네트워크 디바이스가 상기 패킷을 기본 경로에서 제1 보호 경로로 전환하도록 허용되는지 여부를 나타내는 데 사용되며, 상기 제1 보호 경로는 상기 기본 경로를 보호하는 데 사용되고, 상기 제1 보호 경로 상의 인그레스 노드는 상기 제1 네트워크 디바이스임 - 과,

상기 기본 경로에 결함이 있다고 결정하도록 구성된 결정 모듈과,

상기 보호 플래그가 상기 패킷이 상기 기본 경로에서 상기 제1 보호 경로로 전환되도록 허용되지 않음을 나타내

는 경우, 상기 기본 경로에 결함이 있다는 결정된 사실 및 상기 패킷이 상기 기본 경로에서 상기 제1 보호 경로로 전환되도록 허용되지 않음을 나타내는 상기 보호 플래그에 기초하여 상기 패킷을 폐기하도록 구성된 폐기 모듈을 포함하는

패킷 처리 장치.

청구항 21

제20항에 있어서,

상기 기본 경로에서 제2 보호 경로로 전환하기 위한 트리거 조건은 상기 기본 경로 상의 트래픽에서 패킷 손실이 검출되는 것이고, 상기 제2 보호 경로는 상기 기본 경로를 보호하기 위한 백업 경로이며, 상기 제2 보호 경로는 상기 기본 경로와 동일한 인그레스 노드를 갖는

패킷 처리 장치.

청구항 22

제20항 또는 제21항에 있어서,

상기 장치는, 상기 보호 플래그가 상기 패킷이 상기 기본 경로에서 상기 제1 보호 경로로 전환되도록 허용됨을 나타내는 경우, 상기 기본 경로에 결함이 있다는 결정된 사실 및 상기 패킷이 상기 기본 경로에서 상기 제1 보호 경로로 전환되도록 허용됨을 나타내는 상기 보호 플래그에 기초하여 상기 제1 보호 경로를 통해 상기 패킷을 전송하도록 구성된 전송 모듈을 더 포함하는

패킷 처리 장치.

청구항 23

제22항에 있어서,

상기 전송 모듈은, 상기 보호 플래그가 상기 패킷이 중간점(Midpoint) TI-LFA 경로로 전환되도록 허용되지만 토폴로지 독립 루프 프리 대체 고속 리라우트(TI-LFA FRR) 경로로 전환되도록 허용되지 않음을 나타내는 경우, 상기 기본 경로에 결함이 있다는 결정된 사실 및 상기 패킷이 상기 중간점 TI-LFA 경로로 전환되도록 허용되지만 상기 TI-LFA FRR 경로로 전환되도록 허용되지 않음을 나타내는 상기 보호 플래그에 기초하여 상기 중간점 TI-LFA 경로를 통해 상기 패킷을 전송하도록 구성되는

패킷 처리 장치.

청구항 24

제22항에 있어서,

상기 전송 모듈은, 상기 보호 플래그가 상기 패킷이 TI-LFA FRR 경로로 전환되도록 허용되지만 중간점 TI-LFA 경로로 전환되도록 허용되지 않음을 나타내는 경우, 상기 기본 경로에 결함이 있다는 결정된 사실 및 상기 패킷이 상기 TI-LFA FRR 경로로 전환되도록 허용되지만 상기 중간점 TI-LFA 경로로 전환되도록 허용되지 않음을 나타내는 상기 보호 플래그에 기초하여 상기 TI-LFA FRR 경로를 통해 상기 패킷을 전송하도록 구성되는

패킷 처리 장치.

청구항 25

패킷 처리 장치로서,

상기 장치는,

패킷을 생성하도록 구성된 생성 모듈 - 상기 패킷은 보호 플래그를 포함하고, 상기 보호 플래그는 제1 네트워크 디바이스가 상기 패킷을 기본 경로에서 제1 보호 경로로 전환하도록 허용되는지 여부를 나타내는 데 사용되며, 상기 제1 보호 경로는 상기 기본 경로를 보호하는 데 사용되고, 상기 제1 보호 경로 상의 인그레스 노드는 상기 제1 네트워크 디바이스임 - 과,

상기 패킷을 상기 제1 네트워크 디바이스로 전송하도록 구성된 전송 모듈을 포함하는

패킷 처리 장치.

청구항 26

제25항에 있어서,

상기 장치는,

상기 기본 경로 상의 트래픽에서 패킷 손실이 발생한다고 결정하도록 구성된 결정 모듈과,

상기 기본 경로 상의 트래픽에서 상기 패킷 손실이 발생한다는 결정된 사실에 기초하여 상기 기본 경로를 제2 보호 경로로 전환하도록 구성된 전환 모듈을 더 포함하는

패킷 처리 장치.

청구항 27

네트워크 디바이스로서,

프로세서를 포함하되,

상기 프로세서는 명령어를 실행하여 상기 네트워크 디바이스가 제1항 내지 제19항 중 어느 한 항에 따른 방법을 수행하도록 구성되는

네트워크 디바이스.

청구항 28

적어도 하나의 명령어를 저장하는 컴퓨터 판독가능 저장 매체로서,

상기 명령어는 프로세서에 의해 판독되어 네트워크 디바이스가 제1항 내지 제19항 중 어느 한 항에 따른 방법을 수행하도록 하는

컴퓨터 판독가능 저장 매체.

발명의 설명

기 술 분 야

[0001] 본 출원은 "패킷 처리 방법 및 장치, 네트워크 디바이스 및 저장 매체"라는 명칭으로 2020년 2월 26일에 출원된 중국 특허 출원 제202010119485.1호에 대한 우선권을 주장하며, 이는 그 전체가 본 명세서에 참조로 포함된다.

[0002] 본 출원은 통신 기술 분야에 관한 것으로, 특히, 패킷 처리 방법 및 장치, 네트워크 디바이스 및 저장 매체에 관한 것이다.

배 경 기 술

[0003] 네트워크의 신뢰성을 보장하기 위해, 일반적으로 보호 메커니즘이 네트워크에 사전 배치된다. 따라서, 현재 작업 경로의 노드 또는 링크에 결함이 발생한 후, 트래픽은 결함이 없는 다른 경로로 전환될 수 있다. 보호 메커

니즘은 종단 간 보호 메커니즘과 로컬 보호 메커니즘을 포함한다. 종단 간 보호 메커니즘은 전역 보호 메커니즘이다. 종단 간 기본 경로와 종단 간 보호 경로는 네트워크에 미리 계획되어 있다. 기본 경로의 헤드 노드가 기본 경로에 결함이 있음을 검출하면, 헤드 노드는 기본 경로의 트래픽을 종단 간 보호 경로로 전환하여 전송한다. 로컬 보호 메커니즘은 지역성 보호 메커니즘이다. 기본 경로의 중간 노드(transit node)가 기본 경로에 결함이 있음을 검출하면, 중간 노드는 로컬로 패킷을 보호 경로로 전환하여 패킷이 중간 노드에서 보호 경로로 들어가도록 한다.

[0004] 현재, 종단 간 보호 메커니즘과 로컬 보호 메커니즘은 일반적으로 네트워크 상에 공존한다. 구체적으로, 종단 간 기본 경로와 종단 간 백업 경로가 네트워크에 계획될 뿐만 아니라 기본 경로의 각 중간 노드에서 로컬 보호 메커니즘이 가능해진다. 이 시나리오에서, 중간 노드가 기본 경로에 결함이 있음을 검출하면, 중간 노드는 연속 전송을 위한 로컬 보호 메커니즘을 기반으로 로컬로 기본 경로의 트래픽을 보호 경로로 우선적으로 전환한다. 일반적으로, 기본 경로와 종단 간 보호 경로는 서비스 수준 계약(Service Level Agreement, SLA) 요구사항을 충족하며, 중간 노드가 전환을 수행하는 보호 경로는 경로 연결만 보장할 수 있고, SLA 요구사항을 충족할 수는 없다. 그러나, 전술한 방법을 이용하여, 중간 노드가 기본 경로 상의 패킷(예를 들어, 양방향 포워딩 검출(Bidirectional Forwarding Detection, BFD) 패킷)을 전송을 위해 로컬 보호 경로로 전환한 후, 패킷이 목적지 종단으로 정상적으로 전송되므로, 목적지 종단은 BFD 패킷을 기반으로 헤드 노드에 응답을 보낼 수 있다. 결과적으로, 헤드 노드는 BFD 패킷에 대한 응답을 수신하고 이에 따라 기본 경로가 연결된 것으로 간주한다. 이 경우, 헤드 노드는 기본 경로에 결함이 있음을 적시에 검출할 수 없다. 헤드 노드는 기본 경로에 결함이 있음을 검출하는 트리거 조건 하에서만 기본 경로에서 종단 간 보호 경로로 전환을 수행한다. 헤드 노드는 기본 경로에 결함이 있음을 적시에 검출할 수 없기 때문에, 헤드 노드는 기본 경로에서 종단 간 보호 경로로의 전환을 적시에 수행할 수 없다. 결과적으로, 트래픽은 SLA를 충족할 수 없는 보호 경로를 통해 장기간 전송되고, SLA 요구사항이 충족될 수 없다.

발명의 내용

[0005] 본 출원의 실시예는 기본 경로를 통해 전송되는 패킷이 로컬 보호 경로로 전환되는 것을 방지하기 위한 패킷 처리 방법 및 장치, 네트워크 디바이스, 및 저장 매체를 제공한다. 기술 솔루션은 다음과 같다:

[0006] 제1 양상에 따르면, 패킷 처리 방법이 제공된다. 방법에서, 제1 네트워크 디바이스는 패킷을 수신한다. 패킷은 보호 플래그를 포함하고, 보호 플래그는 제1 네트워크 디바이스가 패킷을 기본 경로에서 제1 보호 경로로 전환하도록 허용되는지 여부를 나타내는 데 사용되며, 제1 보호 경로는 기본 경로를 보호하는 데 사용되고, 제1 보호 경로 상의 인그레스 노드는 제1 네트워크 디바이스이다. 제1 네트워크 디바이스는 기본 경로에 결함이 있다고 결정한다. 보호 플래그가 패킷이 기본 경로에서 제1 보호 경로로 전환되도록 허용되지 않음을 나타내는 경우, 제1 네트워크 디바이스는 기본 경로에 결함이 있다는 결정된 사실 및 패킷이 기본 경로에서 상기 제1 보호 경로로 전환되도록 허용되지 않음을 나타내는 보호 플래그에 기초하여 패킷을 폐기한다.

[0007] 이 방법에서, 로컬 보호가 허용되는지 여부를 나타낼 수 있는 식별자가 패킷에 추가된다. 보호 플래그를 전달하는 패킷이 기본 경로를 따라 전송되는 과정에서, 경로를 따른 노드가 기본 경로에 결함이 있다고 결정하지만, 보호 플래그가 보호 경로로의 로컬 전환이 허용되지 않음을 나타내는 경우, 경로를 따른 노드는 로컬 보호를 수행하지 않으므로 경로를 따른 노드에 의해 보호 경로로 패킷이 전환되지 않는다. 이는 기본 경로에 결함이 있을 때 경로를 따른 노드를 인그레스로 하여 패킷이 보호 경로를 통과하는 것을 방지하고, 경로를 따른 노드로부터 보호 경로로 패킷이 진입한 후 발생하는 문제를 해결한다.

[0008] 특히, 대부분의 경우, 경로를 따른 노드는 로컬 보호만 수행할 수 있으며 종단 간 보호 경로로 전환할 수 없다. 따라서, 인그레스로서 경로를 따른 노드가 있는 보호 경로는 일반적으로 사전계획된 종단 간 보호 경로 대신 로컬 보호 경로이다. 이 경우, 패킷이 로컬 보호 경로로 전환되면, 기본 경로 상의 트래픽이 오랫동안 로컬 보호 경로로 우회된다. 그러나, 패킷에 보호 플래그가 추가되어 패킷이 로컬 보호 경로로 전송되지 않는다. 따라서, 기본 경로 상의 트래픽은 적시에 종단 간 보호 경로로 전환될 수 있다.

[0009] 또한, 경로를 따른 노드가 패킷을 폐기하기 때문에, 패킷 송신 측은 적시에 기본 경로 상의 트래픽에서 패킷 손실을 검출할 수 있다. 보호 전환을 트리거하기 위해 패킷 손실이 검출되는 다양한 시나리오에서, 패킷 송신 측은 기본 경로 상의 트래픽을 종단 간 보호 경로로 적시에 전환할 수 있으므로 패킷 송신 측은 서비스 장애 및 기본 경로 상의 결함의 원인을 적시에 검출할 수 있다.

[0010] 선택적으로, 기본 경로에서 제2 보호 경로로 전환하기 위한 트리거 조건은 기본 경로 상의 트래픽에서 패킷 손

실이 검출되는 것이다.

[0011] 선택적으로, 제2 보호 경로는 기본 경로를 보호하기 위한 백업 경로이며, 제2 보호 경로는 기본 경로와 동일한 인그레스 노드를 갖는다.

[0012] 선택적으로, 제2 보호 경로는 SLA를 충족한다.

[0013] 이 SLA 보증 시나리오에서, 패킷이 보호 플래그를 전달하지 않을 때, 패킷이 기본 경로를 따라 전송되는 과정에서, 경로를 따른 노드가 기본 경로에 결함이 있다고 결정하면, 노드는 패킷을 보호 경로로 로컬로 전환한다. 경로를 따른 노드가 패킷을 전환하는 보호 경로는 일반적으로 SLA를 충족하지 않기 때문에, 경로를 따른 노드가 패킷을 전환하는 보호 경로의 전송 성능은 대역폭, 지연 등의 측면에서 보장될 수 없다. 결과적으로, 기본 경로 상의 트래픽은 SLA를 충족하지 않는 경로로 우회되고, 서비스 SLA 보증이 달성될 수 없다. 그러나, 이 선택적 방식에서, 로컬 보호가 허용되는지 여부를 나타낼 수 있는 식별자가 패킷에 추가된다. 보호 플래그를 전달하는 패킷이 기본 경로를 따라 전송되는 과정에서, 경로를 따른 노드가 기본 경로에 결함이 있다고 결정하지만, 보호 플래그가 보호 경로로의 로컬 전환이 허용되지 않음을 나타내는 경우, 경로를 따른 노드는 로컬 보호를 수행하지 않으므로 경로를 따른 노드에 의해 보호 경로로 패킷이 전환되지 않는다. 이는 패킷이 경로를 따른 노드로부터 보호 경로에 들어간 후 발생하는, 기본 경로 상의 트래픽이 SLA를 충족하지 않는 경로에서 장기간 전송되는 문제를 방지한다. 또한, 경로를 따른 노드는 패킷을 폐기하기 때문에, 헤드 노드는 기본 경로 상의 트래픽에서 패킷 손실을 적시에 검출할 수 있으므로, 헤드 노드는 기본 경로 상의 트래픽을 적시에 SLA를 충족하는 보호 경로로 전환할 수 있으며, 서비스 SLA 보증을 달성할 수 있다.

[0014] 선택적으로, 패킷은 세그먼트 라우팅(영문: Segment Routing, 줄여서 SR) 패킷이다. 제1 네트워크 디바이스는 패킷의 세그먼트 식별자(Segment ID, SID)에 기초하여, SID에 대응하는 아웃바운드 인터페이스 또는 다음 홉을 결정한다. 아웃바운드 인터페이스 또는 다음 홉에 결함이 있는 경우, 제1 네트워크 디바이스는 기본 경로에 결함이 있다고 결정한다.

[0015] SR 터널에서 기본 경로를 통해 패킷을 전송하는 과정에서, 기본 경로에 결함이 있는 경우, 경로를 따른 각 홉 노드는 노드의 다음 홉 또는 아웃바운드 인터페이스에 기초하여 기본 경로에 결함이 있다고 결정할 수 있었다. 따라서, 경로를 따라 각 홉 노드는 기본 경로에 결함이 있다고 결정할 가능성이 있다. 이 경우, 경로를 따른 노드가 로컬 보호 메커니즘을 사전배치하면, 기본 경로 상의 패킷이 노드를 통과할 때, 노드는 패킷을 로컬 보호 경로로 전환한다. 따라서, 패킷이 보호 플래그를 전달하지 않는 경우, 기본 경로 상의 임의의 노드 또는 링크에 결함이 있으면, 경로를 따른 임의의 홉 노드는 패킷을 로컬 보호 경로로 전환할 가능성이 있음을 증명할 수 있다. 그러나, 보호 플래그가 패킷에 추가되어 기본 경로를 따른 각 홉 노드가 수신한 패킷이 보호 플래그를 전달한다. 따라서, 패킷을 수신한 다음 기본 경로에 결함이 있다고 결정하는 경로를 따른 홉 노드에 관계없이, 보호 플래그는 이미 보호 경로로의 전환이 허용되지 않음을 나타내므로, 홉 노드는 보호 플래그에 의해 표시된 바와 같이 패킷을 폐기할 수 있고, 패킷을 로컬 보호 경로로 전환하지 않는다. 따라서, 이 방법에서는, 기본 경로 상의 패킷이 로컬 보호 경로로 전환되지 않고, 경로를 따른 노드가 패킷이 전달한 보호 플래그에 기초하여 로컬 보호 전환을 수행할지 여부를 결정할 수 있으므로, 구현이 비교적 쉽고 서비스 배치 복잡성이 감소함을 알 수 있다.

[0016] 선택적으로, 패킷은 세그먼트 라우팅 오버 인터넷 프로토콜 버전 6(영문: segment routing over internet protocol version 6, 줄여서 SRv6) 패킷이고, SRv6 패킷은 세그먼트 라우팅 헤더(Segment Routing Header, SRH)를 포함하며, 보호 플래그는 SRH에 있다.

[0017] 이 선택적 방식에서, 로컬 보호가 허용되는지 여부를 나타낼 수 있는 식별자가 SRv6 패킷의 SRH에 추가된다. 보호 플래그를 전달하는 패킷이 SR 터널의 기본 라벨 전환 경로(Label Switched Path, LSP)를 따라 전송되는 과정에서, 기본 LSP 상의 중간 노드가 기본 경로에 결함이 있다고 결정하지만, 보호 플래그가 로컬 보호가 허용되지 않음을 나타내는 경우, 경로를 따른 노드는 로컬 보호를 수행하지 않으므로 중간 노드에 의해 인그레스로서의 중간 노드를 가진 백업 LSP로 패킷이 전환되지 않는다. 이는 패킷이 기본 경로에 결함이 있을 때 로컬 보호를 위해 백업 LSP를 통과하지 못하게 하고, 패킷이 경로를 따른 노드로부터 로컬 보호를 위해 백업 LSP에 진입한 후 발생하는 문제를 해결한다.

[0018] 선택적으로, 보호 플래그는 SRH의 플래그(Flags) 필드에 있다.

[0019] 이 선택적 방식에서, 새로운 플래그 필드는 패킷에 대해 확장되고, 플래그 필드는 보호 플래그를 전달하는 데 사용된다. 기본 경로에 결함이 있는 경우, 패킷이 플래그 필드를 포함하기 때문에, 수신 측이 플래그 필드에서

보호 플래그를 식별한 후, 패킷은 제1 보호 경로를 통과하지 않는다. 제1 보호 경로가 로컬 보호 경로인 경우, 패킷은 로컬 보호 경로를 통과하지 않는다.

[0020] 선택적으로, 보호 플래그가 SRH에 있는 것은 보호 플래그가 SRH의 유형-길이-값(Type-Length-Value, TLV)에 있는 것을 포함한다.

[0021] 이 선택적 방식에서, 새로운 TLV는 패킷에 대해 확장되고, TLV는 보호 플래그를 전달하는 데 사용된다. 기본 경로에 결함이 있는 경우, 수신 측이 TLV를 식별한 후, 패킷은 제1 보호 경로를 통과하지 않는다. 제1 보호 경로가 로컬 보호 경로인 경우, 패킷은 로컬 보호 경로를 통과하지 않는다.

[0022] 선택적으로, 방법은 보호 플래그가 패킷이 기본 경로에서 제1 보호 경로로 전환되도록 허용됨을 나타내는 경우, 제1 네트워크 디바이스가 기본 경로에 결함이 있다는 결정된 사실 및 패킷이 기본 경로에서 제1 보호 경로로 전환되도록 허용됨을 나타내는 보호 플래그에 기초하여 제1 보호 경로를 통해 패킷을 전송하는 단계를 더 포함한다.

[0023] 이 선택적 방식에서, 보호 플래그가 패킷에 추가되어, 보호 플래그는 패킷이 기본 경로에서 보호 경로로 전환되도록 허용되는지 여부를 나타낼 수 있다. 기본 경로에 결함이 있는 경우, 그 경로를 따른 노드 역할을 하는 네트워크 디바이스가 보호 플래그를 전달하는 패킷을 수신하면, 기본 경로에 결함이 있다고 결정하고 보호 플래그는 패킷이 보호 경로로 전환되도록 허용됨을 나타내므로, 패킷은 보호 경로를 통해 전송되고, 경로를 따른 노드는 패킷이 전달한 보호 플래그를 사용하여 패킷을 로컬 보호 경로로 전환하도록 안내되고, 경로를 따른 노드는 패킷을 특정 보호 경로로 전환하도록 추가 안내될 수 있다. 이는 유연성을 향상시킨다.

[0024] 선택적으로, 보호 플래그가 패킷이 중간점 토폴로지 독립 루프 프리 대체(Midpoint Topology-Independent Loop-free Alternate, 중간점 TI-LFA) 경로로 전환되도록 허용되지만 토폴로지 독립 루프 프리 대체 고속 리라우트(Topology-Independent Loop-free Alternate Fast Reroute, TI-LFA FRR) 경로로 전환되도록 허용되지 않음을 나타내는 경우, 제1 네트워크 디바이스는 기본 경로에 결함이 있다는 결정된 사실 및 패킷이 중간점 TI-LFA 경로로 전환되도록 허용되지만 TI-LFA FRR 경로로 전환되도록 허용되지 않음을 나타내는 보호 플래그에 기초하여 중간점 TI-LFA 경로를 통해 패킷을 전송한다.

[0025] 선택적으로, 보호 플래그가 패킷이 TI-LFA FRR 경로로 전환되도록 허용되지만 중간점 TI-LFA 경로로 전환되도록 허용되지 않음을 나타내는 경우, 제1 네트워크 디바이스는 기본 경로에 결함이 있다는 결정된 사실 및 패킷이 TI-LFA FRR 경로로 전환되도록 허용되지만 중간점 TI-LFA 경로로 전환되도록 허용되지 않음을 나타내는 보호 플래그에 기초하여 TI-LFA FRR 경로를 통해 패킷을 전송한다.

[0026] 선택적으로, 보호 플래그는 패킷의 제1 비트를 점유하고, 제1 비트가 설정되면, 패킷이 기본 경로에서 제1 보호 경로로 전환되도록 허용되지 않음을 나타내거나, 또는 제1 비트가 설정되지 않으면, 패킷이 기본 경로에서 제1 보호 경로로 전환되도록 허용됨을 나타낸다.

[0027] 선택적으로, 보호 플래그는 패킷의 제2 비트 및 제3 비트를 점유하고, 제2 비트와 제3 비트가 모두 설정되면, 패킷이 기본 경로에서 중간점 TI-LFA 경로 또는 TI-LFA FRR 경로로 전환되도록 허용되지 않음을 나타내거나, 제2 비트가 설정되고 제3 비트가 설정되지 않으면, 패킷이 중간점 TI-LFA 경로로 전환되도록 허용되지 않지만 TI-LFA FRR 경로로 전환되도록 허용됨을 나타내거나, 제2 비트가 설정되지 않고 제3 비트가 설정되면, 패킷이 중간점 TI-LFA 경로로 전환되도록 허용되지만 TI-LFA FRR 경로로 전환되도록 허용되지 않음을 나타내거나, 또는 제2 비트도 제3 비트도 설정되지 않으면, 패킷이 기본 경로에서 중간점 TI-LFA 경로 또는 TI-LFA FRR 경로로 전환되도록 허용됨을 나타낸다.

[0028] 선택적으로, 패킷은 데이터 패킷을 포함하고, 데이터 패킷은 기본 경로의 서비스 데이터를 전달하는 데 사용되거나, 또는 패킷은 검출 패킷을 포함하고, 검출 패킷은 기본 경로의 연결성 또는 전송 성능 파라미터 중 적어도 하나를 검출하는 데 사용된다.

[0029] 선택적으로, 패킷이 검출 패킷을 포함하는 경우, 검출 패킷은 양방향 포워딩 검출(BFD) 패킷이다.

[0030] BFD 시나리오에서, 헤드 노드(예를 들어, 제2 네트워크 디바이스)는 보호 플래그와 함께 BFD 패킷을 전송하고, 보호 플래그를 사용하여 보호 경로로의 로컬 전환이 허용되지 않음을 나타낸다. 따라서, BFD 패킷이 기본 경로를 따라 전송되는 과정에서, 기본 경로에 결함이 있는 경우, 보호 플래그가 보호 경로로의 로컬 전환이 허용되지 않음을 나타내므로, BFD 패킷을 수신할 때, 경로를 따른 노드(예컨대, 제1 네트워크 디바이스)는 로컬 보호 메커니즘을 사용하여 BFD 패킷을 로컬 보호 경로로 전환하지 않고, BFD 패킷을 폐기한다. 이 경우, BFD 패킷의

전송은 경로를 따른 노드에서 중단되고, BFD 패킷은 목적지 노드로 전송되지 않는다. 목적지 노드는 BFD 패킷을 수신하지 않기 때문에, 목적지 노드는 BFD 패킷에 응답하지 않고, 헤드 노드는 목적지 노드로부터 응답 패킷을 수신하지 않는다. 이 경우, 헤드 노드에 의해 수행되는 BFD 검출은 다운(down) 상태에 있다. 따라서, BFD 검출이 다운 상태에 있다는 사실을 기반으로, 헤드 노드는 1차 경로에 결함이 있음을 적시에 검출할 수 있으므로 헤드 노드는 기본 경로에 대한 결함의 원인을 적시에 검출하고 서비스 장애를 적시에 검출할 수 있다. 이는 기본 경로 상의 결함을 적시에 수정하고 장기적인 서비스 장애를 방지하는 데 도움이 된다.

[0031] 선택적으로, 패킷이 검출 패킷을 포함하는 경우, 검출 패킷은 패킷 인터넷 그로퍼(PING) 검출 패킷이다.

[0032] 선택적으로, 패킷이 검출 패킷을 포함하는 경우, 검출 패킷은 운영, 관리 및 유지보수(Operations, Administration and Maintenance, OAM) 검출 패킷이다.

[0033] 선택적으로, 패킷이 검출 패킷을 포함하는 경우, 검출 패킷은 양방향 능동 측정 프로토콜(two-Way Active Measurement Protocol, TWAMP) 검출 패킷이다.

[0034] 선택적으로, 패킷이 검출 패킷을 포함하는 경우, 검출 패킷은 인터넷 프로토콜 데이터 흐름 기반 채널 관련 OAM 성능 측정(인시투 흐름 정보 원격측정(in-situ Flow information Telemetry, IFIT)) 패킷이다.

[0035] 제2 양상에 따르면, 패킷 처리 방법이 제공된다. 방법에서, 제2 네트워크 디바이스는 패킷을 생성한다. 패킷은 보호 플래그를 포함하고, 보호 플래그는 제1 네트워크 디바이스가 패킷을 기본 경로에서 제1 보호 경로로 전환하도록 허용되는지 여부를 나타내는 데 사용되며, 제1 보호 경로는 기본 경로를 보호하는 데 사용되고, 제1 보호 경로 상의 인그레스 노드는 제1 네트워크 디바이스이다. 제2 네트워크 디바이스는 패킷을 제1 네트워크 디바이스로 전송한다.

[0036] 이 방법에서, 로컬 보호가 허용되는지 여부를 나타낼 수 있는 식별자가 패킷에 추가된다. 보호 플래그를 전달하는 패킷이 기본 경로를 따라 전송되는 과정에서, 경로를 따른 노드가 기본 경로에 결함이 있다고 결정하지만, 보호 플래그가 보호 경로로의 로컬 전환이 허용되지 않음을 나타내는 경우, 경로를 따른 노드는 로컬 보호를 수행하지 않으므로 경로를 따른 노드에 의해 패킷이 보호 경로로 전환되지 않는다. 이는 기본 경로에 결함이 있을 때 경로를 따른 노드를 인그레스로 하여 패킷이 보호 경로를 통과하는 것을 방지하고, 경로를 따른 노드에서 보호 경로로 패킷이 진입한 후 발생하는 문제를 해결한다.

[0037] 특히, 대부분의 경우, 경로를 따른 노드는 로컬 보호만 수행할 수 있으며 종단 간 보호 경로로 전환할 수 없다. 따라서, 인그레스로서 경로를 따른 노드가 있는 보호 경로는 일반적으로 사전계획된 종단 간 보호 경로 대신 로컬 보호 경로이다. 이 경우, 패킷이 로컬 보호 경로로 전환되면, 기본 경로 상의 트래픽이 오랫동안 로컬 보호 경로로 우회된다. 그러나, 패킷에 보호 플래그가 추가되어 패킷이 로컬 보호 경로로 전송되지 않는다. 따라서, 기본 경로 상의 트래픽은 적시에 종단 간 보호 경로로 전환될 수 있다.

[0038] 선택적으로, 제2 네트워크 디바이스가 패킷을 상기 제1 네트워크 디바이스로 전송한 후에, 제2 네트워크 디바이스는 기본 경로 상의 트래픽에서 패킷 손실이 발생한다고 결정하고, 제2 네트워크 디바이스는 기본 경로 상의 트래픽에서 패킷 손실이 발생한다는 결정된 사실에 기초하여 기본 경로를 제2 보호 경로로 전환한다.

[0039] 경로를 따른 노드가 패킷을 폐기하기 때문에, 패킷 송신 측은 적시에 기본 경로 상의 트래픽에서 패킷 손실을 검출할 수 있다. 보호 전환을 트리거하기 위해 패킷 손실이 검출되는 다양한 시나리오에서, 패킷 송신 측은 기본 경로 상의 트래픽을 종단 간 보호 경로로 적시에 전환할 수 있으므로 패킷 송신 측은 서비스 장애 및 기본 경로 상의 결함의 원인을 적시에 검출할 수 있다.

[0040] 선택적으로, 보호 경로는 기본 경로를 보호하기 위한 백업 경로이고, 제2 보호 경로는 기본 경로와 동일한 인그레스 노드를 갖는다.

[0041] 선택적으로, 제2 보호 경로는 SLA를 충족한다.

[0042] 선택적으로, 패킷은 SRv6 패킷이고, SRv6 패킷은 세그먼트 라우팅 헤더(SRH)를 포함하며, 보호 플래그는 SRH에 있다.

[0043] 선택적으로, 보호 플래그가 SRH에 있는 것은, 보호 플래그가 SRH의 플래그 필드에 있거나, 또는 보호 플래그가 SRH의 유형-길이-값(TLV)에 있는 것을 포함한다.

[0044] 선택적으로, 보호 플래그는 패킷의 제1 비트를 점유하고, 제1 비트가 설정되면, 패킷이 기본 경로에서 제1 보호 경로로 전환되도록 허용되지 않음을 나타내거나, 또는 제1 비트가 설정되지 않으면, 패킷이 기본 경로에서 제1

보호 경로로 전환되도록 허용됨을 나타내거나, 또는 보호 플래그는 패킷의 제2 비트 및 제3 비트를 점유하고, 제2 비트와 제3 비트가 모두 설정되면, 패킷이 기본 경로에서 중간점 TI-LFA 경로 및 TI-LFA FRR 경로로 전환되도록 허용되지 않음을 나타내거나, 제2 비트가 설정되고 제3 비트가 설정되지 않으면, 패킷이 중간점 TI-LFA 경로로 전환되도록 허용되지 않지만 TI-LFA FRR 경로로 전환되도록 허용됨을 나타내거나, 제2 비트가 설정되지 않고 제3 비트가 설정되면, 패킷이 중간점 TI-LFA 경로로 전환되도록 허용되지만 TI-LFA FRR 경로로 전환되도록 허용되지 않음을 나타내거나, 또는 제2 비트도 제3 비트도 설정되지 않으면, 패킷이 기본 경로에서 중간점 TI-LFA 경로 또는 TI-LFA FRR 경로로 전환되도록 허용됨을 나타낸다.

[0045] 선택적으로, 패킷은 데이터 패킷을 포함하고, 데이터 패킷은 기본 경로의 서비스 데이터를 전달하는 데 사용되거나, 또는 패킷은 검출 패킷을 포함하고, 검출 패킷은 기본 경로의 연결성 또는 전송 성능 파라미터 중 적어도 하나를 검출하는 데 사용된다.

[0046] 선택적으로, 검출 패킷은 BFD 패킷이거나, 또는 검출 패킷은 PING 검출 패킷이거나, 또는 검출 패킷은 OAM 검출 패킷이거나, 또는 검출 패킷은 TWAMP 검출 패킷이거나, 또는 검출 패킷은 IFIT 패킷이다.

[0047] 제3 양상에 따르면, 패킷 처리 장치가 제공된다. 패킷 처리 장치는 제1 양상또는 제1 양상의 선택적 방식 중 어느 하나에서 패킷 처리를 구현하는 기능을 갖는다. 패킷 처리 장치는 적어도 하나의 모듈을 포함하고, 적어도 하나의 모듈은 제1 양상 또는 제1 양상의 선택적 방식 중 어느 하나에 따른 패킷 처리 방법을 구현하도록 구성된다. 제3 양상에 따른 패킷 처리 장치의 세부사항에 대해서는, 제1 양상 또는 제1 양상의 선택적 방식 중 어느 하나를 참조한다. 세부사항은 여기에서 다시 설명되지 않는다.

[0048] 제4 양상에 따르면, 패킷 처리 장치가 제공된다. 패킷 처리 장치는 제2 양상또는 제2 양상의 선택적 방식 중 어느 하나에서 패킷 처리를 구현하는 기능을 갖는다. 패킷 처리 장치는 적어도 하나의 모듈을 포함하고, 적어도 하나의 모듈은 제2 양상 또는 제2 양상의 선택적 방식 중 어느 하나에 따른 패킷 처리 방법을 구현하도록 구성된다. 제4 양상에 따른 패킷 처리 장치의 세부사항에 대해서는, 제2 양상 또는 제2 양상의 선택적 방식 중 어느 하나를 참조한다. 세부사항은 여기에서 다시 설명되지 않는다.

[0049] 제5 양상에 따르면, 네트워크 디바이스가 제공된다. 네트워크 디바이스는 프로세서를 포함하고, 프로세서는 명령어를 실행하도록 구성되어 네트워크 디바이스가 제1 양상 또는 제1 양상의 선택적 방식 중 어느 하나에 따른 패킷 처리 방법을 수행한다. 제5 양상에 따른 네트워크 디바이스의 세부사항에 대해서는, 제1 양상 또는 제1 양상의 선택적 방식 중 어느 하나를 참조한다. 세부사항은 여기에서 다시 설명되지 않는다.

[0050] 제6 양상에 따르면, 네트워크 디바이스가 제공된다. 네트워크 디바이스는 프로세서를 포함하고, 프로세서는 명령을 실행하도록 구성되어 네트워크 디바이스가 제2 양상 또는 제2 양상의 선택적 방식 중 어느 하나에 따른 패킷 처리 방법을 수행한다. 제6 양상에 따른 네트워크 디바이스의 세부사항은, 제2 양상 또는 제2 양상의 선택적 방식 중 어느 하나를 참조한다. 세부사항은 여기에서 다시 설명되지 않는다.

[0051] 제7 양상에 따르면, 컴퓨터 판독가능 저장 매체가 제공된다. 저장 매체는 적어도 하나의 명령어를 저장하고, 프로세서에 의해 명령어가 판독될 때, 네트워크 디바이스는 제1 양상 또는 제1 양상의 선택적 방식 중 어느 하나에 따른 패킷 처리 방법을 수행할 수 있다.

[0052] 제8 양상에 따르면, 컴퓨터 판독가능 저장 매체가 제공된다. 저장 매체는 적어도 하나의 명령어를 저장하고, 명령어는 프로세서에 의해 판독되어 네트워크 디바이스가 제2 양상 또는 제2 양상의 선택적 방식 중 어느 하나에 따른 패킷 처리 방법을 수행한다.

[0053] 제9 양상에 따르면, 컴퓨터 프로그램 제품이 제공된다. 컴퓨터 프로그램 제품이 네트워크 디바이스에서 실행될 때, 네트워크 디바이스는 제1 양상 또는 제1 양상의 선택적 방식 중 어느 하나에 따른 패킷 처리 방법을 수행할 수 있다.

[0054] 제10 양상에 따르면, 컴퓨터 프로그램 제품이 제공된다. 컴퓨터 프로그램 제품이 네트워크 디바이스에서 실행될 때, 네트워크 디바이스는 제2 양상 또는 제2 양상의 선택적 방식 중 어느 하나에 따른 패킷 처리 방법을 수행할 수 있다.

[0055] 제11 양상에 따르면, 칩이 제공된다. 칩이 네트워크 디바이스에서 실행될 때, 네트워크 디바이스는 제1 양상 또는 제1 양상의 선택적 방식 중 어느 하나에 따른 패킷 처리 방법을 수행할 수 있다.

[0056] 제12 양상에 따르면, 칩이 제공된다. 칩이 네트워크 디바이스에서 실행될 때, 네트워크 디바이스는 제2 양상 또

는 제2 양상의 선택적 방식 중 어느 하나에 따른 패킷 처리 방법을 수행할 수 있다.

[0057] 제13 양상에 따르면, 패킷 처리 시스템이 제공된다. 패킷 처리 시스템은 제1 네트워크 디바이스 및 제2 네트워크 디바이스를 포함한다. 제1 네트워크 디바이스는 제1 양상 또는 제1 양상의 선택적 방식 중 어느 하나에 따른 방법을 수행하도록 구성되고, 제2 네트워크 디바이스는 제2 양상 또는 제2 양상의 선택적 방식 중 어느 하나에 따른 방법을 수행하도록 구성된다.

도면의 간단한 설명

[0058] 도 1은 본 출원의 실시예에 따른 패킷 처리 시스템의 아키텍처도이다.

도 2는 본 출원의 실시예에 따른 로컬 터널 보호 솔루션의 개략도이다.

도 3은 본 출원의 실시예에 따른 종단 간 터널 보호 솔루션의 개략도이다.

도 4는 본 출원의 실시예에 따른 로컬 터널 보호와 종단 간 터널 보호를 결합한 솔루션의 개략도이다.

도 5는 본 출원의 실시예에 따른 VPN FRR 기술의 개략도이다.

도 6은 본 출원의 실시예에 따라 로컬 보호가 발생할 때 사용되는 BFD 검출 메커니즘의 개략도이다.

도 7은 본 출원의 실시예 1에 따른 패킷 처리 방법의 흐름도이다.

도 8은 본 출원의 실시예에 따른 SRv6 패킷의 개략도이다.

도 9는 본 출원의 실시예에 따른 SRH의 개략도이다.

도 10은 본 출원의 실시예에 따른 보호 플래그를 전달하는 플래그 필드의 개략도이다.

도 11은 본 출원의 실시예에 따른 보호 플래그를 전달하는 플래그 필드의 개략도이다.

도 12는 본 출원의 실시예에 따른 보호 플래그를 전달하는 TLV의 개략도이다.

도 13은 본 출원의 실시예에 따른 보호 플래그를 전달하는 IFIT 패킷 헤더의 개략도이다.

도 14는 본 출원의 실시예에 따른 보호 플래그를 전달하는 IFIT 패킷의 개략도이다.

도 15는 본 출원의 실시예 2에 따른 패킷 처리 방법의 흐름도이다.

도 16은 본 출원의 실시예 3에 따른 패킷 처리 방법의 흐름도이다.

도 17은 본 출원의 실시예 4에 따른 패킷 처리 방법의 흐름도이다.

도 18은 본 출원의 실시예 5에 따른 패킷 처리 방법의 흐름도이다.

도 19는 본 출원의 실시예에 따른 패킷 처리 장치(110)의 구조의 개략도이다.

도 20은 본 출원의 실시예에 따른 패킷 처리 장치(120)의 구조의 개략도이다.

도 21은 본 출원의 실시예에 따른 네트워크 디바이스(1300)의 구조의 개략도이다.

도 22는 본 출원의 실시예에 따른 네트워크 디바이스(1300)에서 인터페이스 보드(1330)의 구조의 개략도이다.

발명을 실시하기 위한 구체적인 내용

[0059] 본 출원의 목적, 기술적 솔루션 및 이점을 보다 명확하게 하기 위해, 다음은 첨부 도면을 참조하여 본 출원의 구현예를 상세히 설명한다.

[0060] 본 출원에서, "제1" 및 "제2"와 같은 용어는 기본적으로 동일한 기능을 갖는 동일한 항목 또는 유사한 항목을 구별하는 데 사용된다. "제1"과 "제2" 사이에는 논리적 또는 시간 순서 종속성이 없으며, 수량 및 실행 순서가 제한되지 않음을 이해해야 한다. "제1" 및 "제2"와 같은 용어가 다양한 요소를 설명하기 위해 다음 설명에서 사용되지만, 이러한 요소는 용어에 의해 제한되어서는 안 된다는 것을 추가로 이해해야 한다. 이러한 용어는 단지 한 요소를 다른 요소와 구별하는 데 사용된다. 예를 들어, 다양한 실시예의 범위를 벗어나지 않으면서, 제1 네트워크 디바이스는 제2 네트워크 디바이스로 지칭될 수 있다. 유사하게, 제2 네트워크 디바이스는 제1 네트워크 디바이스로 지칭될 수 있다. 제1 네트워크 디바이스와 제2 네트워크 디바이스는 모두 네트워크 디바이스일 수 있으며, 경우에 따라 별개의 서로 다른 네트워크 디바이스일 수 있다. 예를 들어, 다양한 예의 범위를 벗어나지

않으면서, 제1 보호 경로는 제2 보호 경로로 지칭될 수 있다. 유사하게, 제2 보호 경로는 제1 보호 경로로 지칭될 수 있다. 제1 보호 경로와 제2 보호 경로는 모두 보호 경로일 수 있으며, 경우에 따라 별개의 서로 다른 보호 경로일 수 있다.

[0061] 본 출원에서 용어 "적어도 하나"는 하나 이상을 의미하고, 본 출원에서 용어 "복수"는 둘 이상을 의미한다. 예를 들어, "복수의 세그먼트 식별자(Segment ID, SID)"는 둘 이상의 SID를 의미한다.

[0062] 본 명세서에서 다양한 예에 대한 설명에서 사용된 용어들은 단지 특정한 예를 설명하기 위해 의도된 것일뿐, 제한을 구성하기 위해 의도되지 않은 것으로 이해되어야 한다. 다양한 실시예의 설명 및 첨부된 청구범위에 사용된 단수 형태의 용어 "하나(one)"("a" 또는 "an") 및 "the"는 문맥에서 명확하게 달리 명시되지 않는 한 복수 형태도 포함하도록 의도된다.

[0063] 프로세스의 순서 번호는 본 출원의 다양한 실시예에서 실행 순서를 의미하지 않는다는 것이 추가로 이해되어야 한다. 프로세스의 실행 순서는 프로세스의 기능 및 내부 로직을 기반으로 결정되어야 하며, 본 출원의 실시예의 구현 프로세스에 대한 임의의 제한으로 해석되어서는 안 된다.

[0064] A에 기초하여 B를 결정하는 것은 B가 A에만 기초하여 결정된다는 것을 의미하는 것이 아니라, B가 대안적으로 A 및/또는 다른 정보에 기초하여 결정될 수 있다는 것을 이해해야 한다.

[0065] 본 명세서에서 사용된 용어 "포함하다"("포함하다", "포함하는", "내포하다" 및/또는 "내포하는"으로도 지칭됨)는 언급된 특징, 정수, 단계, 동작, 요소 및/또는 구성요소의 존재를 명시한다는 것을 더 이해해야 하며, 하나 이상의 다른 특징, 정수, 단계, 동작, 요소, 구성요소 및/또는 해당 구성요소의 존재 또는 추가는 배제되지 않는다.

[0066] "만약" 및 "~라고 가정하면"이라는 용어는 "때"("때" 또는 "시"), "결정에 응답하여", "검출에 응답하여" 또는 "기초하여"를 의미하는 것으로 해석될 수 있음을 추가로 이해해야 한다. 유사하게, 문맥에 따라, "~라고 결정될 때" 또는 "(명시된 조건 또는 이벤트)가 검출되면"이라는 문구는 "~라고 결정될 때", "결정에 응답하여", "(명시된 조건 또는 이벤트)가 검출될 때", "(명시된 조건 또는 이벤트) 검출에 응답하여", 또는 "결정된(명시된 조건 또는 이벤트)에 기초하여"의 의미로 해석될 수 있다.

[0067] 명세서 전체에서 언급되는 "일 실시예", "실시예" 및 "가능한 구현예"는 실시예 또는 구현예와 관련된 특정 특징, 구조 또는 특성이 본 출원의 적어도 하나의 실시예에 포함된다는 것을 의미함을 이해해야 한다. 따라서, 본 명세서 전체에 걸쳐 나타나는 "일 실시예에서", "실시예에서" 또는 "가능한 구현예에서"가 반드시 동일한 실시예를 의미하는 것은 아니다. 또한, 이러한 특정 특징, 구조 또는 특성은 임의의 적절한 방식을 사용하여 하나 이상의 실시예에서 결합될 수 있다.

[0068] 본 출원의 실시예에서 제공되는 패킷 처리 방법은 SLA 보증이 필요한 시나리오, 예를 들어 대역폭, 지연 또는 다른 전송 성능 파라미터가 보장되어야 하는 시나리오에 적용될 수 있다. 구체적으로, 본 출원의 실시예에서 패킷 처리 방법은 BFD 검출 시나리오, PING 검출 연결 시나리오, OAM 검출 시나리오, TWAMP 검출 시나리오, IFIT 시나리오 또는 데이터 패킷 전송 시나리오에 적용될 수 있다. 본 출원의 실시예에서의 패킷 처리 방법은 SRv6 시나리오, SR-TE 시나리오 또는 다른 시나리오를 포함하지만 이에 제한되지 않는 소스 라우팅에 기초하여 패킷이 전송되는 임의의 시나리오에 적용될 수 있다.

[0069] 다음은 몇몇 용어를 개별적으로 간략하게 설명한다.

[0070] 서비스 수준 계약(전체 이름: service level agreement, 줄여서 SLA): 서비스 수준 계약은 일반적으로 서비스 제공자와 사용자 또는 서로 다른 서비스 제공자 간에 체결되는 계약이며, 서비스 제공자가 제공한 서비스 수준 및 품질을 지정한다. 원격통신 네트워크 기술 분야에서, SLA 파라미터 또는 성능 표시자는 일반적으로 지연, 대역폭, 처리량, 가용성, 패킷 손실률 등을 포함한다. SLA 보증이 필요한 시나리오에서, 종단 간 서비스에는 안정적인 대역폭과 지연이 필요하다. 이를 고려하여, 일반적으로 서비스 경로에 대해 별개의 활성 및 백업 경로가 사전계획된다. 사전계획된 활성 및 백업 경로는 모두 대역폭 요구사항 또는 지연 요구사항과 같은 SLA 요구사항을 충족한다. 그러나, 로컬 보호 경로는 최대 링크 연결만 보장할 수 있지만, 대역폭이나 지연을 보장할 수는 없다. 기본 경로에 로컬 결함이 발생하면, 기본 경로를 따르는 노드가 로컬 보호 메커니즘을 가능하게 하므로, 기본 경로 상의 트래픽이 로컬 보호 경로로 전환된다. 그러나, 이 경우, 로컬 보호 경로는 서비스의 종단 간 SLA 보증 요구사항을 충족할 수 없으며, 서비스는 종단 간 백업 경로로 빠르게 전환되어야 한다.

[0071] 양방향 포워딩 검출(Bidirectional Forwarding Detection, BFD): BFD는 네트워크 상의 링크 또는 IP 경로의 포

워딩 연결 상황을 모니터링하기 위한 빠른 검출에 사용된다. BFD는 다양한 내부 게이트웨이 프로토콜(Interior Gateway Protocol, IGP) 및 경계 게이트웨이 프로토콜(Border Gateway Protocol, BGP)과 함께 자주 사용되어 빠른 수렴을 달성한다. BFD 세션이 설정되고, BFD 검출 패킷이 디폴트로 사전설정된 간격(예컨대, 1초)으로 전송된다. BFD 구현 원리는 소스 노드가 검출 패킷을 보내고, 목적지 노드가 검출 패킷을 수신한 후 검출 패킷에 응답하고, 헤드 노드가 응답 패킷을 수신한 후 검출이 성공한 것으로 간주하는 것이다. 결함 시나리오에서, 헤드 노드가 보낸 검출 패킷은 결함이 있는 중간 노드에 의해 폐기되고 목적지 노드로 성공적으로 전송될 수 없다. 결과적으로, 목적지 노드는 대응하는 응답 패킷을 보낼 수 없다. 마지막으로, 헤드 노드는 응답 패킷을 수신하지 않아서 링크 결함이 발생한 것으로 간주한다.

[0072] 패킷 인터넷 그로퍼(Packet Internet Groper, PING): PING은 주로 네트워크 연결 및 호스트 도달 가능성을 체크하는 데 사용된다. 소스 호스트는 ICMP(Internet Control Message Protocol) 요청 패킷을 목적지 호스트로 보내고, 목적지 호스트는 ICMP 응답 패킷을 소스 호스트로 보낸다. PING 커맨드는 네트워크 디바이스의 액세스 가능성을 체크하기 위한 가장 일반적인 디버깅 툴이다. 이 툴은 ICMP 에코 정보를 사용하여 원격 디바이스의 사용가능 여부를 판단하고, 원격 디바이스의 왕복(round-trip) 통신에서 지연(delay) 패킷(packet)의 손실 상황을 검출하는데, 예를 들면, PING을 사용하여 IPv4 패킷을 전달하는 라벨 분배 프로토콜(Label Distribution Protocol, LDP) 터널의 연결 및 IPv6 패킷과 IPv4 패킷을 전달하는 트래픽 엔지니어링(Traffic Engineering, TE) 터널의 LDP 터널의 연결을 검출할 수 있거나 또는 트레서트(Tracert) 커맨드를 사용하여 IPv4 패킷을 전달하는 LDP 터널의 경로 정보 또는 결함 위치 및 IPv4 패킷을 전달하는 TE 터널의 경로 정보 또는 결함 위치를 검출할 수 있다.

[0073] 운영, 관리 및 유지보수(Operations, Administration and Maintenance, OAM): OAM은 주로 경로 연결을 모니터링하고 결함을 신속하게 검출하는 데 사용된다. SR OAM(Operations, Administration and Maintenance)은 주로 라벨 전환 경로(LSP) 연결을 모니터링하고 결함을 신속하게 검출하는 데 사용된다. 현재, SR OAM은 주로 PING과 Tracert를 통해 구현되고 있다.

[0074] 양방향 능동 측정 프로토콜(two-Way Active Measurement Protocol, TWAMP): TWAMP는 인터넷 프로토콜(Internet Protocol, IP) 링크에 사용되는 성능 측정 기술이고, 순방향 및 역방향으로 양방향 성능 측정을 수행할 수 있다. TWAMP는 사용자 데이터그램 프로토콜(User Datagram Protocol, UDP) 데이터 패킷을 측정 프로브로서 사용하여 양방향 네트워크 지연 및 지터 측정을 수행한다. 또한, 프로토콜은 안전하며 제어 및 측정 기능의 분리를 보장할 수 있다. TWAMP가 배치된 네트워크 디바이스 간의 협력을 통해, 디바이스 간의 IP 성능 통계 데이터가 효과적으로 획득될 수 있다.

[0075] 인터넷 프로토콜 데이터 흐름 기반 채널 관련 OAM 성능 측정(인시투 흐름 정보 원격측정(in-situ Flow information Telemetry, IFIT)): IFIT는 실제 서비스 흐름에 기반한 인시투 흐름 측정 기술이다. 구체적으로, IFIT는 실제 서비스 흐름에 피처 마킹(컬러링(coloring))을 수행하고, 피처 필드에 대한 패킷 손실 및 지연 측정의 인시튜 흐름 검출을 수행한다. 기존의 능동 및 수동 측정 기술에 비해, IFIT는 측정 정밀도가 높고 운영, 관리 및 유지보수가 간단하다. 또한, iOAM/INT와 같은 인시튜 흐름 측정 기술에 비해, IFIT는 오버헤드가 적고 보다 정확한 경계를 구현한다. 또한, IP 흐름 성능 측정(IP Flow Performance Measurement, IP FPM)에 비해, IFIT는 기존 네트워크와 더 잘 호환되고, 배치하기 쉬우며, 확장이 더 유연하다. IP RAN IFIT는 IP 서비스 흐름 수준 종단 간 및 홉별 SLA(주로 패킷 손실률, 지연, 지터 및 실시간 트래픽을 포함)를 측정하는 기능을 제공하고, 네트워크 결함을 신속하게 검출하고 정확한 경계 및 문제 해결을 수행할 수 있으며, 미래 5G 모바일 베어러 네트워크에서 운영, 관리 및 유지보수를 수행하는 중요한 방법이다.

[0076] 본 출원은 SR 기술의 적용에 관한 것이기 때문에, 이하에서는 SR 기술의 몇몇 용어를 설명한다.

[0077] 세그먼트 라우팅(Segment Routing, 줄여서 SR): SR은 네트워크에서 패킷을 포워딩하기 위해 소스 라우팅을 기반으로 설계된 기술이다. 세그먼트 라우팅은 네트워크 경로를 세그먼트로 나누고, 네트워크 상의 세그먼트 및 포워딩 노드에 세그먼트 식별자(세그먼트 ID(Segment ID), SID)를 할당한다. SID를 순차적으로 배열하여 세그먼트 목록(Segment List)을 얻는다. 세그먼트 목록은 패킷 포워딩 경로를 나타낼 수 있다. SR 기술을 기반으로, 세그먼트 목록을 전달하는 패킷이 통과하는 경로 및 노드가 지정되어 트래픽 최적화 요구사항을 충족할 수 있다. 예를 들어, 패킷은 수하물에 비유될 수 있고, SR은 수하물의 라벨에 비유될 수 있다. A 지역에서 D 지역으로 B 지역과 C 지역을 거쳐 수하물을 보내야 하는 경우, "먼저 B 지역으로, 다음으로 C 지역으로, 마지막으로 D 지역으로"라는 라벨을 출발지 지역, 즉 A 지역에서 수하물에 부착할 수 있다. 이렇게 하여, 각 지역에서, 수하물 상의 라벨만 식별하면 되며, 수하물의 라벨에 기초하여 한 지역에서 다른 지역으로 수하물이 운송된다. SR 기술을 기

반으로, 소스 노드는 패킷에 라벨을 추가하고, 중간 노드는 패킷이 목적지 노드에 도달할 때까지 라벨에 기초하여 다음 노드로 패킷을 포워딩할 수 있다. 예를 들어, <SID1, SID2, SID3>는 패킷의 패킷 헤더에 삽입된다. 이 경우, 패킷은 먼저 SID1에 대응하는 노드로 포워딩되고, SID2에 해당하는 노드로 포워딩된 다음 SID3에 대응하는 노드로 포워딩된다.

[0078] SR 터널(SR Tunnel): SR 터널은 헤드 노드가 세그먼트 목록을 패킷 헤더로 캡슐화하는 터널이며, 관리자에 의해 수동으로 생성될 수 있거나, NETCONF 또는 PCEP와 같은 인터페이스 프로토콜를 통해 제어기에 의해 자동으로 생성될 수 있다. 하나의 SR 터널은 트래픽 엔지니어링 TE, OAM, FRR 등에 사용될 수 있다.

[0079] SR 라벨 전환 경로(Label Switched Path, LSP): SR LSP는 SR 기술을 사용하여 설정된 라벨 포워딩 경로이다. 접두사 또는 노드 세그먼트는 데이터 패킷 포워딩을 안내하는 데 사용된다. 하나의 SR 터널은 하나 이상의 SR LSP를 포함할 수 있다.

[0080] 세그먼트 라우팅-트래픽 엔지니어링(Segment Routing-Traffic Engineering, SR-TE): SR-TE는 SR을 제어 프로토콜로서 사용하는 새로운 TE 터널 기술이다. 제어기는 터널 포워딩 경로를 계산하고 포워더에 그 경로에 엄격하게 대응하는 라벨 스택을 전달하는 것을 담당한다. SR-TE 터널의 인그레스 노드에서, 포워더는 라벨 스택을 기반으로 네트워크에서 패킷의 전송 경로를 제어할 수 있다. 라벨 스택은 라벨 배열 세트이며 완전한 라벨 전환 경로(Label Switched Path, LSP)를 식별하는 데 사용된다. 라벨 스택의 각 인접 라벨은 특정 인접을 식별하고, 전체 라벨 스택은 완전한 라벨 전환 경로(LSP)의 모든 인접을 식별한다. 패킷 포워딩 동안, 라벨 스택의 각 인접 라벨에 기초하여 해당 인접을 찾고 각 라벨이 팝 아웃된 후 포워딩된다. 라벨 스택의 모든 인접 라벨이 팝 아웃된 후, 패킷은 완전한 LSP를 통과하여 SR-TE 터널의 목적지 디바이스에 도달한다.

[0081] SRv6 기술: SRv6 기술은 SR 기술을 IPv6 네트워크에 적용하는 것을 의미한다. SRv6 SID는 IPv6 주소(128 비트)를 사용하여 인코딩되고 SRv6 확장 헤더(SRH)에 캡슐화된다. 패킷 포워딩 중에, SRv6 인식 노드는 패킷의 목적지 주소(Destination Address, DA)를 기반으로 로컬 SID 테이블(local SID table)을 검색한다. 패킷의 목적지 주소가 로컬 SID 테이블의 임의의 SID와 일치하면, 목적지 주소가 로컬 SID 테이블에 적중한 것으로 결정된다. 이 경우, 해당 동작은 SID에 해당하는 토폴로지, 명령어 또는 서비스에 기초하여 수행된다. 패킷의 목적지 주소가 로컬 SID 테이블의 어떠한 SID와도 일치하지 않으면, 목적지 주소를 기반으로 IPv6 라우팅 및 포워딩 테이블이 검색되고, 패킷은 라우팅 및 포워딩 테이블에서 목적지 주소에 적중한 라우팅 및 포워딩 테이블을 기반으로 포워딩된다.

[0082] 로컬 SID 테이블(local SID table, 로컬 SID 테이블이라고도 함): 로컬 SID 테이블은 SRv6 가능 노드에 의해 유지되는 테이블이다. 로컬 SID 테이블은 로컬 노드에 의해 생성된 SRv6 SID를 포함한다. SRv6 포워딩 테이블 FIB는 로컬 SID 테이블을 기반으로 생성될 수 있다. 로컬 SID 테이블에는 다음과 같은 세 가지 기능이 있다: 1. 로컬로 생성된 SID, 예컨대, End.X SID를 정의함. 2. 이들 SID에 바인딩된 명령어를 지정함. 3. 명령어와 관련된 포워딩 정보, 예컨대, 아웃바운드 인터페이스 및 다음 홉을 저장함. 일부 실시예에서, 커맨드 "display segment-routing ipv6 local-sid"가 입력된 후, 디바이스에 구성된 SRv6의 로컬 SID 테이블이 보일 수 있다. 커맨드는 SRv6 End의 로컬 SID 테이블을 보도록 지정하기 위해 파라미터 End를 전달할 수 있다. 커맨드는 SRv6 End.X의 로컬 SID 테이블을 보도록 지정하기 위해 파라미터 End.X를 전달할 수 있다. 커맨드는 SRv6 End.DT4의 로컬 SID 테이블을 보도록 지정하기 위해 파라미터 End.DT4를 전달할 수 있다.

[0083] SRv6 패킷: IPv6 패킷은 표준 IPv6 헤더, 확장 헤더(0...n) 및 페이로드(payload)로 구성된다. IPv6 포워딩 평면을 기반으로 SRv6을 구현하기 위해, SRH라고 하는 IPv6 확장 헤더가 추가된다. 확장 헤더는 IPv6 명시적 경로를 지정하고 IPv6 세그먼트 목록 정보를 저장한다. 확장 헤더의 기능은 SR MPLS에서 세그먼트 목록의 기능과 동일하다. 헤드 노드는 IPv6 패킷에 SRH 확장 헤더를 추가하여 중간 노드가 SRH 확장 헤더에 포함된 경로 정보를 기반으로 패킷을 포워딩할 수 있다. 확장 헤더를 추가함으로써, SR은 원래의 IPv6 포워딩 평면과 원활하게 통합된다.

[0084] SRv6 패킷의 IPv6 헤더는 소스 주소(source address, SA) 및 목적지 주소(destination address, DA)를 포함할 수 있다. 공통 IPv6 패킷에서, IPv6 DA는 고정되어 있다. SRv6에서, IPv6 DA는 현재 패킷의 다음 노드를 식별한다. SR 터널에서, SR 노드는 목적지 주소를 지속적으로 업데이트하여 홉별 포워딩을 구현할 수 있다. IPv6 헤더의 목적지 주소가 전달하는 SID를 활성 SID라고 할 수 있다.

[0085] SRv6 패킷의 SRH는 IPv6 확장 헤더이다. SRH는 IPv6 포워딩 평면을 기반으로 SRv6을 구현하는 데 사용된다. SRH는 세그먼트 목록을 포함할 수 있다. 세그먼트 목록은 하나 이상의 SID를 포함할 수 있으며, 각 SID는 IPv6 주

소의 형태일 수 있다. 따라서, 세그먼트 목록은 명시적 IPv6 주소 스택으로도 이해될 수 있다. 세그먼트 목록은 세그먼트 목록[n]으로 표시될 수 있고, 세그먼트 목록[n]의 길이는 128*n 비트이며, 세그먼트 목록은 경로의 마지막 세그먼트부터 인코딩될 수 있다. 세그먼트 목록은 IPv6 주소의 형식이다.

[0086] SRH는 (2.1) 내지 (2.9)를 포함할 수 있다.

[0087] (2.1) 세그먼트 목록

[0088] 세그먼트 목록은 하나 이상의 SID를 포함할 수 있고, 각 SID는 IPv6 주소의 형식일 수 있다. 따라서, 세그먼트 목록은 명시적 IPv6 주소 스택으로도 이해될 수 있다. 세그먼트 목록은 세그먼트 목록[n]으로 표시될 수 있고, 세그먼트 목록[n]의 길이는 128*n 비트이며, 세그먼트 목록은 경로의 마지막 세그먼트부터 인코딩될 수 있다. 세그먼트 목록은 IPv6 주소의 형식이다.

[0089] (2.2) 남은 세그먼트(Segments Left, SL)

[0090] SL은 목적지 노드에 도달하기 전에 여전히 액세스될 필요가 있는 중간 노드의 수를 나타내는 데 사용되며, SL 필드는 나머지 노드 필드로도 지칭될 수 있다. SL 필드의 값은 세그먼트 목록에서 활성 SID를 나타낼 수 있다. SL의 길이는 8비트일 수 있다. 예를 들어, 세그먼트 목록이 5개의 SID(SID0, SID1, SID2, SID3, SID4)를 포함하고 SL 값이 2이면, 세그먼트 목록에 처리되지 않은 2개의 SID(SID0 및 SID1)가 있고, 세그먼트 목록에 현재 처리될 1개의 SID(SID2)가 있으며, 세그먼트 목록에 2개의 처리된 SID(SID3 및 SID4)가 있다.

[0091] (2.3) 하나 이상의 TLV

[0092] TLV는 인코딩 포맷이며, TLV는 유형(Type), 길이(Length) 및 값(Value)을 포함한다. SRH는 하나의 TLV를 포함할 수 있거나, 복수의 TLV를 포함할 수 있다. SRH의 상이한 TLV 간에 병렬 관계 또는 중첩 관계가 있을 수 있다.

[0093] 또한, 도 9에 도시된 바와 같이, SRH는 다음 필드를 더 포함할 수 있다:

[0094] (2.4) 다음 헤더(Next Header): SRv6 패킷은 확장 헤더 뒤에 하나 이상의 확장 헤더 또는 하나 이상의 상위 계층 헤더를 더 포함할 수 있으며, 다음 헤더는 SRH 바로 다음에 오는 헤더의 유형을 즉시 식별하는 데 사용된다. 다음 헤더 필드의 길이는 8비트일 수 있다.

[0095] (2.5) 헤더 확장 길이(영문: Header Extended Length, 줄여서 Hdr Ext Len) 필드: Hdr Ext Len 필드는 SRH 헤더의 길이를 나타내는 데 사용된다. Hdr Ext Len 필드는 주로 세그먼트 목록[0]에서 세그먼트 목록[n]까지의 길이를 나타낸다. 헤더 확장 길이 필드는 8비트일 수 있다.

[0096] (2.6) 라우팅 유형(Routing Type) 필드: 라우팅 유형 필드는 라우트 헤더 유형을 식별하는 데 사용되며, 값 4는 SRH 유형을 식별한다. 라우팅 유형 필드의 길이는 8비트일 수 있다.

[0097] (2.7) 마지막 엔트리(Last Entry) 필드: 마지막 엔트리 필드는 세그먼트 목록에서 마지막 요소의 인덱스이다. 마지막 엔트리 필드의 길이는 8비트일 수 있다.

[0098] (2.8) 플래그(Flags) 필드: 플래그 필드는 데이터 패킷의 일부 식별자를 표시하는 데 사용된다. 플래그 필드의 길이는 8비트일 수 있다.

[0099] (2.9) 태그 필드: 태그 필드는 데이터 패킷의 동일한 그룹을 식별하는 데 사용된다. 태그 필드의 길이는 16비트일 수 있다.

[0100] SRv6 패킷의 페이로드는 IPv4 패킷, IPv6 패킷, 또는 이더넷(영문: Ethernet) 프레임일 수 있다.

[0101] 세그먼트 라우팅-트래픽 엔지니어링(Segment Routing-Traffic Engineering, SR-TE)은 SR을 제어 프로토콜로서 사용하는 새로운 TE 터널 기술이다. 제어기는 터널 포워딩 경로를 계산하고 포워더에 그 경로에 엄격하게 대응하는 라벨 스택을 전달하는 역할을 한다. SR-TE 터널의 인그레스 노드에서, 포워더는 라벨 스택을 기반으로 네트워크에서 패킷의 전송 경로를 제어할 수 있다.

[0102] 라벨 스택은 라벨 배열 세트이며 완전한 라벨 전환 경로(Label Switched Path, LSP)를 식별하는 데 사용된다. 라벨 스택의 각 인접 라벨은 특정 인접을 식별하고, 전체 라벨 스택은 완전한 라벨 전환 경로(LSP)의 모든 인접을 식별한다. 패킷 포워딩 동안, 라벨 스택의 각 인접 라벨에 기초하여 해당 인접을 찾고, 각 라벨이 팝 아웃된 후 포워딩된다. 라벨 스택의 모든 인접 라벨이 팝 아웃된 후, 패킷은 완전한 LSP를 통과하여 SR-TE 터널의 목적

지 디바이스에 도달한다.

[0103] 본 출원의 실시예는 보호 전환 기술의 적용, 특히 종단 간 보호 기술 및 로컬 보호 기술의 적용에 관한 것이다. 쉬운 이해를 위해, 다음은 먼저 본 출원의 실시예에서 보호 전환 기술의 관련 개념을 설명한다.

[0104] 터널은 두 지점 사이의 종단 간 경로 세트이다. 두 지점을 각각 터널의 시작점과 터널의 끝점이라고 한다. 터널은 하나 이상의 경로를 포함한다. 선택적으로, 터널에 포함된 경로는 LSP이다. 도 1에 도시된 바와 같이, 예를 들어, 터널 1은 PE1과 PE3 사이의 경로 세트이다. 터널 1은 2개의 경로를 포함한다. 터널 1에 포함된 하나의 경로는 PE1->P1->P3->PE3이고, 경로는 터널 1에 포함된 기본 경로이다. 터널 1에 포함된 다른 경로는 PE1->PE2->P2->P4->PE4->PE3이고, 경로는 터널 1에 포함된 백업 경로이다. 다른 예로, 터널 2는 PE2와 PE4 사이의 경로 세트이다. 터널 2는 2개의 경로를 포함한다. 터널 2에 포함된 하나의 경로는 PE2->P2->P4->PE4이고, 경로는 터널 2에 포함된 기본 경로이다. 터널 2에 포함된 다른 경로는 PE2->PE1->P1->P3->PE3->PE4이며, 경로는 터널 2에 포함된 백업 경로이다. PE는 제공자 에지(Provider Edge, PE) 디바이스를 의미하고, P는 제공자(Provider, P) 디바이스를 의미한다.

[0105] 기본 경로는 종단 간을 위해 계획된 주요 경로이다. 선택적으로, 하나의 터널에 복수의 서로 다른 LSP가 사전계획되어 있는 경우, 기본 경로는 터널의 기본 LSP이다. 선택적으로, 터널에 하나의 LSP만 사전계획된 경우, 기본 경로는 LSP이거나 터널일 수 있다. 기본 경로에서 발생하는 결함은 기본 경로의 노드 결함과 기본 경로의 링크 결함을 포함한다. 특히, 계획된 종단 간 경로는 노드 및 서로 다른 노드 간의 링크라는 두 가지 요소를 포함한다. 기본 경로에서 결함 검출이 수행되면, 소스 노드는 기본 경로 상의 이그레스 노드로 패킷을 보낸다. 기본 경로 상의 중간 노드에 결함이 있거나 중간 노드에 연결된 링크에 결함이 있으면, 기본 경로에 결함이 있다.

[0106] 로컬 보호 경로는 결함 지점을 통과하지 않는 보호 경로이다. 예를 들어, 로컬 결함이 노드 결함인 경우, 로컬 보호 경로는 결함이 있는 노드를 통과하지 않는 경로이고, 로컬 결함이 링크 결함인 경우, 로컬 보호 경로는 결함이 있는 링크를 통과하지 않는 경로이다. 일반적으로, 로컬 보호 경로는 결함이 있는 노드 또는 결함이 있는 링크를 건너뛰는 제약만 충족하며, 기본 경로를 대체하지 않는다. 로컬 보호 경로 상의 헤드 노드는 일반적으로 기본 경로 상의 중간 노드이다. 로컬 보호 경로는 토폴로지 독립 루프 프리 대체 고속 리라우트(Topology-Independent Loop-free Alternate FRR, TI-LFA FRR) 경로 및 중간점 토폴로지 독립 루프 프리 대체(Midpoint TI-LFA) 경로를 포함한다.

[0107] 로컬 보호 알고리즘은 로컬 보호 경로로 전환하기 위해 중간 노드에 의해 사용되는 알고리즘이다. 예를 들어, 결함 노드의 이전 홉 노드는 로컬 보호 알고리즘을 사용하여 결함 노드를 건너뛰기 위한 다른 경로를 계산하고, 계산된 경로는 로컬 보호 경로이다.

[0108] TI-LFA FRR은 SR 터널에 대한 링크 및 노드 보호를 제공한다. 링크나 노드에 결함이 있으면, 트래픽을 신속하게 백업 경로로 전환하여 지속적인 포워딩을 함으로써 트래픽 손실을 최소화한다. 일부 LFA FRR 및 원격 LFA(Remote LFA) 시나리오에서, P 공간과 Q 공간은 교차하거나 직접 이웃을 갖지 않는다. 결과적으로, 백업 경로를 계산할 수 없으며, 안정성 요구사항을 충족할 수 없다. 이 경우, TI-LFA가 구현된다. TI-LFA 알고리즘을 사용하여, 보호 경로를 기반으로 P 공간, Q 공간 및 수렴 후(Post-convergence) 최단 경로 트리가 계산되고, 서로 다른 시나리오에 따라 수리 목록(Repair List)이 계산되며, 소스 노드와 PQ 노드 사이에 SR 터널이 설정되어 백업 다음 홉 보호를 형성한다. 보호 링크에 결함이 있으면, 트래픽을 자동으로 터널 백업 경로로 전환하여 지속적인 포워딩을 함으로써 네트워크 안정성을 향상시킨다. 기존의 LFA 기술은 적어도 하나의 이웃이 목적지 노드에 대해 루프가 없는 다음 홉을 갖는다는 것을 보장해야 한다. RLFA 기술은 네트워크에 적어도 하나의 노드가 존재하고 소스 노드에서 노드로의 경로 및 노드에서 목적지 노드로의 경로가 결함이 있는 노드를 통과하지 않음을 보장해야 한다. TI-LFA 기술은 명시적 경로를 사용하여 백업 경로를 나타내고, 토폴로지에 제한을 두지 않으며, FRR 기술에 더 높은 신뢰성을 제공할 수 있다. TI-LFA가 SRv6 네트워크에 배치되면, 로컬 보호의 50ms 전환 성능을 충족할 수 있다. 또한, SRv6 TE 정책 목록을 위한 SBFD가 배치되어 종단 간 결함을 신속하게 감지하여 종단 간 서비스의 50ms 전환 성능을 충족할 수 있다.

[0109] 종단 간 보호 경로는 전역 보호 경로이다. 특히, 종단 간 기본 경로의 경우, 종단 간 백업 경로를 제공함으로써 종단 간 보호가 구현되고, 백업 경로는 종단 간 보호 경로이다. 종단 간 보호 경로는 다음 구현을 포함한다.

[0110] 방식 1: 2개의 서로 다른 LSP가 하나의 터널(tunnel)에 계획된다. 2개의 서로 다른 LSP는 각각 기본 LSP와 백업 LSP이며, 백업 LSP는 기본 LSP의 종단 간 보호 경로이다. 예를 들어, 2개의 종단 간 경로, 즉 경로1 "A-B-D"와 경로2 "A-C-D"가 노드 A와 노드 D 사이에 배치될 수 있다. 경로1과 경로2 사이에는 기본/백업 관계가 있고, 경

로1은 기본 경로로서 계획되며, 경로2는 백업 경로로서 계획될 수 있다.

[0111] 방식 2: 소스에서 목적지까지 2개의 터널이 있다. 2개의 터널은 동일한 소스와 싱크를 갖는다. 즉, 소스 노드는 동일하고 싱크 노드는 동일하다. 2개의 터널은 각각 기본 터널과 백업 터널이다. 백업 터널은 기본 터널의 종단 간 보호 경로이다. 기본 터널과 백업 터널은 2개의 가상 사설 네트워크(Virtual Private Network, VPN) 서비스에 의해 반복되며, VPN 보호가 구현된다.

[0112] 본 출원의 실시예에서 제공되는 패킷 처리 방법은 로컬 보호 메커니즘과 종단 간 보호 메커니즘이 공존하는 시나리오에 적용될 수 있다. 이 시나리오에서, 서비스는 우선적으로 로컬 보호 경로를 따라 이동한다. 예를 들어, 고객은 네트워크에 대한 특정 SLA 요구사항을 가지고 있으며, 이는 SLA 요구사항을 충족하는 상이한 경로를 계획함으로써 구현될 수 있다. 다른 예로, 고객이 네트워크에 로컬 보호(예컨대, TI-LFA 또는 중간점 TI-LFA)를 배치한다. 이 경우, 노드 또는 링크에 결함이 있으면, 디바이스는 우선적으로 로컬 보호 경로로 전환하지만, 종단 간 보호 경로로 빠르게 전환할 수 없다. 예를 들어, 로컬 보호 TI-LFA/중간점 TI-LFA 및 종단 간 BFD 검출 기술이 SRv6 네트워크에 배치된다. BFD 검출 패킷과 서비스 데이터 패킷은 동일한 경로를 통해 전송된다. 또한, 로컬 보호가 구현될 때, 프로토콜 패킷 상호작용은 여전히 TI-LFA 보호 경로를 통해 구현될 수 있다. 이 경우, 링크 결함을 빠르게 검출할 수 없으며 서비스를 백업 경로로 전환할 수 없다. 결과적으로, 트래픽은 오랫동안 알려지지 않은 경로로 우회된다. 결함이 발생하면, 서비스 경로는 제어기 또는 다른 경로 계산 모듈이 서비스를 트리거하여 헤드 노드 상의 백업 경로로 전환하거나 SLA 요구사항을 충족하는 경로를 헤드 노드에 재전달하기를 기다려야 한다. 새로운 경로에서, 현재 서비스 경로는 오랫동안 TI-LFA 보호 경로로 우회된다. 이 경우, 경로가 SLA 요구사항을 충족할 수 없다. 그러나, 다음 실시예에서는, 검출 패킷에 보호 플래그가 추가되어 검출 패킷이 로컬 보호 경로를 거치는 것을 방지할 수 있다. 따라서, 로컬 결함이 발생하면, 검출 패킷이 손실되어 검출 패킷의 소스 노드가 패킷을 종단 간 보호 경로로 전환하도록 트리거할 수 있다.

[0113] 다음은 본 출원에서 시스템 아키텍처의 예를 설명한다.

[0114] 도 1은 본 출원의 실시예에 따른 패킷 처리 시스템을 도시한다. 도 1에 도시된 바와 같이, 시스템은 복수의 네트워크 디바이스를 포함하며, 서로 다른 네트워크 디바이스는 네트워크를 통해 서로 연결되어 있다. 복수의 네트워크 디바이스는 고객 에지(Customer Edge, CE) 디바이스, 제공자(Provider, P) 디바이스, 및 제공자 에지(Provider Edge, PE) 디바이스를 포함하지만, 이에 제한되지 않는다. 시스템 아키텍처(100)는 기본 경로 및 기본 경로를 보호하는 데 사용되는 보호 경로를 배치한다.

[0115] 구체적으로, 패킷 처리 시스템은 CE1, PE1, PE2, P1, P2, P3, P4, PE3, PE4, 및 CE2를 포함한다. 패킷 처리 시스템에서, 몇몇 제공자는 대역폭 요구사항 또는 지연 요구사항과 같은 고객의 SLA 품질 요구사항을 충족하는 데 터널링 기술을 사용한다. 터널에서, 도 1에 도시된 바와 같이 고객의 요구사항에 따라 상이한 경로가 계획될 수 있다. PE1과 PE3 사이에 터널 1이 설정되고, 터널 1에 대해 완전히 분리된 2개의 경로가 계획된다. 터널 1의 기본 경로는 PE1->P1->P3->PE3이고, 터널 1의 기본 경로 상의 헤드 노드는 PE1이며, 터널 1 상의 중간 노드는 P1 및 P3이고, 터널 1 상의 이그레스 노드는 PE3이다. 터널 1의 백업 경로는 PE1->PE2->P2->P4->PE4->PE3이다. 터널 1의 백업 경로 상의 헤드 노드는 PE1이고, 터널 1의 백업 경로 상의 중간 노드는 PE2, P2, P4 및 PE4를 포함하며, 터널 1의 백업 경로 상의 이그레스 노드는 PE3이다. 터널 1의 백업 경로는 터널 1의 기본 경로의 종단 간 보호 경로이다. 터널 1의 기본 경로와 터널 1의 백업 경로는 하나의 터널에 있는 2개의 서로 다른 LSP이며, 2개의 LSP는 기본/백업 LSP 관계를 형성한다.

[0116] PE2와 PE4 사이에 터널 2가 설정되고, 터널 2에 대해 완전히 분리된 2개의 경로가 계획된다. 터널 2의 기본 경로는 PE2->P2->P4->PE4이다. 터널 2의 기본 경로 상의 헤드 노드는 PE2이고, 터널 2의 기본 경로 상의 중간 노드는 P2 및 P4를 포함하며, 터널 2의 기본 경로 상의 이그레스 노드는 PE4이다. 터널 2의 백업 경로는 PE2->PE1->P1->P3->PE3->PE4이다. 터널 2의 백업 경로는 터널 2의 기본 경로의 종단 간 보호 경로이다. 터널 2의 기본 경로와 터널 2의 백업 경로는 하나의 터널에 있는 2개의 서로 다른 LSP이며, 2개의 LSP는 기본/백업 LSP 관계를 형성한다.

[0117] 터널 1 및 터널 2는 선택적으로 서로 다른 SLA 요구사항을 충족한다. 예를 들어, 터널 1은 고대역폭 요구사항을 충족한다. 고객에게 대역폭 요구사항이 있는 서비스가 있는 경우, 터널 1을 사용하여 서비스를 전달할 수 있다. 터널 2는 지연 요구사항을 충족한다. 고객에게 지연 요구사항이 있는 서비스가 있는 경우, 터널 2를 사용하여 서비스를 전달할 수 있다.

[0118] 터널은 서비스를 외부적으로 전달하는 데 사용되지만, 터널에서 계획된 경로는 트래픽 포워딩을 안내하는 데 사

용된다. 서비스 트래픽이 터널을 통해 전달될 때, 서비스 트래픽 연속성이 보장되어야 한다. 물리적 네트워크 요소 결함 또는 소프트웨어 결함으로 인해 서비스 트래픽 연속성이 중단될 수는 없다. 따라서, 서비스 트래픽이 터널을 통해 전달될 때, 물리적 네트워크 요소 결함(네트워크 요소의 링크 결함 또는 전체 네트워크 요소의 결함) 또는 소프트웨어(프로토콜) 결함이 발생하면, 터널을 통해 전달되는 서비스가 중단되지 않거나 오랫동안 중단되지 않음을 보장하기 위해 터널에 보호 메커니즘이 제공되어야 한다. SLA 품질 요구사항이 있는 서비스의 경우, 네트워크 요소 결함 또는 링크 결함이 발생할 때 SLA 품질 요구사항을 여전히 충족해야 한다. 이 보증 수단은 터널 보호 솔루션과 서비스 보호 솔루션으로 분류된다. 터널 보호 솔루션은 로컬 터널 보호 기술과 종단 간 터널 보호 기술을 포함한다. 서비스 보호 솔루션은 VPN FRR 보호 수단을 포함한다. 서비스 보호는 VPN에서 실행되는 서비스를 보호하는 것을 의미한다.

[0119] 로컬 터널 보호 솔루션의 경우, 로컬 터널 보호 기술은 결함(네트워크 요소 결함 또는 링크 결함)이 발생할 때 현재 서비스 트래픽을 전달하고 있는 터널이 통과하는 경로를 로컬로 조정하는 것을 의미한다. 도 2에 도시된 바와 같이, 굵은 실선은 터널 내 포워딩 경로를 나타내며, 포워딩 경로는 PE1->RT_1->RT_3->RT_5->RT_7->PE2이다. RT_3과 RT_5 사이의 링크에 결함이 있는 경우, RT_3은 로컬 보호 메커니즘을 시작한다. 마지막으로, 서비스 트래픽을 전달하는 경로가 로컬 보호 경로로 전환된다. 로컬 보호 경로는 도 2에 점선으로 도시되고, 로컬 보호 경로는 RT_3->RT_4->RT_6->RT_5이고, 로컬 보호 경로 상의 인그레스 노드는 RT_3이다.

[0120] 종단 간 터널 보호 솔루션의 경우, 종단 간 보호 기술은 서비스 트래픽을 전달할 수 있는 적어도 2개의 경로가 터널에 존재하는 것을 요구한다. 한 경로는 기본 경로이고, 다른 경로는 백업 경로이다. 서비스는 한 번에 한 경로에서만 전달된다. 서비스를 전달하는 기본 경로에 결함이 있으면, 터널의 헤드 노드가 서비스를 백업 경로로 전환한다. 도 3에 도시된 바와 같이, 서비스는 원래 기본 경로를 통해 전달된다. RT_3과 RT_5 사이의 경로에 결함이 있으면, 헤드 노드 PE1은 서비스를 백업 경로로 전환한다. 기본 경로는 도 3에서 굵은 실선으로 도시되고, 기본 경로는 PE1->RT_1->RT_3->RT_5->RT_7->PE2이다. 백업 경로는 도 3에서 점선으로 도시되고, 백업 경로는 PE1->RT_2->RT_4->RT_6->RT_8->PE2이다.

[0121] 로컬 터널 보호와 종단 간 터널 보호의 결합의 경우, 로컬 보호는 단일 경로에 대한 보호이며, 종단 간 보호 기술에서 기본 경로를 보호하는 데에도 사용할 수 있다. 예를 들어, 기본 경로의 네트워크 요소에 결함이 있거나 네트워크 요소 간의 링크에 결함이 있는 경우, 기본 경로의 연결성을 보장하기 위해 로컬 보호가 먼저 수행될 수 있다. 그런 다음, 관련 SLA 요구사항을 충족하기 위해 종단 간 보호가 수행되어 서비스를 다른 백업 경로로 전환한다. 도 4에 도시된 바와 같이, 서비스는 기본 경로에서 전달된다. 도 4의 기본 경로는 굵은 실선으로 도시되어 있고, 도 4의 기본 경로는 PE1->RT_1->RT_3->RT_5->RT_7->PE2이다. RT_3과 RT_5 사이의 경로에 결함이 있는 경우, 노드 RT_3은 로컬 보호 메커니즘을 시작하여 서비스를 로컬 보호 경로로 전환하여 서비스 연속성을 보장한다. 로컬 보호 경로는 도 4에서 점선으로 도시되고, 로컬 보호 경로는 RT_3->RT_4->RT_6->RT_5이다. 그러나, 이 경우, 로컬 보호 경로는 SLA 요구사항을 충족하지 않는다. 기본 경로에 결함이 있음을 검출하면, 헤드 노드 PE1은 서비스를 백업 경로로 전환한다.

[0122] 종단 간 서비스 보호(VPN FRR 기술)의 경우, VPN FRR 기술은 종단 간 서비스 보호 기술이다. 이 기술은 터널을 사용하여 서비스를 전달하며, 터널의 목적지 주소는 서로 다른 원격 PE 노드이다(하나의 CE가 2개의 PE에 액세스함). 터널에 상이한 경로가 배치될 수 있으며, 이는 종단 간 터널 보호 및 로컬 터널 보호 기술이 사용될 수 있음을 의미한다. 서비스 트래픽을 전달하는 터널에 결함이 있으면, VPN FRR 기술을 사용하여 서비스를 다른 백업 터널로 전환할 수 있다. 도 5에 도시된 바와 같이, PE1을 인그레스로 하여 2개의 터널이 설정되고, 2개의 터널 내의 기본 터널은 PE1->P1->P3->PE3이고, 2개의 터널 내의 백업 터널은 PE1->PE2->P2->P4->PE4이다. 기본 터널의 인그레스 PE와 백업 터널의 인그레스 PE는 모두 PE1이고, 기본 터널의 이그레스 PE는 PE3이며, 백업 터널의 이그레스 PE는 PE4이다. 기본 터널에 결함이 있으면, PE1은 VPN FRR을 통해 터널 전환을 결정한다. 가능한 구현예에서, PE1은 PE3에 도달하는 데 사용되는 라우팅 정보와 PE4에 도달하는 데 사용되는 라우팅 정보를 라우팅 및 포워딩 테이블에 사전저장한다. PE1이 기본 터널에 결함이 있다고 결정하면, PE1이 트래픽을 수신한 후, 라우팅 및 포워딩 테이블에서 PE4에 도달하는 데 사용된 라우팅 정보를 기반으로 PE1은 PE3으로 원래 전송된 트래픽을 PE4로 전송하여, 서비스를 기본 터널에서 백업 터널로 전환한다.

[0123] Rv6 네트워크에서, TI-LFA 및 중간점 TI-LFA는 로컬 터널 보호 기술이다. 경로 상의 네트워크 요소 또는 링크에 결함이 있는 경우, 2개의 기술 TI-LFA 및 중간점 TI-LFA가 로컬 보호를 구현하는 데 사용될 수 있다. 그러나, 2개의 로컬 보호 기술은 링크 연결만 보장할 수 있고, 서비스 SLA 품질은 보장할 수 없다.

[0124] SRv6 TE 정책 목록을 위한 SBFD는 종단 간 터널 결함 검출 및 고속 수렴을 구현(종단 간 터널 보호를 구현)하는

보호 기술이다. 먼저, SLA 요구사항을 충족하는 2개의 경로(목록이라고도 함)를 SRv6 TE 정책 터널에 배치해야 하고, 기본 경로와 백업 경로를 구분하고 완전히 분리해야 한다. 또한, 기본 경로 및 백업 경로를 검출하기 위해 BFD가 수행된다. BFD가 기본 경로에 결함이 있음을 검출하면, 서비스를 신속하게 백업 경로로 전환하여 고속 서비스 수렴을 구현할 수 있다.

[0125] 로컬 보호 기술 TI-LFA/중간점 TI-LFA 및 종단 간 BFD 검출 기술이 모두 SRv6 네트워크에 배치되는 경우, BFD 검출 패킷 및 서비스 데이터 패킷은 동일한 경로를 통해 포워딩된다. 예를 들어, 도 6에 도시된 바와 같이, 결함이 발생하기 전에, 기본 경로 상의 BFD 검출 패킷은 경로 PE1->P1->P3->PE3을 통해 PE1에서 PE3으로 전송되고, 서비스 트래픽은 경로 CE1->PE1->P1->P3->PE3->CE2를 통해 CE1에서 CE2로 전송된다.

[0126] 로컬 보호가 발생할 때, BFD 검출 메커니즘은 여전히 TI-LFA 보호 경로를 통해 BFD 검출 패킷 교환을 완료할 수 있다. 예를 들어, 도 6에 도시된 바와 같이, P1과 P3 사이의 링크에 결함이 발생한 후, P1은 BFD 검출 패킷을 TI-LFA 보호 경로로 전환하므로, 기본 경로 상의 BFD 검출 패킷은 경로 PE1->P1->P2->P4->P3->PE3 경로를 통해 PE1에서 PE3으로 전송되어, PE3이 BFD 검출 패킷을 수신하고 응답할 수 있다. 이 경우, 터널 상의 헤드 노드는 링크 결함을 빠르게 검출할 수 없으며 백업 경로로 빠르게 전환되도록 헤드 노드에서 서비스가 트리거될 수 없다. 결과적으로, 트래픽은 오랫동안 로컬 보호 경로로 우회되고, 오랫동안 로컬 보호 경로로 우회된 트래픽은 고객의 SLA 요구사항을 충족할 수 없다. 로컬 보호가 발생하고 헤드 노드가 백업 경로로의 전환을 빠르게 수행할 수 없는 경우, 제어기 또는 다른 경로 계산 모듈만 사용하여 헤드 노드 상의 백업 경로 또는 SLA 요구사항이 헤드 노드로 재전달되는 것을 충족하는 경로를 통해 서비스가 전송되도록 트리거할 수 있다. 이 과정은 시간이 오래 걸리며, 결과적으로 현재 서비스가 오랫동안 TI-LFA 보호 경로로 우회될 수 있다.

[0127] 앞에서는 시스템 아키텍처를 설명하고, 이하에서는 예를 사용하여 패킷 포워딩 방법의 절차를 설명한다.

[0128] 실시예 1

[0129] 도 7은 본 출원의 실시예 1에 따른 패킷 처리 방법을 도시한다. 실시예 1은 S201 내지 S208을 포함한다. 선택적으로, 실시예 1의 S201, S202, S207 및 S208은 하나의 네트워크 디바이스에 의해 수행될 수 있으며, 예를 들어, 도 2의 PE1에 의해 수행될 수 있다. 실시예 1의 S203 내지 S206은 다른 네트워크 디바이스에 의해 수행될 수 있으며, 예를 들어, 도 2의 RT_3에 의해 수행될 수 있다.

[0130] 선택적으로, 실시예 1은 중앙 처리 장치(central processing unit, CPU)에 의해 처리된다. 선택적으로, 실시예 1은 네트워크 프로세서(Network Processor, 줄여서 NP)에 의해 처리된다. 선택적으로, 실시예 1은 CPU와 NP에 의해 공동으로 처리된다. 선택적으로, 실시예 1은 CPU 또는 NP에 의해 처리되지 않을 수 있지만, 패킷 포워딩에 적합한 다른 프로세서, 예를 들어, 필드 프로그램가능 게이트 어레이(Field Programmable Gate Array, FPGA) 칩 또는 다른 주문형 집적 회로(application-specific integrated circuit, ASIC) 칩에 의해 처리될 수 있다. 이것은 본 출원에서 제한되지 않는다.

[0131] S201: 제2 네트워크 디바이스는 보호 플래그를 포함하는 패킷을 생성한다.

[0132] 이 실시예에서, 보호 플래그가 패킷에 추가되고, 보호 플래그에 대한 다중 측 상호작용 절차가 설명된다. 이 실시예는 패킷을 수신한 디바이스가 보호 플래그를 기반으로 처리를 수행하는 방법에 관한 것이고, 패킷을 전송하는 디바이스가 패킷에 보호 플래그를 추가하는 방법에 관한 것이다. 서로 다른 네트워크 디바이스를 구별하기 위해, 패킷 수신 측으로서 역할을 하는 네트워크 디바이스는 제1 네트워크 디바이스로 지칭되고, 패킷 송신 측으로서 역할을 하는 네트워크 디바이스는 제2 네트워크 디바이스로 지칭된다. 선택적으로, 보호 플래그는 T 플래그 및 M 플래그 중 적어도 하나를 포함한다. T 플래그의 T는 TI-LFA를 나타낸다. T 플래그는 제1 네트워크 디바이스가 패킷을 기본 경로에서 TI-LFA 보호 경로로 전환하도록 허용되지 여부를 나타내는 데 사용된다. M 플래그의 M은 중간점(Midpoint) TI-LFA를 나타낸다. M 플래그는 제1 네트워크 디바이스가 패킷을 기본 경로에서 중간점 TI-LFA 보호 경로로 전환하도록 허용되는지 여부를 나타내는 데 사용된다.

[0133] 선택적으로, 제2 네트워크 디바이스는 기본 경로 상의 헤드 노드이다. 즉, 제2 네트워크 디바이스는 기본 경로 상의 인그레스 노드이다. 예를 들어, 도 1에 도시된 바와 같이, 제2 네트워크 장치는 PE1이고, PE1은 기본 경로 상의 헤드 노드이다. 예를 들어, SR 시나리오에서, 기본 경로는 SR 터널의 LSP이고, 제2 네트워크 디바이스는 SR 터널의 헤드 노드이다. SID 목록은 제2 네트워크 디바이스의 패킷으로 푸시되고, SID 목록의 각 SID는 SR 터널의 LSP 상의 각 노드를 식별하는 데 사용된다. 제2 네트워크 디바이스가 아웃바운드 인터페이스로부터 패킷을 보낸 후, 패킷은 SID 목록을 사용하여 SR 터널의 LSP를 통해 전송될 수 있다. 이 경우, 패킷은 제2 네트워크 디바이스로부터 SR 터널의 LSP로 유입된다. SR MPLS의 SR-TE 시나리오에서, SID 목록은 라벨 스택으로 지칭될 수

있다. SRv6 시나리오에서, SID 목록은 SRH의 세그먼트 목록일 수 있다. 물리적 하드웨어 측면에서, 제2 네트워크 디바이스는 예를 들어, 스위치 또는 라우터이다.

[0134] 선택적으로, 제1 네트워크 디바이스는 기본 경로를 따른 노드이고, 제1 네트워크 디바이스는 기본 경로 상의 중간 노드일 수 있다. 기본 경로 상의 패킷은 전송 중에 제1 네트워크 디바이스를 통과한다. 예를 들어, 도 1에 도시된 바와 같이, 제1 네트워크 디바이스는 도 1에서 P1이다. 다른 예를 들면, 도 2에 도시된 바와 같이, 제1 네트워크 디바이스는 도 2에서 RT_3이다. 물리적 하드웨어의 측면에서, 제1 네트워크 디바이스는 예를 들어 스위치 또는 라우터이다.

[0135] 보호 플래그는 제1 네트워크 디바이스가 패킷을 기본 경로에서 제1 보호 경로로 전환하도록 허용되는지 여부를 표시하는 데 사용된다. 예를 들어, 도 2에 도시된 바와 같이, 보호 플래그는 RT_3가 패킷을 기본 경로에서 계산을 통해 RT_3에 의해 획득된 로컬 보호 경로로 전환하도록 허용되는지 여부를 나타내는 데 사용된다.

[0136] 제1 보호 경로는 기본 경로를 보호하는 데 사용된다. 제1 보호 경로는 기본 경로의 로컬 보호 경로이다. 제1 보호 경로 상의 인그레스 노드는 제1 네트워크 디바이스이다. 제1 보호 경로와 기본 경로는 동일한 터널에 속할 수 있다. 예를 들어, 도 2에 도시된 바와 같이, 기본 경로는 PE1->RT_1->RT_3->RT_5->RT_7->PE2를 포함하고, 기본 경로는 PE1과 PE2 사이의 터널에서 LSP이다. 제1 보호 경로는 RT_3->RT_4->RT_6->RT_5를 포함하며, 제1 보호 경로는 PE1과 PE2 사이의 터널에 있는 또 다른 LSP이다. 제1 네트워크 디바이스는, 예를 들어, 도 2에서 RT_3이고, 기본 경로는 RT_3에서 제1 보호 경로로 전환되기 시작한다. 여기서 ->는 패킷 전송 방향을 나타내고, ->의 좌측은 패킷 송신단을 식별하고, ->의 우측은 패킷 수신단을 식별한다. 예를 들어, PE1->RT_1은 PE1이 패킷을 RT_1로 보낸다는 것을 나타낸다.

[0137] 선택적으로, 제1 보호 경로는 로컬 보호 경로이고, 개념 도입 부분에서 로컬 보호 경로의 임의의 특징을 갖는다. 구체적으로, 제1 보호 경로는 기본 경로 상의 노드를 보호하는 데 사용될 수 있다. 기본 경로 상의 노드에 결함이 있는 경우, 제1 보호 경로가 충족하는 제약은 제1 보호 경로가 기본 경로 상의 결함이 있는 노드를 통과하지 않는다는 것일 수 있다. 이와 달리, 제1 보호 경로를 사용하여 기본 경로 상의 링크를 보호할 수 있다. 기본 경로 상의 링크에 결함이 있는 경우, 제1 보호 경로가 충족하는 제약은 제1 보호 경로가 기본 경로 상의 결함이 있는 링크를 통과하지 않는다는 것일 수 있다. 일반적으로, 제1 보호 경로는 선택적으로 기본 경로 상의 결함 노드 또는 결함 링크를 건너뛰는 경로이며, 일반적으로 전체 기본 경로를 대체하지 않는다.

[0138] 예를 들어, 제1 보호 경로는 TI-LFA FRR 경로를 포함하고, 제1 보호 경로는 "TI-LFA FRR 백업 경로"로 지칭될 수 있으며, 제1 보호 경로는 TI-LFA 알고리즘을 사용하여 계산을 통해 제1 네트워크 디바이스에 의해 획득된 경로이다. 다른 예로, 제1 보호 경로는 중간점 TI-LFA 경로를 포함하고, 제1 보호 경로는 "바이패스(bypass) CR-LSP"로 지칭될 수 있다.

[0139] 선택적으로, 기본 경로가 작동할 때, 제1 보호 경로는 유휴 상태에 있고 서비스 데이터를 독립적으로 전달하지 않는다.

[0140] 선택적으로, SLA 보증 시나리오에서, 기본 경로는 SLA를 충족하는 경로이고, 제1 보호 경로는 SLA를 충족하지 않는 경로이다. 예를 들어, 기본 경로의 지연은 SLA 지연 요구사항을 충족하고, 제1 보호 경로의 지연은 SLA 지연 요구사항을 충족하지 않는다. 예를 들어, 기본 경로의 지연은 지연 임계값보다 작고, 제1 보호 경로의 지연은 지연 임계값보다 크다. 다른 예로, 기본 경로의 대역폭은 SLA 대역폭 요구사항을 충족하고, 제1 보호 경로의 대역폭은 SLA 대역폭 요구사항을 충족하지 않는다. 예를 들어, 기본 경로의 대역폭은 대역폭 임계값보다 크고, 제1 보호 경로의 대역폭은 대역폭 임계값보다 작다.

[0141] 다음은 복수의 관점에서 보호 플래그를 구체적으로 설명하고 기술한다.

[0142] 다음은 경우 A 및 경우 B를 예로서 사용하여 보호 플래그의 기능의 관점에서 보호 플래그를 설명한다.

[0143] 경우 A: 보호 플래그는 패킷이 제1 보호 경로를 통과하도록 허용되는지 여부를 나타낼 수 있을 뿐만 아니라 허용되는 제1 보호 경로의 유형 또는 허용되지 않는 제1 보호 경로의 유형도 나타낼 수 있다. 예를 들어, 제1 네트워크 디바이스는 복수의 로컬 보호 메커니즘을 가능하게 하고, 제1 네트워크 디바이스는 복수의 로컬 보호 경로 중 하나를 통해 패킷을 포워딩할 수 있다. 이 시나리오에서, 보호 플래그는 복수의 로컬 보호 경로에서 사용되도록 허용되는 로컬 보호 경로 및 사용되도록 허용되지 않는 로컬 보호 경로의 유형을 나타내어, 패킷은 복수의 로컬 보호 경로에서 지정된 로컬 보호 경로를 통과하지 않는다.

[0144] 이것은 유연성을 향상시킨다.

[0145] 다음은 경우 A1 내지 경우 A4를 예로서 사용하여 경우 A를 설명한다. 경우 A1 내지 경우 A4에서, 중간점 TI-LFA 경로와 TI-LFA FRR 경로는 제1 보호 경로의 두 가지 특정 경우이다.

[0146] 경우 A1: 보호 플래그는 제1 네트워크 디바이스가 패킷을 기본 경로에서 중간점 TI-LFA 경로 및 TI-LFA FRR 경로로 전환하도록 허용되지 않음을 나타낸다. 중간점 TI-LFA 경로와 TI-LFA FRR 경로는 제1 보호 경로의 두 가지 특정 경우이다. 경우 A1에서, 보호 플래그를 전달하는 패킷은 중간점 TI-LFA 경로를 통과하도록 허용되지 않으며, 보호 플래그를 전달하는 패킷도 TI-LFA FRR 경로를 통과하도록 허용되지 않는다.

[0147] 경우 A2: 보호 플래그는 제1 네트워크 디바이스가 패킷을 중간점 TI-LFA 경로로 전환하도록 허용되지 않지만, 패킷을 TI-LFA FRR 경로로 전환하도록 허용됨을 나타낸다. 경우 A2에서, 보호 플래그를 전달하는 패킷은 중간점 TI-LFA 경로를 통과하도록 허용되지 않지만, 보호 플래그를 전달하는 패킷은 TI-LFA 경로를 통과하도록 허용된다.

[0148] 경우 A3: 보호 플래그는 제1 네트워크 디바이스가 패킷을 중간점 TI-LFA 경로로 전환하도록 허용되지만, 패킷을 TI-LFA FRR 경로로 전환하는 것은 허용되지 않음을 나타낸다. 경우 A3에서, 보호 플래그를 전달하는 패킷은 TI-LFA 경로를 통과하도록 허용되지 않지만, 보호 플래그를 전달하는 패킷은 중간점 TI-LFA 경로를 통과하도록 허용된다.

[0149] 경우 A4: 보호 플래그는 제1 네트워크 디바이스가 패킷을 기본 경로에서 중간점 TI-LFA 경로 또는 TI-LFA FRR 경로로 전환하도록 허용됨을 나타낸다. 경우 A4에서, 보호 플래그를 전달하는 패킷은 TI-LFA 경로를 통과하도록 허용되고, 보호 플래그를 전달하는 패킷은 중간점 TI-LFA 경로도 통과하도록 허용된다.

[0150] 경우 B: 보호 플래그는 보호 경로로의 전환이 허용되는지 여부만 나타낼 뿐 보호 경로의 특정 유형을 나타내지는 않는다. 선택적으로, 보호 플래그는 제1 네트워크 디바이스가 패킷을 기본 경로에서 제1 보호 경로로 전환하도록 허용되지 않음을 나타낸다. 경우 B에서, 보호 플래그를 전달하는 패킷은 제1 보호 경로를 통과하도록 허용되지 않는다. 선택적으로, 제1 보호 경로는 로컬 보호 경로이고, 제1 네트워크 디바이스는 복수의 로컬 보호 메커니즘을 가능하게 한다. 이 경우, 경우 B는 경우 B1과 경우 B2를 선택적으로 포함한다.

[0151] 경우 B1: 보호 플래그는 제1 네트워크 디바이스가 패킷을 기본 경로에서 모든 제1 보호 경로로 전환하도록 허용되지 않음을 나타낸다.

[0152] 경우 B2: 보호 플래그는 제1 네트워크 디바이스가 패킷을 기본 경로에서 사전구성된 제1 보호 경로로 전환하도록 허용되지 않음을 나타낸다. 예를 들어, 로컬 보호 경로는 제1 네트워크 디바이스에 사전구성되어 있고, 로컬 보호 경로가 사용되도록 허용되는지 여부는 보호 플래그를 이용하여 표시될 수 있다. 이 경우, 보호 플래그는 패킷이 사전구성된 로컬 보호 경로를 통과하도록 허용되지 않음을 나타낸다.

[0153] 보호 플래그의 데이터 형태의 관점에서, 보호 플래그는 패킷에서 하나 이상의 비트를 점유할 수 있고, 비트의 값은 0 또는 1일 수 있다. 보호 플래그는 상이한 비트 값을 사용하여 패킷이 기본 경로에서 제1 보호 경로로 전환되도록 허용되는지 여부를 나타낼 수 있다. 보호 플래그로부터의 데이터 형태는 구체적으로 복수의 경우를 포함할 수 있다. 다음은 경우 C와 경우 D를 예로서 사용하여 데이터 형태의 관점에서 보호 플래그를 설명한다.

[0154] 경우 C: 보호 플래그는 2개의 비트를 점유하고, 2개의 비트의 값은 제1 네트워크 디바이스가 패킷을 기본 경로에서 제1 보호 경로로 전환하도록 허용되는지 여부를 나타내는 데 사용될 수 있다. 예를 들어, 도 8은 본 출원의 실시예에 따른 SRv6 패킷의 개략도이다. 보호 플래그는 SRv6 패킷에서 2개의 비트를 점유한다. 예를 들어, SRv6 패킷의 SRH는 2개의 비트를 점유한다. 도 9에 도시된 바와 같이, SRv6 패킷의 SRH는 플래그 필드(Flags field)와 TLV를 포함한다. 선택적으로, 보호 플래그는 플래그 필드에서 2개의 비트를 점유한다. 선택적으로, 보호 플래그는 TLV에서 2개의 비트를 점유한다. 플래그 필드에서 2개의 비트를 점유하거나 TLV에서 2개의 비트를 점유하는 것은 설명을 위한 예로서 사용되며, 보호 플래그에 의해 점유되는 패킷 내의 2개의 비트는 이 실시예에서 제한되지 않는다는 것을 이해해야 한다. 선택적으로, 보호 플래그는 패킷의 예약된 필드에서 2개의 비트를 점유하고, 예약된 필드는 선택적으로 패킷 헤더의 필드, 예를 들어, 확장 헤더의 필드이다.

[0155] 선택적으로, 2개의 비트는 인접 비트이고, 2개의 비트는 4개의 값: 00, 01, 10 및 11을 포함하므로 4개의 값을 사용하여 상이한 경우를 나타낼 수 있다.

[0156] 보호 플래그가 패킷에서 제2 비트와 제3 비트를 점유하는 예는 아래에서 경우 C1.1 내지 경우 C1.4를 사용하여 경우 C를 설명하는 데 사용된다. 여기서 제2 비트와 제3 비트는 임의의 두 개의 다른 비트일 수 있고, 제2 비트는 필드에서 2번째 비트로 제한되지 않으며, 제3 비트도 필드에서의 3번째 비트로 제한되지 않고, 제2 비트는

제3 비트 앞에 있는 것으로 제한되지 않는다.

[0157] 예를 들어, 도 10에 도시된 바와 같이, 플래그 필드(Flags field)에서, 1번째 비트는 비트0이고, 2번째 비트는 비트1이며, 제2 비트는 비트7, 즉, 제2 비트는 비트6이다. 제3 비트는 플래그 필드에서 8번째 비트이며, 즉, 제3 비트는 비트7이다. 즉, 보호 플래그는 플래그 필드에서 비트6과 비트7을 점유한다. 보호 플래그는 도 10에서 "T/M"이다.

[0158] 또한, 도 10에서 U는 미사용 플래그를 나타내며, U는 향후 사용을 위한 플래그로서 제공될 수 있다. 또한, U는 전송 중에는 설정되지 않아야 하며, 수신단은 U를 무시해야 한다. P 플래그(P Flag)는 보호된 플래그를 나타낸다. 패킷이 FRR 메커니즘을 사용하여 SR 종단 노드에 의해 리라우팅된 경우, P 플래그가 설정된다. O 플래그(O flag)는 OAM 플래그이다. O 플래그가 설정되면, 패킷이 OAM 패킷임을 나타낸다. A 플래그(A flag)는 경보 플래그이다. A 플래그가 존재하면, 패킷에 중요한 TLV 객체가 존재함을 나타낸다. H 플래그(H Flag)는 HMAC 플래그를 나타낸다. H 플래그가 설정되면, 패킷에 HMAC TLV가 존재함을 나타내며, HMAC TLV는 SRH의 마지막 TLV로서 인코딩된다. 즉, SRH의 마지막 36 옥텟은 HMAC 정보를 나타낸다. 도 10에서, T는 T 플래그이다. T 플래그가 설정되면, 패킷은 TI-LFA 경로를 통과할 필요가 없다. 도 10에서, M은 M 플래그이다. M 플래그가 설정되면, 패킷은 중간점 TI-LFA 경로를 통과할 필요가 없다.

[0159] 경우 C1: 제2 비트와 제3 비트가 모두 설정되면, 제1 네트워크 디바이스는 패킷을 기본 경로에서 중간점 TI-LFA 경로 및 TI-LFA FRR 경로로 전환하도록 허용되지 않음을 나타낸다.

[0160] 경우 C1에서, 제2 비트의 값이 1이고, 제3 비트의 값도 1이면, 패킷이 기본 경로에서 중간점 TI-LFA 경로 또는 TI-LFA FRR 경로로 전환하도록 허용되지 않음을 나타낸다. 예를 들어, 도 10에 도시된 바와 같이, 플래그 필드에서 비트6은 T 플래그를 전달한다. T 플래그가 설정되면, 패킷이 TI-LFA 보호 경로를 통과할 수 없음을 나타낸다. 또한, 플래그 필드에서 비트7은 M 플래그를 전달한다. M 플래그가 설정되면, 패킷이 중간점 TI-LFA 보호 경로를 통과할 수 없음을 나타낸다. 플래그 필드에서 비트6 및 비트7(도 10의 T/M) 값이 "11"이면, 패킷이 TI-LFA 경로를 통과하도록 허용되지 않고 패킷이 중간점 TI-LFA 경로도 통과하도록 허용되지 않음을 나타낸다.

[0161] 경우 C2: 제2 비트가 설정되고 제3 비트가 설정되지 않으면, 제1 네트워크 디바이스가 패킷을 중간점 TI-LFA 경로로 전환하도록 허용되지 않지만 패킷을 TI-LFA FRR 경로로 전환하도록 허용됨을 나타낸다.

[0162] 경우 C2에서, 제2 비트의 값이 1이고, 제3 비트의 값이 0이면, 패킷이 중간점 TI-LFA 경로로 전환되도록 허용되지 않지만 TI-LFA FRR 경로로 전환되도록 허용됨을 나타낸다. 예를 들어, 도 10에 도시된 바와 같이, 플래그 필드에서 비트6 및 비트7(도 10의 T/M) 값이 "10"인 경우, 패킷이 TI-LFA 경로를 통과하도록 허용되지만, 패킷이 중간점 TI-LFA 경로를 통과하도록 허용되지 않음을 나타낸다.

[0163] 경우 C3: 제2 비트가 설정되지 않고 제3 비트가 설정되면, 제1 네트워크 디바이스가 패킷을 중간점 TI-LFA 경로로 전환하도록 허용되지만 패킷을 TI-LFA FRR 경로로 전환하도록 허용되지 않음을 나타낸다.

[0164] 경우 C3에서, 제2 비트의 값이 0이고, 제3 비트의 값이 1이면, 패킷이 중간점 TI-LFA 경로로 전환되도록 허용되지만 TI-LFA FRR 경로로 전환되도록 허용되지 않음을 나타낸다. 예를 들어, 도 10에 도시된 바와 같이, 플래그 필드에서 비트6 및 비트7(도 10의 T/M) 값이 "01"이면, 패킷이 중간점 TI-LFA 경로를 통과하도록 허용되지만, 패킷이 TI-LFA 경로를 통과하도록 허용되지 않음을 나타낸다.

[0165] 경우 C4: 제2 비트도 제3 비트도 설정되지 않은 경우, 제1 네트워크 디바이스가 패킷을 기본 경로에서 중간점 TI-LFA 경로 또는 TI-LFA FRR 경로로 전환하도록 허용됨을 나타낸다.

[0166] 경우 C4에서, 제2 비트의 값이 0이고, 제3 비트의 값이 0이면, 패킷이 기본 경로에서 중간점 TI-LFA 경로 또는 TI-LFA FRR 경로로 전환되도록 허용됨을 나타낸다. 예를 들어, 플래그 필드에서 비트6과 비트7(도 10의 T/M)의 값이 "00"인 경우, 패킷이 중간점 TI-LFA 경로를 통과하도록 허용되고, 패킷이 TI-LFA FRR 경로를 통과하는 것도 허용됨을 나타낸다. 경우 C4의 경우, 기본 경로에 결함이 있으면, ㅈ중간점 TI-LFA와 TI-LFA FRR 사이의 우선순위에 기초하여 패킷이 중간점 TI-LFA 경로로 전환될지 또는 TI-LFA FRR 경로로 전환될지가 선택적으로 결정된다. 자세한 내용은 실시예 2의 경우 V3에 대한 설명을 참조한다.

[0167] 경우 C1 내지 경우 C4는 경우 C의 필수 구현예보다는 경우 C의 선택적 구현예라는 것을 이해해야 한다. 일부 다른 실시예에서, 경우 C는 선택적으로 다른 방식을 포함한다. 예를 들어, 비트가 설정되지 않은 경우, 패킷이 기본 경로에서 중간점 TI-LFA 경로 또는 TI-LFA FRR 경로로 전환되도록 허용되지 않음을 나타낸다.

[0168] 경우 D: 보호 플래그는 하나의 비트를 점유하고, 하나의 비트의 값은 제1 네트워크 디바이스가 패킷을 기본 경

로에서 제1 보호 경로로 전환하도록 허용되는지 여부를 나타내는 데 사용된다. 예를 들어, 도 8에 도시된 바와 같이, 보호 플래그는 SRv6 패킷에서 하나의 비트를 점유한다. 예를 들어, SRv6 패킷에서 SRH는 하나의 비트를 점유한다. 도 9에 도시된 바와 같이, SRv6 패킷에서 SRH는 플래그 필드(Flags field)와 TLV를 포함한다. 선택적으로, 보호 플래그는 플래그 필드에서 하나의 비트를 점유한다. 선택적으로, 보호 플래그는 TLV에서 하나의 비트를 점유한다. 플래그 필드에서 하나의 비트를 점유하거나 TLV에서 하나의 비트를 점유하는 것은 설명을 위한 예로서 사용되며, 보호 플래그가 점유하는 패킷의 하나의 비트는 이 실시예에서 제한되지 않는다는 것을 이해해야 한다. 선택적으로, 보호 플래그는 패킷의 예약된 필드에서 하나의 비트를 점유하고, 예약된 필드는 선택적으로 패킷 헤더의 필드, 예를 들어, 확장 헤더의 필드이다.

[0169] 선택적으로, 경우 D는 제1 네트워크 디바이스가 하나의 로컬 보호 메커니즘만을 가능하게 하는 경우에 적용가능하다. 예를 들어, 제1 네트워크 디바이스는 TI-LFA 메커니즘을 가능하게 하지만 중간점 TI-LFA 메커니즘을 가능하게 하지 않으며, 제1 비트의 값은 제1 네트워크 디바이스가 패킷을 기본 경로에서 TI-LFA 보호 경로로 전환하도록 허용되는지 여부를 나타내는 데 사용될 수 있다. 다른 예로, 제1 네트워크 디바이스는 중간점 TI-LFA 메커니즘을 가능하게 하지만 TI-LFA 메커니즘을 가능하게 하지 않으며, 제1 비트의 값은 제1 네트워크 디바이스가 패킷을 기본 경로에서 중간점 TI-LFA 보호 경로로 전환하도록 허용되는지 여부를 나타내는 데 사용될 수 있다.

[0170] 선택적으로, 경우 D는 제1 네트워크 디바이스가 복수의 로컬 보호 메커니즘을 가능하게 하고, 보호 플래그와 하나의 로컬 보호 메커니즘 간의 바인딩 관계가 사전구성된 경우에 적용가능하다. 예를 들어, 제1 네트워크 디바이스는 TI-LFA 메커니즘과 중간점 TI-LFA 메커니즘을 가능하게 하고, TI-LFA 메커니즘과 보호 플래그 간의 바인딩 관계가 커맨드 라인을 사용하거나 다른 방식으로 사전구성되어, 보호 플래그의 값에 기초하여, TI-LFA 메커니즘을 사용할지 여부를 결정하도록 제1 네트워크 디바이스에 표시한다. 따라서, 제1 비트의 값은 제1 네트워크 디바이스가 패킷을 기본 경로에서 TI-LFA 보호 경로로 전환하도록 허용되는지 여부를 나타내는 데 사용될 수 있다.

[0171] 하나의 비트의 값은 0과 1의 2개의 값을 포함하며, 두 값은 서로 다른 경우를 나타내는 데 사용될 수 있다. 보호 플래그가 패킷의 제1 비트를 점유하는 예는 경우 D1 및 경우 D2를 사용하여 아래에서 상세한 설명에 사용된다. 여기에서 제1 비트는 패킷 내의 임의의 상이한 비트일 수 있으며, 제1 비트는 필드 내의 1번째 비트로 제한되지 않는다. 예를 들어, 도 11에 도시된 바와 같이, 선택적으로, 플래그 필드에서 제1 비트는 2번째 비트(즉, 도 11의 T/M)이다. 즉, 보호 플래그는 플래그 필드에서 2번째 비트를 점유한다. 선택적으로, 플래그 필드의 1번째 비트가 비트0이면, 보호 플래그는 플래그 필드의 비트1이고, 보호 플래그는 도 11에서 T/M이다.

[0172] 경우 D1: 제1 비트가 설정되면, 패킷이 기본 경로에서 제1 보호 경로로 전환되도록 허용되지 않음을 나타낸다. 선택적으로, 제1 비트가 설정되면, 패킷이 기본 경로에서 TI-LFA 경로로 전환되도록 허용되지 않음을 나타낸다. 예를 들어, 도 11에 도시된 바와 같이, 플래그 필드에서 2번째 비트(즉, 비트1, 즉, 도 11에서 T/M)의 값이 "1"이면, 패킷이 TI-LFA 경로를 통과하도록 허용되지 않음을 나타낸다. 선택적으로, 제1 비트가 설정되면, 패킷이 기본 경로에서 중간점 TI-LFA 경로로 전환되도록 허용되지 않음을 나타낸다. 예를 들어, 도 11에 도시된 바와 같이, 플래그 필드에서 2번째 비트(즉, 비트1, 즉, 도 11에서 T/M)의 값이 "1"이면, 패킷이 중간점 TI-LFA 경로를 통과하도록 허용되지 않음을 나타낸다. 선택적으로, 제1 비트가 설정되면, 패킷이 기본 경로에서 TI-LFA 경로로 전환되도록 허용되지 않으며, 패킷이 기본 경로에서 중간점 TI-LFA 경로로 전환되는 것도 허용되지 않음을 나타낸다. 예를 들어, 도 11에 도시된 바와 같이, 플래그 필드에서 2번째 비트 값이 "1"이면, 패킷이 TI-LFA 경로를 통과하도록 허용되지 않으며, 패킷이 중간점 TI-LFA 경로를 통과하는 것도 허용되지 않음을 나타내다.

[0173] 경우 D2: 제1 비트가 설정되지 않으면, 패킷이 기본 경로에서 제1 보호 경로로 전환되도록 허용됨을 나타낸다. 선택적으로, 제1 비트가 설정되지 않으면, 패킷이 기본 경로에서 TI-LFA 경로로 전환되도록 허용됨을 나타낸다. 예를 들어, 도 11에 도시된 바와 같이, 플래그 필드에서 2번째 비트의 값이 "0"이면, 패킷이 TI-LFA 경로를 통과하도록 허용됨을 나타낸다. 선택적으로, 제1 비트가 설정되지 않으면, 패킷이 기본 경로에서 중간점 TI-LFA 경로로 전환되도록 허용됨을 나타낸다. 예를 들어, 도 11에 도시된 바와 같이, 플래그 필드에서 2번째 비트의 값이 "0"이면, 패킷이 중간점 TI-LFA 경로를 통과하도록 허용됨을 나타낸다. 선택적으로, 제1 비트가 설정되지 않으면, 패킷이 기본 경로에서 TI-LFA 경로로 전환되도록 허용되며 패킷이 기본 경로에서 중간점 TI-LFA 경로로 전환되는 것도 허용됨을 나타낸다. 예를 들어, 도 11에 도시된 바와 같이, 플래그 필드에서 2번째 비트의 값이 "0"이면, 패킷이 TI-LFA 경로를 통과하도록 허용되며, 패킷이 중간점 TI-LFA 경로를 통과하는 것도 허용됨을 나타낸다.

[0174] 경우 D1 및 경우 D2는 경우 D의 필수 구현예가 아니라 경우 D의 선택적인 구현예라는 것을 이해해야 한다. 일부

다른 실시예에서, 경우 D는 선택적으로 다른 방식을 포함한다. 예를 들어, 제1 비트가 설정되지 않은 경우, 패킷이 기본 경로에서 제1 보호 경로로 전환되도록 허용되지 않음을 나타낸다.

[0175] 경우 C 및 경우 D 둘 다 보호 플래그의 필수 구현예가 아니라 보호 플래그의 선택적 구현예라는 것을 이해해야 한다. 선택적으로, 보호 플래그는 2개의 비트 이상을 점유하고, 2개의 비트 이상을 사용하여 보호 플래그를 나타내는 방식은 보호 플래그의 구현예의 특정 경우이며, 본 출원의 이 실시예의 보호 범위에도 속해야 한다.

[0176] 패킷에서 보호 플래그의 위치는 복수의 경우를 포함할 수 있다. 다음은 경우 E1과 경우 E2를 예로 들어 보호 플래그의 위치의 관점에서 보호 플래그를 설명한다.

[0177] 경우 E1: 보호 플래그가 플래그 필드에 있다. 즉, 패킷은 플래그 필드를 포함하고, 패킷은 플래그 필드를 이용하여 보호 플래그를 전달한다. 보호 플래그를 전달하는 데 사용되는 플래그 필드를 T/M 플래그라고 할 수 있다. 플래그 필드는 다른 벤더 또는 시나리오에 따라 다른 이름을 가질 수도 있다.

[0178] 선택적으로, 보호 플래그를 전달하는 플래그 필드는 패킷 헤더에 위치한다. 선택적으로, 플래그 필드를 포함하는 패킷 헤더는 외부 패킷 헤더 또는 내부 패킷 헤더이다. 선택적으로, 보호 플래그를 전달하는 플래그 필드는 확장 헤더에 위치한다. 선택적으로, 보호 플래그를 전달하는 플래그 필드는 SRH에 위치한다. 선택적으로, 도 9에 도시된 바와 같이, 보호 플래그를 전달하는 플래그 필드는 도 9의 마지막 엔트리 필드와 태그 필드 사이의 플래그 필드이다. 선택적으로, SRH의 TLV는 플래그 필드를 포함하고, 보호 플래그를 전달하는 플래그 필드는 TLV에 포함된 플래그 필드이다. 선택적으로, 보호 플래그를 전달하는 플래그 필드는 SRH에 있는 것이 아니라, SRH의 다른 확장 헤더에 있다. 예를 들어, 보호 플래그를 전달하는 플래그 필드는 홉별 옵션 헤더(hop-by-hop options header)에 위치한다. 선택적으로, 보호 플래그를 전달하는 플래그 필드는 패킷이 전달하는 검출 패킷의 패킷 헤더에 있거나, 데이터 패킷의 패킷 헤더에 있다.

[0179] 전술한 열거된 경우들은 모두 경우 E1의 선택적인 구현예이며, 본 출원의 이 실시예의 보호 범위 내에 속해야 함을 이해해야 한다.

[0180] 경우 E1에서, 새로운 플래그 필드는 패킷에 대해 확장되고, 플래그 필드는 보호 플래그를 전달하는 데 사용된다. 기본 경로에 결함이 있는 경우, 패킷이 플래그 필드를 포함하기 때문에, 수신 측이 플래그 필드에서 보호 플래그를 식별한 후, 패킷은 제1 보호 경로를 통과하지 않는다. 제1 보호 경로가 로컬 보호 경로인 경우, 패킷은 로컬 보호 경로를 통과하지 않는다.

[0181] 경우 E2: 보호 플래그가 TLV에 있다. 즉, 패킷은 TLV를 포함하며, TLV는 보호 플래그를 전달하는 데 사용된다. 선택적으로, TLV는 보호 플래그를 전달하는 전용 TLV이다. 선택적으로, 보호 플래그를 전달하기 위해 원래의 TLV에 비트가 점유되어, 보호 경로로의 로컬 전환이 허용되는지 여부를 나타내는 기능이 원래의 기능을 기반으로 TLV에 의해 확장된다. 경우 E2에서, 보호 플래그를 전달하는 데 사용되는 TLV는 보호 TLV 또는 보호 없음 TLV(no protection TLV)로 지칭될 수 있다. TLV는 상이한 벤더 또는 시나리오에 따라 다른 이름을 가질 수도 있다.

[0182] 선택적으로, 패킷이 TLV를 전달하는지 여부는 패킷이 기본 경로에서 제1 보호 경로로 전환되도록 허용되는지 여부를 나타내는 데 사용된다. 예를 들어, 패킷이 TLV를 전달하는 경우, 기본 경로에 결함이 있으면 패킷이 로컬 보호 경로를 통과하도록 허용되지 않음을 나타낸다. 패킷이 TLV를 전달하지 않는 경우, 기본 경로에 결함이 있으면 패킷이 로컬 보호 경로를 통과하도록 허용됨을 나타낸다.

[0183] 선택적으로, 패킷의 TLV에 있는 값(value) 필드의 값은 패킷이 기본 경로에서 제1 보호 경로로 전환되도록 허용되는지 여부를 표시하는 데 사용된다. 예를 들어, 전술한 경우 C1 내지 경우 C8을 참조하면, TLV의 값 필드는 제2 비트와 제3 비트를 포함하고, 값 필드의 2개의 비트의 값은 패킷이 기본 경로에서 제1 보호 경로로 전환되도록 허용되는지 여부를 나타내는 데 사용된다. 예를 들어, 경우 C1을 참조하면, 값 필드의 제2 비트와 제3 비트가 모두 설정되면, 제1 네트워크 디바이스가 패킷을 기본 경로에서 중간점 TI-LFA 경로 및 TI-LFA FRR 경로로 전환하도록 허용되지 않음을 나타낸다. 경우 C2를 참조하면, 값 필드의 제2 비트가 설정되고 제3 비트가 설정되지 않으면, 제1 네트워크 디바이스가 패킷을 중간점 TI-LFA 경로로 전환하도록 허용되지 않지만 패킷을 TI-LFA FRR 경로로 전환하도록 허용됨을 나타낸다. TI-LFA FRR 및 중간점 TI-LFA를 표시하는 데 사용되는 TLV의 값 필드의 2개의 비트는 이 실시예에서 제한되지 않는다는 것을 이해해야 한다. 다른 예로, 전술한 경우 D를 참조하면, TLV의 값 필드는 제1 비트를 포함하고, 값 필드의 하나의 비트 값은 패킷이 기본 경로에서 제1 보호 경로로 전환되도록 허용되는지 여부를 나타내는 데 사용된다. 예를 들어, 경우 D1을 참조하면, 값 필드의 제1 비트가 설정되면, 패킷이 기본 경로에서 제1 보호 경로로 전환되도록 허용되지 않음을 나타낸다. TI-LFA FRR 또는 중간

점 TI-LFA를 표시하는 데 사용되는 TLV의 값 필드의 하나의 비트는 이 실시예에서 제한되지 않는다는 것을 이해해야 한다.

[0184] 선택적으로, 보호 플래그를 전달하는 데 사용되는 TLV는 유형(type)을 사용하여 식별된다. 구체적으로, 보호 플래그를 전달하는 데 사용되는 TLV의 유형 필드의 값은 사전설정된 값이고, 사전설정된 값은 TLV가 보호 TLV, 즉, 패킷이 기본 경로에서 제1 보호 경로로 전환되도록 허용되는지 여부를 나타내는 데 사용되는 TLV임을 나타낸다. 패킷 수신 측은 TLV에서 유형 필드의 값을 식별한다. TLV의 유형 필드의 값이 사전설정된 값인 경우, 수신 측은 TLV가 보호 TLV인 것으로 결정할 수 있다. 사전설정된 값은 새로 적용된 값일 수 있다.

[0185] 선택적으로, 보호 플래그를 전달하는 데 사용되는 TLV의 길이(length) 필드의 값의 범위는 0 내지 5이다.

[0186] 선택적으로, 보호 플래그를 전달하는 데 사용되는 TLV는 패킷 헤더에 위치한다. 선택적으로, TLV를 포함하는 패킷 헤더는 외부 패킷 헤더 또는 내부 패킷 헤더이다. 선택적으로, 보호 플래그를 전달하는 데 사용되는 TLV는 확장 헤더에 위치한다. 선택적으로, 보호 플래그를 전달하는 데 사용되는 TLV는 SRH에 위치한다. 도 9에 도시된 바와 같이, 보호 플래그를 전달하는 TLV는 SRH의 TLV이다. 선택적으로, 보호 플래그를 전달하는 TLV는 SRH에 있는 것이 아니라, SRH가 아닌 확장 헤더에 있다. 예를 들어, 보호 플래그를 전달하는 TLV는 홉별 옵션 헤더(hop-by-hop options header)에 위치한다. 선택적으로, 보호 플래그를 전달하는 TLV는 패킷이 전달하는 검출 패킷의 패킷 헤더에 있거나, 데이터 패킷의 패킷 헤더에 있다.

[0187] 선택적으로, 보호 플래그를 전달하는 데 사용되는 TLV는 새로운 최상위(top) TLV이고, 보호 플래그를 전달하는 데 사용되는 TLV의 유형은 최상위 TLV의 미사용 유형이다. 선택적으로, 보호 플래그를 전달하는 데 사용되는 TLV는 최상위 TLV의 새로운 하위 TLV이고, 보호 플래그를 전달하는 데 사용되는 TLV의 유형은 하위 TLV의 미사용 유형이다. 선택적으로, 보호 플래그를 전달하는 데 사용되는 TLV는 최상위 TLV의 새로운 하위 TLV(sub-TLV)이고, 보호 플래그를 전달하는 데 사용되는 TLV의 유형은 하위 TLV의 미사용 유형이다. 선택적으로, 보호 플래그를 전달하는 데 사용되는 TLV는 최상위 TLV의 새로운 하위 하위 TLV(sub-sub-TLV)이고, 보호 플래그를 전달하는 데 사용되는 TLV의 유형은 하위 하위 TLV의 미사용 유형이다. 보호 플래그를 전달하는 데 사용되는 TLV가 최상위 TLV인지, 하위 TLV인지, 또는 하위 하위 TLV인지는 이 실시예에서 제한되지 않는다.

[0188] 선택적으로, 보호 플래그를 전달하는 데 사용되는 TLV의 유형은 IANA에 의해 할당된 값일 수 있다. 선택적으로, TLV의 유형의 값은 6이다. 보호 플래그를 전달하는 데 사용되는 TLV의 길이의 값의 범위는 0 내지 5일 수 있다.

[0189] 선택적으로, 보호 플래그를 전달하는 데 사용되는 TLV의 값은 8바이트 패딩 필드일 수 있다. 패딩 필드의 비트는 의미론적 의미가 없을 수 있다. 패딩 필드의 값은 전송 동안 0으로 설정되며, 패딩 필드는 패킷 수신 동안 무시된다.

[0190] 전술한 열거된 경우들은 모두 경우 E2의 선택적인 구현예이며, 본 출원의 이 실시예의 보호 범위 내에 속해야 함을 이해해야 한다.

[0191] 경우 E2에서, 새로운 TLV가 패킷에 대해 확장되고, TLV는 보호 플래그를 전달하는 데 사용된다. 기본 경로에 결함이 있는 경우, 수신 측이 TLV를 식별한 후, 패키은 제1 보호 경로를 통과하지 않는다. 제1 보호 경로가 로컬 보호 경로인 경우, 패킷은 로컬 보호 경로를 통과하지 않는다.

[0192] 전술한 내용은 복수의 관점에서 보호 플래그의 다양한 가능한 경우를 설명한다. 보호 플래그를 전달하는 패킷은 또한 복수의 경우를 포함할 수 있다. 즉, S201에서, 제2 네트워크 디바이스는 복수의 유형의 패킷에 보호 플래그를 추가할 수 있다. 다음은 예를 사용하여 보호 플래그를 전달하는 패킷의 다양한 경우를 설명한다. 전술한 보호 플래그의 다양한 경우는 다음 패킷의 다양한 경우에 적용될 수 있음을 이해해야 한다.

[0193] 보호 플래그를 전달하는 패킷은 선택적으로 경우 H와 경우 I를 포함한다.

[0194] 경우 H: 패킷은 검출 패킷을 포함한다. 검출 패킷은 기본 경로의 연결성 또는 전송 성능 파라미터 중 적어도 하나를 검출하는 데 사용된다. 전송 성능 파라미터는 지연, 패킷 손실률, 지연 변동, 실시간 트래픽, 패킷 수, 바이트 수 중 적어도 하나를 포함한다.

[0195] 선택적으로, 제2 네트워크 디바이스에 의해 전송된 패킷의 페이로드는 검출 패킷을 포함하고, 보호 플래그는 검출 패킷의 외부 패킷 헤더에 있다. 도 8에 도시된 바와 같이, 선택적으로, 제2 네트워크 디바이스에 의해 전송된 패킷은 도 8에 도시된 SRv6 패킷이고, SRv6 패킷의 페이로드는 검출 패킷을 포함하며, 검출 패킷의 외부 패킷 헤더는 SRH를 포함하고, 보호 플래그는 SRH에 있다. 선택적으로, 제2 네트워크 디바이스에 의해 전송된 패킷은 SR-TE 패킷이고, SR-TE 패킷의 페이로드는 검출 패킷을 포함하며, 검출 패킷의 외부 패킷 헤더는 라벨 스택

및 보호 플래그를 포함한다. 선택적으로, 제2 네트워크 디바이스에 의해 전송된 패킷이 SRv6 또는 SR-TE 이외의 다른 소스 라우팅 방식으로 포워딩되는 경우, 검출 패킷의 외부 패킷 헤더는 소스 라우팅에 사용된 다른 패킷 헤더이고, 다른 패킷 헤더는 보호 플래그를 포함한다. 선택적으로, 보호 플래그는 검출 패킷 내부에 위치한다. 예를 들어, 검출 패킷의 패킷 헤더는 확장되고, 검출 패킷의 패킷 헤더는 보호 플래그를 전달한다.

[0196] 다음은 경우 H1 내지 경우 H5를 예로서 사용하여 경우 H를 설명한다.

[0197] 경우 H1: 검출 패킷은 양방향 포워딩 검출 BFD 패킷이다.

[0198] 경우 H1은 전술한 BFD 검출 응용 시나리오에 적용가능하다. BFD 패킷은 SBFD 제어 패킷(SBFD Control Packet)일 수 있고, 제2 네트워크 디바이스는 SBFD 개시자일 수 있다. 도 8에 도시된 바와 같이, 선택적으로, 제2 네트워크 디바이스가 보낸 패킷은 SRv6 BFD 패킷이고, SRv6 BFD 패킷의 페이로드는 BFD 패킷을 포함한다. 선택적으로, 제2 네트워크 디바이스가 보낸 패킷은 SR-TE BFD 패킷이고, SR-TE BFD 패킷의 페이로드는 BFD 패킷을 포함한다.

[0199] 선택적으로, 보호 플래그는 BFD 패킷 외부에 위치한다. 예를 들어, 보호 플래그를 전달하는 패킷의 페이로드는 BFD 패킷을 포함하고, 보호 플래그를 전달하는 패킷의 패킷 헤더는 보호 플래그를 포함한다. 선택적으로, 보호 플래그는 BFD 패킷 내부에 위치한다. 예를 들어, BFD 패킷의 패킷 헤더가 확장되고, BFD 패킷의 패킷 헤더에 보호 플래그가 추가된다.

[0200] 경우 H2: 검출 패킷은 PING 검출 패킷이다.

[0201] 경우 H2는 전술한 PING 검출 연결 응용 시나리오에 적용가능하다. PING 검출 패킷은 ICMP 에코 요청 패킷으로 지칭될 수 있다. 도 8에 도시된 바와 같이, 선택적으로, 제2 네트워크 디바이스에 의해 전송된 패킷은 SRv6 PING 검출 패킷이고, SRv6 PING 검출 패킷의 페이로드는 PING 검출 패킷을 포함한다. 선택적으로, 제2 네트워크 디바이스에 의해 전송된 패킷은 SR-TE PING 검출 패킷이고, SR-TE PING 패킷의 페이로드는 PING 검출 패킷을 포함한다.

[0202] 선택적으로, 보호 플래그는 PING 검출 패킷 외부에 위치한다. 예를 들어, 보호 플래그를 전달하는 패킷의 페이로드는 PING 검출 패킷을 포함하고, 보호 플래그를 전달하는 패킷의 패킷 헤더는 보호 플래그를 포함한다. 선택적으로, 보호 플래그는 PING 검출 패킷 내부에 위치한다. 예를 들어, PING 검출 패킷의 패킷 헤더가 확장되고, PING 검출 패킷의 패킷 헤더에 보호 플래그가 추가된다.

[0203] 경우 H3: 검출 패킷은 OAM 검출 패킷이다.

[0204] 경우 H3은 전술한 OAM 검출 응용 시나리오에 적용가능하다. 경우 H3에, OAM 검출 패킷은 Y.1731 검출 패킷 또는 ICMPv6 에코 요청 패킷이라고도 할 수 있다. 도 8에 도시된 바와 같이, 선택적으로, 제2 네트워크 디바이스에 의해 전송된 패킷은 SRv6 OAM 검출 패킷이고, SRv6 BFD 패킷의 페이로드는 OAM 검출 패킷을 포함한다. 선택적으로, 제2 네트워크 디바이스에 의해 전송된 패킷은 SR-TE OAM 검출 패킷이고, SR-TE OAM 패킷의 페이로드는 OAM 검출 패킷을 포함한다.

[0205] 선택적으로, 보호 플래그는 OAM 탐지 패킷 외부에 위치한다. 예를 들어, 보호 플래그를 전달하는 패킷의 페이로드는 OAM 검출 패킷을 포함하고, 보호 플래그를 전달하는 패킷의 패킷 헤더는 보호 플래그를 포함한다. 선택적으로, 보호 플래그는 OAM 검출 패킷 내부에 위치한다. 예를 들어, OAM 검출 패킷의 패킷 헤더가 확장되고, OAM 검출 패킷의 패킷 헤더에 보호 플래그가 추가된다.

[0206] 경우 H4: 검출 패킷은 TWAMP 검출 패킷이다.

[0207] 경우 H4는 전술한 TWAMP 검출 응용 시나리오에 적용가능하다. 경우 H4에서, TWAMP 검출 패킷은 TWAMP-테스트-요청 패킷으로도 지칭될 수 있다. 도 8에 도시된 바와 같이, 선택적으로, 제2 네트워크 디바이스에 의해 전송된 패킷은 SRv6 TWAMP 검출 패킷이고, SRv6 TWAMP 패킷의 페이로드는 TWAMP 검출 패킷을 포함한다. 선택적으로, 제2 네트워크 디바이스에 의해 전송된 패킷은 SR-TE TWAMP 검출 패킷이고, SR-TE TWAMP 패킷의 페이로드는 TWAMP 검출 패킷을 포함한다.

[0208] 선택적으로, 보호 플래그는 TWAMP 검출 패킷 외부에 위치한다. 예를 들어, 보호 플래그를 전달하는 패킷의 페이로드는 TWAMP 검출 패킷을 포함하고, 보호 플래그를 전달하는 패킷의 패킷 헤더는 보호 플래그를 포함한다. 선택적으로, 보호 플래그는 TWAMP 검출 패킷 내부에 위치한다. 예를 들어, TWAMP 검출 패킷의 패킷 헤더가 확장되고, TWAMP 검출 패킷의 패킷 헤더에 보호 플래그가 추가된다.

[0209] 경우 H5: 검출 패킷은 IFIT 패킷이다.

[0210] 경우 H5는 전술한 IFIT 응용 시나리오에 적용가능하다. 선택적으로, 경우 H5의 IFIT 패킷은 ICMPv6 에코 요청 패킷이라고도 한다. IFIT 패킷은 IFIT 패킷 헤더를 포함한다. 선택적으로, 보호 플래그는 IFIT 패킷 헤더 내부에 위치한다. 선택적으로, 보호 플래그는 IFIT 패킷 헤더의 외부 패킷 헤더에 있다.

[0211] 예를 들어, 도 13은 본 출원의 실시예에 따른 IFIT 패킷 헤더의 개략도이다. IFIT 패킷은 보호 플래그를 포함한다. 가능한 구현예에서, IFIT 패킷 헤더는 흐름 명령 헤더(Flow ID Header, FIH) 및 흐름 명령 확장 헤더(Flow ID Ext Header, FIEH)를 포함한다. 선택적으로, FIH는 보호 플래그를 포함한다. 도 14는 본 출원의 실시예에 따른 FIH의 개략도이다. 선택적으로, 보호 플래그는 도 14에서 T/M이다. 보호 플래그는 FIH에서 D 플래그 필드와 HTI 필드 사이에 위치한다.

[0212] FIH는 흐름 ID, 컬러링 표시자 비트 및 검출 헤더 유형 표시를 포함하는, IFIT 인시튜 흐름 검출에 사용되는 기본 정보를 전달한다. FIEH는 IFIT 확장 능력을 지원하는 데 사용되는 정보를 전달한다. 흐름 명령 확장 헤더는 종단 간 확장 헤더와 홉별 확장 헤더의 두 가지 유형을 포함한다. 확장 필드는 확장 흐름 ID, 검출 주기 표시, 역류 자동 학습 등을 포함한다. 선택적으로, FIH는 보호 플래그를 포함할 뿐만 아니라, 다음 필드(a) 내지 (f)도 포함한다.

[0213] (a) 흐름 ID: 서비스 흐름을 고유하게 식별하는 데 사용되는 비트0 내지 비트19, 흐름 ID는 검출 영역의 전체 네트워크에서 고유해야 하며, IP 무선 액세스 네트워크(IP Radio Access Network, IP RAN) 네트워크 요소는 흐름 ID를 기반으로 흐름 식별을 수행한다.

[0214] (b) L 플래그: 손실 플래그, 즉, 손실 측정 플래그.

[0215] (c) D 플래그: 지연 플래그, 즉, 지연 측정 플래그, 1은 지연 측정이 필요함을 나타내고, 0은 지연 측정이 필요하지 않음을 나타낸다.

[0216] (d) R: 예약 비트, 향후 확장을 위해 예약됨.

[0217] (e) R/S: 부트 라벨이 스택 하단 라벨인 경우, 플래그는 R이고 디폴트로 1로 설정된다. 부트 라벨이 스택 하단 라벨이 아닌 경우, 플래그는 S이다.

[0218] (f) HTI(Header Type Type Indicator): 확장 데이터 유형을 표시하고 확장 헤더가 전달되는지 여부를 표시함:

[0219] 0x00: 예약됨;

[0220] 0x01: FIH가 기본 종단 간 검출 정보이고 확장 헤더를 전달하지 않음을 나타냄;

[0221] 0x02: FIH가 기본 홉별 검출 정보이고 확장 헤더를 전달하지 않음을 나타냄;

[0222] 0x03: FIH가 확장된 종단 간 검출 정보이고 확장 헤더를 전달하며, FIEH가 유효함을 나타냄;

[0223] 0x04: FIH가 확장된 홉별 검출 정보이고 확장 헤더를 전달하며, FIEH가 유효함을 나타냄;

[0224] 0x05 내지 0xFF: 향후 확장을 위해 예약됨.

[0225] 경우 I: 패킷은 데이터 패킷을 포함하고, 데이터 패킷은 기본 경로의 서비스 데이터를 전달하는 데 사용되며, 데이터 패킷은 보호 플래그를 포함한다. 선택적으로, 보호 플래그는 데이터 패킷 외부에 위치한다. 예를 들어, 제2 네트워크 디바이스가 보낸 패킷의 페이로드는 데이터 패킷을 포함하고, 데이터 패킷의 외부 패킷 헤더는 보호 플래그를 포함한다. 도 8에 도시된 바와 같이, 선택적으로, 제2 네트워크 장치에 의해 전송된 패킷은 도 8에 도시된 SRv6 패킷이고, SRv6 패킷의 페이로드는 데이터 패킷을 포함하며, 데이터 패킷의 외부 패킷 헤더는 SRH를 포함하고, SRH는 보호 플래그를 포함한다. 선택적으로, 제2 네트워크 디바이스에 의해 전송된 패킷은 SR-TE 패킷이고, SR-TE 패킷의 페이로드는 데이터 패킷을 포함하며, 데이터 패킷의 외부 패킷 헤더는 라벨 스택 및 보호 플래그를 포함한다. 선택적으로, 제2 네트워크 디바이스가 보낸 패킷이 SRv6 또는 SR-TE가 아닌 다른 소스 라우팅 방식으로 포워딩되는 경우, 데이터 패킷의 외부 패킷 헤더는 소스 라우팅에 사용되는 다른 패킷 헤더이고, 다른 패킷 헤더는 보호 플래그를 포함한다. 선택적으로, 보호 플래그는 데이터 패킷 내부에 위치한다. 예를 들어, 데이터 패킷의 패킷 헤더가 확장되고, 보호 플래그가 데이터 패킷의 패킷 헤더에 추가된다.

[0226] 선택적으로, 데이터 패킷이 전달한 서비스 데이터는 제2 네트워크 디바이스에 의해 수신된 서비스 데이터이다. 예를 들어, 도 1에 도시된 바와 같이, CE1이 PE1으로 전송하는 패킷은 서비스 데이터를 포함하고, PE1(제2 네트

워크 디바이스)이 P1(제1 네트워크 디바이스)으로 전송하는 패킷은 서비스 데이터를 포함한다. 다른 예를 들면, 도 2에 도시된 바와 같이, PE1(제2 네트워크 디바이스)이 RT_3(제1 네트워크 디바이스)으로 전송하는 패킷은 서비스 데이터를 포함한다.

[0227] 전술한 내용은 보호 플래그의 다양한 경우와 패킷의 다양한 경우를 별도로 설명하였다. 전술한 보호 플래그의 다양한 경우와 패킷의 다양한 경우는 임의의 방식으로 조합될 수 있고, 조합 방식은 복수의 경우의 특징을 포함한다는 것을 이해해야 한다.

[0228] S201의 패킷 생성 방식은 선택적으로 복수의 구현예를 포함한다. 다음은 경우 V1과 경우 V2를 예로 사용하여 패킷 생성 방식을 설명한다.

[0229] 경우 V1: 제3 디바이스가 제2 네트워크 디바이스에 패킷을 전송하고, 제2 네트워크 디바이스가 제3 디바이스로부터 패킷을 수신하며, 제3 장치로부터의 패킷에 기초하여, 보호 플래그를 포함하는 패킷을 생성한다. 선택적으로, 제3 디바이스는 네트워크 디바이스이다. 예를 들어, 도 1에 도시된 바와 같이, 제3 디바이스는 선택적으로 도 1의 CE1과 같은 CE 디바이스이고, CE1은 PE1에 패킷을 전송하고, PE1은 CE1으로부터의 패킷을 기반으로 보호 플래그를 포함하는 패킷을 생성한다. 선택적으로, 경우 V1은 데이터 패킷 포워딩 시나리오에 적용할 수 있다. 예를 들어, SR 시나리오에서, 데이터 패킷은 제2 네트워크 디바이스로부터 SR 터널로 들어가기 시작하고, 제2 네트워크 디바이스가 데이터 패킷을 수신할 때, 제2 네트워크 디바이스는 데이터 패킷에 기초하여 SID 목록 및 보호 플래그를 추가하여 SR 데이터 패킷을 획득하고, SR 데이터 패킷을 제1 네트워크 디바이스에 전송한다. SID 목록이 SR 데이터 패킷에 푸시되기 때문에, SR 데이터 패킷이 SR 터널에 도입되어, 데이터 패킷과 보호 플래그가 결합되어 SR 터널의 각 노드에서 전송된다.

[0230] 제2 네트워크 디바이스에 의해 전송된 패킷은 제2 네트워크 디바이스에 의해 수신된 모든 데이터 패킷을 포함할 필요가 있다는 것이 이 실시예의 경우 V1에 제한되지 않는다는 것을 이해해야 한다. 경우 V1은 선택적으로 경우 V11 및 경우 V12를 포함한다.

[0231] 경우 V11: 제2 네트워크 디바이스에 의해 전송된 패킷은 제2 네트워크 디바이스에 의해 수신된 데이터 패킷의 일부 콘텐츠(예컨대, 데이터 패킷이 전달한 서비스 데이터)를 포함하고, 제2 네트워크 디바이스에 의해 수신된 데이터 패킷의 다른 콘텐츠는 변경된다. 구체적으로, 선택적으로, 데이터 패킷을 수신한 후, 제2 네트워크 디바이스는 데이터 패킷의 일부 콘텐츠를 업데이트하는데, 예를 들어, 데이터를 수정하거나, 데이터를 삭제하거나, 데이터 패킷의 패킷 헤더에 대한 데이터를 추가(예컨대, MAC 주소를 수정)하고, 업데이트된 데이터 패킷 및 보호 플래그를 캡슐화하여 패킷을 획득하며, 패킷을 제1 네트워크 디바이스로 전송한다. 따라서, 제2 네트워크 디바이스에 의해 전송된 패킷은 제2 네트워크 디바이스에 의해 수신된 데이터 패킷의 일부 콘텐츠 및 보호 플래그를 포함한다.

[0232] 경우 V12: 제2 네트워크 디바이스에 의해 전송된 패킷은 제2 네트워크 디바이스에 의해 수신된 데이터 패킷의 모든 콘텐츠를 포함한다. 예를 들어, 제2 네트워크 디바이스는 수신된 데이터 패킷을 업데이트하지 않고, 수신된 데이터 패킷, 보호 플래그 및 기타 선택적 정보를 캡슐화하여 패킷을 획득한 다음 패킷을 제1 네트워크 디바이스에 전송한다. 따라서, 제2 네트워크 디바이스가 보낸 패킷은 제2 네트워크 디바이스와 보호 플래그가 수신한 데이터 패킷의 모든 콘텐츠를 포함한다.

[0233] 경우 V2: 제2 네트워크 디바이스가 다른 디바이스가 보낸 패킷을 기반으로 S201을 수행하지 않고, 전체 패킷을 생성하기 위해 어셈블링을 수행한다. 예를 들어, 도 1에 도시된 바와 같이, 제2 네트워크 디바이스가 PE1이고, 제1 네트워크 디바이스가 PE3인 경우, PE1은 PE3과 BFD 세션을 설정하고, PE1은 BFD 패킷을 생성하여 PE3에 BFD 패킷을 전송한다.

[0234] S202: 제2 네트워크 디바이스가 패킷을 제1 네트워크 디바이스로 전송한다.

[0235] S203: 제1 네트워크 디바이스가 패킷을 수신한다.

[0236] 선택적으로, 제2 네트워크 디바이스는 패킷을 기본 경로에 대응하는 아웃바운드 인터페이스를 통해 제1 네트워크 디바이스로 전송한다. 제1 네트워크 디바이스는 기본 경로에 대응하는 인바운드 인터페이스를 통해 패킷을 수신한다.

[0237] S204: 제1 네트워크 디바이스는 기본 경로에 결함이 있다고 결정한다.

[0238] 기본 경로에 결함이 있다고 결정하는 구현예는 구체적으로 복수의 경우를 포함할 수 있다. 다음은 경우 J 및 경

우 K를 예로서 사용하여 결함 결정 구현예를 설명한다.

[0239] 경우 J: 제1 네트워크 디바이스가 기본 경로에 결함이 있음을 능동적으로 검출한다. 예를 들어, 제1 네트워크 디바이스는 기본 경로와 바인딩 관계를 설정하는 아웃바운드 인터페이스를 가지며, 아웃바운드 인터페이스를 통해 전송된 패킷은 기본 경로에 도착할 수 있다. 제1 네트워크 디바이스가 아웃바운드 인터페이스가 다운(down) 상태에 있는 것을 검출하면, 제1 네트워크 디바이스는 기본 경로에 결함이 있다고 결정할 수 있다.

[0240] 경우 K: 다른 디바이스가 제1 네트워크 디바이스에 기본 경로에 결함이 있음을 알린다. 예를 들어, 제1 네트워크 디바이스의 다음 홉 노드는 제1 네트워크 디바이스에 결함 통지 메시지를 전송한다. 결함 통지 메시지를 수신한 후, 제1 네트워크 디바이스는 결함 통지 메시지에 기초하여 기본 경로에 결함이 있다고 결정한다. 결함 통지 메시지는 기본 경로에 결함이 있음을 나타내며, 결함 통지 메시지는 선택적으로 시그널링을 통해 전달된다. 선택적으로, 결함 통지 메시지는 제1 네트워크 디바이스의 다음 홉 노드에 의해 생성된다. 예를 들어, 결함을 검출한 후, 다음 홉 노드는 결함 통지 메시지를 생성하고, 제1 네트워크 디바이스에 결함 통지 메시지를 전송한다. 선택적으로, 결함 통지 메시지는 제1 네트워크 디바이스의 다음 홉 노드로부터 기본 경로 상의 이그레스 노드로의 임의의 노드에 의해 생성된다. 결함을 검출한 후, 노드는 홉별 백홀 방식으로 제1 네트워크 디바이스에 결함 통지 메시지를 반환한다.

[0241] 선택적으로, 실시예 1이 SR 시나리오에 적용될 때, 패킷은 SR 패킷이고, 기본 경로는 SR 터널에 포함된다. 예를 들어, 기본 경로는 SR 터널의 하나의 LSP이다. SR 시나리오에서 기본 경로에 결함이 있다고 결정하는 방식은 경우 L, 경우 M 및 경우 N을 예로 사용하여 후술된다.

[0242] 경우 L: 제1 네트워크 디바이스는 패킷의 SID에 기초하여 SID에 대응하는 아웃바운드 인터페이스를 결정한다. SID에 대응하는 아웃바운드 인터페이스에 결함이 있으면, 제1 네트워크 디바이스는 기본 경로에 결함이 있다고 결정한다.

[0243] 예를 들어, 패킷은 SRv6 패킷이다. SRv6 패킷의 외부 IPv6 헤더에 있는 목적지 주소 필드는 SID를 전달하거나, SRv6 패킷의 SRH에 있는 SID 목록은 SID를 전달한다. 목적지 주소 필드의 SID는 SID 목록의 활성 SID(active SID)일 수 있다.

[0244] 경우 L에서, "패킷의 SID에 기초하여"는 "패킷의 외부 IPv6 헤더에 있는 목적지 주소 필드의 SID에 기초하여" 또는 "패킷의 SRH에 있는 SID 목록의 활성 SID에 기초하여"로 해석될 수 있다.

[0245] "SID에 대응하는 아웃바운드 인터페이스"는 경우 L1 내지 경우 L3을 예로 사용하여 아래에 설명된다.

[0246] 경우 L1: SID 유형(FuncType)이 End, 즉 SID가 End SID임.

[0247] 예를 들어, SRv6 패킷을 수신한 후, 제1 네트워크 디바이스는 SRv6 패킷의 외부 IPv6 헤더에서 목적지 주소 필드를 읽어서 목적지 주소를 획득하고, 목적지 주소에 기초하여 로컬 SID 테이블(local SID table)을 쿼리한다. 목적지 주소가 로컬 SID 테이블에 적중하고 SID 유형이 End이면 제1 네트워크 디바이스는 IPv6 라우팅 및 포워딩 테이블을 계속 쿼리하고, IPv6 라우팅 및 포워딩 테이블에서 아웃바운드 인터페이스를 찾는다.

[0248] 경우 L2: SID 유형이 End.X, 즉, SID가 End.X SID임.

[0249] 경우 L2에서, "SID에 대응하는 아웃바운드 인터페이스"는 제1 네트워크 디바이스의 로컬 SID 테이블에서 End.X SID에 바인딩된 아웃바운드 인터페이스이다. 특히, SRv6 패킷을 수신한 후, 제1 네트워크 디바이스는 SRv6 패킷의 외부 IPv6 헤더에서 목적지 주소 필드를 읽어서 목적지 주소를 획득하고, 목적지 주소에 기초하여 로컬 SID 테이블을 쿼리한다. 목적지 주소가 로컬 SID 테이블에 적중하고 SID 유형이 End.X인 경우, 제1 네트워크 디바이스는 로컬 SID 테이블을 쿼리하고, End.X SID에 바인딩된 아웃바운드 인터페이스를 찾는다.

[0250] 경우 L3: SID는 제1 네트워크 디바이스에 의해 발급된 SID가 아니다.

[0251] 경우 L3에서, "SID에 대응하는 아웃바운드 인터페이스"는 SID에 기초한 IPv6 라우팅 및 포워딩 테이블로부터의 매칭을 통해 제1 네트워크 디바이스에 의해 획득된 아웃바운드 인터페이스이다. 예를 들어, SRv6 패킷을 수신한 후, 제1 네트워크 디바이스는 SRv6 패킷의 외부 IPv6 헤더에서 대상 주소 필드를 읽어서 목적지 주소를 획득하고, 목적지 주소에 기초하여 로컬 SID 테이블을 쿼리한다. 제1 네트워크 디바이스가 로컬 SID 테이블에서 일치하는 SID를 찾지 못하면, 제1 네트워크 디바이스는 계속 SID를 사용하여 IPv6 라우팅 및 포워딩 테이블을 쿼리하고, IPv6 라우팅 및 포워딩 테이블에서 아웃바운드 인터페이스를 찾는다.

[0252] 경우 M: 제1 네트워크 디바이스는 패킷의 SID에 기초하여 SID에 대응하는 다음 홉을 결정한다. 다음 홉에 결함

이 있으면, 제1 네트워크 디바이스는 기본 경로에 결함이 있다고 결정한다.

[0253] 경우 M에서, "패킷의 SID에 기초하여"는 "패킷의 외부 IPv6 헤더에 있는 목적지 주소 필드의 SID에 기초하여" 또는 "패킷의 SRH에 있는 SID 목록의 활성 SID에 기초하여"로 해석될 수 있다.

[0254] "SID에 대응하는 다음 홉"은 경우 M1 내지 경우 M3을 예로서 사용하여 후술된다.

[0255] 경우 M1: SID 유형은 End, 즉, SID는 End SID이다.

[0256] 예를 들어, SRv6 패킷을 수신한 후, 제1 네트워크 디바이스는 SRv6 패킷의 외부 IPv6 헤더에서 목적지 주소 필드를 읽어서 목적지 주소를 획득하고, 목적지 주소에 기초하여 로컬 SID 테이블을 쿼리한다. 목적지 주소가 로컬 SID 테이블에 적중하고 SID 유형이 End이면, 제1 네트워크 디바이스는 IPv6 라우팅 및 포워딩 테이블을 계속 쿼리하고, IPv6 라우팅 및 포워딩 테이블에서 다음 홉을 찾는다.

[0257] 경우 M2: SID 유형이 End.X, 즉, SID는 End.X SID이다.

[0258] 경우 M2에서 "SID에 대응하는 다음 홉"은 제1 네트워크 디바이스의 로컬 SID 테이블에서 End.X SID에 바인딩된 다음 홉이다. 예를 들어, SRv6 패킷을 수신한 후, 제1 네트워크 디바이스는 SRv6 패킷의 외부 IPv6 헤더에서 목적지 주소 필드를 읽어서 목적지 주소를 획득하고, 목적지 주소를 기반으로 로컬 SID 테이블을 쿼리한다. 목적지 주소가 로컬 SID 테이블에 적중하고 SID 유형이 End.X인 경우, 제1 네트워크 디바이스는 로컬 SID 테이블을 쿼리하고, End.X SID에 바인딩된 다음 홉을 찾는다.

[0259] 경우 M3: SID는 제1 네트워크 디바이스에 의해 발급된 SID가 아니다.

[0260] 예를 들어, SRv6 패킷을 수신한 후, 제1 네트워크 디바이스는 SRv6 패킷의 외부 IPv6 헤더에서 목적지 주소 필드를 읽어서 목적지 주소를 획득하고, 목적지 주소를 기반으로 로컬 SID 테이블을 쿼리한다. 제1 네트워크 디바이스가 로컬 SID 테이블에서 일치하는 SID를 찾지 못하면, 제1 네트워크 디바이스는 계속 SID를 사용하여 IPv6 라우팅 및 포워딩 테이블을 쿼리하고, IPv6 라우팅 및 포워딩 테이블에서 다음 홉을 찾는다.

[0261] 경우 N: 제1 네트워크 디바이스는 패킷의 SID에 기초하여 SID에 대응하는 아웃바운드 인터페이스 및 다음 홉을 결정한다. 아웃바운드 인터페이스와 다음 홉에 결함이 있으면, 제1 네트워크 디바이스는 기본 경로에 결함이 있다고 결정한다.

[0262] 경우 N의 세부사항에 대해서는 경우 M 및 경우 N을 참조한다. 세부사항은 여기에서 다시 설명되지 않는다.

[0263] 경우 L, 경우 M 및 경우 N으로부터, SR 터널에서 기본 경로를 통해 패킷을 전송하는 과정에서, 기본 경로에 결함이 있는 경우, 경로를 따른 각 홉 노드는 노드의 다음 홉 또는 아웃바운드 인터페이스에 기초하여 기본 경로에 결함이 있다고 결정할 수 있음을 알 수 있다. 따라서, 경로를 따라 각 홉 노드는 기본 경로에 결함이 있다고 결정할 가능성이 있다. 이 경우, 경로를 따른 노드가 로컬 보호 메커니즘을 사전배치하면, 기본 경로 상의 패킷이 노드를 통과할 때, 노드는 패킷을 로컬 보호 경로로 전환한다. 따라서, 패킷이 보호 플래그를 전달하지 않는 경우, 기본 경로 상의 임의의 노드 또는 링크에 결함이 있으면, 경로를 따른 임의의 홉 노드는 패킷을 로컬 보호 경로로 전환할 가능성이 있음을 증명할 수 있다. 그러나, 보호 플래그가 패킷에 추가되어 기본 경로를 따른 각 홉 노드가 수신한 패킷이 보호 플래그를 전달한다. 따라서, 패킷을 수신한 다음 기본 경로에 결함이 있다고 결정하는 경로를 따른 홉 노드에 관계없이, 보호 플래그는 이미 보호 경로로의 전환이 허용되지 않음을 나타내므로, 홉 노드는 보호 플래그에 의해 표시된 바와 같이 패킷을 폐기할 수 있고, 패킷을 로컬 보호 경로로 전환하지 않는다. 따라서, 이 방법에서는, 기본 경로 상의 패킷이 로컬 보호 경로로 전환되지 않고, 경로를 따른 노드가 패킷이 전달한 보호 플래그에 기초하여 로컬 보호 전환을 수행할지 여부를 결정할 수 있으므로, 구현이 비교적 쉽고 서비스 배치 복잡성이 감소함을 알 수 있다.

[0264] S205: 제1 네트워크 디바이스는 패킷이 기본 경로에서 제1 보호 경로로 전환되도록 허용되지 않는다는 것을 보호 플래그가 표시한다고 결정한다.

[0265] 다음은 경우 01 내지 경우 07을 예시로 사용하여 복수의 관점에서 S205를 설명한다.

[0266] 경우 01: 경우 C1을 참조하여, 제1 네트워크 디바이스는 제2 비트와 제3 비트가 모두 설정되었는지를 결정한다. 제2 비트와 제3 비트가 모두 설정되면, 제1 네트워크 디바이스는 보호 플래그가 패킷이 기본 경로에서 중간점 TI-LFA 경로 또는 TI-LFA FRR 경로로 전환되도록 허용되지 않음을 나타낸다고 결정한다. 예를 들어, 제1 네트워크 디바이스가 지정된 2개의 비트가 "11"임을 식별하면, 제1 네트워크 디바이스는 패킷이 기본 경로에서 중간점 TI-LFA 경로로 전환되도록 허용되지 않고, 패킷이 기본 경로에서 TI-LFA FRR 경로로 전환되는 것도 허용되지 않

는다고 결정한다.

[0267] 선택적으로, 경우 O1에서, 제1 네트워크 디바이스는 패킷의 플래그 필드 또는 TLV로부터 제2 비트 및 제3 비트를 획득한다.

[0268] 경우 O3: 경우 D1을 참조하여, 제1 네트워크 디바이스는 제1 비트가 설정되는지 여부를 결정한다. 제1 비트가 설정되면, 제1 네트워크 디바이스는 보호 플래그가 패킷이 기본 경로에서 제1 보호 경로로 전환되도록 허용되지 않음을 표시한다고 결정한다. 예를 들어, 제1 네트워크 디바이스가 하나의 비트의 값이 "1"임을 식별하면, 제1 네트워크 디바이스는 패킷이 기본 경로에서 중간점 TI-LFA 경로로 전환되도록 허용되지 않는다고 결정한다. 다른 예를 들어, 제1 네트워크 디바이스가 하나의 비트의 값이 "1"임을 식별하면, 제1 네트워크 디바이스는 패킷이 기본 경로에서 TI-LFA FRR 경로로 전환되도록 허용되지 않는다고 결정한다.

[0269] 경우 O4: 경우 D2를 참조하여, 제1 네트워크 디바이스는 제1 비트가 설정되지 않았는지 여부를 결정한다. 제1 비트가 설정되지 않은 경우, 제1 네트워크 디바이스는 보호 플래그가 패킷이 기본 경로에서 제1 보호 경로로 전환되도록 허용되지 않음을 나타낸다고 결정한다. 예를 들어, 제1 네트워크 디바이스가 하나의 비트의 값이 "0"임을 식별하면, 제1 네트워크 디바이스는 패킷이 기본 경로에서 중간점 TI-LFA 경로로 전환되도록 허용되지 않는다고 결정한다. 다른 예를 들어, 제1 네트워크 디바이스가 하나의 비트의 값이 "0"임을 식별하면, 제1 네트워크 디바이스는 패킷이 기본 경로에서 TI-LFA FRR 경로로 전환되도록 허용되지 않는다고 결정한다.

[0270] 선택적으로, 경우 O3 및 경우 O4에서, 제1 네트워크 디바이스는 패킷의 플래그 필드에서 제1 비트를 읽는다. 선택적으로, 경우 O3 및 경우 O4에서, 제1 네트워크 디바이스는 패킷의 TLV로부터 제1 비트를 획득한다.

[0271] 경우 O5: 경우 E1을 참조하여, 제1 네트워크 디바이스는 패킷이 보호 플래그를 전달하는 플래그 필드를 포함하는지 여부를 결정할 수 있다. 패킷이 보호 플래그를 전달하는 플래그 필드를 포함하는 경우, 제1 네트워크 디바이스는 패킷이 기본 경로에서 제1 보호 경로로 전환되도록 허용되지 않는다고 결정하고, 따라서 제1 보호 경로를 통해 패킷을 전송하지 않는다. 경우 O5는 선택적으로 복수의 케이스를 포함한다. 구체적으로, 보호 플래그를 전달하는 플래그 필드의 특정 위치에 대해서는 경우 E1의 전술한 설명을 참조한다. 선택적으로, 보호 플래그를 전달하는 플래그 필드는 SRH, SRH가 아닌 다른 확장 헤더, 검출 패킷의 패킷 헤더 또는 데이터 패킷의 패킷 헤더에 위치한다. 이에 대응하여, 제1 네트워크 디바이스가 패킷이 보호 플래그를 전달하는 플래그 필드를 포함하는지 여부를 결정하는 경우는 복수의 경우, 예를 들어, 패킷 내의 SRH가 보호 필드를 전달하는 플래그 필드를 포함하는지 여부를 결정하는 경우, SRH가 아닌 다른 확장 헤더가 보호 플래그를 전달하는 플래그 필드를 포함하는지 여부를 결정하는 경우, 검출 패킷의 패킷 헤더가 보호 플래그를 전달하는 플래그 필드를 포함하는지 여부를 결정하는 경우, 및 데이터 패킷의 패킷 헤더가 보호 플래그를 전달하는 플래그 필드를 포함하는지 여부를 결정하는 경우를 포함할 수 있다.

[0272] 경우 O6: 경우 E2를 참조하여, 제1 네트워크 디바이스는 패킷이 보호 플래그를 전달하는 TLV를 포함하는지 여부를 결정할 수 있다. 패킷이 보호 플래그를 전달하는 TLV를 포함하는 경우, 제1 네트워크 디바이스는 패킷이 기본 경로에서 제1 보호 경로로 전환되도록 허용되지 않는다고 결정하므로, 제1 보호 경로를 통해 패킷을 보내지 않는다. 경우 O6은 선택적으로 복수의 경우를 포함한다. 구체적으로, 보호 플래그를 전달하는 TLV의 특정 위치에 대해서는 전술한 경우 E2의 설명을 참조한다. 선택적으로, 보호 플래그를 전달하는 TLV는 SRH, SRH가 아닌 다른 확장 헤더, 검출 패킷의 패킷 헤더 또는 데이터 패킷의 패킷 헤더에 위치한다. 이에 대응하여, 제1 네트워크 디바이스가 패킷이 보호 플래그를 전달하는 TLV를 포함하는지 여부를 결정하는 경우는 복수의 경우, 예를 들어, 패킷 내의 SRH가 보호 플래그를 전달하는 TLV를 포함하는지 여부를 결정하는 경우, SRH가 아닌 다른 확장 헤더가 보호 플래그를 전달하는 TLV를 포함하는지 여부를 결정하는 경우, 검출 패킷의 패킷 헤더가 보호 플래그를 전달하는 TLV를 포함하는지 여부를 결정하는 경우 및 데이터 패킷의 패킷 헤더가 보호 플래그를 전달하는 TLV를 포함하는지 여부를 결정하는 경우를 포함할 수 있다.

[0273] 경우 O7: 경우 H를 참조하여, 선택적으로, 제1 네트워크 디바이스는 검출 패킷의 외부 패킷 헤더로부터 보호 플래그를 획득한다. 선택적으로, 제1 네트워크 디바이스는 검출 패킷의 패킷 헤더로부터 보호 플래그를 획득한다.

[0274] 예를 들어, 경우 H1을 참조하여, 선택적으로, 제1 네트워크 디바이스는 BFD 패킷의 외부 패킷 헤더로부터 보호 플래그를 획득한다. 선택적으로, 제1 네트워크 디바이스는 BFD 패킷의 패킷 헤더로부터 보호 플래그를 획득한다.

[0275] 예를 들어, 경우 H2를 참조하여, 선택적으로, 제1 네트워크 디바이스는 PING 검출 패킷의 외부 패킷 헤더로부터 보호 플래그를 획득한다. 선택적으로, 제1 네트워크 디바이스는 PING 검출 패킷의 패킷 헤더로부터 보호 플래그

를 획득한다.

[0276] 예를 들어, 경우 H3을 참조하여, 선택적으로, 제1 네트워크 디바이스는 OAM 검출 패킷의 외부 패킷 헤더로부터 보호 플래그를 획득한다. 선택적으로, 제1 네트워크 디바이스는 OAM 검출 패킷의 패킷 헤더로부터 보호 플래그를 획득한다.

[0277] 예를 들어, 경우 H4를 참조하여, 선택적으로, 제1 네트워크 디바이스는 TWAMP 검출 패킷의 외부 패킷 헤더로부터 보호 플래그를 획득한다. 선택적으로, 제1 네트워크 디바이스는 TWAMP 검출 패킷의 패킷 헤더로부터 보호 플래그를 획득한다.

[0278] 예를 들어, 경우 H5를 참조하여, 선택적으로, 제1 네트워크 디바이스는 IFIT 패킷의 외부 패킷 헤더로부터 보호 플래그를 획득한다. 선택적으로, 제1 네트워크 디바이스는 IFIT 패킷의 패킷 헤더로부터 보호 플래그를 획득한다. 예를 들어, 선택적으로, 제1 네트워크 디바이스는 IFIT 패킷의 FIH로부터 보호 플래그를 획득할 수 있다. 예를 들어, 도 13 및 도 14에 도시된 바와 같이, 제1 네트워크 디바이스는 IFIT 패킷에서 FIH의 T/M 필드를 읽고, FIH의 T/M 필드의 값을 식별하여, 패킷이 제1 보호 경로를 통과하도록 허용되는지 여부를 결정할 수 있다.

[0279] 경우 01 내지 경우 07 중 하나만 존재할 수도 있거나, 조합 방식으로 복수의 경우가 있을 수 있음을 이해해야 한다.

[0280] S204 및 S205의 시간 순서는 이 실시예에서 제한되지 않는다는 것을 더 이해해야 한다. 다음은 예를 사용하여 S204 및 S205의 두 가지 가능한 시간 순서 경우를 설명한다. 다음 시간 순서 경우 1 및 시간 순서 경우 2는 이 실시예에서 제공되는 2개의 선택적인 구현예이며, 둘 다 본 출원의 이 실시예의 보호 범위 내에 있어야 한다.

[0281] 시간 시퀀스 경우 1: S204가 먼저 수행된 다음 S205가 수행된다. 예를 들어, 제1 네트워크 디바이스는 먼저 패킷을 수신한 다음 패킷을 기반으로 다음 홉 또는 아웃바운드 인터페이스를 결정하고, 다음 홉 또는 아웃바운드 인터페이스에 결함이 있는지 여부를 결정한다. 다음 홉 또는 아웃바운드 인터페이스에 결함이 있는 경우, 제1 네트워크 디바이스는 패킷에서 보호 플래그를 추가로 식별하고, 보호 플래그가 패킷이 기본 경로에서 제1 보호 경로로 전환되도록 허용됨을 나타내는지 여부를 결정한다. 보호 플래그가 패킷이 기본 경로에서 제1 보호 경로로 전환되도록 허용되지 않음을 나타내면, S206이 수행되어 패킷을 폐기한다. 다음 홉 또는 아웃바운드 인터페이스에 결함이 없으면, 제1 네트워크 디바이스는 패킷에서 보호 플래그를 식별하지 않고 결정된 다음 홉 또는 아웃바운드 인터페이스를 통해 패킷을 직접 포워딩한다.

[0282] 시간 순서 경우 2: S205가 먼저 수행된 다음 S204가 수행된다. 예를 들어, 제1 네트워크 디바이스가 패킷을 수신하기 전에, 기본 경로에 대응하는 아웃바운드 인터페이스가 다운 상태에 있거나, 제1 네트워크 디바이스가 다음 홉 노드가 전송한 결함 통지 메시지를 수신하므로, 보호 플래그를 전달하는 패킷을 수신하기 전에, 제1 네트워크 디바이스는 기본 경로에 결함이 있다고 미리 결정하였다. 그런 다음 제1 네트워크 디바이스는 보호 플래그를 전달하는 패킷을 수신한다. 제1 네트워크 디바이스는 패킷에서 보호 플래그를 식별하고, 보호 플래그가 패킷이 기본 경로에서 제1 보호 경로로 전환되도록 허용됨을 나타내는지 여부를 결정한다. 보호 플래그가 패킷이 기본 경로에서 제1 보호 경로로 전환되도록 허용되지 않음을 나타내는 경우, 제1 네트워크 디바이스가 기본 경로에 결함이 있다고 미리 결정하기 때문에, 제1 네트워크 디바이스는 S206을 수행하여 패킷을 폐기한다.

[0283] S206: 제 1 네트워크 디바이스는 기본 경로에 결함이 있다는 결정된 사실 및 패킷이 기본 경로에서 제1 보호 경로로 전환되도록 허용되지 않음을 나타내는 보호 플래그에 기초하여 패킷을 폐기한다.

[0284] 제1 네트워크 디바이스가 패킷을 폐기한 후, 패킷은 목적지 디바이스로 전송될 수 없다.

[0285] 선택적으로, S201 내지 S206에 설명된 패킷은 기본 경로 상의 트래픽에 있는 패킷일 수 있다. 트래픽(데이터 흐름 또는 패킷 흐름이라고도 함)은 소스 종단에서 목적지 종단까지의 일련의 패킷을 의미한다. 목적지 종단은 다른 호스트일 수 있으며, 복수의 호스트의 멀티캐스트 그룹 또는 브로드캐스트 영역을 포함한다.

[0286] 선택적으로, 제2 네트워크 디바이스는 S201 및 S202를 여러 번 수행하여 기본 경로를 통해 제1 네트워크 디바이스로 트래픽을 전송하고, 제1 네트워크 디바이스는 S203 내지 S206을 여러 번 수행하여 흐름에서 패킷을 폐기하여, 트래픽이 제1 네트워크 디바이스로 전송될 때 중단되고 목적지 디바이스로 전송될 수 없고, S207이 더 트리거된다.

[0287] S207: 제2 네트워크 디바이스는 기본 경로 상의 트래픽에서 패킷 손실이 발생한다고 결정한다.

[0288] 선택적으로, S207에서, S201 내지 S206에서 설명된 패킷이 손실된 것으로 결정된다. 선택적으로, S207에서,

S201 내지 S206에서 설명된 패킷에서 다른 패킷이 손실된 것으로 결정된다. 다른 패킷도 기본 경로 상의 트래픽이다. 다른 패킷의 전송 절차는 S201 내지 S206에서의 전송 절차와 유사하다.

[0289] 선택적으로, S207은 전술한 경우 H에 적용가능하다. 구체적으로, 경우 H에서, 검출 패킷은 패킷의 목적지 디바이스의 응답에 기초하여 연결성 또는 전송 성능 파라미터를 검출할 수 있다. 목적지 디바이스의 응답이 타임아웃 전에 수신되지 않으면, 검출 패킷의 개시자는 기본 경로에서 패킷 손실이 발생했다고 결정한다. 그러나, 제1 네트워크 디바이스가 검출 패킷을 폐기하기 때문에, 제1 네트워크 디바이스에서 트래픽이 중단된다. 따라서, 검출 패킷의 목적지 노드는 검출 패킷을 수신할 수 없으며, 목적지 노드는 제1 네트워크 디바이스에 응답을 반환하지 않는다. 이 경우, 제1 네트워크 디바이스는 목적지 노드로부터 응답을 수신할 수 없고, 제1 네트워크 디바이스는 타임아웃 전에 목적지 노드의 응답을 수신하지 않은 사실에 기초하여 기본 경로 상의 트래픽에 패킷 손실이 발생한 것으로 결정한다.

[0290] 제2 네트워크 디바이스가 패킷 손실을 결정하는 경우는 경우 H1 내지 경우 H5를 예로 사용하여 설명된다.

[0291] 경우 H1: 기본 경로에서 제2 네트워크 디바이스에 의해 전송된 패킷은 BFD 패킷을 포함한다. 이 경우, 제2 네트워크 디바이스가 패킷 손실이 기본 경로에서 발생했다고 결정하는 방식은 제2 네트워크 디바이스가 BFD 검출이 다운 상태에 있다고 결정하는 것일 수 있다. 예를 들어, 타이머가 만료되기 전에 제2 네트워크 디바이스가 반환된 루프백 SBFD 패킷을 수신하지 않으면, 제2 네트워크 디바이스는 로컬 상태를 다운 상태로 유지한다.

[0292] 경우 H2: 기본 경로에서 제2 네트워크 디바이스에 의해 전송된 패킷은 PING 검출 패킷을 포함한다. 이 경우, 제2 네트워크 디바이스가 기본 경로에서 패킷 손실이 발생했다고 결정하는 방식은 제2 네트워크 디바이스가 PING 검출 패킷이 손실되었다고 결정하는 것일 수 있다.

[0293] 경우 H3: 기본 경로에서 제2 네트워크 디바이스에 의해 전송된 패킷은 OAM 검출 패킷을 포함한다. 이 경우, 제2 네트워크 디바이스가 기본 경로에서 패킷 손실이 발생했다고 결정하는 방식은 제2 네트워크 디바이스가 OAM 검출 패킷이 손실된 것으로 결정하는 것일 수 있다. 예를 들어, 제2 네트워크 디바이스가 타임아웃 전에 에코 응답 패킷을 수신하지 않으면, 제2 네트워크 디바이스는 PING 검출 패킷이 손실된 것으로 결정한다.

[0294] 경우 H4: 기본 경로에서 제2 네트워크 디바이스에 의해 전송된 패킷은 TWAMP 검출 패킷을 포함한다. 이 경우, 제2 네트워크 디바이스가 기본 경로에서 패킷 손실이 발생했다고 결정하는 방식은 제2 네트워크 디바이스가 TWAMP 검출 패킷이 손실된 것으로 결정하는 것일 수 있다.

[0295] 경우 H5: 기본 경로에서 제2 네트워크 디바이스에 의해 전송된 패킷은 IFIT 검출 패킷을 포함한다. 이 경우, 제2 네트워크 디바이스가 기본 경로에서 패킷 손실이 발생했다고 결정하는 방식은 제2 네트워크 디바이스가 IFIT 검출 패킷이 손실된 것으로 결정하는 것일 수 있다.

[0296] 선택적으로, 패킷이 데이터 패킷인 경우, 제2 네트워크 디바이스는 수동 검출 방식으로 기본 경로 상의 트래픽에서 패킷 손실이 발생한다고 결정할 수 있다. 예를 들어, 기본 경로 상의 다운스트림 노드는 기본 경로에 결함이 있음을 홉별 백홀 방식으로 제2 네트워크 디바이스에 알린다. 이와 달리, 패킷을 보낼 때, 제2 네트워크 디바이스는 보호 플래그를 전달하는 데이터 패킷을 보낼 뿐만 아니라 보호 플래그를 전달하는 검출 패킷도 보낸다. 제2 네트워크 디바이스가 검출 패킷이 손실되었다고 결정하면, 검출 패킷과 데이터 패킷이 함께 전송되기 때문에, 제2 네트워크 디바이스는 데이터 패킷도 손실된 것으로 결정한다.

[0297] S208: 제2 네트워크 디바이스는 패킷 손실이 기본 경로 상의 트래픽에서 발생한다는 결정된 사실에 기초하여 기본 경로를 제2 보호 경로로 전환한다.

[0298] S208은 필수 단계가 아닌 선택적 단계이다. S208은 기본 경로에서 제2 보호 경로로 전환하기 위한 트리거 조건이 기본 경로 상의 트래픽에서 패킷 손실이 검출되는 경우에 적용가능하다.

[0299] 제2 보호 경로는 또한 기본 경로의 백업 경로이다. 제2 보호 경로는 기본 경로를 보호하는 데 사용된다. 제2 보호 경로는 기본 경로와 동일한 인그레스 노드를 갖는다. 예를 들어, 이 실시예에서, 기본 경로 상의 인그레스 노드는 제2 네트워크 디바이스이고, 제2 보호 경로 상의 인그레스 노드는 또한 제2 네트워크 디바이스이다. 예를 들어, 도 1에 도시된 바와 같이, 기본 경로 상의 인그레스 노드는 PE1이고, 제2 보호 경로는 진입 노드로서의 PE1을 가진 보호 경로일 수 있으며, 예를 들어, 터널 1의 백업 경로일 수 있다. 선택적으로, 제2 보호 경로는 종단 간 보호 경로이며, 개념 도입 부분에서 종단 간 보호 경로의 임의의 특징을 갖는다. 특히, 제2 보호 경로는 전체 기본 경로를 보호한다. 선택적으로, 기본 경로가 작동할 때, 제2 보호 경로는 유휴 상태에 있으며 서비스 데이터를 독립적으로 전달하지 않는다. 기본 경로에 결함이 있으면, 제2 보호 경로가 기본 경로의 작업을

대신하여 서비스 데이터를 전달하기 위해 기본 경로를 대체한다. 선택적으로, 제2 보호 경로는 사전계획된 경로이다. 예를 들어, 사용자는 대역폭 임계값보다 큰 대역폭을 갖는 백업 경로를 미리 계획하고, 백업 경로는 제2 보호 경로일 수 있다. 다른 예로, 사용자는 지연 임계값보다 짧은 지연을 갖는 백업 경로를 미리 계획하고, 백업 경로는 제2 보호 경로일 수 있다.

[0300] 다음은 경우 Y1 및 경우 Y2를 예로서 사용하여 제2 보호 경로를 설명한다.

[0301] 경우 Y1: 제2 보호 경로와 기본 경로는 동일한 터널에 속할 수 있다. 예를 들어, 제2 보호 경로와 기본 경로는 동일한 터널에 있는 2개의 LSP이고, 기본 경로는 터널에 있는 기본 LSP이고, 제2 보호 경로는 터널에 있는 백업 LSP이다. 예를 들어, 도 1에 도시된 바와 같이, 터널 1은 PE1과 PE3 사이에 존재하고, 제2 보호 경로는 터널 1의 백업 경로이며, 기본 경로는 터널 1의 기본 경로이다. 이러한 방식으로, 제2 보호 경로와 기본 경로 사이의 보호 메커니즘은 동일한 터널에 있는 두 LSP 간의 상호 보호에 속한다. 기본 LSP에 결함이 있는 경우, 패킷은 로컬 보호 경로를 통과하지 않음을 나타내는 보호 플래그를 전달하기 때문에, 기본 LSP를 통해 전송될 트래픽은 적시에 백업 LSP로 전환된다. 이는 종단 간 보호를 제공한다.

[0302] 경우 Y2: 제2 보호 경로와 기본 경로는 서로 다른 터널에 속할 수 있다. 즉, 제2 보호 경로와 기본 경로는 2개의 터널이고, 2개의 터널은 기본/백업 관계에 있다. 특히, 기본 경로는 기본 터널이고, 제2 보호 경로는 백업 터널이며, 기본 터널 상의 소스 노드는 백업 터널 상의 소스 노드와 동일하고, 기본 터널 상의 싱크 노드는 백업 터널 상의 싱크 노드와 동일하다. 기본 터널과 백업 터널은 2개의 VPN 서비스에 의해 반복되며, VPN 보호가 구현된다. 예를 들어, 도 5에 도시된 바와 같이, 기본 경로는 PE1과 PE3 사이의 기본 터널이고, 제2 보호 경로는 PE2와 PE4 사이의 백업 터널이다. 이 방식으로, 기본 터널에 결함이 있는 경우, 패킷이 로컬 보호 경로를 통과하지 않음을 나타내는 보호 플래그를 전달하기 때문에, 기본 터널을 통해 전송될 트래픽이 적시에 백업 터널로 전환된다. 이것은 터널 수준 보호를 제공합니다.

[0303] 선택적으로, SLA 보증 시나리오에서, 제2 보호 경로는 SLA를 충족하는 경로이다. 예를 들어, 제2 보호 경로의 지연은 SLA 지연 요구사항을 충족한다. 예를 들어, 제2 보호 경로의 지연은 지연 임계값보다 작다. 다른 예로, 제2 보호 경로의 대역폭은 SLA 대역폭 요구사항을 충족한다. 예를 들어, 제2 보호 경로의 대역폭은 대역폭 임계값보다 크다.

[0304] 이 시나리오에서, 패킷이 보호 플래그를 전달하지 않을 때, 패킷이 기본 경로를 따라 전송되는 과정에서, 경로를 따른 노드가 기본 경로에 결함이 있다고 결정하면, 노드는 패킷을 보호 경로로 로컬로 전환한다. 경로를 따른 노드가 패킷을 전환하는 보호 경로는 일반적으로 SLA를 충족하지 않기 때문에, 경로를 따른 노드가 패킷을 전환하는 보호 경로의 전송 성능은 대역폭, 지연 등의 측면에서 보장될 수 없다. 결과적으로, 기본 경로 상의 트래픽은 SLA를 충족하지 않는 경로로 우회되고, 서비스 SLA 보증이 달성될 수 없다. 그러나, 이 실시예에서, 로컬 보호가 허용되는지 여부를 나타낼 수 있는 식별자가 패킷에 추가된다. 보호 플래그를 전달하는 패킷이 기본 경로를 따라 전송되는 과정에서, 경로를 따른 노드가 기본 경로에 결함이 있다고 결정하지만, 보호 플래그가 보호 경로로의 로컬 전환이 허용되지 않음을 나타내는 경우, 경로를 따른 노드는 로컬 보호를 수행하지 않으므로 경로를 따른 노드에 의해 보호 경로로 패킷이 전환되지 않는다. 이는 패킷이 경로를 따른 노드로부터 보호 경로에 들어간 후 발생하는, 기본 경로 상의 트래픽이 SLA를 충족하지 않는 경로에서 장기간 전송되는 문제를 방지한다. 또한, 경로를 따른 노드는 패킷을 폐기하기 때문에, 헤드 노드는 기본 경로 상의 트래픽에서 패킷 손실을 적시에 검출할 수 있으므로, 헤드 노드는 기본 경로 상의 트래픽을 적시에 SLA를 충족하는 보호 경로로 전환할 수 있으며, 서비스 SLA 보증을 달성할 수 있다.

[0305] 기본 경로를 제2 보호 경로로 전환한 후, 제2 네트워크 디바이스는 제2 보호 경로를 통해 패킷을 전송한다. 선택적으로, 제2 네트워크 디바이스가 제2 보호 경로를 통해 패킷을 전송하는 방식은 S201 및 S202에서 패킷을 전송하는 방식과 유사하며, S201 및 S202에서 설명된 패킷의 임의의 특징을 포함한다. 예를 들어, 제2 보호 경로를 통해 제2 네트워크 디바이스에 의해 전송된 패킷은 선택적으로 보호 플래그를 포함한다.

[0306] 선택적으로, 제2 네트워크 디바이스는 기본 경로 상의 트래픽에서 패킷 손실이 발생한다고 결정하고, 기본 경로 상의 결함의 원인을 검출한다. 이 경우, 패킷이 제1 보호 경로를 통과하지 않기 때문에, 제2 네트워크 디바이스는 패킷 손실을 적시에 결정하고, 기본 경로에서 결함의 원인을 적시에 검출하여, 서비스 장애를 적시에 검출하고, 적시에 기본 경로의 결함을 수정하는 데 도움이 될 수 있다.

[0307] S207 및 S208은 선택적 단계라는 것을 이해해야 한다. 일부 다른 실시예에서, 선택적으로, S207 및 S208은 수행되지 않는다. 선택적으로, S207은 수행되지만, S208은 수행되지 않는다.

[0308] 예를 들어, S208은 경우 H에 적용가능하고, 특히 검출 패킷이 기본/백업 경로 전환을 트리거할 수 있는 임의의 시나리오에 적용될 수 있다.

[0309] 경우 H1이 예로서 사용된다. BFD 시나리오에서, BFD 검출 원리는 소스 노드가 BFD 패킷을 전송하고, 목적지 노드가 BFD 패킷을 수신한 다음 BFD 패킷에 응답하고, 소스 노드가 응답 패킷을 수신한 후 검출이 성공한 것으로 간주하는 것이다. 헤드 노드가 BFD 패킷을 보낼 때, 헤드 노드가 BFD 패킷과 보호 플래그를 함께 전송하지 않으면, 기본 경로에 결함이 있는 경우, 경로를 따른 노드가 BFD 패킷을 로컬 보호 경로로 전환하고, 로컬 보호 경로를 통해 목적지 노드에 BFD 패킷을 전송한다. 이 경우, 목적지 노드는 BFD 패킷을 수신한 다음 BFD 패킷에 응답한다. 헤드 노드가 응답 패킷을 수신한 후, BFD 검출은 UP 상태에 있다. 이 경우, BFD 검출이 성공하므로, 헤드 노드는 트래픽이 기본 경로에서 로컬 보호 경로로 우회되었음을 알 수 없다. 결과적으로, 헤드 노드는 기본 경로 상의 결함을 적시에 검출할 수 없고, 헤드 노드는 트래픽의 서비스 장애를 적시에 검출할 수 없으며, 헤드 노드는 기본 경로 상의 결함의 원인을 적시에 검출할 수 없다. 특히, BFD 고장을 검출함으로써 경로 전환이 트리거되는 시나리오에서는 헤드 노드가 수행한 BFD 검출이 성공하므로, 경로 전환 트리거 조건을 충족할 수 없다. 결과적으로, 헤드 노드는 기본 경로 상의 트래픽을 적시에 종단 간 보호 경로로 전환할 수 없다.

[0310] 그러나, 전술한 방법 실시예에서, 헤드 노드(예를 들어, 제2 네트워크 디바이스)는 보호 플래그와 함께 BFD 패킷을 전송하고, 보호 플래그를 사용하여 보호 경로로의 로컬 전환이 허용되지 않음을 표시한다. 따라서, BFD 패킷이 기본 경로를 따라 전송되는 과정에서, 기본 경로에 결함이 있는 경우, 보호 플래그가 보호 경로로의 로컬 전환이 허용되지 않음을 나타내므로, BFD 패킷을 수신할 때, 경로를 따른 노드(예컨대, 제1 네트워크 디바이스)는 로컬 보호 메커니즘을 사용하여 BFD 패킷을 로컬 보호 경로로 전환하지 않고 BFD 패킷을 폐기한다. 이 경우, BFD 패킷의 전송은 경로를 따른 노드에서 중단되고, BFD 패킷은 목적지 노드로 전송되지 않는다. 목적지 노드가 BFD 패킷을 수신하지 않기 때문에, 목적지 노드는 BFD 패킷에 응답하지 않으며, 헤드 노드는 목적지 노드로부터 응답 패킷을 수신하지 않는다. 이 경우 헤드 노드가 수행하는 BFD 검출은 다운 상태에 있다. 따라서, BFD 검출이 다운 상태에 있다는 사실에 기초하여, 헤드 노드는 기본 경로에 결함이 있음을 적시에 검출할 수 있으므로, 헤드 노드는 기본 경로 상의 결함의 원인을 적시에 검출하고 서비스 장애를 적시에 검출할 수 있다. 이는 기본 경로 상의 결함을 적시에 수정하고 장기적인 서비스 장애를 방지하는 데 도움이 된다.

[0311] 또한, 선택적으로, 경로 전환 트리거 조건은 헤드 노드에 사전구성된다. 경로 전환 트리거 조건은 BFD 검출이 다운 상태에 있을 때 기본 경로가 종단 간 보호 경로로 전환되는 것이다. 따라서, 전술한 방법에서는 헤드 노드가 수행하는 BFD 검출이 다운 상태에 있기 때문에, 사전구성된 트리거 조건이 충족되어 헤드 노드가 기본 경로 상의 트래픽을 종단 간 보호 경로로 전환하여, BFD 시나리오에서 기본 경로와 종단 간 보호 경로 간의 적시 전환을 구현한다.

[0312] 또한, 선택적으로, 종단 간 보호 경로는 SLA 요구사항에 따라 헤드 노드 상의 SLA를 충족하는 경로로서 사전구성된다. 따라서, 기본 경로에 결함이 있는 경우, 헤드 노드가 기본 경로 상의 트래픽을 종단 간 보호 경로로 전환하므로, 트래픽이 결함이 있는 기본 경로에서 SLA를 충족하는 경로로 전환되어, 트래픽은 SLA를 충족하는 경로를 통해 목적지 노드로 전송될 수 있으며, SLA 보증이 달성될 수 있다.

[0313] 유사하게, PING 검출 시나리오, OAM 검출 시나리오, TWAMP 검출 시나리오, 및 IFIT 검출 시나리오는 각각 BFD 검출 시나리오의 원리와 유사한 원리에 기초한다. 이러한 방식으로, 헤드 노드는 적시에 패킷 손실을 검출하고 적시에 기본/백업 경로 전환을 트리거할 수 있다.

[0314] 또한, 선택적으로, 경로 전환 트리거 조건은 헤드 노드에 사전구성된다. 경로 전환 트리거 조건은 IFIT 검출이 실패할 때 기본 경로가 종단 간 보호 경로로 전환되는 것이다. 따라서, 전술한 방법에서는 헤드 노드가 수행한 IFIT 검출이 실패했기 때문에, 사전구성된 트리거 조건이 충족되어 헤드 노드가 기본 경로 상의 트래픽을 종단 간 보호 경로로 전환하여 IFIT 검출 시나리오에서 기본 경로와 종단 간 보호 경로 간에 적시 전환을 구현한다. 또한, 선택적으로, 종단 간 보호 경로는 SLA 요구사항에 따라 헤드 노드 상의 SLA를 충족하는 경로로서 사전구성된다. 따라서, 기본 경로에 결함이 있는 경우, 헤드 노드가 기본 경로 상의 트래픽을 종단 간 보호 경로로 전환하므로, 트래픽이 결함이 있는 기본 경로에서 SLA를 충족하는 경로로 전환되어 트래픽은 SLA를 충족하는 경로를 통해 목적지 노드로 전송될 수 있으며, SLA 보증이 달성될 수 있다.

[0315] 이 실시예에서 제공되는 방법에서, 로컬 보호가 허용되는지 여부를 나타낼 수 있는 식별자가 패킷에 추가된다. 보호 플래그를 전달하는 패킷이 기본 경로를 따라 전송되는 과정에서, 경로를 따른 노드가 기본 경로에 결함이 있다고 결정하지만, 보호 플래그가 보호 경로로의 로컬 전환이 허용되지 않음을 나타내는 경우, 경로를 따른 노드는 로컬 보호를 수행하지 않으므로 경로를 따른 노드에 의해 보호 경로로 패킷이 전환되지 않는다. 이는 기본

경로에 결함이 있을 때 경로를 따른 노드를 인그레스로 하여 패킷이 보호 경로를 통과하는 것을 방지하고, 경로를 따른 노드로부터 보호 경로로 패킷이 진입한 후 발생하는 문제를 해결한다.

[0316] 특히, 대부분의 경우, 경로를 따른 노드는 로컬 보호만 수행할 수 있으며 종단 간 보호 경로로 전환할 수 없다. 따라서, 인그레스로서 경로를 따른 노드가 있는 보호 경로는 일반적으로 사전계획된 종단 간 보호 경로 대신 로컬 보호 경로이다. 이 경우, 패킷이 로컬 보호 경로로 전환되면, 기본 경로 상의 트래픽이 오랫동안 로컬 보호 경로로 우회된다. 그러나, 패킷에 보호 플래그가 추가되어 패킷이 로컬 보호 경로로 전송되지 않는다. 따라서, 기본 경로 상의 트래픽은 적시에 종단 간 보호 경로로 전환될 수 있다.

[0317] 또한, 경로를 따른 노드가 패킷을 폐기하기 때문에, 패킷 송신 측은 적시에 기본 경로 상의 트래픽에서 패킷 손실을 검출할 수 있다. 보호 전환을 트리거하기 위해 패킷 손실이 검출되는 다양한 시나리오에서, 패킷 송신 측은 기본 경로 상의 트래픽을 종단 간 보호 경로로 적시에 전환할 수 있으므로 패킷 송신 측은 서비스 장애 및 기본 경로 상의 결함의 원인을 적시에 검출할 수 있다.

[0318] 실시예 1은 수신된 패킷의 보호 플래그가 패킷이 기본 경로에서 제1 보호 경로로 전환되도록 허용되지 않음을 나타낼 때 제1 네트워크 디바이스가 처리를 수행하는 방식을 설명한다. 실시예 2는 보호 플래그가 패킷이 기본 경로에서 제1 보호 경로로 전환되도록 허용됨을 나타낼 때 제1 네트워크 디바이스가 처리를 수행하는 방식을 설명한다. 실시예 2는 실시예 1과의 차이점에 초점을 맞춘다는 것을 이해해야 한다. 실시예 1과 유사한 실시예 2의 단계 또는 다른 특징에 대해서는, 실시예 1을 참조한다. 세부사항은 실시예 2에서 설명되지 않는다.

[0319] 실시예 2

[0320] 도 15는 본 출원의 실시예 2에 따른 패킷 처리 방법의 흐름도이다. 실시예 2는 S301 내지 S309를 포함한다.

[0321] S301: 제2 네트워크 디바이스는 보호 플래그를 포함하는 패킷을 생성한다.

[0322] S302: 제2 네트워크 디바이스는 패킷을 제1 네트워크 디바이스로 전송한다.

[0323] S303: 제1 네트워크 디바이스는 패킷을 수신한다.

[0324] S304: 제1 네트워크 디바이스는 기본 경로에 결함이 있다고 결정한다.

[0325] S305: 제1 네트워크 디바이스는 보호 플래그가 패킷이 기본 경로에서 제1 보호 경로로 전환되도록 허용된다는 것을 표시한다고 결정한다.

[0326] 선택적으로, S305에서 "패킷이 기본 경로에서 제1 보호 경로로 전환되도록 허용됨"은 패킷이 모든 제1 보호 경로로 전환되도록 허용되거나 패킷이 몇몇 지정된 제1 보호 경로로 전환되도록 허용되지만 패킷이 몇몇 다른 지정된 제1 보호 경로로 전환되도록 허용되지 않음을 포함한다.

[0327] 다음은 경우 W1 내지 경우 W6을 예로서 사용하여 복수의 관점에서 S305를 설명한다.

[0328] 경우 W1: 경우 C2를 참조하여, 제1 네트워크 디바이스는 제2 비트가 설정되고 제3 비트가 설정되지 않는지 여부를 결정할 수 있다. 제2 비트가 설정되고 제3 비트가 설정되지 않은 경우, 제1 네트워크 디바이스는 보호 플래그가 패킷이 중간점 TI-LFA 경로로 전환되도록 허용되지 않지만 TI-LFA FRR 경로로 전환되도록 허용됨을 나타낸다고 결정한다. 예를 들어, 제1 네트워크 디바이스는 제2 비트와 제3 비트의 값이 "10"임을 발견하고 기본 경로 상의 패킷은 TI-LFA 경로를 통과하도록 허용되지만 기본 경로 상의 패킷은 중간점 TI-LFA 경로를 통과하도록 허용되지 않는다고 결정한다. 이 경우, TI-LFA 경로가 허용되므로, 제1 네트워크 디바이스는 TI-LFA 경로를 통해 패킷을 포워딩한다.

[0329] 경우 W2: 경우 C3을 참조하여, 제1 네트워크 디바이스는 제2 비트가 설정되지 않고 제3 비트가 설정되는지 여부를 결정할 수 있다. 제2 비트가 설정되지 않고 제3 비트가 설정되면, 제1 네트워크 디바이스는 보호 플래그가 패킷이 중간점 TI-LFA 경로로 전환되도록 허용되지만 TI-LFA FRR 경로로 전환되도록 허용되지 않음을 나타낸다고 결정한다. 예를 들어, 제1 네트워크 디바이스는 제2 비트와 제3 비트의 값이 "01"임을 발견하고, 기본 경로 상의 패킷이 중간점 TI-LFA 경로를 통과하도록 허용되지만 기본 경로 상의 패킷은 TI-LFA 경로를 통과하도록 허용되지 않는다고 결정한다. 이 경우, 중간점 TI-LFA 경로가 허용되기 때문에, 제1 네트워크 디바이스는 중간점 TI-LFA 경로를 통해 패킷을 포워딩한다.

[0330] 경우 W3: 경우 C4를 참조하여, 제1 네트워크 디바이스는 제2 비트가 설정되지 않고 제3 비트가 설정되지 않는지 여부를 결정할 수 있다. 제2 비트도 제3 비트도 설정되지 않은 경우, 제1 네트워크 디바이스는 보호 플래그가

패킷이 기본 경로에서 중간점 TI-LFA 경로 또는 TI-LFA FRR 경로로 전환되도록 허용됨을 나타낸다고 결정한다. 예를 들어, 제1 네트워크 디바이스는 제2 비트와 제3 비트의 값이 "00"임을 발견하고, 기본 경로 상의 패킷이 중간점 TI-LFA 경로를 통과하도록 허용되고 기본 경로 상의 패킷이 TI-LFA 경로를 통과하는 것도 허용된다고 결정한다. 이 경우, 중간점 TI-LFA 경로와 TI-LFA 경로가 허용되기 때문에, 제1 네트워크 디바이스는 중간점 TI-LFA 경로 또는 TI-LFA 경로를 통해 패킷을 전송한다. 제1 네트워크 디바이스는 중간점 TI-LFA 경로 및 TI-LFA 경로 중 하나의 경로를 결정하고, 결정된 경로를 통해 패킷을 전송할 수 있다.

[0331] 경우 W4: 경우 D1을 참조하여, 제1 네트워크 디바이스는 제1 비트가 설정되지 않는지 여부를 결정할 수 있다. 제1 비트가 설정되지 않은 경우, 제1 네트워크 디바이스는 보호 플래그가 패킷이 기본 경로에서 제1 보호 경로로 전환되도록 허용됨을 나타낸다고 결정한다. 예를 들어, 제1 네트워크 디바이스가 플래그 필드의 2번째 비트가 0임을 발견하면, 제1 네트워크 디바이스는 패킷이 제1 보호 경로를 통과하도록 허용된다고 결정한다. 선택적으로, 제1 네트워크 디바이스는 복수의 보호 메커니즘을 가능하게 한다. 경우 W4는 제1 네트워크 디바이스가 보호 플래그가 패킷이 TI-LFA FRR 경로로 전환되도록 허용됨을 나타낸다고 결정하는 것을 포함한다. 경우 W4는 제1 네트워크 디바이스가 보호 플래그가 패킷이 중간점 TI-LFA 경로로 전환되도록 허용됨을 나타낸다고 결정하는 것을 포함한다.

[0332] 경우 W5: 경우 E1을 참조하여, 제1 네트워크 디바이스는 패킷이 보호 플래그를 전달하는 플래그 필드를 포함하는지 여부를 결정할 수 있다. 패킷이 보호 플래그를 전달하는 플래그 필드를 포함하지 않으면, 제1 네트워크 디바이스는 패킷이 기본 경로에서 제1 보호 경로로 전환되도록 허용된다고 결정하므로, 제1 보호 경로를 통해 패킷을 보낸다.

[0333] 경우 W6: 경우 E2를 참조하면, 제1 네트워크 디바이스는 패킷이 보호 플래그를 전달하는 TLV를 포함하는지 여부를 결정할 수 있다. 패킷이 보호 플래그를 전달하는 TLV를 포함하지 않는 경우, 제1 네트워크 디바이스는 패킷이 기본 경로에서 제1 보호 경로로 전환되도록 허용된다고 결정하고, 제1 보호 경로를 통해 패킷을 보낸다.

[0334] 경우 W1 내지 경우 W7 중 하나만 있을 수도 있고, 조합 방식으로 복수의 경우가 있을 수도 있음을 이해해야 한다.

[0335] S304 및 S305의 시간 순서는 이 실시예에서 제한되지 않는다는 것을 더 이해해야 한다. 다음은 예를 사용하여 S304 및 S305의 두 가지 가능한 시간 시퀀스 경우를 설명한다. 다음 시간 시퀀스 경우 1 및 시간 시퀀스 경우 2는 이 실시예에서 제공되는 2개의 선택적인 구현예이며, 둘 다 본 출원의 이 실시예의 보호 범위 내에 있어야 한다.

[0336] 시간 순서 경우 1: S304가 먼저 수행된 다음 S305가 수행된다. 예를 들어, 제1 네트워크 디바이스는 먼저 패킷을 수신한 후 패킷을 기반으로 다음 홉 또는 아웃바운드 인터페이스를 결정하고, 다음 홉 또는 아웃바운드 인터페이스에 결함이 있는지 여부를 결정한다. 다음 홉 또는 아웃바운드 인터페이스에 결함이 있는 경우, 제1 네트워크 디바이스는 패킷에서 보호 플래그를 추가로 식별하고, 보호 플래그가 패킷이 기본 경로에서 제1 보호 경로로 전환되도록 허용됨을 나타내는지 여부를 결정한다. 보호 플래그가 패킷이 기본 경로에서 제1 보호 경로로 전환되도록 허용됨을 나타내면, S306이 수행되어 패킷을 포워딩한다. 다음 홉 또는 아웃바운드 인터페이스에 결함이 없으면, 제1 네트워크 디바이스는 패킷에서 보호 플래그를 식별하지 않고, 결정된 다음 홉 또는 아웃바운드 인터페이스를 통해 패킷을 직접 포워딩한다.

[0337] 시간 순서 경우 2: S305가 먼저 수행된 다음 S304가 수행된다. 예를 들어, 제1 네트워크 디바이스가 패킷을 수신하기 전에, 기본 경로에 대응하는 아웃바운드 인터페이스가 다운 상태에 있거나, 제1 네트워크 디바이스가 다음 홉 노드가 전송한 결함 통지 메시지를 수신하므로, 보호 플래그를 전달하는 패킷을 수신하기 전에, 제1 네트워크 디바이스는 기본 경로에 결함이 있다고 미리 결정하였다. 그런 다음 제1 네트워크 디바이스는 보호 플래그를 전달하는 패킷을 수신한다. 제1 네트워크 디바이스는 패킷에서 보호 플래그를 식별하고, 보호 플래그가 패킷이 기본 경로에서 제1 보호 경로로 전환되도록 허용됨을 나타내는지 여부를 결정한다. 보호 플래그가 패킷이 기본 경로에서 제1 보호 경로로 전환되도록 허용됨을 나타내는 경우, 제1 네트워크 디바이스는 기본 경로에 결함이 있다고 미리 결정하므로, 제1 네트워크 디바이스는 S306을 수행하여 패킷을 포워딩한다.

[0338] S306: 제1 네트워크 디바이스는 기본 경로에 결함이 있다는 결정된 사실 및 패킷이 기본 경로에서 제1 보호 경로로 전환되도록 허용됨을 나타내는 보호 플래그에 기초하여 제1 보호 경로를 통해 패킷을 전송한다.

[0339] 예를 들어, 도 4에 도시된 바와 같이, 제1 네트워크 디바이스는 RT_3이다. RT_3은 기본 경로에 결함이 있다는 결정된 사실과 패킷이 기본 경로에서 제1 보호 경로로 전환되도록 허용됨을 나타내는 보호 플래그에 기초하여

로컬 보호 메커니즘을 가능하게 한다. RT_3은 패킷을 점선으로 표시된 경로를 통해 RT_4에 전송하여 패킷이 RT_3으로부터 RT_4에 도착하고, RT_4로부터 RT_6에 도착하며, RT_6으로부터 RT_5에 도착하고, RT_5로부터 RT_7에 도착하며, RT_7로부터 PE2에 도착한다.

[0340] 다음은 경우 V1 내지 경우 V3을 예로서 사용하여 복수의 관점에서 S305를 설명한다.

[0341] 경우 V1: 제1 네트워크 디바이스는 기본 경로에 결함이 있다는 결정된 사실 및 패킷이 중간점 TI-LFA 경로로 전환되도록 허용되지만 TI-LFA FRR 경로로 전환하도록 허용되지 않음을 나타내는 보호 플래그에 기초하여 중간점 TI-LFA 경로를 통해 패킷을 전송한다. 이러한 방식으로, 제1 네트워크 디바이스는 패킷을 기본 경로에서 중간점 TI-LFA 경로로 전환하지만, 패킷을 기본 경로에서 TI-LFA FRR 경로로 전환하지 않는다. 패킷이 TI-LFA FRR 경로를 통과하지 않기 때문에, 패킷이 TI-LFA FRR 경로로 전환된 후 발생하는 문제를 방지할 수 있다.

[0342] 경우 V2: 제1 네트워크 디바이스는 기본 경로에 결함이 있다는 결정된 사실 및 패킷이 TI-LFA FRR 경로로 전환되도록 허용되지만 중간점 TI-LFA 경로로 전환하는 것은 허용되지 않음을 나타내는 보호 플래그에 기초하여 TI-LFA FRR 경로를 통해 패킷을 전송한다. 이러한 방식으로, 제1 네트워크 디바이스는 패킷을 기본 경로에서 TI-LFA FRR 경로로 전환하지만, 패킷을 기본 경로에서 중간점 TI-LFA 경로로 전환하지 않는다. 패킷이 중간점 TI-LFA 경로를 통과하지 않기 때문에, 패킷이 ㅈ중간점 TI-LFA 경로로 전환된 후 발생하는 문제를 방지할 수 있다.

[0343] 경우 V3: 제1 네트워크 디바이스는 1차 경로에 결함이 있다는 결정된 사실 및 패킷이 기본 경로에서 중간점 TI-LFA 경로 또는 TI-LFA FRR 경로로 전환되도록 허용됨을 나타내는 보호 플래그에 기초하여 TI-LFA FRR 경로 또는 TI-LFA FRR 경로를 통해 패킷을 전송한다.

[0344] 경우 V3에서, TI-LFA FRR 경로가 허용되고, TI-LFA FRR 경로도 허용되기 때문에, 제1 네트워크 디바이스는 TI-LFA FRR 경로 및 TI-LFA FRR 경로 중에서 하나의 경로를 결정할 수 있고, 결정된 경로를 통해 패킷을 보낼 수 있다. 예를 들어, 제1 네트워크 디바이스는 중간점 TI-LFA 보호 메커니즘의 우선순위와 TI-LFA 보호 메커니즘의 우선순위를 사전설정하고, 제1 네트워크 디바이스는 중간점 TI-LFA 보호 메커니즘의 우선순위와 TI-LFA 보호 메커니즘의 우선순위를 기반으로 중간점 TI-LFA 경로와 TI-LFA 경로 중 하나의 경로를 결정한다.

[0345] 예를 들어, 제1 네트워크 디바이스는 중간점 TI-LFA 경로 및 TI-LFA FRR 경로 중에서 더 높은 우선순위를 갖는 경로를 결정하고, 더 높은 우선순위를 갖는 경로를 통해 패킷을 전송한다. 예를 들어, 제1 네트워크 디바이스는 중간점 TI-LFA 보호 메커니즘의 우선순위가 TI-LFA 보호 메커니즘의 우선순위보다 높다고 사전설정한다. 중간점 TI-LFA와 TI-LFA를 모두 사용할 수 있는 경우, 중간점 TI-LFA를 우선적으로 사용한다. 이 경우, 제1 네트워크 디바이스는 중간점 TI-LFA 경로를 통해 패킷을 전송한다. 이와 달리, 제1 네트워크 디바이스는 TI-LFA 보호 메커니즘의 우선순위가 중간점 TI-LFA 보호 메커니즘의 우선순위보다 더 높다는 것을 사전설정한다. 중간점 TI-LFA와 TI-LFA를 모두 사용할 수 있는 경우, TI-LFA를 우선적으로 사용한다. 이 경우, 제1 네트워크 디바이스는 TI-LFA 경로를 통해 패킷을 전송한다.

[0346] 선택적으로, 중간점 TI-LFA 보호 메커니즘 및 TI-LFA 보호 메커니즘에서 더 높은 우선순위를 갖는 보호 메커니즘에 결함이 발생하는 경우, 제1 네트워크 디바이스는 더 낮은 우선순위를 갖지만 일반적으로 사용될 수 있는 보호 메커니즘을 사용하여 패킷을 포워딩할 수 있다. 예를 들어, 제1 네트워크 디바이스는 중간점 TI-LFA 보호 메커니즘의 우선순위가 TI-LFA 보호 메커니즘의 우선순위보다 높다고 사전설정한다. 그러나, 현재 중간점 TI-LFA 보호 메커니즘은 사용될 수 없지만, 현재 TI-LFA 보호 메커니즘은 사용될 수 있다. 이 경우, 제1 네트워크 디바이스는 TI-LFA 경로를 통해 패킷을 전송한다. 다른 예를 들어, 제1 네트워크 디바이스는 TI-LFA 보호 메커니즘의 우선순위가 중간점 TI-LFA 보호 메커니즘의 우선순위보다 높다고 사전설정한다. 그러나, 현재 TI-LFA 보호 메커니즘이 사용될 수 없지만, 현재 중간점 TI-LFA 보호 메커니즘이 사용될 수 있다. 이 경우, 제1 네트워크 디바이스는 중간점 TI-LFA 경로를 통해 패킷을 전송한다.

[0347] S307: 제3 네트워크 디바이스가 패킷을 수신한다.

[0348] 예를 들어, 제3 네트워크 디바이스는 기본 경로의 이그레스 노드이고, 제3 네트워크 디바이스는 기본 경로가 속한 터널 상의 싱크 노드이다. 예를 들어, 도 1에 도시된 바와 같이, 제3 네트워크 디바이스는 도 1에서 PE3이다.

[0349] S308: 제3 네트워크 디바이스는 수신된 패킷에 기초하여 응답 패킷을 제1 네트워크 디바이스에 전송한다.

[0350] S309: 제1 네트워크 디바이스는 응답 패킷에 기초하여 기본 경로가 연결 상태에 있다고 결정한다.

[0351] S308 및 S309는 선택적 단계이다. S308 및 S309는 경우 H에서 설명된 검출 패킷 전송 시나리오에 적용할 수 있

다. 이 시나리오에서, 제1 네트워크 디바이스는 검출 패킷의 개시 노드이고, 제3 네트워크 디바이스는 검출 패킷의 목적지 노드이다. 예를 들어, 경우 H1에서, 제1 네트워크 디바이스는 BFD 패킷의 개시 노드이고, 제3 네트워크 디바이스는 BFD 패킷의 목적지 노드이다.

[0352] 이 실시예에서 제공되는 방법에서, 보호 플래그가 패킷에 추가되어, 보호 플래그는 패킷이 기본 경로에서 보호 경로로 전환되도록 허용되는지 여부를 나타낼 수 있다. 기본 경로에 결함이 있는 경우, 그 경로를 따른 노드 역할을 하는 네트워크 디바이스가 보호 플래그를 전달하는 패킷을 수신하면, 기본 경로에 결함이 있다고 결정하고 보호 플래그는 패킷이 보호 경로로 전환되도록 허용됨을 나타내므로, 패킷은 보호 경로를 통해 전송되고, 경로를 따른 노드는 패킷이 전달한 보호 플래그를 사용하여 패킷을 로컬 보호 경로로 전환하도록 안내되고, 경로를 따른 노드는 패킷을 특정 보호 경로로 전환하도록 추가 안내될 수 있다. 이는 유연성을 향상시킨다.

[0353] 선택적으로, 실시예 1은 SR 시나리오에 적용된다. 선택적으로, SR 시나리오에서, 실시예 1의 제2 네트워크 디바이스는 SR 터널 상의 헤드 노드이고, 제1 네트워크 디바이스는 SR 터널 상의 중간 노드이며, 실시예 1의 패킷은 SR 패킷이다. 실시예 1에서, 기본 경로는 SR 터널에 포함된 기본 LSP이다. 제1 보호 경로는 제1 백업 LSP이다. 제2 보호 경로는 제2 백업 LSP이다. SR 시나리오는 SRv6 시나리오 및 세그먼트 라우팅 다중 프로토콜 라벨 전환(segment routing multi-protocol label switching, SR MPLS) 시나리오를 포함한다. SR MPLS 시나리오는 SR-TE 시나리오 및 세그먼트 라우팅 베스트 에포트(Segment Routing-Best Effort, SR-BE) 시나리오를 포함한다. 실시예 3의 특정 경우로서, 이러한 SR 시나리오는 모두 본 출원의 이 실시예의 보호 범위 내에 있어야 한니다.

[0354] 실시예 1이 SR 시나리오에 적용되는 절차는 실시예 3을 사용하여 아래에 설명된다. 즉, 실시예 3은 패킷이 SR 시나리오에서 보호 경로를 통과하지 않는 구현예를 설명한다. 실시예 1의 단계와 유사한 실시예 3의 단계에 대해서는 실시예 1을 참조한다는 것을 이해해야 한다. 세부사항은 실시예 3에서 설명되지 않는다.

[0355] 실시예 3

[0356] 도 16은 본 출원의 실시예 3에 따른 패킷 처리 방법의 흐름도이다. 실시예 3은 S401 내지 S408을 포함한다.

[0357] S401: SR 터널 상의 헤드 노드가 SR 패킷을 생성한다.

[0358] S401에서 설명된 SR 패킷은 경우 A, 경우 B, 경우 C, 경우 D, 경우 E1, 경우 E2, 경우 H, 또는 경우 I에 관련된 임의의 특징을 갖는다.

[0359] 예를 들어, SRv6에서 SR 패킷은 SRv6 패킷이고, SRv6 패킷은 SRH를 포함하고, SRH는 보호 플래그를 포함한다.

[0360] 선택적으로, 헤드 노드는 미리 커맨드 라인을 입력하거나 다른 구성을 수행하여 기능을 추가하는 보호 플래그를 가능하게 한다. 헤드 노드는 SRH를 추가하는 과정에서 보호 플래그를 SRH에 추가할 수 있다. 이 경우, 헤드 노드가 보낸 패킷의 SRH는 보호 플래그를 전달한다.

[0361] 예를 들어, 경우 C를 참조하면, 보호 플래그는 SRH에서 2개의 비트를 점유하고, 2개의 비트의 값은 중간 노드가 SRH를 기본 LSP에서 제1 백업 LSP로 전환하도록 허용되는지 여부를 나타내는 데 사용될 수 있다. 예를 들어, 경우 C1을 참조하면, 보호 플래그는 SRH에서 제2 비트와 제3 비트를 점유하고, 제1 백업 LSP는 중간점 TI-LFA 경로 또는 TI-LFA FRR 경로에 있다. 제2 비트와 제3 비트가 모두 설정되면, 중간 노드가 패킷을 기본 경로에서 중간점 TI-LFA 경로 및 TI-LFA FRR 경로로 전환하도록 허용되지 않음을 나타낸다.

[0362] 예를 들어, 경우 D를 참조하면, 보호 플래그는 SRH에서 하나의 비트를 점유하고, 하나의 비트의 값은 중간 노드가 SRH를 기본 LSP에서 제1 백업 LSP로 전환하도록 허용되는지 여부를 나타내는 데 사용될 수 있다.

[0363] 선택적으로, 플래그 필드의 2번째 비트는 보호 플래그를 전달하는 데 사용되며, 보호 플래그는 도 11에서 T/M이다. 플래그 필드의 2번째 비트 값이 1이면, 패킷이 기본 LSP에서 제1 백업 LSP로 전환되도록 허용되지 않음을 나타낸다. 플래그 필드의 2번째 비트 값이 0일 때, 중간 노드가 패킷을 기본 LSP에서 제1 백업 LSP로 전환하도록 허용됨을 나타낸다.

[0364] 선택적으로, 보호 플래그를 전달하는 플래그 필드는 제외 플래그를 더 포함한다. 제외 플래그는 E Flag(exclude flag)이며, 제외 플래그의 기능은 압축에서 마지막 SID를 제외하는 것이며, 제외 플래그의 기능은 "마지막 SID가 압축에서 제외될 때 설정"으로 번역될 수 있다.

[0365] 선택적으로, 보호 플래그를 전달하는 플래그 필드는 미사용 플래그를 더 포함한다. 미사용 플래그는 U 플래그이다. 사용되지 않고 앞으로 사용될 수 있는 ㅍ플래그 필드에 대해, 패킷의 미사용 플래그 값이 0으로 설정되면, 패킷 수신 단은 미사용 플래그를 무시한다.

[0366] 예를 들어, 경우 E2를 참조하면, 보호 플래그는 SRH의 TLV에 있다. 예를 들어, 도 12에 도시된 바와 같이, 보호 플래그를 전달하는 TLV는 SRH의 TLV이다. TLV는 보호 TLV로 지칭될 수 있다. 보호 TLV는 결함이 발생할 때 SRv6 패킷이 보호 경로를 통과할 수 있는지 여부를 나타내는 데 사용된다. SRv6 패킷이 보호 TLV를 포함하는 경우, 보호 TLV는 SRv6 패킷이 기본 LSP에서 제1 백업 LSP로 전환되도록 허용되지 않음을 나타내므로, 기본 LSP에 결함이 있으면, 중간 노드는 SRv6 패킷을 폐기하므로 SRv6 패킷은 제1 백업 LSP를 통과하지 않는다. 또한, SRv6 패킷이 보호 TLV를 포함하지 않는 경우, 기본 LSP에 결함이 있으면, 중간 노드는 SRv6 패킷을 제1 백업 LSP를 통해 포워딩하므로 SRv6 패킷은 제1 백업 LSP를 통과한다.

[0367] S402: 헤드 노드는 SR 터널의 기본 LSP를 통해 기본 LSP 상의 중간 노드로 SR 패킷을 전송한다.

[0368] 예를 들어, S401에서, 헤드 노드는 SRv6 패킷의 SRH에 SID 목록을 추가한다. SID 목록은 기본 LSP 상의 노드 또는 링크를 식별하여 SRv6 패킷이 기본 LSP를 통해 전송된다.

[0369] S403: SR 터널의 기본 LSP 상의 중간 노드는 SR 패킷을 수신한다.

[0370] S404: 중간 노드는 기본 LSP에 결함이 있다고 결정한다.

[0371] S405: 중간 노드는 보호 플래그가 SRv6 패킷이 기본 LSP에서 제1 백업 LSP로 전환되도록 허용되지 않음을 나타낸다고 결정하고, 제1 백업 LSP는 SR 터널에 포함된 LSP이고, 제1 백업 LSP는 기본 LSP의 로컬 보호 경로이다.

[0372] 중간 노드는 SRv6 패킷의 SRH로부터 보호 플래그를 획득하고, 보호 플래그가 SRv6 패킷이 기본 LSP에서 제1 백업 LSP로 전환되도록 허용되지 않음을 나타내는지 여부를 결정할 수 있다.

[0373] 선택적으로, 도 10에 도시된 바와 같이, 중간 노드는 패킷의 SRH로부터 플래그 필드를 결정하고, 플래그 필드로부터 제2 비트와 제3 비트를 얻는데, 예를 들어 플래그 필드로부터 비트6 및 비트7을 읽는다. 중간 노드는 플래그 필드의 제2 비트의 값과 제3 비트의 값에 기초하여, 보호 플래그가 SRv6 패킷이 기본 LSP에서 제1 백업 LSP로 전환되도록 허용되지 않음을 나타낸다고 결정한다. 예를 들어, 중간 노드가 플래그 필드의 비트6과 비트7이 "11"임을 식별하면, 중간 노드는 패킷이 기본 경로에서 중간점 TI-LFA 경로로 전환되는 것이 허용되지 않고, 패킷이 기본 경로에서 TI-LFA FRR 경로로 전환하는 것도 허용되지 않는다고 결정한다. 물론, "11"은 선택적 방식이다. 다른 선택적인 구현예에서, 중간 노드가 플래그 필드의 비트6 및 비트7이 "00"임을 식별하면, 중간 노드는 패킷이 기본 경로에서 중간점 TI-LFA 경로로 전환되도록 허용되지 않고, 패킷이 기본 경로에서 TI-LFA FRR 경로로 전환되는 것도 허용되지 않는다고 결정한다.

[0374] 또 다른 예를 들면, 도 11에 도시된 바와 같이, 중간 노드는 패킷의 SRH로부터 플래그 필드를 결정하고, 플래그 필드로부터 제1 비트를 얻는데, 예를 들어, 플래그 필드로부터 2번째 비트를 읽는다. 중간 노드는 플래그 필드의 제1 비트의 값을 기반으로 보호 플래그가 SRv6 패킷이 기본 LSP에서 제1 백업 LSP로 전환되도록 허용되지 않음을 표시한다고 결정한다. 예를 들어, 중간 노드가 플래그 필드의 2번째 비트가 "1"임을 식별하면, 중간 노드는 패킷이 기본 경로에서 중간점 TI-LFA 경로로 전환되도록 허용되지 않는다고 결정하거나, 패킷이 기본 경로에서 TI-LFA FRR 경로로 전환되도록 허용되지 않는다고 결정한다. 물론 "1"은 선택적 방식이다. 선택적으로, 중간 노드가 플래그 필드의 2번째 비트가 "0"임을 식별하면, 중간 노드는 패킷이 기본 경로에서 중간점 TI-LFA 경로로 전환되도록 허용되지 않고, 패킷이 기본 경로에서 TI-LFA FRR 경로로 전환되는 것도 허용되지 않는다고 결정한다.

[0375] 선택적으로, 중간 노드는 SRH가 보호 플래그를 전달하는 데 사용되는 TLV를 포함하는지 여부를 결정할 수 있다. SRH가 보호 플래그를 전달하는 데 사용되는 TLV를 포함하는 경우, 중간 노드는 보호 플래그가 SRv6 패킷이 기본 LSP에서 제1 백업 LSP로 전환되도록 허용되지 않음을 표시한다고 결정한다. 예를 들어, 도 12에 도시된 바와 같이, SRH가 도 12에 도시된 TLV를 포함하는 경우, 중간 노드는 보호 플래그가 SRv6 패킷이 기본 LSP에서 제1 백업 LSP로 전환되도록 허용되지 않음을 나타낸다고 결정한다.

[0376] 선택적으로, 중간 노드는 SRH의 TLV에 있는 유형 필드의 값에 기초하여 SRH로부터 보호 플래그를 전달하는 데 사용되는 TLV를 식별할 수 있다. 예를 들어, 중간 노드는 SRH의 TLV에 있는 유형 필드의 값이 보호 TLV에 해당하는 유형 값인지 여부를 결정할 수 있다. SRH의 TLV에 있는 유형 필드의 값이 보호 TLV에 해당하는 유형 값이면, 중간 노드는 SRH가 보호 플래그를 전달하는 데 사용되는 TLV를 포함한다고 결정한다.

[0377] S406: 중간 노드는 기본 LSP에 결함이 있다는 결정된 사실 및 SR 패킷이 기본 LSP에서 제1 백업 LSP로 전환되도록 허용되지 않음을 나타내는 보호 플래그에 기초하여 SR 패킷을 폐기한다.

[0378] S407: SR 터널 상의 헤드 노드는 기본 LSP 상의 트래픽에서 패킷 손실이 발생한다고 결정한다.

[0379] S408: 헤드 노드는 패킷 손실이 기본 LSP의 트래픽에서 발생한다는 결정된 사실에 기초하여 기본 LSP를 제2 백업 LSP로 전환하며, 제2 백업 LSP는 기본 LSP의 종단 간 보호 경로이다.

[0380] 이 실시예에서 제공되는 방법에서, 로컬 보호가 허용되는지 여부를 나타낼 수 있는 식별자가 SRv6 패킷의 SRH에 추가된다. 보호 플래그를 전달하는 패킷이 SR 터널의 기본 LSP를 따라 전송되는 과정에서, 기본 LSP 상의 중간 노드가 기본 경로에 결함이 있다고 결정하지만, 보호 플래그가 로컬 보호가 허용되지 않음을 나타내는 경우, 경로를 따른 노드는 로컬 보호를 수행하지 않으므로 중간 노드에 의해 인그레스로서의 중간 노드를 가진 백업 LSP로 패킷이 전환되지 않는다. 이는 패킷이 기본 경로에 결함이 있을 때 로컬 보호를 위해 백업 LSP를 통과하지 못하게 하고, 패킷이 경로를 따른 노드로부터 로컬 보호를 위해 백업 LSP에 진입한 후 발생하는 문제를 해결한다.

[0381] 또한, 패킷이 중간 노드에 의해 폐기되기 때문에, SR 터널 상의 헤드 노드는 기본 경로의 트래픽에서 패킷 손실을 적시에 검출할 수 있고, SR 터널 상의 헤드 노드는 서비스 장애를 적시에 검출할 수 있으며, SR 터널 상의 헤드 노드는 기본 경로에서 결함의 원인을 검출할 수 있다.

[0382] 또한, 선택적으로, 동일한 SR 터널에서 서로 다른 LSP 간의 전환을 위한 트리거 조건이 헤드 노드에서 사전구성된다. 트리거 조건은 패킷 손실이 검출되면 SR 터널의 기본 LSP가 SR 터널의 백업 LSP로 전환되는 것이다. 따라서, 전술한 방법에서는 헤드 노드가 기본 LSP의 트래픽에서 패킷 손실이 발생했다고 결정하므로, 트리거 조건이 충족되어 헤드 노드가 기본 LSP의 트래픽을 백업 LSP로 적시에 전환하게 된다. 이는 신속한 종단 간 보호 전환을 용이하게 한다.

[0383] 또한, 선택적으로, 백업 LSP는 SLA 요구사항에 따라 SLA를 충족하는 LSP로서 헤드 노드에 사전구성된다. 이 경우, 헤드 노드가 기본 LSP의 트래픽을 SLA를 충족하는 백업 LSP로 전환하기 때문에, 트래픽이 SLA를 충족하는 백업 LSP로 전환될 수 있고, 오랫동안 SLA를 보장하지 않으며 중간 노드가 전환되는 백업 LSP로 우회되지 않는다. 따라서, 트래픽 전송 성능을 보장할 수 있고, SLA 보증을 달성할 수 있다.

[0384] 실시예 3은 SR 시나리오에서 보호 플래그를 기반으로 하나의 터널에서 두 LSP 간의 보호 전환을 구현하는 절차를 보여준다. 이 실시예는 SR 시나리오에서 보호 플래그에 기초한 터널 레벨 보호 전환을 구현하는 절차를 더 제공한다. 다음은 실시예 3을 사용하여 절차를 설명한다. 실시예 3에서 제공되는 실시예 4는 또한 실시예 1이 SR 시나리오에 적용되는 절차이다. 다시 말해서, 실시예 4는 패킷이 SR 시나리오에서 보호 경로를 통과하지 않는 구현예도 설명한다. 실시예 1 및 실시예 3의 단계와 유사한 실시예 4의 단계에 대해서는, 실시예 1 및 실시예 3을 참조한다는 것을 이해해야 한다. 세부사항은 실시예 4에서 설명되지 않는다.

[0385] 실시예 4

[0386] 도 17은 본 출원의 실시예 4에 따른 패킷 처리 방법의 흐름도이다. 실시예 4는 S501 내지 S508을 포함한다.

[0387] S501: 제1 SR 터널 상의 헤드 노드는 SR 패킷을 생성한다.

[0388] S502: 헤드 노드는 SR 패킷을 제1 SR 터널의 기본 LSP를 통해 기본 LSP의 중간 노드로 전송한다.

[0389] S503: 제1 SR 터널의 기본 LSP 상의 중간 노드는 SR 패킷을 수신한다.

[0390] S504: 중간 노드는 기본 LSP에 결함이 있다고 결정한다.

[0391] S505: 중간 노드는 보호 플래그가 SR 패킷이 기본 LSP에서 백업 LSP로 전환되도록 허용되지 않음을 나타낸다고 결정하며, 백업 LSP는 SR 터널에 포함된 LSP이고, 백업 LSP는 기본 LSP의 로컬 보호 경로이다.

[0392] S506: 중간 노드는 기본 LSP에 결함이 있다는 결정된 사실 및 SR 패킷이 기본 LSP에서 백업 LSP로 전환되도록 허용되지 않음을 나타내는 보호 플래그에 기초하여 SR 패킷을 폐기한다.

[0393] S507: 헤드 노드는 기본 LSP의 트래픽에서 패킷 손실이 발생한다고 결정한다.

[0394] S508: 헤드 노드는 기본 LSP의 트래픽에서 패킷 손실이 발생한다는 결정된 사실에 기초하여 제1 SR 터널의 기본 LSP를 제2 SR 터널로 전환하며, 제2 SR 터널과 제1 SR 터널은 동일한 소스 및 싱크를 갖는다.

[0395] 예를 들어, 도 1에 도시된 바와 같이, P1과 P3 사이의 경로에 결함이 있는 경우, P1은 보호 플래그를 기반으로 패킷을 폐기한다. 이 경우, PE1은 패킷 손실을 검출하므로, PE1은 터널 1의 기본 경로를 터널 1의 백업 경로로

전환한다.

[0396] 본 실시예에서 제공하는 방법에 따르면, 패킷 손실을 검출함으로써 보호 전환이 트리거되는 시나리오에서, SR 터널에 결함이 발생하면, 로컬 보호가 허용되는지 여부를 나타낼 수 있는 식별자가 SR 패킷에서 SRH에 추가되기 때문에, 보호 플래그를 전달하는 패킷이 SR 터널을 따라 전송되는 과정에서, 보호 플래그가 로컬 보호가 허용되지 않음을 나타내기 때문에 중간 노드는 로컬 보호를 수행하지 않는다. 따라서, 헤드 노드는 패킷 손실이 발생한다고 결정하기 때문에, 터널 수준의 전환 트리거 조건이 충족되면, SR 터널의 트래픽이 다른 SR 터널로 적시에 전환될 수 있으므로 종단 간 보호 전환이 신속하게 수행될 수 있다.

[0397] 또한, 선택적으로, 다른 SR 터널은 SLA 요구사항에 따라 SLA를 충족하는 터널로서 헤드 노드에 사전구성된다. 이 경우, 헤드 노드가 기본 LSP의 트래픽을 SLA를 충족하는 SR 터널로 전환하기 때문에, 트래픽 전송 성능이 보장될 수 있고, SLA 보증이 달성될 수 있다.

[0398] 선택적으로, 실시예 3 또는 실시예 4는 SRv6 시나리오에 적용되며, 구체적으로 SRv6 검출 패킷을 전송하는 시나리오에 적용된다. 실시예 3 또는 실시예 4가 검출 패킷 전송에 적용되는 절차는 실시예 5를 사용하여 이하에 설명된다. 즉, 실시예 5는 SRv6 시나리오에서 검출 패킷이 보호 경로를 통과하지 않는 구현예를 설명한다. 실시예 3 및 실시예 4의 단계와 유사한 실시예 5의 단계에 대해서는, 실시예 3 및 실시예 4를 참조한다는 것을 이해해야 한다. 세부사항은 실시예 5에서 설명되지 않는다.

[0399] 실시예 5는 검출 패킷이 SRv6 BFD 패킷인 경우를 설명한다. 즉, 실시예 5는 SRv6 시나리오에서 SRv6 BFD 패킷이 보호 경로를 통과하지 않는 구현예를 설명한다.

[0400] 실시예 5

[0401] 도 18은 본 출원의 실시예 5에 따른 패킷 처리 방법의 흐름도이다. 실시예 5는 S601 내지 S608을 포함한다.

[0402] S601: SRv6 터널의 헤드 노드는 SRv6 BFD 패킷을 생성한다.

[0403] S602: 헤드 노드는 SRv6 터널의 기본 LSP를 통해 기본 LSP 상의 중간 노드로 SRv6 BFD 패킷을 전송한다.

[0404] S603: SRv6 터널의 기본 LSP 상의 중간 노드는 SRv6 BFD 패킷을 수신한다.

[0405] S604: 중간 노드는 기본 LSP에 결함이 있다고 결정한다.

[0406] S605: 중간 노드는 보호 플래그가 SRv6 BFD 패킷이 기본 LSP에서 제1 백업 LSP로 전환되도록 허용되지 않음을 표시한다고 결정하며, 제1 백업 LSP는 기본 LSP의 로컬 보호 경로이고, 제1 백업 LSP는 SRv6 터널에 포함된 LSP이다.

[0407] S606: 중간 노드는 기본 LSP에 결함이 있다는 결정된 사실 및 SRv6 BFD 패킷이 기본 LSP에서 제1 백업 LSP로 전환되도록 허용되지 않음을 나타내는 보호 플래그에 기초하여 SRv6 BFD 패킷을 폐기한다.

[0408] S607: SRv6 터널의 헤드 노드는 SRv6 BFD 패킷이 손실된다고 결정한다.

[0409] S608: SRv6 BFD 패킷이 손실된다는 결정된 사실에 기초하여, 헤드 노드는 SRv6 터널의 기본 LSP를 SRv6 터널의 제2 백업 LSP로 전환하며, 제2 백업 LSP는 기본 LSP의 종단 간 보호 경로이거나; 또는 헤드 노드는 SRv6 터널을 다른 SRv6 터널로 전환하며, 다른 SRv6 터널 및 결함이 있는 SRv6 터널은 동일한 소스 및 싱크를 갖는다.

[0410] 본 실시예에서 제공하는 방법에 따르면, SRv6 BFD 패킷의 SRH 헤더는 보호 플래그를 전달하기 때문에, 기본 LSP에서 노드 결함 또는 링크 결함이 발생하면, 경로를 따른 노드가 SRv6 BFD를 수신할 때, SRv6 BFD 패킷의 보호 플래그가 패킷이 로컬 백업 LSP를 통과하도록 허용되지 않음을 나타내기 때문에 경로를 따른 노드는 SRv6 BFD 패킷을 폐기한다. 이 경우, SRv6 BFD 패킷은 BFD 목적지 종단에 도달하지 않고, BFD 목적지 종단은 패킷을 헤드 노드로 반환하지 않는다. 따라서, 헤드 노드 상의 BFD 검출은 다운되도록 트리거되어 헤드 노드는 기본 경로 상의 결함을 적시에 검출할 수 있다. 또한, BFD 검출이 다운되므로 종단 간 보호 전환이 트리거되면, 헤드 노드는 동일한 SRv6 터널에서 적시에 기본/백업 LSP 전환을 수행하여 SRv6 터널의 기본 LSP의 패킷을 SRv6 터널의 백업 LSP로 전환하여 기본/백업 LSP 전환 시간을 줄이거나; 또는 헤드 노드는 적시에 터널 수준 전환을 수행하여 기본 LSP의 패킷을 다른 SRv6 터널로 전환함으로써 두 SRv6 터널 간의 전환 시간을 감소시킨다.

[0411] SRv6 BFD 패킷은 실시예 5에서 설명을 위한 예로서 사용된다는 것을 이해해야 한다. 실시예 5의 SRv6 BFD 패킷은 SRv6 PING 검출 패킷, SRv6 OAM 패킷, SRv6 OAM 검출 패킷 또는 SRv6 TWAMP 검출 패킷으로 대체될 수 있다. 대응하는 처리 절차에 대해서는, 실시예 5를 참조한다. 세부사항은 본 명세서에서 다시 설명되지 않는다.

[0412] 전술한 내용은 본 출원의 실시예들에서의 패킷 처리 방법들을 설명하고, 다음은 본 출원의 실시예들에서의 패킷 처리 장치를 설명한다. 패킷 처리 장치(110)는 전술한 방법에서 제1 네트워크 디바이스의 임의의 기능을 갖고, 패킷 처리 장치(120)는 전술한 방법에서 제2 네트워크 디바이스의 임의의 기능을 갖는다는 것을 이해해야 한다.

[0413] 도 19는 본 출원의 실시예에 따른 패킷 처리 장치(110)의 구조의 개략도이다. 도 19에 도시된 바와 같이, 패킷 처리 장치(110)는 S203, S303, S403, S503 또는 S603 중 적어도 하나를 수행하도록 구성된 수신 모듈(1101); S204, S205, S303, S304, S404, S405, S504, S505, S604, 또는 S605 중 적어도 하나를 수행하도록 구성된 결정 모듈(1102); 및 S206, S406, S506 또는 S606 중 적어도 하나를 수행하도록 구성된 폐기 모듈(1103)을 포함한다.

[0414] 선택적으로, 결정 모듈(1102)은 S305를 수행하도록 더 구성된다. 장치(110)는 S306을 수행하도록 구성된 전송 모듈을 더 포함한다.

[0415] 도 19의 실시예에 제공된 패킷 처리 장치(110)는 전술한 방법 실시예의 제1 네트워크 디바이스에 대응한다는 것을 이해해야 한다. 패킷 처리 장치(110)의 모듈 및 전술한 다른 동작 및/또는 기능은 각각 방법 실시예에서 제1 네트워크 디바이스에 의해 구현되는 다양한 단계 및 방법을 구현하는 데 사용된다. 세부사항은 전술한 방법 실시예를 참조한다. 간결함을 위해, 세부사항은 본 명세서에서 다시 설명하지 않는다.

[0416] 도 19의 실시예에서 제공된 패킷 처리 장치(110)가 패킷을 처리하는 경우, 전술한 기능 모듈로의 분할은 설명을 위한 예로서 사용될 뿐이라는 것을 이해해야 한다. 실제 적용 시, 완성을 위해 필요에 따라 전술한 기능들이 상이한 기능 모듈에 할당될 수 있다. 구체적으로, 패킷 처리 장치(110)의 내부 구조는 전술한 기능의 전부 또는 일부를 완성하기 위해 서로 다른 기능 모듈로 분할된다. 또한, 전술한 실시예에서 제공된 패킷 처리 장치(110)는 전술한 패킷 처리 방법 실시예와 동일한 개념에 속한다. 이의 구체적인 구현 프로세스에 대해서는 방법 실시예를 참조한다. 세부사항은 본 명세서에서 다시 설명되지 않는다.

[0417] 도 20은 본 출원의 실시예에 따른 패킷 처리 장치(120)의 구조의 개략도이다. 도 20에 도시된 바와 같이, 패킷 처리 장치(120)는 S201, S301, S401, S501, 또는 S601 중 적어도 하나를 수행하도록 구성된 생성 모듈(1201); 및 S202, S302, S402, S502, 또는 S602 중 적어도 하나를 수행하도록 구성된 전송 모듈(1202)을 포함한다.

[0418] 선택적으로, 장치(120)는 패킷 손실이 기본 경로 상의 트래픽에서 발생한다고 결정하도록 구성된 결정 모듈; 및 기본 경로 상의 트래픽에서 패킷 손실이 발생한다는 결정된 사실에 기초하여 기본 경로를 제2 보호 경로로 전환하도록 구성된 전환 모듈을 더 포함한다.

[0419] 도 20의 실시예에 제공된 패킷 처리 장치(120)가 전술한 방법 실시예의 제2 네트워크 디바이스에 대응한다는 것을 이해해야 한다. 패킷 처리 장치(120)의 모듈 및 전술한 다른 동작 및/또는 기능은 각각 방법 실시예에서 제2 네트워크 디바이스에 의해 구현되는 다양한 단계 및 방법을 구현하는 데 사용된다. 세부사항은 전술한 방법 실시예를 참조한다. 간결함을 위해, 세부사항은 본 명세서에서 다시 설명하지 않는다.

[0420] 도 20의 실시예에서 제공된 패킷 처리 장치(120)가 패킷을 처리할 때, 전술한 기능 모듈로의 분할은 설명을 위한 예로서 사용될 뿐이라는 것을 이해해야 한다. 실제 적용 시, 완성을 위해 필요에 따라 전술한 기능들이 상이한 기능 모듈에 할당될 수 있다. 구체적으로, 패킷 처리 장치(120)의 내부 구조는 전술한 기능의 전부 또는 일부를 완성하기 위해 서로 다른 기능 모듈로 분할된다. 또한, 전술한 실시예에서 제공되는 패킷 처리 장치(120)는 전술한 패킷 처리 방법 실시예와 동일한 개념에 속한다. 구체적인 구현 프로세스에 대해서는 방법 실시예를 참조한다. 세부사항은 본 명세서에서 다시 설명되지 않는다.

[0421] 다음은 제1 네트워크 디바이스 또는 제2 네트워크 디바이스의 가능한 엔티티 형태를 설명한다.

[0422] 전술한 네트워크 디바이스의 특성을 갖는 모든 형태의 제품이 본 출원의 보호 범위에 속한다는 것을 이해해야 한. 이하의 설명은 단지 예시일 뿐이며, 본 출원의 실시예에서 네트워크 디바이스의 제품 형태는 이에 제한되지 않음을 더 이해해야 한다.

[0423] 본 출원의 실시예는 네트워크 디바이스를 제공한다. 네트워크 디바이스는 전술한 방법 실시예에서 제1 네트워크 디바이스 또는 제2 네트워크 디바이스로서 제공될 수 있다. 네트워크 디바이스는 프로세서를 포함하고, 프로세서는 명령어를 실행하도록 구성되어, 네트워크 디바이스는 전술한 방법 실시예에 따른 패킷 처리 방법을 수행한다.

[0424] 예를 들어, 프로세서는 네트워크 프로세서(Network Processor, 줄여서 NP), 중앙 처리 장치(central processing unit, CPU), 주문형 집적 회로(application-specific integrated circuit, ASIC), 또는 본 출원의

솔루션에서 프로그램 실행을 제어하도록 구성된 집적 회로일 수 있다. 프로세서는 싱글 코어 프로세서(single-CPU)일 수 있거나, 멀티 코어 프로세서(multi-CPU)일 수 있다. 하나 이상의 프로세서가 있을 수 있다.

[0425] 일부 가능한 실시예에서, 네트워크 디바이스는 메모리를 더 포함할 수 있다.

[0426] 메모리는 판독 전용 메모리(read-only memory, ROM), 정적 정보 및 명령어를 저장할 수 있는 다른 유형의 정적 저장 디바이스, 랜덤 액세스 메모리(random access memory, RAM) 또는 정보와 명령어를 저장할 수 있는 다른 유형의 동적 저장 디바이스일 수 있거나 또는 전기적으로 소거가능한 프로그램가능 판독 전용 메모리(electrically erasable programmable read-only memory, EEPROM), 컴팩트 디스크 판독 전용 메모리(compact disc read-only Memory, CD-ROM) 또는 다른 컴팩트 디스크 저장장치, 광학 디스크 저장장치(컴팩트 광학 디스크, 레이저 디스크, 광학 디스크, 디지털 다목적 디스크, 블루레이 디스크 등을 포함함), 자기 디스크 저장 매체 또는 다른 자기 저장 디바이스, 또는 명령어 또는 데이터 구조의 형태로 예상 프로그램 코드를 전달하거나 저장하는 데 사용할 수 있고 컴퓨터에 의해 액세스될 수 있는 임의의 다른 매체일 수 있다. 그러나, 메모리는 이에 제한되지 않는다.

[0427] 메모리와 프로세서는 별개로 배치될 수 있거나, 메모리와 프로세서가 함께 통합될 수 있다.

[0428] 일부 가능한 실시예에서, 네트워크 디바이스는 트랜시버를 더 포함할 수 있다.

[0429] 트랜시버는 다른 디바이스 또는 통신 네트워크와 통신하도록 구성된다. 네트워크 통신 방식은 이더넷, 무선 액세스 네트워크(RAN), 무선 근거리 통신 네트워크(wireless local area network, WLAN) 등일 수 있지만, 이에 제한되지 않는다.

[0430] 일부 가능한 실시예에서, 네트워크 디바이스의 네트워크 프로세서는 전술한 방법 실시예의 단계를 수행할 수 있다. 예를 들어, 네트워크 디바이스는 라우터, 스위치 또는 방화벽일 수 있거나, 확실히 패킷 포워딩 기능을 지원하는 다른 네트워크 디바이스일 수 있다.

[0431] 도 21은 본 출원의 실시예에 따른 네트워크 디바이스(1300)의 구조의 개략도이다. 네트워크 디바이스(1300)는 제1 네트워크 디바이스 또는 제2 네트워크 디바이스로서 구성될 수 있다. 네트워크 디바이스(1300)는 도 1의 시스템 아키텍처 실시예에서 임의의 노드일 수 있으며, 예를 들어, CE1, PE1, PE2, P1, P2, P3, P4, PE3, PE4 또는 CE2일 수 있다.

[0432] 네트워크 디바이스(1300)는 메인 제어 보드(1310), 인터페이스 보드(1330), 전환 보드(1320) 및 인터페이스 보드(1340)를 포함한다. 메인 제어 보드(1310)는 시스템 관리, 디바이스 유지보수, 프로토콜 처리와 같은 기능을 완료하도록 구성된다. 전환 보드(1320)는 인터페이스 보드(인터페이스 보드는 라인 카드 또는 서비스 보드라고도 함) 간의 데이터 교환을 완료하도록 구성된다. 인터페이스 보드(1330) 및 인터페이스 보드(1340)는 다양한 서비스 인터페이스(예컨대, 이더넷 인터페이스 및 POS 인터페이스)를 제공하고, 데이터 패킷 포워딩을 구현하도록 구성된다. 메인 제어 보드(1310), 인터페이스 보드(1330), 인터페이스 보드(1340) 및 전환 보드(1320)는 시스템 버스를 통해 시스템 백보드에 연결되어 상호연동을 구현한다. 인터페이스 보드(1330)의 중앙 처리 장치(1331)는 인터페이스 보드를 제어 및 관리하고, 메인 제어 보드(1310) 상의 중앙 처리 장치(1311)와 통신하도록 구성된다.

[0433] 네트워크 디바이스(1300)가 제1 네트워크 디바이스로서 구성된 경우, 물리적 인터페이스 카드(1333)는 패킷을 수신하고 패킷을 네트워크 프로세서(1332)로 전송하며, 네트워크 프로세서(1332)는 기본 경로에 결함이 있다고 결정하고 패킷의 보호 플래그가 패킷이 기본 경로에서 제1 보호 경로로 전환되도록 허용되지 않음을 나타낸다고 결정한다. 이 경우, 네트워크 프로세서(1332)는 패킷을 폐기한다.

[0434] 일 실시예에서, 네트워크 프로세서(1332)는 SID에 대응하는 아웃바운드 인터페이스 또는 다음 홉을 결정하기 위해 패킷의 SID에 기초하여 포워딩 엔트리 메모리(1334)에 쿼리한다. 아웃바운드 인터페이스 또는 다음 홉에 결함이 있는 경우, 네트워크 프로세서(1332)는 기본 경로에 결함이 있다고 결정한다.

[0435] 일 실시예에서, 네트워크 프로세서(1332)가 보호 플래그가 패킷이 중간점 TI-LFA 경로로 전환되도록 허용되지만, TI-LFA FRR 경로로 전환되도록 허용되지 않음을 표시한다고 결정하면, 네트워크 프로세서는 링크 계층 캡슐화가 완료된 후 아웃바운드 인터페이스와 같은 정보를 기반으로 물리적 인터페이스 카드(1333)로부터 패킷을 전송하여 패킷이 중간점 TI-LFA 경로를 통해 전송된다.

[0436] 일 실시예에서, 네트워크 프로세서(1332)가 보호 플래그가 패킷이 TI-LFA FRR 경로의 전환되도록 허용되지만 중간점 TI-LFA 경로로 전환되도록 허용되지 않음을 표시한다고 결정하면, 네트워크 프로세서는 링크 계층 캡슐화

가 완료된 후 아웃바운드 인터페이스와 같은 정보를 기반으로 물리적 인터페이스 카드(1333)로부터 패킷을 전송하여 패킷이 TI-LFA FRR 경로를 통해 전송된다.

[0437] 네트워크 디바이스(1300)가 제2 네트워크 디바이스로서 구성된 경우, 네트워크 프로세서(1332)는 패킷을 생성하고, 링크 계층 캡슐화가 완료된 후 아웃바운드 인터페이스와 같은 정보를 기반으로 물리적 인터페이스 카드(1333)로부터 패킷을 전송하여 패킷이 제1 네트워크 디바이스로 전송된다.

[0438] 일 실시예에서, 네트워크 프로세서(1332)는 패킷 손실이 기본 경로 상의 트래픽에서 발생한다고 결정하고, 기본 경로를 제2 보호 경로로 전환한다.

[0439] 인터페이스 보드(1340)에 대한 동작은 본 출원의 이 실시예에서 인터페이스 보드(1330)에 대한 동작과 일치한다는 것을 이해해야 한다. 간결함을 위해, 세부사항은 다시 설명되지 않는다. 이 실시예의 네트워크 디바이스(1300)는 전술한 방법 실시예의 제1 네트워크 디바이스 또는 제2 네트워크 디바이스에 대응할 수 있음을 이해해야 한다. 네트워크 디바이스(1300)의 메인 제어 보드(1310), 인터페이스 보드(1330) 및/또는 인터페이스 보드(1340)는 전술한 방법 실시예의 제1 네트워크 디바이스 또는 제2 네트워크 디바이스에 의해 구현된 기능 및/또는 단계를 구현할 수 있다. 간결함을 위해, 세부사항은 본 명세서에서 다시 설명되지 않는다.

[0440] 메인 제어 보드가 복수 개인 경우, 복수의 메인 제어 보드는 기본 메인 제어 보드 및 보조 메인 제어 보드를 포함할 수 있음에 유의해야 한다. 하나 이상의 인터페이스 보드가 있을 수 있으며, 더 강력한 데이터 처리 능력을 가진 네트워크 디바이스는 더 많은 인터페이스 보드를 제공한다. 인터페이스 보드에는 하나 이상의 물리적 인터페이스 카드도 있을 수 있다. 전환 보드가 없거나 하나 이상의 전환 보드가 있을 수 있다. 전환 보드가 복수 개 있는 경우, 로드 밸런싱과 리던던시 백업이 함께 구현될 수 있다. 중앙 집중식 포워딩 아키텍처에서, 네트워크 디바이스는 전환 보드가 필요하지 않을 수 있으며, 인터페이스 보드는 전체 시스템에서 서비스 데이터를 처리하는 기능을 제공한다. 분산 포워딩 아키텍처에서, 네트워크 디바이스는 적어도 하나의 전환 보드를 가질 수 있으며, 복수의 인터페이스 보드 간의 데이터 교환은 전환 보드를 사용하여 구현되어 대용량 데이터 교환 및 처리 능력을 제공한다. 따라서, 분산 아키텍처에서 네트워크 디바이스의 데이터 액세스 및 처리 능력은 중앙 집중식 아키텍처의 디바이스의 데이터 액세스 및 처리 능력보다 우수하다. 선택적으로, 네트워크 디바이스는 이와 달리 단 하나의 카드가 있는 형태일 수 있다. 구체적으로, 전환 보드가 없고, 인터페이스 보드 및 메인 제어 보드의 기능이 카드에 집적되어 있다. 이 경우, 인터페이스 보드 상의 중앙 처리 장치와 메인 제어 보드 상의 중앙 처리 장치를 결합하여 카드 상에 하나의 중앙 처리 장치를 형성하여, 두 개의 중앙 처리 장치를 결합하여 얻은 기능을 수행할 수 있다. 이러한 형태의 디바이스(예컨대, 저가형 스위치 또는 라우터와 같은 네트워크 디바이스)는 비교적 약한 데이터 교환 및 처리 능력을 가지고 있다. 사용될 특정 아키텍처는 특정 네트워킹 배치 시나리오에 의존한다. 이것은 본 명세서에서 제한되지 않는다.

[0441] 도 22는 본 출원의 실시예에 따른 네트워크 디바이스(1300)에서 인터페이스 보드(1330)의 구조의 개략도이다. 인터페이스 보드(1330)는 물리적 인터페이스 카드(physical interface card, PIC)(2630), 네트워크 프로세서(network processor, NP)(2610) 및 트래픽 관리(traffic management) 모듈(2620)을 포함할 수 있다.

[0442] 물리적 인터페이스 카드(physical interface card, PIC)는 물리적 계층 상호연결 기능을 구현하도록 구성된다. 원래의 트래픽은 PIC를 통해 네트워크 디바이스의 인터페이스 보드로 들어가고, 처리된 패킷은 PIC로부터 전송된다.

[0443] 네트워크 프로세서(NP)(2610)는 패킷 포워딩 처리를 구현하도록 구성된다. 구체적으로, 업스트림 패킷 처리는 패킷 인그레스 인터페이스 처리, 및 포워딩 테이블 검색(예를 들어, 전술한 실시예에서 제1 포워딩 테이블 또는 제2 포워딩 테이블의 관련 콘텐츠)을 포함하고; 다운스트림 패킷 처리는 포워딩 테이블 검색(예를 들어, 전술한 실시예에서 제1 포워딩 테이블 또는 제2 포워딩 테이블의 관련 콘텐츠) 등을 포함한다.

[0444] 트래픽 관리(TM)(2620)는 QoS, 회선 속도 포워딩, 대용량 버퍼링 및 큐 관리와 같은 기능을 구현하도록 구성된다. 특히, 업스트림 트래픽 관리는 업스트림 QoS 처리(예컨대, 혼잡 관리 및 큐 스케줄링) 및 슬라이스 처리를 포함하고, 다운스트림 트래픽 관리는 패킷 어셈블리 처리, 멀티캐스트 복제 및 다운스트림 QoS 처리(예컨대, 혼잡 관리 및 큐 스케줄링)를 포함한다.

[0445] 네트워크 디바이스가 복수의 인터페이스 보드(Y30)를 포함하는 경우, 복수의 인터페이스 보드(Y30)는 전환 네트워크(2640)를 통해 서로 통신할 수 있음을 이해할 수 있다.

[0446] 도 22는 NP 내부의 처리 절차 또는 모듈의 예만을 보여준다는 점에 유의해야 한다. 특정 구현 동안 모듈의 처리 순서는 이에 제한되지 않는다. 또한, 실제 적용 동안, 필요에 따라 다른 모듈이나 처리 절차가 배포될 수 있다.

이것은 본 출원의 실시예들에서 제한되지 않는다.

[0447] 일부 가능한 실시예에서, 네트워크 디바이스는 이와 달리 범용 프로세서에 의해 구현될 수 있다. 예를 들어, 범용 프로세서는 칩 형태일 수 있다. 구체적으로, 네트워크 디바이스를 구현하는 범용 프로세서는 처리 회로, 내부적으로 연결되어 처리 회로와 통신하는 인바운드 인터페이스 및 아웃바운드 인터페이스를 포함한다. 처리 회로는 인바운드 인터페이스를 통해 전술한 방법 실시예의 패킷 생성 단계를 수행하도록 구성된다. 처리 회로는 인바운드 인터페이스를 통해 전술한 방법 실시예의 수신 단계를 수행하도록 구성된다. 처리 회로는 아웃바운드 인터페이스를 통해 전술한 방법 실시예의 전송 단계를 수행하도록 구성된다. 선택적으로, 범용 프로세서는 저장 매체를 더 포함할 수 있다. 처리 회로는 저장 매체를 통해 전술한 방법 실시예의 저장 단계를 수행하도록 구성된다. 저장 매체는 처리 회로에 의해 실행되는 명령어를 저장할 수 있다. 처리 회로는 전술한 방법 실시예를 수행하기 위해 저장 매체에 저장된 명령어를 실행하도록 구성된다.

[0448] 가능한 제품 형태에서, 본 출원의 이 실시예의 네트워크 디바이스는 이와 달리 다음을 사용하여 구현될 수 있다: 하나 이상의 필드 프로그램가능 게이트 어레이(영문 전체 이름: field programmable gate array, 줄여서 FPGA), 프로그램가능 로직 디바이스(영문 전체 이름: programmable logic device, 줄여서 PLD), 제어기, 상태 머신, 게이트 로직, 개별 하드웨어 구성요소, 기타 적절한 회로 또는 본 출원에 설명된 다양한 기능을 실행할 수 있는 회로의 임의의 조합.

[0449] 일부 가능한 실시예에서, 네트워크 디바이스는 이와 달리 컴퓨터 프로그램 제품을 사용하여 구현될 수 있다. 구체적으로, 본 출원의 실시예는 컴퓨터 프로그램 제품을 제공한다. 컴퓨터 프로그램 제품이 네트워크 디바이스에서 실행될 때, 네트워크 디바이스는 전술한 방법 실시예에서 패킷 처리 방법을 수행할 수 있다.

[0450] 전술한 제품 형태의 네트워크 디바이스는 전술한 방법 실시예에서 네트워크 디바이스의 임의의 기능을 별개로 갖는다는 것을 이해해야 한다. 세부사항은 여기에서 설명하지 않는다.

[0451] 당업자는 본 명세서에 개시된 실시예에 설명된 예와 결합하여 방법 단계 및 유닛이 전자 하드웨어, 컴퓨터 소프트웨어 또는 이들의 조합에 의해 구현될 수 있음을 알 수 있다. 하드웨어와 소프트웨어 간의 호환성을 명확하게 설명하기 위해, 전술한 내용은 기능에 따른 각 실시예의 단계 및 구성을 일반적으로 설명하였다. 기능이 하드웨어에 의해 수행되는지 또는 소프트웨어에 의해 수행되는지는 기술 솔루션의 특정 애플리케이션 및 설계 제약에 의존한다. 당업자는 각각의 특정 애플리케이션에 대해 설명된 기능을 구현하기 위해 상이한 방법을 사용할 수 있지만, 구현이 본 출원의 범위를 벗어나는 것으로 간주되어서는 안 된다.

[0452] 편리하고 간략한 설명을 위해, 앞서 설명한 시스템, 장치 및 유닛의 상세한 작업 과정에 대해서는 전술한 방법 실시예의 해당 과정을 참조하는 것이 당업자에 의해 명확하게 이해될 수 있다. 세부사항은 여기에서 다시 설명되지 않는다.

[0453] 본 출원에 제공된 여러 실시예에서, 개시된 시스템, 장치 및 방법은 다른 방식으로 구현될 수 있음을 이해해야 한다. 예를 들어, 설명된 장치 실시예는 예일 뿐이다. 예를 들어, 유닛으로의 분할은 단지 논리적 기능 분할이며 실제 구현에서 또 다른 분할이 될 수 있다. 예를 들어, 복수의 유닛 또는 구성요소가 다른 시스템에 결합되거나 통합될 수 있거나, 일부 특징은 무시되거나 수행되지 않을 수 있다. 또한, 표시되거나 논의된 상호 결합 또는 직접 결합 또는 통신 연결은 몇몇 인터페이스를 통해 구현될 수 있다. 장치 또는 유닛 사이의 간접 결합 또는 통신 연결은 전자, 기계 또는 다른 형태로 구현될 수 있다.

[0454] 별개의 부분으로 설명된 유닛은 물리적으로 분리되거나 분리되지 않을 수 있으며, 유닛으로 표시된 부분은 물리적 유닛일 수도 있고 아닐 수도 있고, 즉, 한 위치에 있거나 복수의 네트워크 유닛에 분산될 수 있다. 유닛의 일부 또는 전부는 본 출원의 실시예의 솔루션의 목적을 달성하기 위한 실제 요구사항에 따라 선택될 수 있다.

[0455] 또한, 본 출원의 실시예에서 기능 유닛은 하나의 처리 유닛으로 통합될 수 있고, 각각의 유닛은 물리적으로 단독으로 존재할 수 있거나, 또는 둘 이상의 유닛이 하나의 유닛으로 통합될 수 있다. 통합 유닛은 하드웨어의 형태로 구현될 수도 있고, 소프트웨어 기능 유닛의 형태로 구현될 수도 있다.

[0456] 통합 유닛이 소프트웨어 기능 유닛의 형태로 구현되어 독립적인 제품으로 판매되거나 사용되는 경우, 통합 유닛은 컴퓨터 판독가능 저장 매체에 저장될 수 있다. 이러한 이해를 바탕으로, 본 출원의 기술 솔루션은 본질적으로, 또는 기존 기술에 기여하는 부분, 또는 기술 솔루션의 전부 또는 일부는 소프트웨어 제품의 형태로 구현될 수 있다. 컴퓨터 소프트웨어 제품은 저장 매체에 저장되며 컴퓨터 디바이스(개인용 컴퓨터, 서버, 네트워크 디바이스 등이 될 수 있음)가 본 출원의 실시예에 설명된 방법의 단계의 전체 또는 일부를 수행하도록 표시하기 위한 여러 명령어를 포함한다. 저장 매체는 USB 플래시 드라이브, 탈착가능 하드 디스크, 판독 전용 메모리

(read-only memory, ROM), 랜덤 액세스 메모리(random access memory, RAM), 자기 디스크 또는 광학 디스크와 같은 프로그램 코드를 저장할 수 있는 임의의 매체를 포함한다.

[0457] 전술한 설명은 본 출원의 특정 구현일 뿐이며, 본 출원의 보호 범위를 제한하려는 의도는 아니다. 본 출원에 개시된 기술적 범위 내에서 당업자에 의해 용이하게 파악된 균등한 수정 또는 대체는 본 출원의 보호 범위에 속한다. 따라서, 본 출원의 보호 범위는 청구범위의 보호 범위에 따라야 한다.

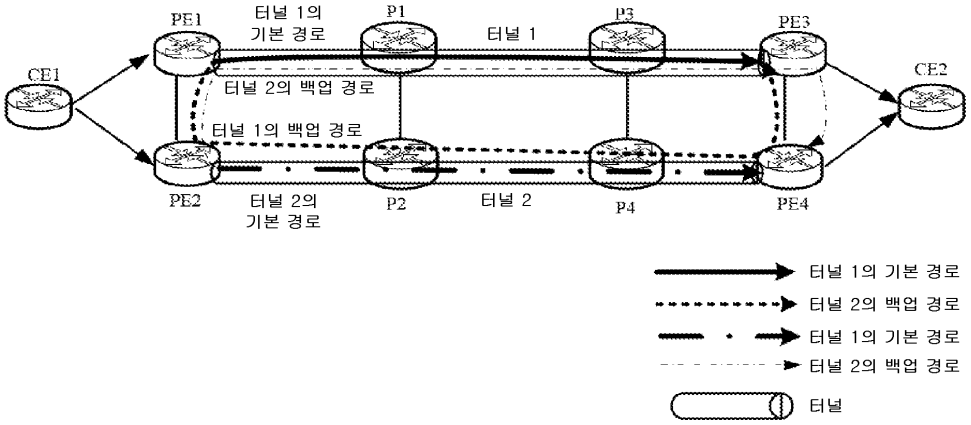
[0458] 실시예의 전부 또는 일부는 소프트웨어, 하드웨어, 펌웨어, 또는 이들의 임의의 조합을 사용해서 구현될 수 있다. 소프트웨어가 실시예를 구현하는 데 사용되는 경우, 실시예의 전부 또는 일부는 컴퓨터 프로그램 제품의 형태로 구현될 수 있다. 컴퓨터 프로그램 제품은 하나 이상의 컴퓨터 프로그램 명령어를 포함한다. 컴퓨터 프로그램 명령어가 컴퓨터에 로딩되어 실행되는 경우, 본 출원의 실시예에 따른 절차 또는 기능의 전부 또는 일부가 생성된다. 컴퓨터는 범용 컴퓨터, 전용 컴퓨터, 컴퓨터 네트워크, 또는 다른 프로그램가능 장치일 수 있다. 컴퓨터 명령어는 컴퓨터 판독가능 저장 매체에 저장될 수 있거나 또는 컴퓨터 판독가능 저장 매체에서 다른 컴퓨터 판독가능 저장 매체로 전송될 수 있다. 예컨대, 컴퓨터 프로그램 명령어는 웹사이트, 컴퓨터, 서버, 또는 데이터 센터로부터 다른 웹사이트, 컴퓨터, 서버, 또는 데이터 센터로 유선 또는 무선 방식으로 전송될 수 있다. 컴퓨터 판독가능 저장 매체는 컴퓨터가 액세스할 수 있는 임의의 사용 가능한 매체, 또는 하나 이상의 사용 가능한 매체를 통합하는 서버 또는 데이터 센터와 같은 데이터 저장 디바이스일 수 있다. 사용 가능한 매체는 자기 매체(예컨대, 플로피 디스크, 하드 디스크 또는 자기 테이프), 광학 매체(예를 들어, 디지털 비디오 디스크(digital video disc, DVD)), 반도체 매체(예를 들어, 고체 상태 드라이브)일 수 있다.

[0459] 당업자는 실시예의 단계의 전부 또는 일부가 하드웨어 또는 관련 하드웨어에 지시하는 프로그램에 의해 구현될 수 있음을 이해할 수 있다. 프로그램은 컴퓨터 판독가능 저장 매체에 저장될 수 있다. 저장 매체는 판독 전용 메모리, 자기 디스크, 광학 디스크 등일 수 있다.

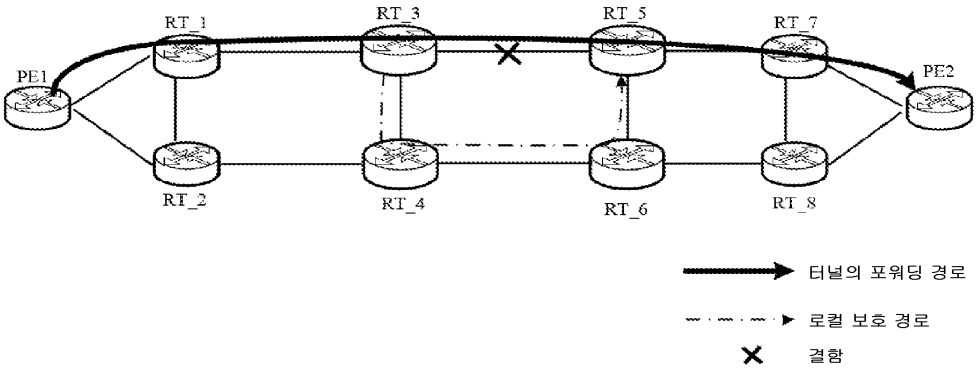
[0460] 전술한 설명은 단지 본 출원의 선택적인 실시예일 뿐, 본 출원을 제한하려는 것은 아니다. 본 출원의 사상과 원칙을 벗어나지 않고 이루어진 임의의 수정, 균등한 교체 또는 개선은 본 출원의 보호 범위에 속한다.

도면

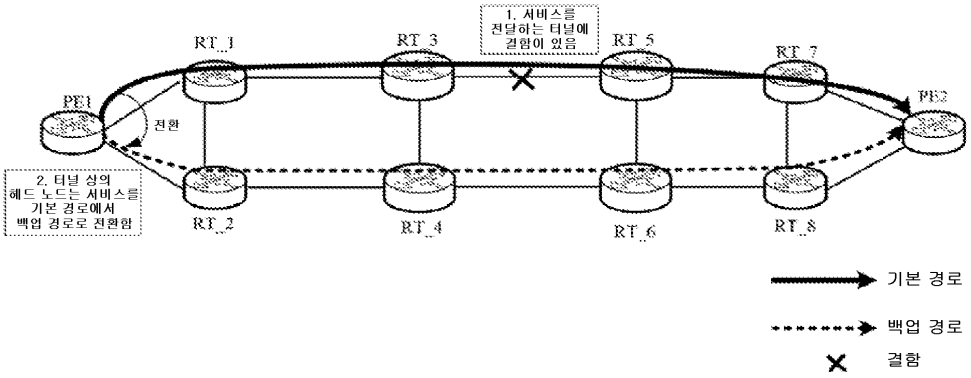
도면1



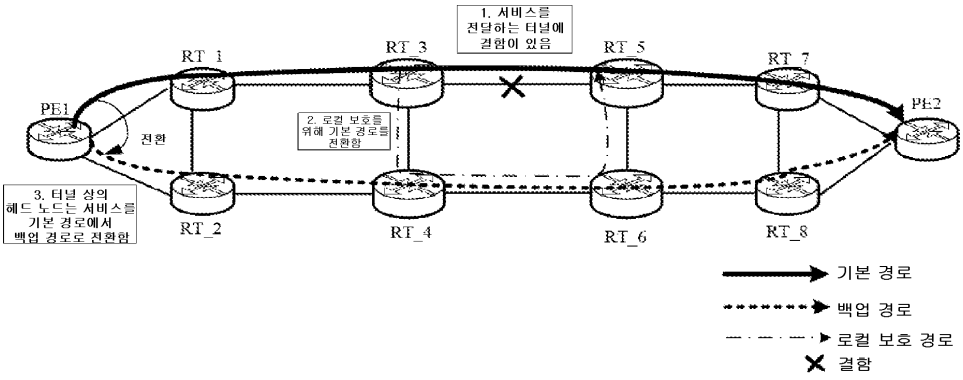
도면2


RT_1
RT_3
RT_5
RT_7
PE1
PE2
RT_2
RT_4
RT_6
RT_8
터널의 포워딩 경로
로컬 보호 경로
결함

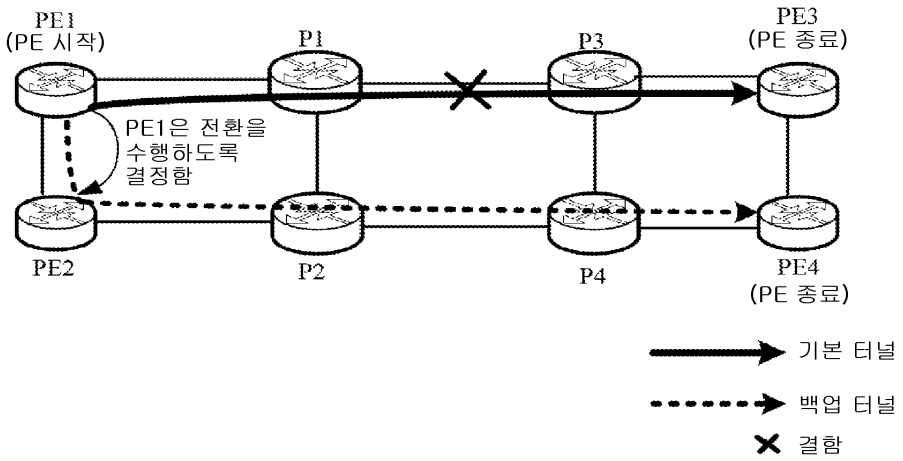
도면3


1. 서비스를 전달하는 터널에 결함이 있음
RT_1
RT_3
RT_5
RT_7
PE1
전환
PE2
2. 터널 상의 헤드 노드는 서비스를 기본 경로에서 백업 경로로 전환함
RT_2
RT_4
RT_6
RT_8
기본 경로
백업 경로
결함

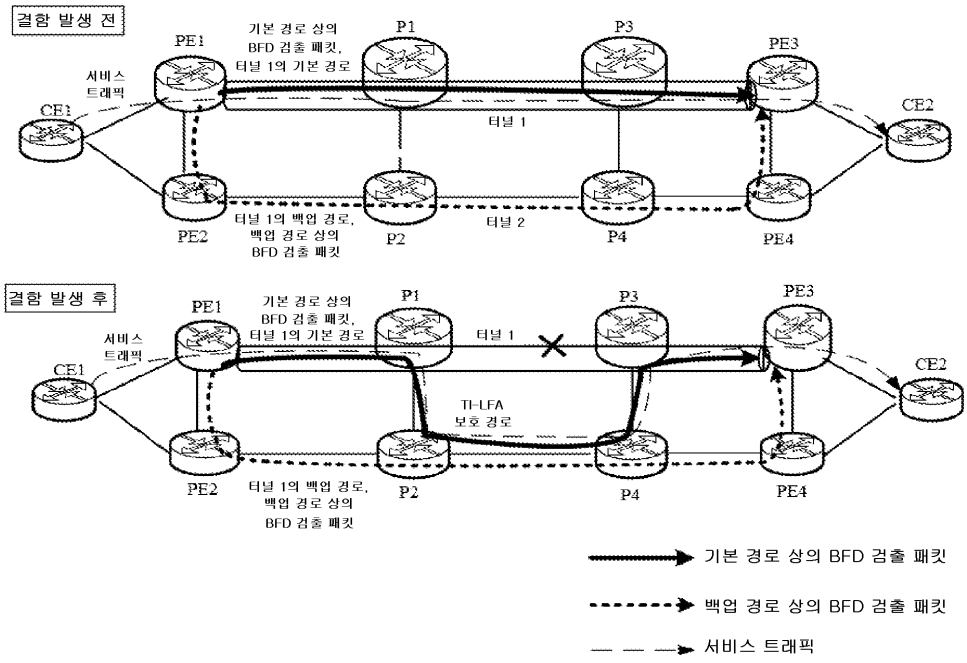
도면4


1. 서비스를 전달하는 터널에 결함이 있음
RT_1
RT_3
RT_5
RT_7
PE1
전환
2. 로컬 보호를 위해 기본 경로를 전환함
PE2
3. 터널 상의 헤드 노드는 서비스를 기본 경로에서 백업 경로로 전환함
RT_2
RT_4
RT_6
RT_8
기본 경로
백업 경로
로컬 보호 경로
결함

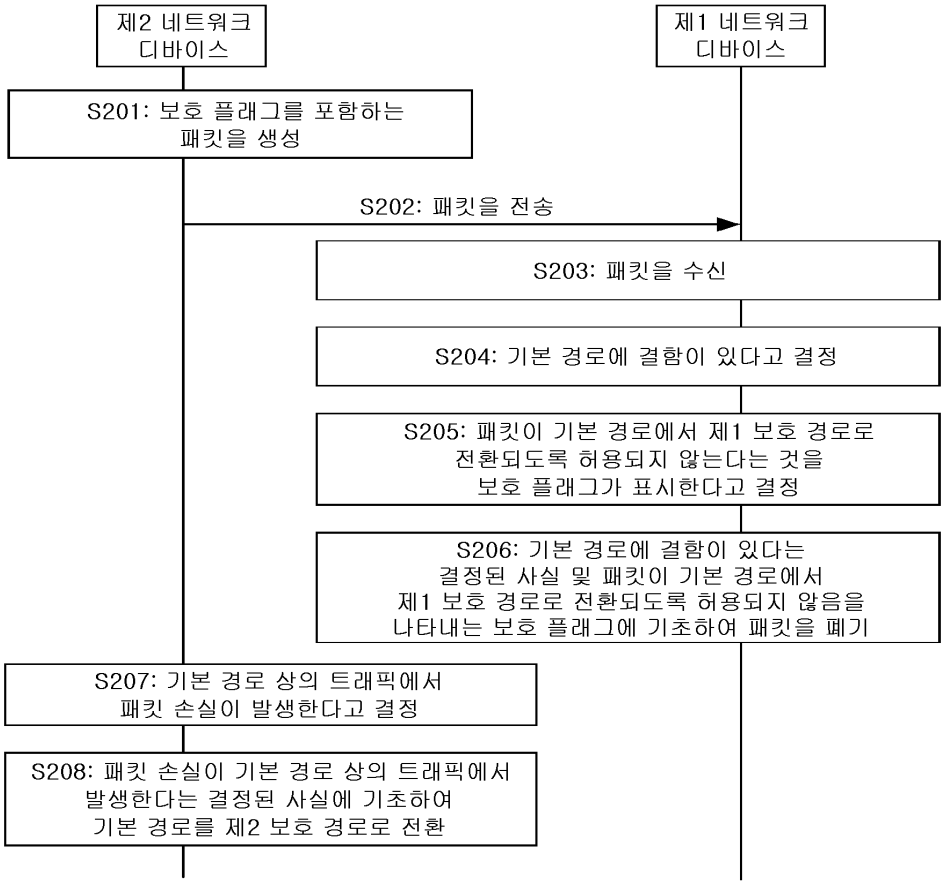
도면5


PE1
(PE 시작)
P1
P3
PE3
(PE 종료)
PE1은 전환을
수행하도록
결정함
PE2
P2
P4
PE4
(PE 종료)
기본 터널
백업 터널
결함

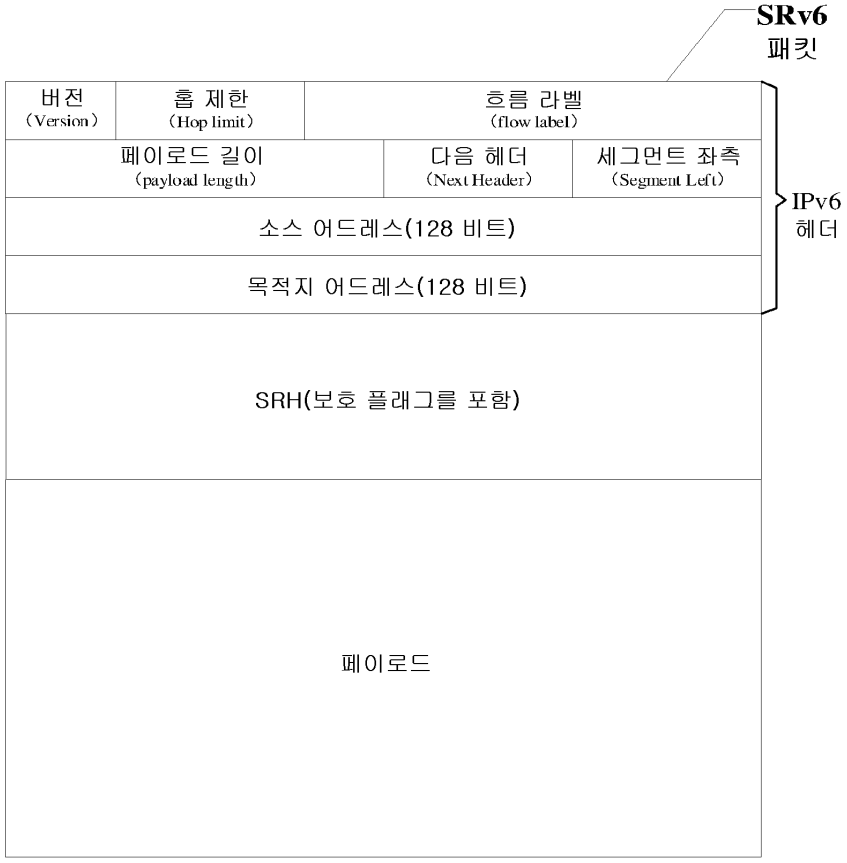
도면6


결함 발생 전
PE1
기본 경로 상의
BFD 검출 패킷,
터널 1의 기본 경로
P1
P3
PE3
서비스
트래픽
CE1
CE2
터널 1
PE2
터널 1의 백업 경로,
백업 경로 상의
BFD 검출 패킷
P2
터널 2
P4
PE4
결함 발생 후
PE1
기본 경로 상의
BFD 검출 패킷,
터널 1의 기본 경로
P1
터널 1
P3
PE3
서비스
트래픽
CE1
CE2
TI-LFA
보호 경로
PE2
터널 1의 백업 경로,
백업 경로 상의
BFD 검출 패킷
P2
P4
PE4
기본 경로 상의 BFD 검출 패킷
백업 경로 상의 BFD 검출 패킷
서비스 트래픽

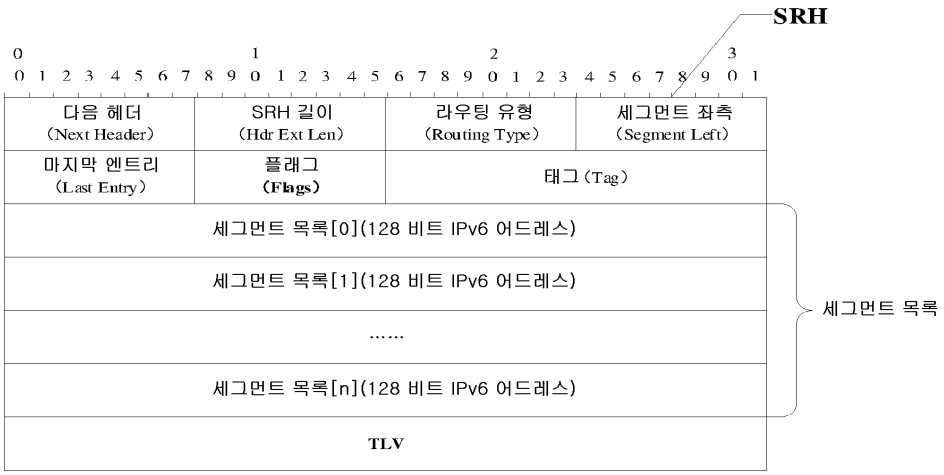
도면7


제2 네트워크 디바이스
제1 네트워크 디바이스
S201: 보호 플래그를 포함하는 패킷을 생성
S202: 패킷을 전송
S203: 패킷을 수신
S204: 기본 경로에 결함이 있다고 결정
S205: 패킷이 기본 경로에서 제1 보호 경로로 전환되도록 허용되지 않는다는 것을 보호 플래그가 표시한다고 결정
S206: 기본 경로에 결함이 있다는 결정된 사실 및 패킷이 기본 경로에서 제1 보호 경로로 전환되도록 허용되지 않음을 나타내는 보호 플래그에 기초하여 패킷을 폐기
S207: 기본 경로 상의 트래픽에서 패킷 손실이 발생한다고 결정
S208: 패킷 손실이 기본 경로 상의 트래픽에서 발생한다는 결정된 사실에 기초하여 기본 경로를 제2 보호 경로로 전환

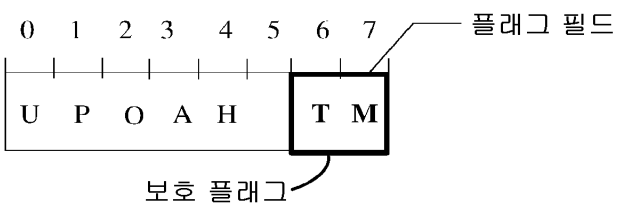
도면8


SRv6
패킷
버전
(Version)
홉 제한
(Hop limit)
흐름 라벨
(flow label)
페이로드 길이
(payload length)
다음 헤더
(Next Header)
세그먼트 좌측
(Segment Left)
소스 어드레스(128 비트)
목적지 어드레스(128 비트)
IPv6
헤더
SRH(보호 플래그를 포함)
페이로드

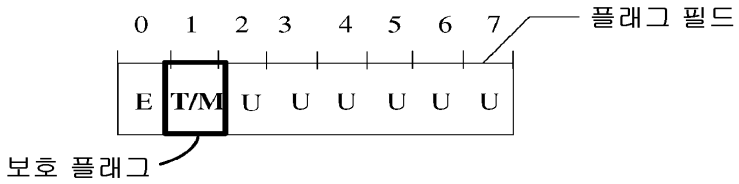
도면9


SRH
0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
다음 헤더
(Next Header)
SRH 길이
(Hdr Ext Len)
라우팅 유형
(Routing Type)
세그먼트 좌측
(Segment Left)
마지막 엔트리
(Last Entry)
플래그
(Flags)
태그(Tag)
세그먼트 목록[0](128 비트 IPv6 어드레스)
세그먼트 목록[1](128 비트 IPv6 어드레스)
.....
세그먼트 목록[n](128 비트 IPv6 어드레스)
세그먼트 목록
TLV

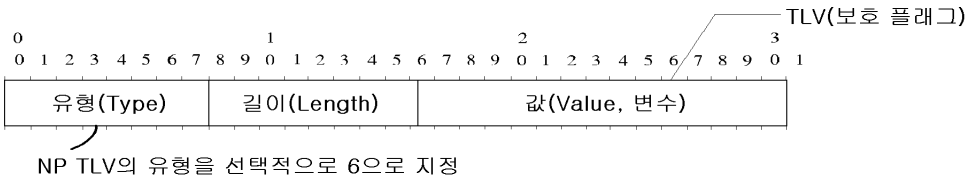
도면10


0 1 2 3 4 5 6 7
플래그 필드
U P O A H T M
보호 플래그

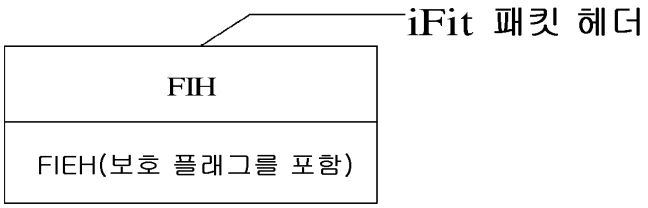
도면11



도면12

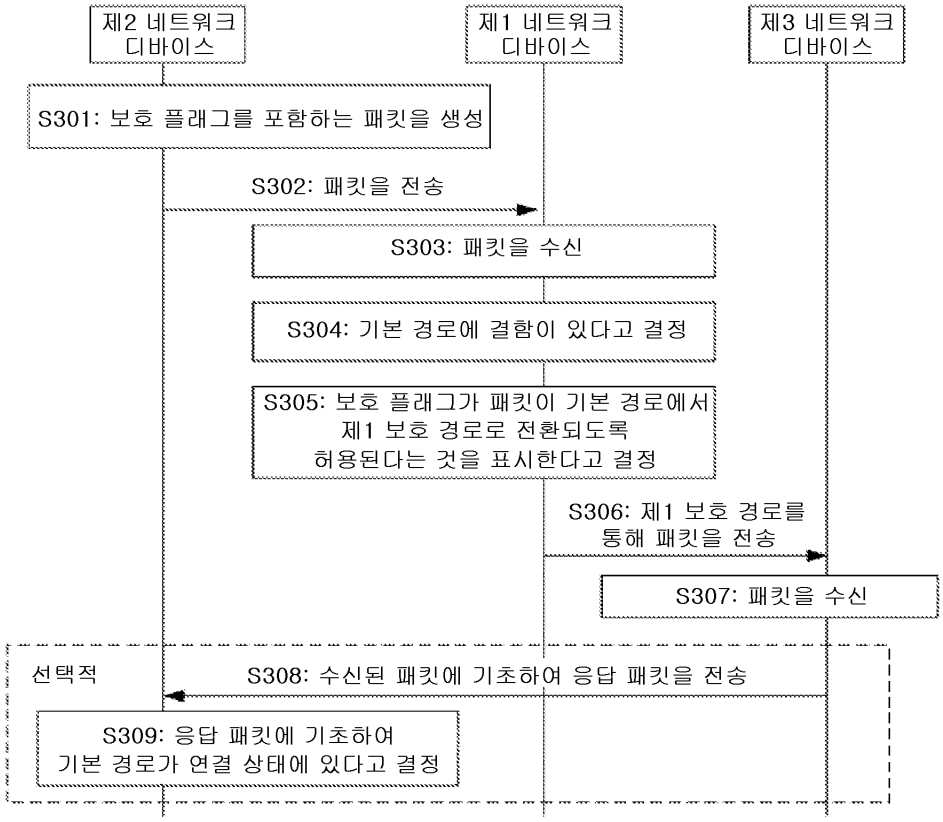


도면13

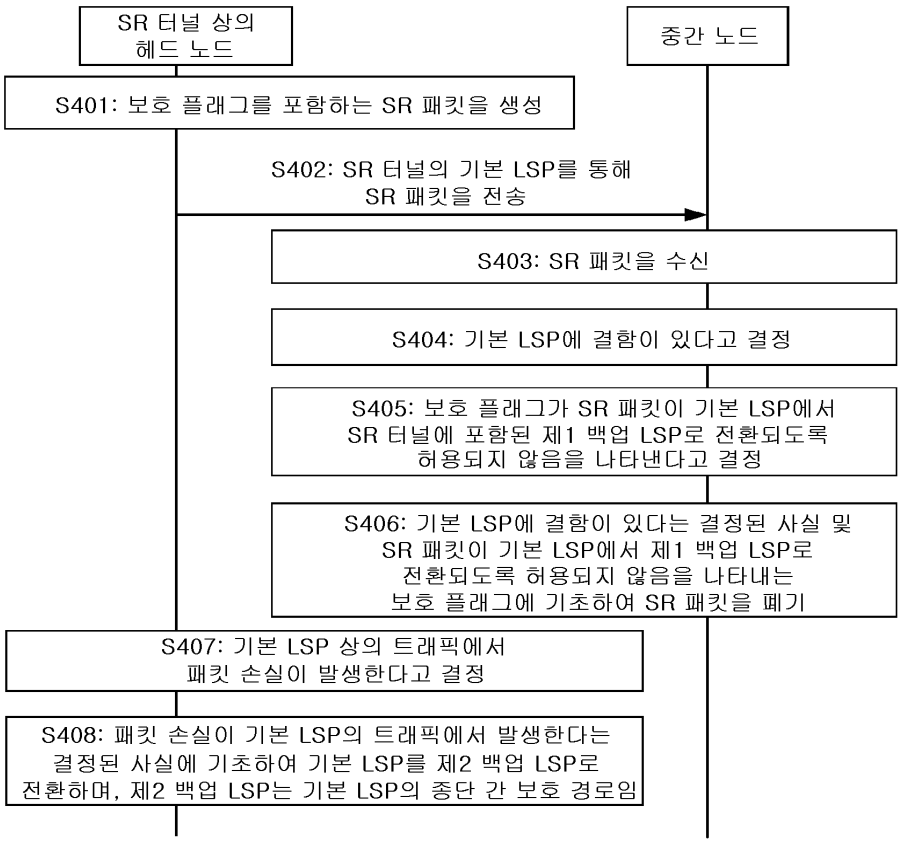


도면14

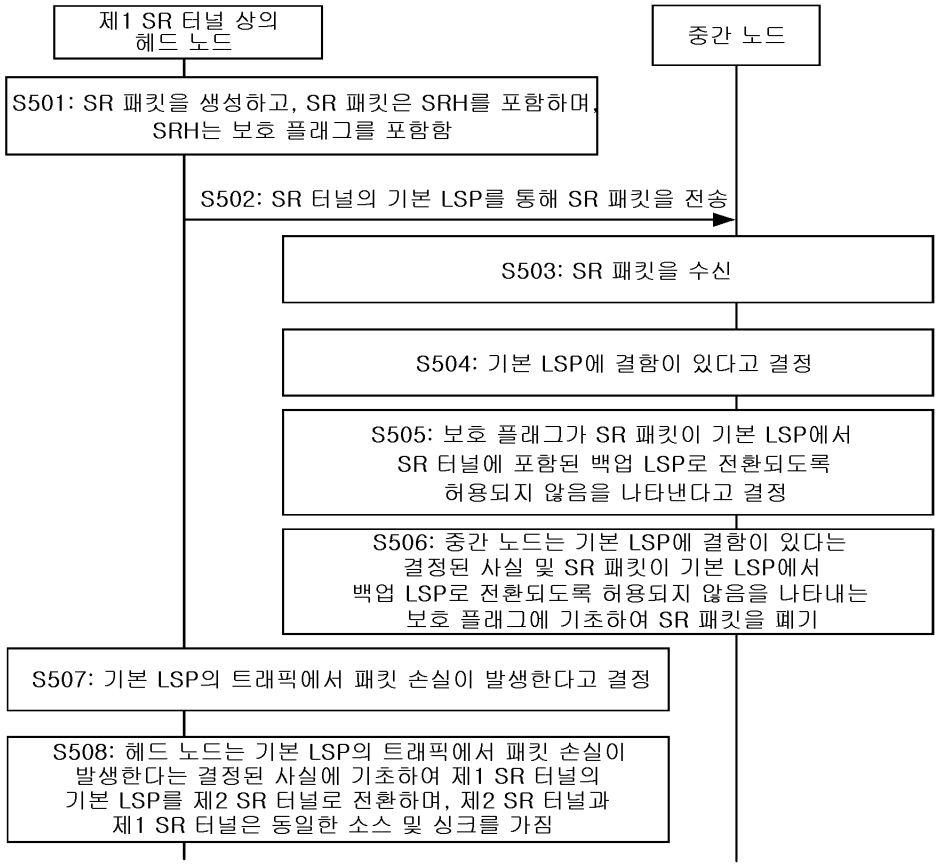
도면15


제2 네트워크 디바이스
제1 네트워크 디바이스
제3 네트워크 디바이스
S301: 보호 플래그를 포함하는 패킷을 생성
S302: 패킷을 전송
S303: 패킷을 수신
S304: 기본 경로에 결함이 있다고 결정
S305: 보호 플래그가 패킷이 기본 경로에서 제1 보호 경로로 전환되도록 허용된다는 것을 표시한다고 결정
S306: 제1 보호 경로를 통해 패킷을 전송
S307: 패킷을 수신
선택적
S308: 수신된 패킷에 기초하여 응답 패킷을 전송
S309: 응답 패킷에 기초하여 기본 경로가 연결 상태에 있다고 결정

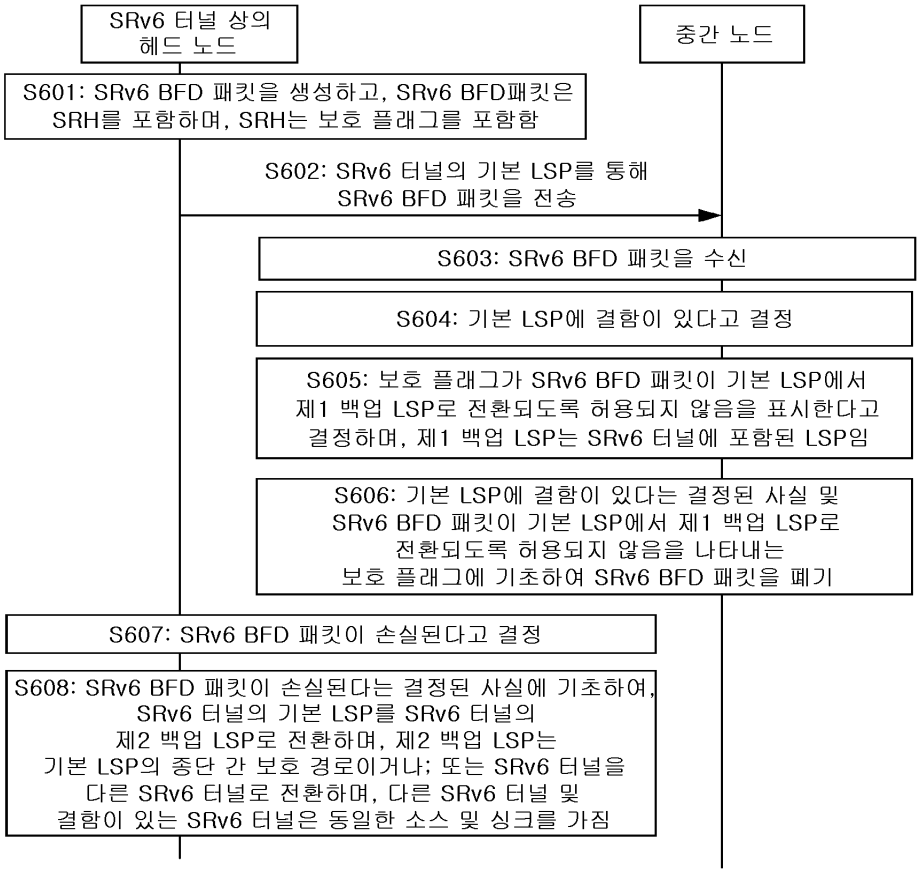
도면16


SR 터널 상의 헤드 노드
중간 노드
S401: 보호 플래그를 포함하는 SR 패킷을 생성
S402: SR 터널의 기본 LSP를 통해 SR 패킷을 전송
S403: SR 패킷을 수신
S404: 기본 LSP에 결함이 있다고 결정
S405: 보호 플래그가 SR 패킷이 기본 LSP에서 SR 터널에 포함된 제1 백업 LSP로 전환되도록 허용되지 않음을 나타낸다고 결정
S406: 기본 LSP에 결함이 있다는 결정된 사실 및 SR 패킷이 기본 LSP에서 제1 백업 LSP로 전환되도록 허용되지 않음을 나타내는 보호 플래그에 기초하여 SR 패킷을 폐기
S407: 기본 LSP 상의 트래픽에서 패킷 손실이 발생한다고 결정
S408: 패킷 손실이 기본 LSP의 트래픽에서 발생한다는 결정된 사실에 기초하여 기본 LSP를 제2 백업 LSP로 전환하며, 제2 백업 LSP는 기본 LSP의 종단 간 보호 경로임

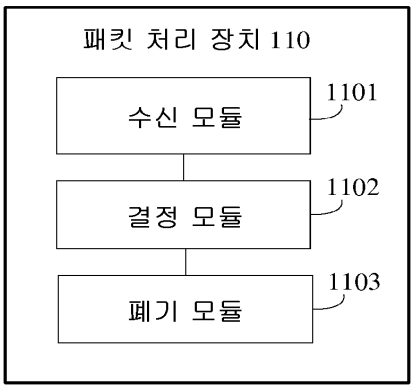
도면17


제1 SR 터널 상의
헤드 노드
중간 노드
S501: SR 패킷을 생성하고, SR 패킷은 SRH를 포함하며,
SRH는 보호 플래그를 포함함
S502: SR 터널의 기본 LSP를 통해 SR 패킷을 전송
S503: SR 패킷을 수신
S504: 기본 LSP에 결함이 있다고 결정
S505: 보호 플래그가 SR 패킷이 기본 LSP에서
SR 터널에 포함된 백업 LSP로 전환되도록
허용되지 않음을 나타낸다고 결정
S506: 중간 노드는 기본 LSP에 결함이 있다는
결정된 사실 및 SR 패킷이 기본 LSP에서
백업 LSP로 전환되도록 허용되지 않음을 나타내는
보호 플래그에 기초하여 SR 패킷을 폐기
S507: 기본 LSP의 트래픽에서 패킷 손실이 발생한다고 결정
S508: 헤드 노드는 기본 LSP의 트래픽에서 패킷 손실이
발생한다는 결정된 사실에 기초하여 제1 SR 터널의
기본 LSP를 제2 SR 터널로 전환하며, 제2 SR 터널과
제1 SR 터널은 동일한 소스 및 싱크를 가짐

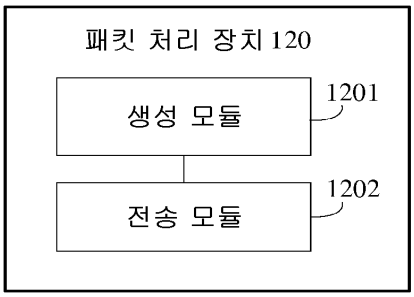
도면18



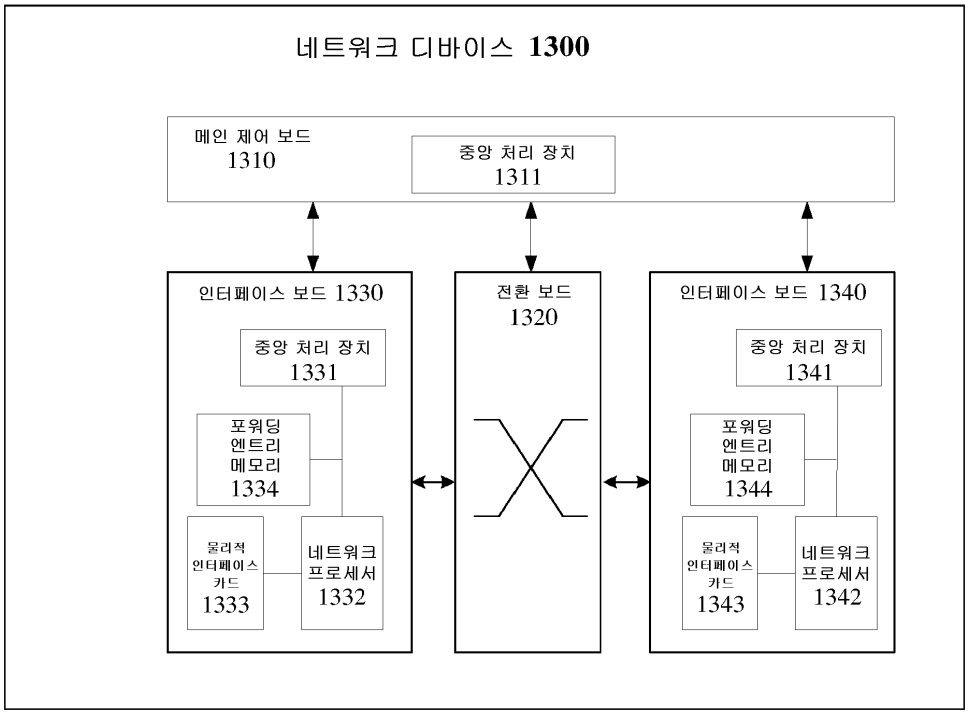
도면19



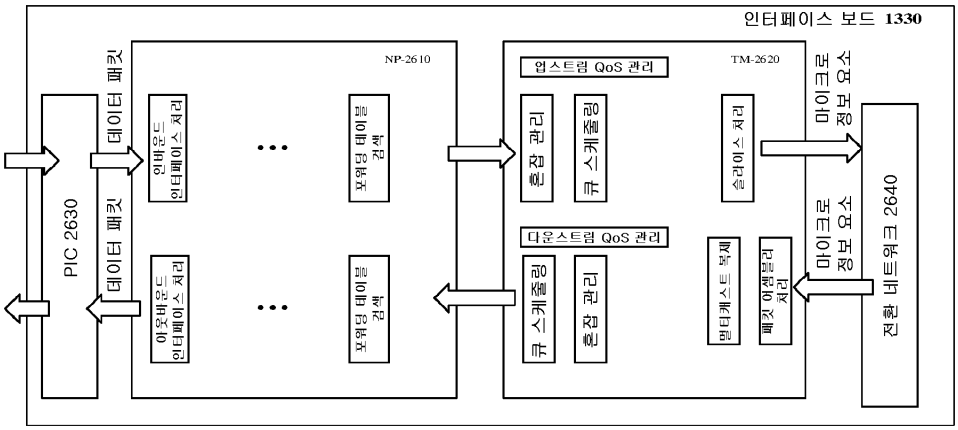
도면20



도면21


네트워크 디바이스 1300
메인 제어 보드
1310
중앙 처리 장치
1311
인터페이스 보드 1330
중앙 처리 장치
1331
포워딩
엔트리
메모리
1334
물리적
인터페이스
카드
1333
네트워크
프로세서
1332
전환 보드
1320
인터페이스 보드 1340
중앙 처리 장치
1341
포워딩
엔트리
메모리
1344
물리적
인터페이스
카드
1343
네트워크
프로세서
1342

도면22


인터페이스 보드 1330
NP-2610
TM-2620
PIC 2630
데이터 패킷
데이터 패킷
인바운드
인터페이스 처리
아웃바운드
인터페이스 처리
포워딩 데이블
검색
포워딩 데이블
검색
업스트림 QoS 관리
혼잡 관리
큐 스케줄링
다운스트림 QoS 관리
큐 스케줄링
혼잡 관리
슬라이스 처리
멀티캐스트 복제
패킷 어셈블리
처리
마이크로
정보 요소
마이크로
정보 요소
전환 네트워크 2640