



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2024-0131626
(43) 공개일자 2024년09월02일

(51) 국제특허분류(Int. Cl.)
H04L 45/7453 (2022.01) H04L 49/112 (2022.01)
(52) CPC특허분류
H04L 45/7453 (2022.05)
H04L 49/112 (2022.05)
(21) 출원번호 10-2023-0024892
(22) 출원일자 2023년02월24일
심사청구일자 2023년02월24일

(71) 출원인
이화여자대학교 산학협력단
서울특별시 서대문구 이화여대길 52 (대현동, 이화여자대학교)
(72) 발명자
양대현
서울특별시 서초구 서초중앙로 200, 17동 901호
장룡호
인천광역시 미추홀구 인하로 100, 1008호
(74) 대리인
한상수

전체 청구항 수 : 총 14 항

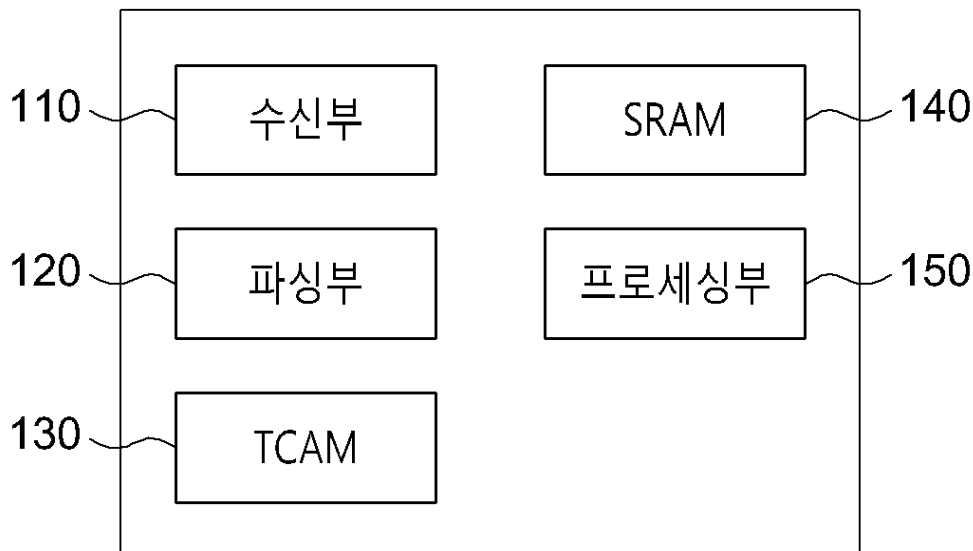
(54) 발명의 명칭 데이터 플레인에서 해시테이블 기반으로 패킷을 매칭하는 네트워크 스위치 및 이의 패킷 매칭 방법

(57) 요약

본 발명의 일실시예에 따른 데이터 플레인에서 해시테이블 기반으로 패킷을 매칭하는 네트워크 스위치는, 네트워크 스위치에서 패킷을 수신하는 수신부; 상기 패킷의 헤더를 파싱하여 소스(source) IP, 목적지(destination) IP, 프로토콜(protocol), 소스 포트(source port), 목적지 포트(destination port)를 추출하는 파싱부; 상기 패 (뒷면에 계속)

대표도 - 도1

100



킷의 매칭 규칙(matching rule)들이 저장되어 있고 상기 패킷의 소스 IP, 목적지 IP, 프로토콜에 대응하는 제1매칭 값들이 저장되어 있는 TCAM(Ternary Content Addressable Memory); 상기 패킷의 포트 범위 매칭을 위한 해시 테이블을 포함하고, 상기 TCAM을 이용한 매칭이 이루어지는 경우 상기 해시테이블을 이용하여 상기 패킷의 소스 포트 및 목적지 포트의 범위에 매칭되는 제2매칭 값들의 엔트리들이 저장되어 있는 SRAM(Static Random Access Memory); 및 상기 TCAM을 이용한 제1매칭과 상기 SRAM을 이용한 제2매칭을 수행하고, 상기 제2매칭의 수행 간에 매칭이 이루어지는 경우 상기 패킷을 드랍하고, 상기 제1매칭 또는 제2매칭의 수행 간에 매칭이 이루어지지 않는 경우 라우팅 테이블 또는 ACL(Access Control List)을 이용하여 상기 패킷을 라우팅하는 프로세싱부를 포함할 수 있다.

(72) 발명자

정창훈

인천광역시 서구 비즈니스로 165, 603동 2103호

김시안

서울특별시 양천구 목동중앙북로16길 28, 201호

이 발명을 지원한 국가연구개발사업

과제고유번호	1711166713
과제번호	2016K1A1A2912757
부처명	과학기술정보통신부
과제관리(전문)기관명	한국연구재단
연구사업명	집단연구지원
연구과제명	빅데이터 기반의 DDoS공격의 분석, 모델링, 방어 기술 연구
기 여 율	1/2
과제수행기관명	이화여자대학교
연구기간	2022.03.01 ~ 2022.06.30

이 발명을 지원한 국가연구개발사업

과제고유번호	1711166443
과제번호	2020R1A2C2009372
부처명	과학기술정보통신부
과제관리(전문)기관명	한국연구재단
연구사업명	개인기초연구(과기정통부)
연구과제명	스케치 기반의 실시간 플로우별 네트워크 트래픽 측정 및 모니터링 시스템
기 여 율	1/2
과제수행기관명	이화여자대학교
연구기간	2022.03.01 ~ 2023.02.28

명세서

청구범위

청구항 1

네트워크 스위치에서 패킷을 수신하는 수신부;

상기 패킷의 헤더를 파싱하여 소스(source) IP, 목적지(destination) IP, 프로토콜(protocol), 소스 포트(source port), 목적지 포트(destination port)를 추출하는 파싱부;

상기 패킷의 매칭 규칙(matching rule)들이 저장되어 있고 상기 패킷의 소스 IP, 목적지 IP, 프로토콜에 대응하는 제1매칭 값들이 저장되어 있는 TCAM(Ternary Content Addressable Memory);

상기 패킷의 포트 범위 매칭을 위한 해시테이블을 포함하고, 상기 TCAM을 이용한 매칭이 이루어지는 경우 상기 해시테이블을 이용하여 상기 패킷의 소스 포트 및 목적지 포트의 범위에 매칭되는 제2매칭 값들의 엔트리들이 저장되어 있는 SRAM(Static Random Access Memory); 및

상기 TCAM을 이용한 제1매칭과 상기 SRAM을 이용한 제2매칭을 수행하고, 상기 제2매칭의 수행 간에 매칭이 이루어지는 경우 상기 패킷을 드랍하고, 상기 제1매칭 또는 제2매칭의 수행 간에 매칭이 이루어지지 않는 경우 라우팅 테이블 또는 ACL(Access Control List)을 이용하여 상기 패킷을 라우팅하는 프로세싱부를 포함하는, 네트워크 스위치.

청구항 2

제1항에 있어서,

상기 해시테이블은 패킷의 포트의 번호에 해당하는 위치의 엔트리가 1로 사전 설정되어 있으며,

상기 프로세싱부는, 상기 SRAM에서 해시 함수를 이용하여 상기 소스 포트 및 목적지 포트를 해시한 후, 상기 소스 포트 및 목적지 포트의 번호에 기초하여 상기 해시테이블의 해당하는 엔트리 위치를 확인하여 그 엔트리가 1로 설정된 경우 매칭된 것으로 인식하여 상기 제2매칭을 수행하는 것을 특징으로 하는, 네트워크 스위치.

청구항 3

제1항에 있어서,

상기 해시테이블은 레지스터(register)로 구현된 어레이(array)이고, 상기 어레이의 각 엔트리는 2^n 비트(bit)를 구비하고 상기 n은 정수로서 상기 네트워크 스위치의 모델에 따라 정의되며,

상기 프로세싱부는, 상기 SRAM에서 해시 함수를 이용하여 상기 소스 포트 및 목적지 포트의 번호를 2^n 으로 나눈 몫을 이용하여 해시하고 상기 몫에 해당하는 위치의 엔트리 값과 상기 소스 및 목적지의 포트의 번호를 2^n 으로 나눈 나머지 값에 해당하는 비트맵(bitmap) 값을 AND 연산하여 매칭함으로서 상기 제2매칭을 수행하고,

상기 프로세싱부는, 상기 몫에 해당하는 위치의 엔트리 값과 상기 나머지 값에 해당하는 비트맵 값을 AND 연산한 결과 값이 1인 경우 상기 패킷을 드랍하는 것을 특징으로 하는, 네트워크 스위치.

청구항 4

제1항에 있어서,

상기 SRAM은 미리정해진 패킷의 포트 범위를 반전시키는 반전 플래그(Reverse Flag)를 포함하여 상기 반전된 포트 범위에 해당하는 각 엔트리의 모든 비트맵을 1로 설정하도록 이루어지고,

상기 프로세싱부는, 상기 SRAM에서 해시 함수를 이용하여 상기 소스 포트 및 목적지 포트를 해시한 후, 상기 반전 플래그를 이용하여 상기 소스 포트 및 목적지 포트의 번호에 대응하는 각 엔트리의 비트맵이 1로 설정된 경우 매칭된 것으로 인식하여 상기 제2매칭을 수행하는 것을 특징으로 하는, 네트워크 스위치.

청구항 5

제1항에 있어서,

상기 해시테이블은 소스 포트 애니(Src Port ANY), 목적지 포트 애니(Dst Port ANY), 노 애니(No ANY) 중 하나의 구성으로 이루어진 하나 이상의 해시테이블을 포함하고,

상기 프로세싱부는,

(a)상기 해시테이블이 소스 포트 애니 구성을 구비하는 경우에는 상기 목적지 포트만을 해시하여 상기 해시테이블 상의 엔트리의 위치를 찾아 상기 제2매칭을 수행하고,

(b)상기 해시테이블이 목적지 포트 애니 구성을 구비하는 경우에는, 상기 소스 포트만을 해시하여 상기 해시테이블 상의 엔트리의 위치를 찾아 상기 제2매칭을 수행하고,

(c)상기 해시테이블이 노 애니의 구성을 구비하는 경우에는, 상기 소스 포트 및 목적지 포트 모두를 해시하여 상기 해시테이블 상의 엔트리의 위치를 찾아 상기 제2매칭을 수행하는 것을 특징으로 하는, 네트워크 스위치.

청구항 6

제1항에 있어서,

상기 파싱부는, 상기 네트워크 스위치에서 수신한 복수의 패킷이 복수의 상이한 IP, 및 프로토콜에 대하여 동일한 포트 범위를 가지는 경우에, 상기 복수의 패킷에 동일한 값의 포트 범위 ID를 부여하고,

상기 프로세싱부는, 상기 복수의 패킷의 소스 포트 및 목적지 포트를 해시할 때 파라미터로 상기 동일한 포트 범위 ID를 이용하여 상기 해시테이블의 동일한 엔트리와 매칭하여 제2매칭을 수행하는 것을 특징으로 하는, 네트워크 스위치.

청구항 7

제4항 및 제6항에 있어서,

상기 SRAM은 복수의 패킷에 대응하는 SRAM 해시테이블을 위한 복수의 반전 플래그, 복수의 포트 범위 ID가 저장되어 있으며, 상기 복수의 포트 범위 ID는 각 포트 범위 ID에 따라 해당하는 엔트리의 비트맵이 설정되어 있는 것을 특징으로 하는, 네트워크 스위치.

청구항 8

네트워크 스위치에서 패킷을 수신하는 수신 단계;

상기 패킷의 헤더를 파싱하여 소스(source) IP, 목적지(destination) IP, 프로토콜(protocol), 소스 포트(source port), 목적지 포트(destination port)를 추출하는 추출 단계;

상기 패킷의 매칭 규칙(matching rule)들이 저장된 TCAM(Ternary Content Addressable Memory)을 이용하여 상기 소스 IP, 목적지 IP, 프로토콜을 매칭하는 제1매칭 단계;

상기 제1매칭 단계에서 매칭이 이루어지는 경우, 포트 범위 매칭을 위한 해시테이블을 포함하는 SRAM(Static Random Access Memory)에서 상기 해시테이블을 이용하여 상기 소스 포트 및 목적지 포트의 범위를 매칭하는 제2매칭 단계;

상기 제2매칭 단계에서 매칭이 이루어지는 경우, 상기 패킷을 드랍하는 드랍 단계; 및

상기 제1매칭 단계 또는 제2매칭 단계에서 매칭이 이루어지지 않는 경우, 라우팅 테이블 또는 ACL(Access Control List)을 이용하여 상기 패킷을 라우팅하는 라우팅 단계를 포함하는, 네트워크 스위치의 데이터 플레인에서의 패킷 매칭 방법.

청구항 9

제8항에 있어서,

상기 해시테이블은 패킷의 포트의 번호에 해당하는 위치의 엔트리가 1로 사전 설정되어 있으며,

상기 제2매칭 단계는, 상기 SRAM에서 해시 함수를 이용하여 상기 소스 포트 및 목적지 포트를 해시한 후, 상기 소스 포트 및 목적지 포트의 번호에 기초하여 상기 해시테이블의 해당하는 엔트리 위치를 확인하여 그 엔트리가 1로 설정된 경우 매칭된 것으로 인식하는 단계를 포함하는 것을 특징으로 하는, 네트워크 스위치의 데이터 플레인에서의 패킷 매칭 방법.

청구항 10

제8항에 있어서,

상기 해시테이블은 레지스터(register)로 구현된 어레이(array)이고, 상기 어레이의 각 엔트리는 2^n 비트(bit)를 구비하고 상기 n은 정수로서 상기 네트워크 스위치의 모델에 따라 정의되며,

상기 제2매칭 단계는, 상기 SRAM에서 해시 함수를 이용하여 상기 소스 포트 및 목적지 포트의 번호를 2^n 으로 나눈 몫을 이용하여 해시하고 상기 몫에 해당하는 위치의 엔트리 값과 상기 소스 및 목적지의 포트의 번호를 2^n 으로 나눈 나머지 값에 해당하는 비트맵(bitmap) 값을 AND 연산하여 매칭하는 단계를 포함하고,

상기 드랍 단계는, 상기 몫에 해당하는 위치의 엔트리 값과 상기 나머지 값에 해당하는 비트맵 값을 AND 연산한 결과 값이 1인 경우 상기 패킷을 드랍하는 단계를 포함하는 것을 특징으로 하는, 네트워크 스위치의 데이터 플레인에서의 패킷 매칭 방법.

청구항 11

제8항에 있어서,

상기 SRAM은 미리정해진 패킷의 포트 범위를 반전시키는 반전 플래그(Reverse Flag)를 포함하여 상기 반전된 포트 범위에 해당하는 각 엔트리의 모든 비트맵을 1로 설정하도록 이루어지고,

상기 제2매칭 단계는, 상기 SRAM에서 해시 함수를 이용하여 상기 소스 포트 및 목적지 포트를 해시한 후, 상기 반전 플래그를 이용하여 상기 소스 포트 및 목적지 포트의 번호에 대응하는 각 엔트리의 비트맵이 1로 설정된 경우 매칭된 것으로 인식하는 단계를 포함하는 것을 특징으로 하는, 네트워크 스위치의 데이터 플레인에서의 패킷 매칭 방법.

청구항 12

제8항에 있어서,

상기 해시테이블은 소스 포트 애니(Src Port ANY), 목적지 포트 애니(Dst Port ANY), 노 애니(No ANY) 중 하나의 구성으로 이루어진 하나 이상의 해시테이블을 포함하고,

상기 제2매칭 단계에서,

(a)상기 해시테이블이 소스 포트 애니 구성을 구비하는 경우에는 상기 목적지 포트만을 해시하여 상기 해시테이

블 상의 엔트리의 위치를 찾아 매칭을 수행하고,

(b)상기 해시테이블이 목적지 포트 애니 구성을 구비하는 경우에는, 상기 소스 포트만을 해시하여 상기 해시테이블 상의 엔트리의 위치를 찾아 매칭을 수행하고,

(c)상기 해시테이블이 노 애니의 구성을 구비하는 경우에는, 상기 소스 포트 및 목적지 포트 모두를 해시하여 상기 해시테이블 상의 엔트리의 위치를 찾아 매칭을 수행하는 것을 특징으로 하는, 네트워크 스위치의 데이터 플레인에서의 패킷 매칭 방법.

청구항 13

제8항에 있어서,

상기 네트워크 스위치에서 수신한 복수의 패킷이 복수의 상이한 IP, 및 프로토콜에 대하여 동일한 포트 범위를 가지는 경우에, 상기 복수의 패킷에 동일한 값의 포트 범위 ID를 부여하고,

상기 제2매칭 단계는, 상기 복수의 패킷의 소스 포트 및 목적지 포트를 해시할 때 파라미터로 상기 동일한 포트 범위 ID를 이용하여 상기 해시테이블의 동일한 엔트리와 매칭하는 단계를 포함하는 것을 특징으로 하는, 네트워크 스위치의 데이터 플레인에서의 패킷 매칭 방법.

청구항 14

제13항에 있어서,

상기 SRAM은 복수의 패킷에 대응하는 SRAM 해시테이블을 위한 복수의 반전 플래그, 복수의 포트 범위 ID가 저장되어 있으며, 상기 복수의 포트 범위 ID 는 각 포트 범위 ID에 따라 해당하는 엔트리의 비트맵이 설정되어 있는 것을 특징으로 하는, 네트워크 스위치의 데이터 플레인에서의 패킷 매칭 방법.

발명의 설명

기술 분야

[0001] 본 발명은 통신 패킷을 라우팅 또는 드랍하는 네트워크 스위치에 관한 것으로, 더욱 상세하게는 패킷의 5-튜플(tuple) 기반 규칙에 의해 처리되는 라우팅 또는 드랍을 실행하는 네트워크 스위치 데이터 플레인(data plane)의 매칭 프로세스에서 보다 경제적이면서 뛰어난 보안 성능을 만족하는 네트워크 스위치의 데이터 플레인에서의 패킷 매칭 방법 및 이를 수행하는 네트워크 스위치에 관한 것이다.

배경 기술

[0003] 네트워크 스위치의 주요 기능은 TCAM(Ternary Content Addressable Memory)에 존재하는 라우팅 테이블 또는 ACL(Access Control List)을 이용하여 패킷(packet)을 라우팅하거나 드랍하는 것이다. 라우팅 또는 드랍은 패킷의 5-튜플(5-tuple) 기반의 규칙(Rule)에 의해서 처리되며, 5-튜플은 소스(source) IP, 목적지(destination) IP, 프로토콜(protocol), 소스 포트(source port), 목적지 포트(destination port)를 의미한다.

[0004] 예를 들어, [1.1.1.1, 2.2.2.2, TCP, 80, 443] 패킷이 스위치에 도착하면, 라우팅 테이블 또는 ACL에 해당하는 규칙이 등록되어 있는지 검색을 하고, 매칭되는 규칙이 있다면 이에 따라 라우팅되거나 드랍된다. 라우팅 테이블과 ACL의 규칙은 일반적으로 네트워크 관리자에 의해 사전에 셋팅된다.

[0005] ACL을 이용한 패킷 드랍은 네트워크 스위치의 보안 측면에서 중요한 기능이며, 최근 DDoS/DoS 공격이 빈번하게 발생함에 따라, ACL의 중요성도 점점 더 높아지고 있다. 종래와 같이 ACL 매칭에 TCAM을 사용하는 경우 SRAM에 비해 매우 빠른 검색시간을 보장하는 대신에 비용측면에서 비싸고 적은 용량을 가지고 있다는 문제점이 있다. 따라서, ACL이 TCAM을 사용할 경우 라우팅 테이블과 TCAM을 공유하기 때문에, TCAM에서 ACL로 사용할 수 있는 메모리의 양은 제한적이다. 특히 포트 범위를 매칭할 때, 포트 범위는 프리픽스 규칙(Prefix Rule)로 변환(확장)되고, 이로 인해 메모리 사용 측면에서 많은 부담이 있다. 예를 들어, 패킷의 Port 번호가 1023 ~

65535인 패킷들을 드랍하기 위하여 ACL에 규칙을 등록한다고 하면, 6개의 TCAM 엔트리(PrefixRule: 000001*, 00001*, 0001*, 001*, 01*, 1*)가 필요하기 때문이다.

[0006] 결과적으로 네트워크 공격이 발생하여 많은 수의 악성 패킷을 드랍해야 할 때, ACL이 사용하고 있는 TCAM 메모리의 양이 제한적이면, 보안적으로 큰 문제가 발생할 수 있다. 따라서, 최근 보안적 이슈가 중요시 되면서, TCAM 내부에서 ACL로 사용되는 용량을 어떻게 최소화할지가 네트워크 스위치 분야에서 중요한 문제로 대두되고 있다.

[0007] 이를 해결하려면 고가의 TCAM을 더 사용하거나, 필요한 매칭 규칙의 개수는 그대로이지만 요구되는 TCAM 메모리의 양을 효과적으로 줄일 수 있는 기술이 필요하다.

선행기술문헌

특허문헌

[0009] (특허문헌 0001) 미국 등록특허공보 제10511532호

발명의 내용

해결하려는 과제

[0010] 상기와 같은 문제점을 해결하기 위한 본 발명의 목적은, 네트워크 스위치의 데이터 플레인에서 라우팅 또는 드랍시 데이터 처리 속도의 개선과 TCAM의 확장성(scalability)을 증가시키고 네트워크 스위치 데이터 플레인(data plane)의 매칭 프로세스에서 보다 경제적이면서 뛰어난 보안 성능을 만족시키는 네트워크 스위치의 데이터 플레인에서의 패킷 매칭 방법 및 이를 수행하는 네트워크 스위치를 제공하는 것이다.

[0011] 본 발명의 또다른 목적은, 네트워크 스위치의 데이터 플레인에서 라우팅 또는 드랍시 데이터 처리 속도의 개선과 TCAM의 확장성(scalability)을 증가시킬 뿐 아니라 SRAM의 확장성 또한 높일 수 있어 데이터 처리의 속도와 효율을 현저하게 개선할 수 있는 네트워크 스위치의 데이터 플레인에서의 패킷 매칭 방법 및 이를 수행하는 네트워크 스위치를 제공하는 것이다.

[0012] 본 발명이 이루고자 하는 기술적 과제는 이상에서 언급한 기술적 과제로 제한되지 않으며, 언급되지 않은 또 다른 기술적 과제들은 아래의 기재로부터 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0014] 상기 기술적 과제를 달성하기 위하여, 본 발명의 일실시예에 따른 데이터 플레인에서 해시테이블 기반으로 패킷을 매칭하는 네트워크 스위치는 네트워크 스위치에서 패킷을 수신하는 수신부; 상기 패킷의 헤더를 파싱하여 소스(source) IP, 목적지(destination) IP, 프로토콜(protocol), 소스 포트(source port), 목적지 포트(destination port)를 추출하는 파싱부; 상기 패킷의 매칭 규칙(matching rule)들이 저장되어 있고 상기 패킷의 소스 IP, 목적지 IP, 프로토콜에 대응하는 제1매칭 값들이 저장되어 있는 TCAM(Ternary Content Addressable Memory); 패킷의 포트 범위 매칭을 위한 해시테이블을 포함하고, 상기 TCAM을 이용한 매칭이 이루어지는 경우 상기 해시테이블을 이용하여 상기 패킷의 소스 포트 및 목적지 포트의 범위에 매칭되는 제2매칭 값들의 엔트리들이 저장되어 있는 SRAM(Static Random Access Memory); 및 상기 TCAM을 이용한 제1매칭과 상기 SRAM을 이용한 제2매칭을 수행하고, 상기 제2매칭의 수행간에 매칭이 이루어지는 경우 상기 패킷을 드랍하고, 상기 제1매칭 또는 제2매칭의 수행간에 매칭이 이루어지지 않는 경우 라우팅 테이블 또는 ACL(Access Control List)을 이용하여 상기 패킷을 라우팅하는 프로세싱부를 포함할 수 있다.

[0015] 본 발명의 실시예에 있어서, 상기 해시테이블은 패킷의 포트의 번호에 해당하는 위치의 엔트리가 1로 사전 설정되어 있으며, 상기 프로세싱부는, 상기 SRAM에서 해시 함수를 이용하여 상기 소스 포트 및 목적지 포트를 해시한 후, 상기 소스 포트 및 목적지 포트의 번호에 기초하여 상기 해시테이블의 해당하는 엔트리 위치를 확인하여

그 엔트리가 1로 설정된 경우 매칭된 것으로 인식하여 상기 제2매칭을 수행할 수 있다.

[0016] 본 발명의 실시예에 있어서, 상기 해시테이블은 레지스터(register)로 구현된 어레이(array)이고, 상기 어레이의 각 엔트리는 2^n 비트(bit)를 구비하고 상기 n은 정수로서 상기 네트워크 스위치의 모델에 따라 정의되며, 상기 프로세싱부는, 상기 SRAM에서 해시 함수를 이용하여 상기 소스 포트 및 목적지 포트의 번호를 2^n 으로 나눈 몫을 이용하여 해시하고 상기 몫에 해당하는 위치의 엔트리 값과 상기 소스 및 목적지의 포트의 번호를 2^n 으로 나눈 나머지 값에 해당하는 비트맵(bitmap) 값을 AND 연산하여 매칭함으로써 상기 제2매칭을 수행하고, 상기 프로세싱부는, 상기 몫에 해당하는 위치의 엔트리 값과 상기 나머지 값에 해당하는 비트맵 값을 AND 연산한 결과가 1인 경우 상기 패킷을 드랍할 수 있다.

[0017] 본 발명의 실시예에 있어서, 상기 SRAM은 미리정해진 패킷의 포트 범위를 반전시키는 반전 플래그(Reverse Flag)를 포함하여 상기 반전된 포트 범위에 해당하는 각 엔트리의 모든 비트맵을 1로 설정하도록 이루어지고, 상기 프로세싱부는, 상기 SRAM에서 해시 함수를 이용하여 상기 소스 포트 및 목적지 포트를 해시한 후, 상기 반전 플래그를 이용하여 상기 소스 포트 및 목적지 포트의 번호에 대응하는 각 엔트리의 비트맵이 1로 설정된 경우 매칭된 것으로 인식하여 상기 제2매칭을 수행할 수 있다.

[0018] 본 발명의 실시예에 있어서, 상기 해시테이블은 소스 포트 애니(Src Port ANY), 목적지 포트 애니(Dst Port ANY), 노 애니(No ANY) 중 하나의 구성으로 이루어진 하나 이상의 해시테이블을 포함하고, 상기 프로세싱부는, (a) 상기 해시테이블이 소스 포트 애니 구성을 구비하는 경우에는 상기 목적지 포트만을 해시하여 상기 해시테이블 상의 엔트리의 위치를 찾아 상기 제2매칭을 수행하고, (b) 상기 해시테이블이 목적지 포트 애니 구성을 구비하는 경우에는, 상기 소스 포트만을 해시하여 상기 해시테이블 상의 엔트리의 위치를 찾아 상기 제2매칭을 수행하고, (c) 상기 해시테이블이 노 애니의 구성을 구비하는 경우에는, 상기 소스 포트 및 목적지 포트 모두를 해시하여 상기 해시테이블 상의 엔트리의 위치를 찾아 상기 제2매칭을 수행할 수 있다.

[0019] 본 발명의 실시예에 있어서, 상기 과징부는, 상기 네트워크 스위치에서 수신한 복수의 패킷이 복수의 상이한 IP, 및 프로토콜에 대하여 동일한 포트 범위를 가지는 경우에, 상기 복수의 패킷에 동일한 값의 포트 범위 ID를 부여하고, 상기 프로세싱부는, 상기 복수의 패킷의 소스 포트 및 목적지 포트를 해시할 때 파라미터로 상기 동일한 포트 범위 ID를 이용하여 상기 해시테이블의 동일한 엔트리와 매칭하여 제2매칭을 수행할 수 있다.

[0020] 본 발명의 실시예에 있어서, 상기 SRAM은 복수의 패킷에 대응하는 SRAM 해시테이블을 위한 복수의 반전 플래그, 복수의 포트 범위 ID가 저장되어 있으며, 상기 복수의 포트 범위 ID는 각 포트 범위 ID에 따라 해당하는 엔트리의 비트맵이 설정되어 있다.

[0021] 본 발명의 일실시예에 따른 네트워크 스위치의 데이터 플레인에서의 패킷 매칭 방법은 네트워크 스위치에서 패킷을 수신하는 수신 단계; 상기 패킷의 헤더를 과징하여 소스(source) IP, 목적지(destination) IP, 프로토콜(protocol), 소스 포트(source port), 목적지 포트(destination port)를 추출하는 추출 단계; 상기 패킷의 매칭 규칙(matching rule)들이 저장된 TCAM(Ternary Content Addressable Memory)을 이용하여 상기 소스 IP, 목적지 IP, 프로토콜을 매칭하는 제1매칭 단계; 상기 제1매칭 단계에서 매칭이 이루어지는 경우, 포트 범위 매칭을 위한 해시테이블을 포함하는 SRAM(Static Random Access Memory)에서 상기 해시테이블을 이용하여 상기 소스 포트 및 목적지 포트의 범위를 매칭하는 제2 매칭 단계; 상기 제2매칭 단계에서 매칭이 이루어지는 경우, 상기 패킷을 드랍하는 드랍 단계; 및 상기 제1매칭 단계 또는 제2매칭 단계에서 매칭이 이루어지지 않는 경우, 라우팅 테이블 또는 ACL(Access Control List)을 이용하여 상기 패킷을 라우팅하는 라우팅 단계를 포함할 수 있다.

[0022] 본 발명의 실시예에 있어서, 상기 해시테이블은 패킷의 포트의 번호에 해당하는 위치의 엔트리가 1로 사전 설정되어 있으며, 상기 제2매칭 단계는, 상기 SRAM에서 해시 함수를 이용하여 상기 소스 포트 및 목적지 포트를 해시한 후, 상기 소스 포트 및 목적지 포트의 번호에 기초하여 상기 해시테이블의 해당하는 엔트리 위치를 확인하여 그 엔트리가 1로 설정된 경우 매칭된 것으로 인식하는 단계를 포함할 수 있다.

[0023] 본 발명의 실시예에 있어서, 상기 해시테이블은 레지스터(register)로 구현된 어레이(array)이고, 상기 어레이의 각 엔트리는 2^n 비트(bit)를 구비하고 상기 n은 정수로서 상기 네트워크 스위치의 모델에 따라 정의되며, 상기 제2매칭 단계는, 상기 SRAM에서 해시 함수를 이용하여 상기 소스 포트 및 목적지 포트의 번호를 2^n 으로 나눈 몫을 이용하여 해시하고 상기 몫에 해당하는 위치의 엔트리 값과 상기 소스 및 목적지의 포트의 번호를 2^n 으로 나눈 나머지 값에 해당하는 비트맵(bitmap) 값을 AND 연산하여 매칭하는 단계를 포함하고, 상기 드랍 단계는,

상기 묶에 해당하는 위치의 엔트리 값과 상기 나머지 값에 해당하는 비트맵 값을 AND 연산한 결과 값이 1인 경우 상기 패킷을 드랍하는 단계를 포함할 수 있다.

[0024] 본 발명의 실시예에 있어서, 상기 SRAM은 미리정해진 패킷의 포트 범위를 반전시키는 반전 플래그(Reverse Flag)를 포함하여 상기 반전된 포트 범위에 해당하는 각 엔트리의 모든 비트맵을 1로 설정하도록 이루어지고, 상기 제2매칭 단계는, 상기 SRAM에서 해시 함수를 이용하여 상기 소스 포트 및 목적지 포트를 해시한 후, 상기 반전 플래그를 이용하여 상기 소스 포트 및 목적지 포트의 번호에 대응하는 각 엔트리의 비트맵이 1로 설정된 경우 매칭된 것으로 인식하는 단계를 포함할 수 있다.

[0025] 본 발명의 실시예에 있어서, 상기 해시테이블은 Src Port ANY, Dst Port ANY, No ANY 중 하나의 구성으로 이루어진 하나 이상의 해시테이블을 포함하고, 상기 제2매칭 단계에서, (a) 상기 해시테이블이 Src Port ANY 구성을 구비하는 경우에는 상기 목적지 포트만을 해시하여 상기 해시테이블 상의 엔트리의 위치를 찾아 매칭을 수행하고, (b) 상기 해시테이블이 Dst Port ANY 구성을 구비하는 경우에는, 상기 소스 포트만을 해시하여 상기 해시테이블 상의 엔트리의 위치를 찾아 매칭을 수행하고, (c) 상기 해시테이블이 No ANY의 구성을 구비하는 경우에는, 상기 소스 포트 및 목적지 포트 모두를 해시하여 상기 해시테이블 상의 엔트리의 위치를 찾아 매칭을 수행할 수 있다.

[0026] 본 발명의 실시예에 있어서, 상기 네트워크 스위치에서 수신한 복수의 패킷의 복수의 상이한 IP, 및 프로토콜의 포트 범위가 동일한 경우에, 상기 복수의 패킷에 동일한 값의 포트 범위 ID를 부여하고, 상기 제2매칭 단계는, 상기 복수의 패킷의 소스 포트 및 목적지 포트를 해시할 때 파라미터로 상기 동일한 포트 범위 ID를 이용하여 상기 해시테이블의 동일한 엔트리와 매칭하는 단계를 포함할 수 있다.

[0027] 본 발명의 실시예에 있어서, 상기 SRAM은 복수의 패킷에 대응하는 SRAM 해시테이블을 위한 복수의 반전 플래그, 복수의 포트 범위 ID가 저장되어 있으며, 상기 복수의 포트 범위 ID는 각 포트 범위 ID에 따라 해당하는 엔트리의 비트맵이 설정될 수 있다.

발명의 효과

[0029] 본 발명의 실시예에 따르면, 네트워크 스위치의 데이터 플레인에서 라우팅 또는 드랍시 TCAM을 이용하여 소스(source) IP, 목적지(destination) IP, 프로토콜(protocol) 매칭한 후 포트 범위 매칭은 SRAM을 이용하여 수행하여 데이터 처리 속도의 개선과 TCAM의 확장성(scalability)을 증가시키고 네트워크 스위치 데이터 플레인(data plane)의 매칭 프로세스에서 보다 경제적이면서 뛰어난 보안 성능을 만족시키는 네트워크 스위치의 데이터 플레인에서의 패킷 매칭 방법 및 이를 수행하는 네트워크 스위치를 제공할 수 있다.

[0030] 본 발명의 또다른 목적은, 네트워크 스위치의 데이터 플레인에서 라우팅 또는 드랍시 데이터 처리 속도의 개선과 TCAM의 확장성(scalability)을 증가시킬 뿐 아니라 SRAM의 이용을 추가적으로 최적화시킴으로서 SRAM의 확장성 또한 높일 수 있어 데이터 처리의 속도와 효율을 현저하게 개선할 수 있는 네트워크 스위치의 데이터 플레인에서의 패킷 매칭 방법 및 이를 수행하는 네트워크 스위치를 제공할 수 있다.

[0031] 본 발명의 효과는 상기한 효과로 한정되는 것은 아니며, 본 발명의 상세한 설명 또는 특허청구범위에 기재된 발명의 구성으로부터 추론 가능한 모든 효과를 포함하는 것으로 이해되어야 한다.

도면의 간단한 설명

[0033] 도 1은 본 발명의 일실시예에 따른 데이터 플레인에서 해시테이블 기반으로 패킷을 매칭하는 네트워크 스위치의 개략적인 구조도이다.

도 2는 본 발명의 일실시예에 따른 네트워크 스위치의 데이터 플레인에서의 패킷 매칭 방법의 개략적인 구성을 나타낸 흐름도이다.

도 3은 본 발명의 일실시예에 따른 데이터 플레인에서 해시테이블 기반으로 패킷을 매칭하는 네트워크 스위치에서 엔트리의 크기가 32 bit일 때의 비트맵을 매칭하는 예시를 나타낸 모식도이다.

도 4는 본 발명의 일실시예에 따른 데이터 플레인에서 해시테이블 기반으로 패킷을 매칭하는 네트워크 스위치의

포트 범위 매칭의 예시를 나타낸 모식도이다.

도 5는 본 발명의 일실시예에 따른 데이터 플레인에서 해시테이블 기반으로 패킷을 매칭하는 네트워크 스위치에서 포트 번호를 32의 집합으로 나누어 엔트리에 매칭하는 모습을 나타낸 모식도이다.

도 6은 본 발명의 일실시예에 따른 데이터 플레인에서 해시테이블 기반으로 패킷을 매칭하는 네트워크 스위치에서 포트를 엔트리에 매칭하는 로직을 나타낸 모식도이다.

도 7은 본 발명의 일실시예에 따른 네트워크 스위치의 데이터 플레인에서의 패킷 매칭 방법(PortCatcher)과 다른 방법(ACL_{TCAM})의 TCAM에서의 엔트리 소모량을 나타낸 그래프이다.

도 8은 본 발명의 일실시예에 따른 네트워크 스위치의 데이터 플레인에서의 패킷 매칭 방법(PortCatcher)과 다른 방법(ALPM)의 규칙에 따른 평균 지연시간을 나타낸 그래프이다.

도 9는 본 발명의 일실시예에 따른 네트워크 스위치의 데이터 플레인에서의 패킷 매칭 방법(PortCatcher)과 다른 방법(ALPM)의 시간에 따른 규칙 수행 가능 개수를 나타낸 그래프이다.

도 10은 본 발명의 일실시예에 따른 네트워크 스위치의 데이터 플레인에서의 패킷 매칭 방법(PortCatcher)의 규칙에 따른 지연시간 분포를 나타낸 그래프이다.

도 11은 본 발명의 일실시예에 따른 네트워크 스위치의 데이터 플레인에서의 패킷 매칭 방법(PortCatcher)과 다른 방법(ALPM, ACL_{TCAM})들을 사용하는 ACL에서 누락된 패킷과 플로우의 비율을 나타낸 그래프이다.

발명을 실시하기 위한 구체적인 내용

- [0034] 이하에서는 첨부한 도면을 참조하여 본 발명을 설명하기로 한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며, 따라서 여기에서 설명하는 실시예로 한정되는 것은 아니다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.
- [0035] 명세서 전체에서, 어떤 부분이 다른 부분과 "연결(접속, 접촉, 결합)"되어 있다고 할 때, 이는 "직접적으로 연결"되어 있는 경우뿐 아니라, 그 중간에 다른 부재를 사이에 두고 "간접적으로 연결"되어 있는 경우도 포함한다. 또한 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 구비할 수 있다는 것을 의미한다.
- [0036] 본 명세서에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 명세서에서, "포함하다" 또는 "가지다" 등의 용어는 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.
- [0037] 이하에서 본 발명의 네트워크 스위치의 데이터 플레인에서의 패킷 매칭 방법에 따른 ACL 매칭 방식은 포트캐처(PortCatcher)로 지칭하도록 한다. 또한, 이외의 다른 종래의 ACL 매칭 방식들은 TCAM을 사용하는 표준 방식의 ACL_{TCAM}과 상기 선행문헌1에 개시된 ACL 매칭 방식을 지칭하는 ALPM로 나타낸다.
- [0039] 이하에서는 도면을 참조하여 본 발명의 실시예들에 대하여 설명한다.
- [0040] 도 1은 본 발명의 일실시예에 따른 데이터 플레인에서 해시테이블 기반으로 패킷을 매칭하는 네트워크 스위치의 개략적인 구조도이다.
- [0041] 도 1을 참조하면, 네트워크 스위치(100)는 수신부(110), 파싱부(120), TCAM(130), SRAM(140), 프로세싱부(150)를 포함하여 구성될 수 있으나 이러한 구성요소로 한정되지는 않는다.
- [0042] 수신부(110)는 네트워크 스위치로 전송된 패킷을 수신할 수 있다.
- [0043] 파싱부(120)는 수신부(110)에서 수신한 패킷의 헤더를 파싱하여 소스(source) IP, 목적지(destination) IP, 프로토콜(protocol), 소스 포트(source port), 목적지 포트(destination port)를 추출할 수 있다. 또한, 파싱부(120)는 수신부(110)에서 수신한 복수의 패킷이 복수의 상이한 IP, 및 프로토콜에 대하여 동일한 포트 범위를

가지는 경우에, 상기 복수의 패킷에 동일한 값의 포트 범위 ID를 부여할 수 있다.

- [0044] TCAM(130)은 상기 패킷의 매칭 규칙(matching rule)들이 미리 저장되어 있고 상기 패킷의 소스 IP, 목적지 IP, 프로토콜에 대응하는 제1매칭 값들이 저장될 수 있다. 상기 패킷의 매칭 규칙은 바람직하게는, 소스 IP, 목적지 IP, 및 프로토콜의 매칭 규칙으로 구성될 수 있다.
- [0045] SRAM(140)은 패킷의 포트 범위 매칭을 위한 해시테이블을 포함하고, TCAM(130)을 이용한 매칭이 이루어지는 경우 상기 해시테이블을 이용하여 상기 패킷의 소스 포트 및 목적지 포트의 범위에 매칭되는 제2매칭 값들의 엔트리들이 저장될 수 있다.
- [0046] 부가적으로, SRAM(140)은 구체적으로는, 소스 애니, 목적지 애니, 노 애니에 대응하는 상기 해시테이블을 위한 복수의 반전 플래그, 복수의 포트 범위 ID가 저장되고, 상기 복수의 포트 범위 ID는 각 포트 범위 ID에 따라 해당하는 엔트리의 비트맵이 설정될 수도 있다.
- [0047] 상기 해시테이블은 레지스터(register)로 구현된 어레이(array)이고, 상기 어레이의 각 엔트리는 2^n 비트(bit)를 구비하고 상기 n은 정수로서 상기 네트워크 스위치의 모델에 따라 정의되며, 패킷의 포트의 번호에 해당하는 위치의 엔트리가 1로 사전 설정되어 있다. 상기 해시테이블은 미리정해진 패킷의 포트 범위를 반전시키는 반전 플래그(Reverse Flag)를 포함하여 상기 반전된 포트 범위에 해당하는 각 엔트리의 모든 비트맵을 1로 설정하도록 이루어지고, 상기 해시테이블은 소스 포트 애니(Src Port ANY), 목적지 포트 애니(Dst Port ANY), 노 애니(No ANY) 중 하나의 구성으로 이루어진 하나 이상의 해시테이블을 포함할 수 있다.
- [0048] 프로세싱부(150)는 TCAM(130)을 이용한 제1매칭과 상기 SRAM(140)을 이용한 제2매칭을 수행하고, 상기 제2매칭의 수행 간에 매칭이 이루어지는 경우 상기 패킷을 드랍하고, 상기 제1매칭 또는 제2매칭의 수행 간에 매칭이 이루어지지 않는 경우 라우팅 테이블 또는 ACL(Access Control List)을 이용하여 상기 패킷을 라우팅할 수 있다.
- [0049] 프로세싱부(150)는, SRAM(140)에서 해시 함수를 이용하여 상기 소스 포트 및 목적지 포트의 번호를 2^n 으로 나눈 몫을 이용하여 해시하고 상기 몫에 해당하는 위치의 엔트리 값과 상기 소스 및 목적지의 포트의 번호를 2^n 으로 나눈 나머지 값에 해당하는 비트맵(bitmap) 값을 AND 연산하여 매칭함으로서 상기 제2매칭을 수행하고, 상기 몫에 해당하는 위치의 엔트리 값과 상기 나머지 값에 해당하는 비트맵 값을 AND 연산한 결과 값이 1인 경우 상기 패킷을 드랍할 수 있다.
- [0050] 프로세싱부(150)는 상기 반전 플래그가 false를 나타내는 경우 상기 AND 연산한 결과 값이 0이 아닐 때 드랍을 수행하고, 상기 반전 플래그가 true를 나타내는 경우 상기 AND 연산한 결과 값이 0일 때 드랍을 수행할 수 있다.
- [0051] 프로세싱부(150)는, SRAM(140)에서 해시 함수를 이용하여 상기 소스 포트 및 목적지 포트를 해시한 후, 상기 반전 플래그를 이용하여 상기 소스 포트 및 목적지 포트의 번호에 대응하는 각 엔트리의 비트맵이 1로 설정된 경우 매칭된 것으로 인식하여 상기 제2매칭을 수행할 수 있다.
- [0052] 프로세싱부(150)는, 상기 복수의 패킷이 복수의 상이한 IP, 및 프로토콜에 대하여 동일한 포트 범위를 가지는 경우, 소스 포트 및 목적지 포트를 해시할 때 파라미터로 동일한 포트 범위 ID를 이용하여 상기 해시테이블의 동일한 엔트리와 매칭하여 제2매칭을 수행할 수 있다.
- [0053] 또한, 상기 해시테이블이 소스 포트 애니 구성을 구비하는 경우에는 상기 목적지 포트만을 해시하여 상기 해시테이블 상의 엔트리의 위치를 찾아 상기 제2매칭을 수행하고, 상기 해시테이블이 목적지 포트 애니 구성을 구비하는 경우에는, 상기 소스 포트만을 해시하여 상기 해시테이블 상의 엔트리의 위치를 찾아 상기 제2매칭을 수행하고, 상기 해시테이블이 노 애니의 구성을 구비하는 경우에는, 상기 소스 포트 및 목적지 포트 모두를 해시하여 상기 해시테이블 상의 엔트리의 위치를 찾아 상기 제2매칭을 수행한다. SRAM(140)에서 포트범위 전체를 드랍하는 경우, 즉 PORT ANY 방식의 구성을 가지는 경우에는, 예를 들어 포트 범위가 0 ~ 65535인 경우에 2,048(=65536/32)개의 엔트리가 필요한 반면에, 해시 함수에 ANY인 포트를 포함하지 않는 이상과 같은 방식을 이용하면, 2,048개의 엔트리를 절약할 수 있게 된다.
- [0055] 도 2는 본 발명의 일실시예에 따른 네트워크 스위치의 데이터 플레인에서의 패킷 매칭 방법의 개략적인 구성을

나타낸 흐름도이다.

- [0056] 도 2를 참조하면, 네트워크 스위치의 데이터 플레인에서의 패킷 매칭 방법에서 네트워크 스위치에서 패킷을 수신하는 수신 단계(S110); 상기 패킷의 헤더를 파싱하여 소스(source) IP, 목적지(destination) IP, 프로토콜(protocol), 소스 포트(source port), 목적지 포트(destination port)를 추출하는 추출 단계(S120); 상기 패킷의 매칭 규칙(matching rule)들이 저장된 TCAM(Ternary Content Addressable Memory)을 이용하여 상기 소스 IP, 목적지 IP, 프로토콜을 매칭하는 제1매칭 단계(S130); 상기 제1매칭 단계에서 매칭이 이루어지는 경우, 포트 범위 매칭을 위한 해시테이블을 포함하는 SRAM(Static Random Access Memory)에서 상기 해시테이블을 이용하여 상기 소스 포트 및 목적지 포트의 범위를 매칭하는 제2 매칭 단계(S140); 상기 제2매칭 단계에서 매칭이 이루어지는 경우, 상기 패킷을 드랍하는 드랍 단계(S150); 및 상기 제1매칭 단계(S130) 또는 제2매칭 단계(S140)에서 매칭이 이루어지지 않는 경우, 라우팅 테이블 또는 ACL(Access Control List)을 이용하여 상기 패킷을 라우팅하는 라우팅 단계(S160)를 포함할 수 있다.
- [0057] 네트워크 스위치에서 수신한 복수의 패킷의 복수의 상이한 IP, 및 프로토콜의 포트 범위가 동일한 경우에, 상기 복수의 패킷에 동일한 값의 포트 범위 ID를 부여할 수 있다.
- [0058] 상기 SRAM에는 복수의 패킷에 대응하는 SRAM 해시테이블을 위한 복수의 반전 플래그, 복수의 포트 범위 ID가 저장되어 있으며, 상기 복수의 포트 범위 ID 는 각 포트 범위 ID에 따라 해당하는 엔트리의 비트맵이 설정될 수 있다.
- [0059] 상기 해시테이블은 레지스터(register)로 구현된 어레이(array)이고, 상기 어레이의 각 엔트리는 2^n 비트(bit)를 구비하고 상기 n은 정수로서 상기 네트워크 스위치의 모델에 따라 정의되며, 패킷의 포트의 번호에 해당하는 위치의 엔트리가 1로 사전 설정될 수 있다.
- [0060] 상기 SRAM은 미리정해진 패킷의 포트 범위를 반전시키는 반전 플래그(Reverse Flag)를 포함하여 상기 반전된 포트 범위에 해당하는 각 엔트리의 모든 비트맵을 1로 설정하도록 이루어지고, 상기 해시테이블은 소스 포트 애니(Src Port ANY), 목적지 포트 애니(Dst Port ANY), 노 애니(No ANY) 중 하나의 구성으로 이루어진 하나 이상의 해시테이블을 포함할 수 있다.
- [0061] 제2매칭 단계(S140)는 상기 SRAM에서 해시 함수를 이용하여 상기 소스 포트 및 목적지 포트를 해시한 후, 상기 소스 포트 및 목적지 포트의 번호에 기초하여 상기 해시테이블의 해당하는 엔트리 위치를 확인하여 그 엔트리가 1로 설정된 경우 매칭된 것으로 인식하는 단계를 포함할 수 있다. 또한, 제2매칭 단계(S140)에서 상기 복수의 패킷의 소스 포트 및 목적지 포트를 해시할 때 바람직하게는, 동일한 포트 범위 ID의 해시를 통하여 상기 해시테이블의 동일한 엔트리와 매칭을 수행할 수 있다.
- [0062] 또한, 제2매칭 단계(S140)는, 상기 SRAM에서 해시 함수를 이용하여 상기 소스 포트 및 목적지 포트의 번호를 2^n 으로 나눈 몫을 이용하여 해시하고 상기 몫에 해당하는 위치의 엔트리 값과 상기 소스 및 목적지의 포트의 번호를 2^n 으로 나눈 나머지 값에 해당하는 비트맵(bitmap) 값을 AND 연산하여 매칭하는 단계를 포함할 수 있다.
- [0063] 제2매칭 단계(S140)는, 상기 SRAM에서 해시 함수를 이용하여 상기 소스 포트 및 목적지 포트를 해시한 후, 상기 반전 플래그를 이용하여 상기 소스 포트 및 목적지 포트의 번호에 대응하는 각 엔트리의 비트맵이 1로 설정된 경우 매칭된 것으로 인식할 수 있다.
- [0064] 제2매칭 단계(S140)에서, 상기 해시테이블이 소스 포트 애니 구성을 구비하는 경우에는 상기 목적지 포트만을 해시하여 상기 해시테이블 상의 엔트리의 위치를 찾아 매칭을 수행하고 상기 해시테이블이 목적지 포트 애니 구성을 구비하는 경우에는, 상기 소스 포트만을 해시하여 상기 해시테이블 상의 엔트리의 위치를 찾아 매칭을 수행하고, 상기 해시테이블이 노 애니의 구성을 구비하는 경우에는, 상기 소스 포트 및 목적지 포트 모두를 해시하여 상기 해시테이블 상의 엔트리의 위치를 찾아 매칭을 수행한다.
- [0065] 드랍 단계(S150)에서 상기 몫에 해당하는 위치의 엔트리 값과 상기 나머지 값에 해당하는 비트맵 값을 AND 연산한 결과 값이 0인지 확인하고, 상기 반전 플래그가 false를 나타내면, 상기 결과값이 0이 아닐 때 드랍을 수행하고, 반전 플래그가 true를 나타내면 상기 결과값이 0일 때 드랍을 수행한다.
- [0067] 도 3은 본 발명의 일실시예에 따른 데이터 플레인에서 해시테이블 기반으로 패킷을 매칭하는 네트워크 스위치에

서 엔트리의 크기가 32 bit일 때의 비트맵을 매칭하는 예시를 나타낸 모식도이다.

- [0068] 도 3을 참조하면, SRAM의 해시테이블은 레지스터(register)로 구현된 어레이이며, 상기 어레이의 각 엔트리 크기로 2^n bit를 가질 수 있다. 본 발명에서는 2^n bit를 가진 하나의 엔트리에서 비트맵을 사용하여 연속적인 포트 범위를 여러 개의 엔트리가 아닌 한 개의 엔트리에 저장한다. 상기 해시테이블에서 하나의 엔트리의 크기가 32 bit일 때 상기 해시테이블에서 포트 범위 0 내지 7(8개의 포트 번호)을 드랍하고 싶다면, 비트맵의 첫 번째부터 여덟 번째까지의 비트맵을 1로 설정한다. 이어서, 패킷의 5-tuple을 해시하여 해당하는 엔트리를 찾을 때에는 포트 번호 대신에, 포트 번호를 32로 나눈 몫을 이용하여 해시한다. 그리고 해당하는 Port 번호를 드랍하기 위하여 매칭을 할 때에는, 패킷의 Port 번호를 32로 나눈 나머지의 값의 해당하는 비트맵 값과 해당하는 위치의 엔트리의 값을 AND 연산하여 결과가 0이 아니라면, 해당 패킷을 드랍한다. 이러한 기법을 통해, 연속적인 Port 번호 0 ~ 63을 드랍해야 할 때, 기존에는 64개의 엔트리가 필요했지만, 32 bit로 결합하는 방식을 통해 2개의 엔트리만 필요하게 되어, TCAM의 확장성뿐 아니라 SRAM의 확장성 또한 높일 수 있다.
- [0070] 도 4는 본 발명의 일실시예에 따른 데이터 플레인에서 해시테이블 기반으로 패킷을 매칭하는 네트워크 스위치의 포트 범위 매칭의 예시를 나타낸 모식도이다.
- [0071] 도 4를 참조하면, 복수의 패킷에서 포트 범위가 같을 때, 상기 복수의 패킷에 동일한 값의 포트 범위 ID를 부여할 수 있으며, 포트 범위 매칭을 하기 위하여 해시를 할 때, 파라미터로 상기 포트 범위 ID를 이용하면, 결과적으로 동일한 엔트리를 가리키게 된다. 도 4의 서로 다른 IP, 및 프로토콜을 가진 패킷들에 대해서, 포트 범위 ID를 35로 부여하면 엔트리의 위치는 Hash(35, 32)가 되므로 결과적으로 해시테이블에서 동일한 엔트리를 가리키게 된다. 이를 통해 동일한 포트 범위를 가진 패킷들은 동일한 엔트리를 공유할 수 있기 때문에, 요구되는 해시테이블의 엔트리의 수를 감소시킬 수 있다.
- [0073] 도 5는 본 발명의 일실시예에 따른 데이터 플레인에서 해시테이블 기반으로 패킷을 매칭하는 네트워크 스위치에서 포트 번호를 32의 집합으로 나누어 엔트리에 매칭하는 모습을 나타낸 모식도이다.
- [0074] 도 5를 참조하면, 예를 들어, 포트 규칙(소스 포트, 목적지 포트)이 (30, 40~180), (30, 215~228), (170~225, 80), (181~219, 200~240)의 포트 범위를 가질 때, 이를 32의 포트 집합으로 나누어 14개로 분류하였고, 이하에서 이러한 분류 방식을 LRM(Linear Range Map)으로 지칭하도록 하였다. 해시테이블과 LRM기반의 포트 매칭을 위해, 연속되는 포트들을 LRME(LRM Entries)라고 하는 소스-목적지 포트 비트맵으로 나타내었다.
- [0075] 도 5에 도시된 것처럼 상기 포트 규칙을 (30, 40~180)을 (30, 40~63), (30, 64~95), (30, 96~127), (30, 128~159), 및 (30, 160~180)의 다섯 개의 연속되는 하위 집합인 LRME로 세분화하였다. 여기서 상기 각 하위 집합들은 소스 포트와 목적지 포트 모두에 대해 최대 32개의 연속되는 포트를 포함할 수 있고, 두 개의 32 bit 비트맵을 사용하여 상기 각 하위 집합을 표현할 수 있다.
- [0076] 상기 모든 포트 규칙에 대해 상기와 같은 동작을 반복함으로써 최종적으로 28개의 32 bit 비트맵으로 상기의 예시된 포트 규칙을 표현할 수 있으며, 상기 결과는 1810개의 32 bit 엔트리를 사용하여 기존의 해시테이블 기반의 방법에 비해 98.5%의 메모리 절약이 가능하다.
- [0077] 해시테이블에서 LRME를 찾기 위해서는 포트 집합 크기(예: 32)로 나눈 LRME의 첫 번째 소스 포트 및 목적지 포트를 사용하여 포트 집합 인덱스(Port Aggregation Index, PAI)를 계산한다. 예를 들어, 포트 쌍 (30, 40~63)의 32-PAI는 도 5에서와 같이 <0, 1>이 된다. 따라서, 모든 LRME에는 해시테이블의 항목 키로 사용할 고유한 PAI가 지정될 수 있다. 또한, 상기 LRME 내의 특정 포트 번호는 오프셋을 통하여 찾을 수 있으며, 상기 오프셋은 상기 소스 포트 및 목적지 포트를 32로 나눈 나머지로 상기 소스 포트 및 목적지 포트 상에서의 상기 특정 포트 번호의 위치를 특정할 수 있다.
- [0079] 도 6은 본 발명의 일실시예에 따른 데이터 플레인에서 해시테이블 기반으로 패킷을 매칭하는 네트워크 스위치에서 포트를 엔트리에 매칭하는 로직을 나타낸 모식도이다.
- [0080] 도 6에서 스테이지 -1은 TCAM에서 수행되는 단계를 의미한다. 해시테이블 기반으로 패킷을 매칭하는 네트워크 스위치에서 패킷을 수신하면, TCAM에서 5 tuple의 소스 IP, 목적지 IP, 및 프로토콜을 상기 패킷의 헤더에서 파

상하여 매칭을 수행한다. 상기 IP 테이블은 상기 패킷의 포트 범위가 같은 프로토콜들에 대하여 동일한 값을 부여한 포트 범위 ID(LRM-ID)와 상기 패킷의 포트 범위를 반전하는 것이 가능한 반전 플래그를 포함할 수 있고, 상기 LRM-ID와 반전 플래그는 소스 애니(Src ANY), 목적지 애니(Dst ANY), 및 노 애니(No ANY) 각각에 대응되도록 3개씩 존재할 수 있다.

[0081] 상기 스테이지-1의 TCAM에서 매칭이 완료되면 스테이지-2에서 상기 LRM-ID와 소스 포트, 목적지 포트, 및 반전 플래그를 입력 받는다. 스테이지-2는 포트 매칭을 위한 SRAM 해시테이블을 포함하고, 상기 해시테이블은 LRM-ID, 소스 포트의 PAI, 및 목적지 포트의 PAI로 매칭이 수행될 수 있다. 도 6의 32 PAI 일 때의 예시에서, 소스 포트의 값이 183일 때, 183을 32로 나눈 몫인 5을 이용하여 해당하는 해시테이블의 위치를 특정하고, 183을 32로 나눈 나머지인 23으로 상기 해당하는 해시테이블에서 비트맵의 정확한 위치에서의 값을 측정할 수 있다. 이후, LRME에서의 값과 비트맵에서의 값에 AND 연산을 수행하여 결과값이 0인지 확인한다. 만약 상기 반전 플래그가 false를 나타내면, 상기 결과값이 0이 아닐 때 드랍을 수행하고, 반전 플래그가 true를 나타내면 상기 결과값이 0일 때 드랍을 수행한다.

[0083] 도 7은 본 발명의 일실시예에 따른 네트워크 스위치의 데이터 플레인에서의 패킷 매칭 방법(PortCatcher)과 다른 방법(ACL_{TCAM})의 TCAM에서의 엔트리 소모량을 나타낸 그래프이다.

[0084] 도 7을 참조하면, ACL_{TCAM}은 최악의 경우 포트 범위 규칙을 소스 애니, 목적지 애니는 최대 30개, 노 애니는 최대 30*30개의 규칙으로 확장하는 내부 이진-프리픽스 기반이라 가정한다. 이와 달리, 포트캐처는 TCAM에서 IP, 및 프로토콜 매칭만 수행하기 때문에 포트캐처에 요구되는 TCAM 엔트리의 수는 최악의 경우에 ACL 규칙 수와 동일하게 설정될 수 있다.

[0085] 보다시피, ac13에서 230%의 가장 높은 증가율을 나타내는데 이는 상기 ac13의 규칙 세트가 다수의 HI(high range) 및 AR(arbitrary range) 포트 규칙을 포함하고 있기 때문이다. ac14에는 비슷한 양의 HI 및 AR포트 규칙이 존재하기 때문에, ACL 규칙 10K는 TCAM엔트리의 21K까지 확장된다. 주요한 확장의 원인은AR 규칙에 의해 발생되지만, ac11과 ac15는 유사한 경우를 보인다. 5개의 규칙 집합 중에서 ac12의 확장률이 130%로 가장 낮는데 이는 상기 ac12의 규칙이 주로 WC(wildcard) 69%와 EM(exact matching) 22%의 포트 규칙으로 구성되었기 때문이다.

[0086] ACL 규칙은 각각의 독립된 설계로 인해 소스 IP, 목적지 IP, 및 프로토콜 정의는 동일하지만 포트 설정은 서로 다른 것이 일반적이므로, 중복된 IP와 프로토콜 엔트리를 제거하는 방식으로 엔트리 수를 더욱 줄일 수 있다. 도 7에서, 포트캐처는 TCAM 항목의 중복을 제거하여 0.07 K 내지 3.53 K의 TCAM 엔트리를 절약할 수 있다. 이러한 결과는 ACL_{TCAM}과 비교할 때, 포트캐처가 TCAM 엔트리의 25% 내지 72%를 절약할 수 있다는 것을 나타낸다.

표 1

[0088]

	LRM	ANY	Dedup.	REV	Aggr.
ac11	0.26T	4.11M (-99%)	0.75M (-81%)	61.08K (-91%)	3.59K (-94%)
ac12	2.73T	41.67M (-99%)	0.25M (-99%)	4.14K (-98%)	0.17K (-95%)
ac13	3.63T	55.42M (-99%)	13.53M (-75%)	272.64K (-97%)	10.74K (-96%)
alc4	3.06T	46.80M (-99%)	6.37M (-86%)	160.88K (-97%)	6.92K (-95%)
alc5	0.29T	4.52M (-99%)	1.74M (-61%)	30.29K (-98%)	2.87K (-90%)

[0089] SRAM은 스위치의 TCAM에 비해 메모리에 여유가 존재하지만, 여전히 수십 메가바이트의 메모리로 제한된다. 따라서 SRAM의 엔트리 수를 줄이기 위해 본 발명인 포트캐처에서는 포트 집합(Aggr.), 포트 범위 반전(REV), 애니 포트 처리(ANY), 및 포트 규칙 중복 제거(Dedup)를 포함하는 최적화를 수행하였다.

[0090] 표 1에서는 임의의 ac11 내지 ac15에서 SRAM의 메모리 절약 효과를 나타내었다. LRM을 기준으로 두고, 포트 애니 처리(ANY), 포트 규칙 중복 제거(Dedup.), 범위 반전(REV), 포트 집합(Aggr.)을 수행하면서 이전 열과 비교하여 감소된 엔트리 비율을 나타낸다.

[0091] 결론적으로, 본 발명의 최적화를 통해 LRME의 수(즉, SRAM 테이블 엔트리)를 줄이고 SRAM 메모리를 절약하는 데

상당한 효과를 나타냈다. 더하여, 상기 테이블 엔트리들은 포트 테이블에서 각각 독립적으로 관리되기 때문에, 상기 테이블 엔트리의 감소는 SRAM의 확장성 문제를 해결할 뿐만 아니라, 규칙의 배치 속도도 증가시킬 수 있다.

- [0093] 도 8은 본 발명의 일실시예에 따른 네트워크 스위치의 데이터 플레인에서의 패킷 매칭 방법(PortCatcher)과 다른 방법(ALPM)의 규칙에 따른 평균 지연시간을 나타낸 그래프이다.
- [0094] 10K의 ACL 규칙들을 스위치의 데이터 플레인 상에 배치하고, 2K의 추가적인 규칙들은 독립적으로 제어 플레인에서 처리되어 데이터 플레인에 배치된다. 이 후, 2K 규칙에 대한 규칙에 따른 지연시간을 측정한다.
- [0095] 도 8(a)는 포트캐처 및 ALPM의 규칙 당 평균 입력 지연시간을 나타낸다. 상기에서 포트캐처를 사용했을 때 5개의 ACL 데이터 세트들에 대한 지연 시간이 0.76 ms 내지 1.59 ms로 평균 2.19 초의 지연시간을 가지는 ALPM보다 훨씬 적은 것을 볼 수 있다. 입력 과정 중에 포트캐처는 규칙 당 평균 0.49개 내지 1.38개의 SRAM 엔트리 입력을 수행하였다. 이와 달리, ALPM은 새로운 포트 범위 규칙을 구성할 때마다 매우 높은 오버헤드를 나타내고, 이는 결국 전체 규칙의 배치를 지연시키는 결과를 야기하였다. 포트캐처의 소비 시간은 주로 생성되는 LRME의 수에 따라 달라지고, 포트캐처의 최적화 설계로 상기 LRME의 수를 크게 감소시킬 수 있다.
- [0096] 새로운 규칙에 대한 메모리 공간을 확보하려면 비활성 규칙을 ACL에서 제거해야 한다. 포트캐처와 ALPM은 모두 ACL 규칙 삭제 기능을 지원하기 때문에, 입력된 규칙을 제거할 때의 지연시간을 도 8(b)에서 비교한다.
- [0097] 도 8(b)에서는 5개의 ACL 규칙 데이터 세트에 대한 규칙 별 삭제 지연시간을 나타낸다. 포트캐처는 상기 5개의 ACL 데이터 세트에 대해 0.72 ms 내지 1.75 ms를 제공하며 규칙 당 0.30개 내지 1.12개의 SRAM 엔트리 제거를 수행한다. 한편, ALPM의 삭제 지연 시간은 상기 ACL 데이터 세트에 따라 0.36 ms 내지 0.92 ms를 보인다. 포트캐처는 acl3을 제외한 모든 acl들에서 ALPM보다 낮은 성능을 보인다. 그러나 포트캐처에서는 수백 KB의 메모리만 사용하여 메모리 절감이 가능하다는 장점과 상기 ALPM에서 포트캐처에 비해 월등히 높은 입력 지연 시간을 가진다는 것을 고려할 때 포트캐처가 전체적으로 더 나은 성능을 보이는 것을 알 수 있다.
- [0099] 도 9는 본 발명의 일실시예에 따른 네트워크 스위치의 데이터 플레인에서의 패킷 매칭 방법(PortCatcher)과 다른 방법(ALPM)의 시간에 따른 규칙 수행 가능 개수를 나타낸 그래프이다.
- [0100] 도 9를 참조하면, 작업 요청(action request) 선과 가까울수록 요청된 규칙이 데이터 평면에 배치되는 속도가 빠르다는 것을 의미한다. 도 9에 도시된 것처럼 본 발명인 포트캐처 방식은 지연 없이 동적 ACL 규칙을 배치할 수 있는 반면 종래의 ALPM은 규칙 배치에 따른 지연시간이 너무 커서 동적 규칙 배치의 처리가 어렵다는 것을 알 수 있다.
- [0102] 도 10은 본 발명의 일실시예에 따른 네트워크 스위치의 데이터 플레인에서의 패킷 매칭 방법(PortCatcher)의 규칙에 따른 지연시간 분포를 나타낸 그래프이다.
- [0103] 도 10을 참조하면, 10K의 규칙 중에서 44.12%가 12 ms 이내에 배치되고 규칙의 76.52%는 13 ms 이내에 배치될 수 있다. 결과적으로, 포트캐처는 단일 규칙을 입력하는데 평균 13.10 ms가 소요되는 것을 확인할 수 있으며, 스위치의 제어 플레인 CPU는 ALPM의 2.19초보다 168배 더 낮다.
- [0105] 도 11은 본 발명의 일실시예에 따른 네트워크 스위치의 데이터 플레인에서의 패킷 매칭 방법(PortCatcher)과 다른 방법(ALPM, ACL_{TCAM})들을 사용하는 ACL에서 누락된 패킷과 플로우의 비율을 나타낸 그래프이다.
- [0106] 도 11을 참조하면, 포트캐처는 총 6,378,442 패킷 중 7.91%의 공격 패킷만 누락했으며, 이는 ALPM에서의 63.36%보다 훨씬 낮은 수치이다. 더욱이, ACL_{TCAM}에서는 TCAM의 메모리 제약이 존재하고, 306,355개의 플로우 중 91.18%의 악의적인 플로우의 누락으로 인해 총 93.54%의 패킷을 누락하였다.
- [0107] 결과적으로, ACL_{TCAM}은 확장성이 낮기 때문에 동적 ACL에서는 사용할 수 없다는 것을 의미한다. 또한, 포트캐처와 ALPM은 어떠한 플로우도 누락하지 않았기 때문에 규칙의 배치에서 발생하는 ALPM의 높은 지연 시간이 대량의 패

킷 누락을 야기했다는 것을 의미할 수 있다.

[0108] 포트캐처는 상기의 ACL 규칙 당 9 byte의 TCAM 및 13 byte의 SRAM 메모리를 사용하였다. 따라서, 플로우 306,355개 전체의 데이터 플레인에서의 메모리 소모량은 TCAM에서 2.62 MB, SRAM에서 3.79 MB이므로 포트캐처는 더 높은 트래픽 용량에서도 동작이 가능하다는 것을 알 수 있다.

[0110] 전술한 본 발명의 설명은 예시를 위한 것이며, 본 발명이 속하는 기술분야의 통상의 지식을 가진 자는 본 발명의 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 쉽게 변형이 가능하다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적이 아닌 것으로 이해해야만 한다. 예를 들어, 단일형으로 설명되어 있는 각 구성 요소는 분산되어 실시될 수도 있으며, 마찬가지로 분산된 것으로 설명되어 있는 구성 요소들도 결합된 형태로 실시될 수 있다.

[0111] 본 발명의 범위는 후술하는 특허청구범위에 의하여 나타내어지며, 특허청구범위의 의미 및 범위 그리고 그 균등 개념으로부터 도출되는 모든 변경 또는 변형된 형태가 본 발명의 범위에 포함되는 것으로 해석되어야 한다.

부호의 설명

[0113] 100: 네트워크 스위치

110: 수신부

120: 파싱부

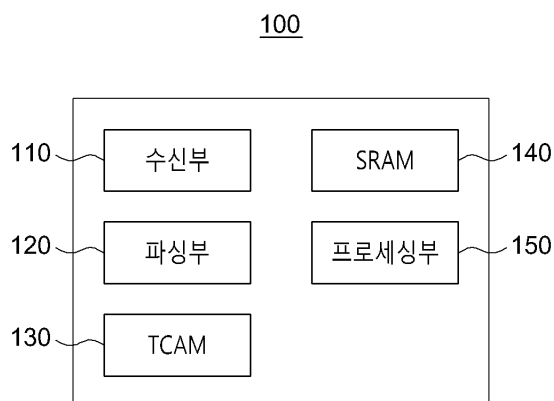
130: TCAM

140: SRAM

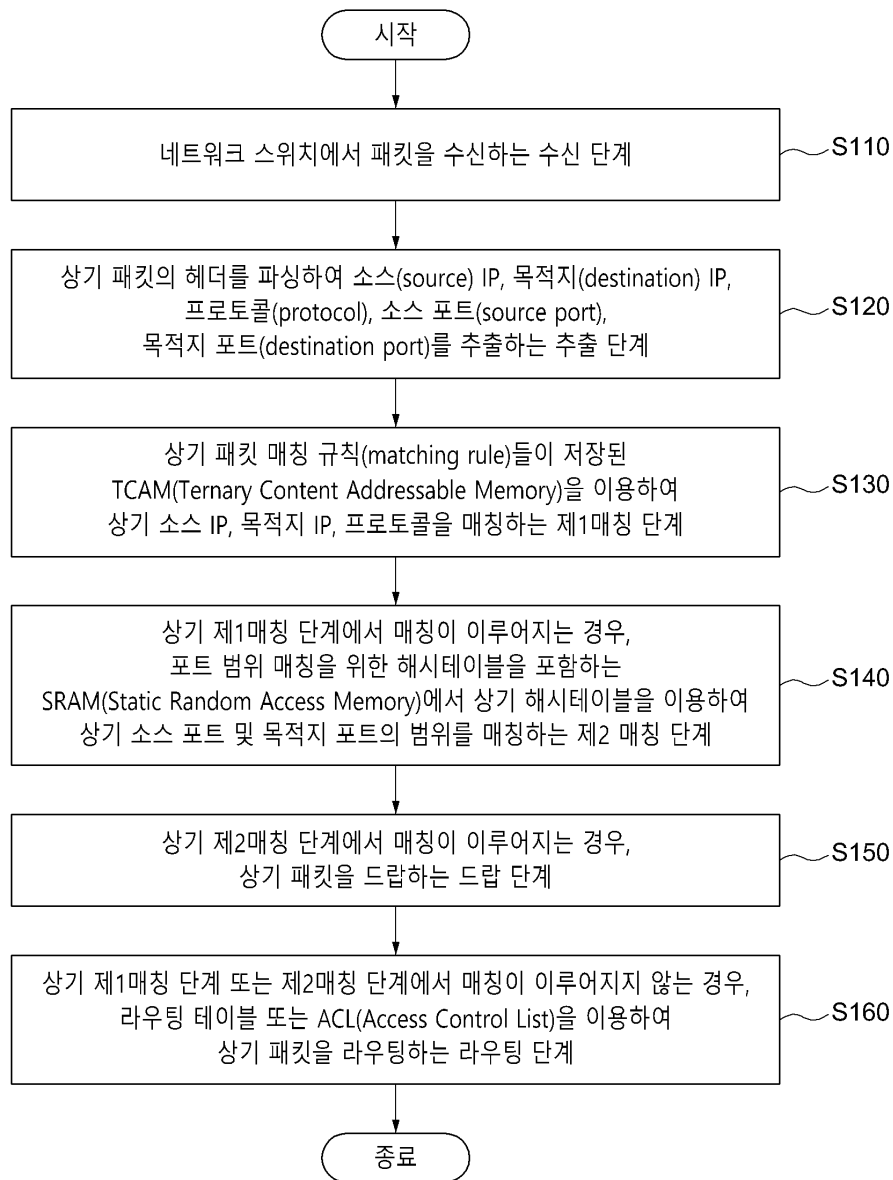
150: 프로세싱부

도면

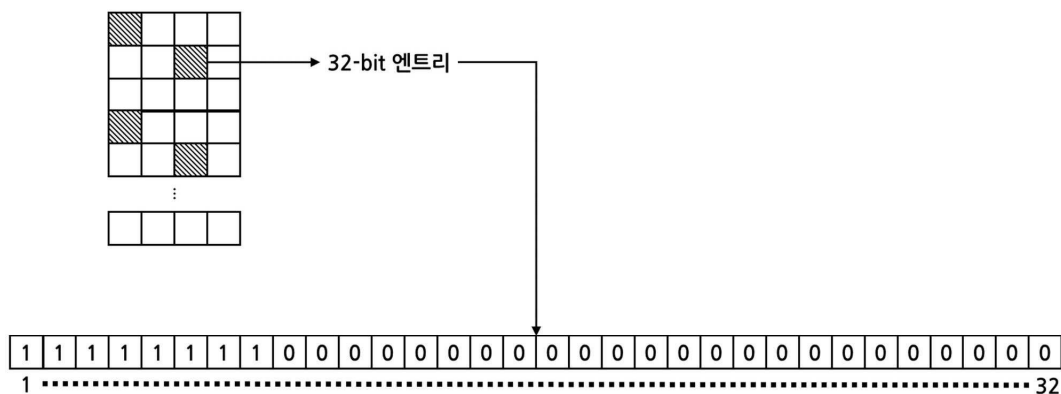
도면1



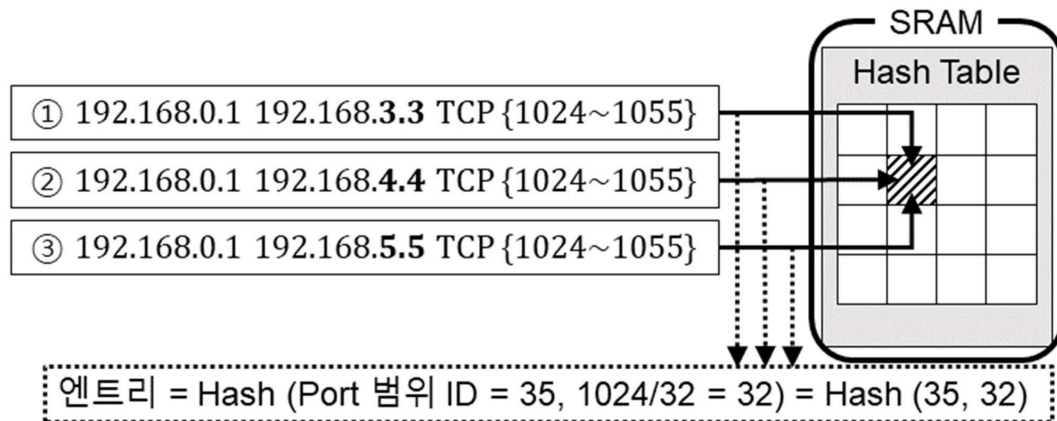
도면2



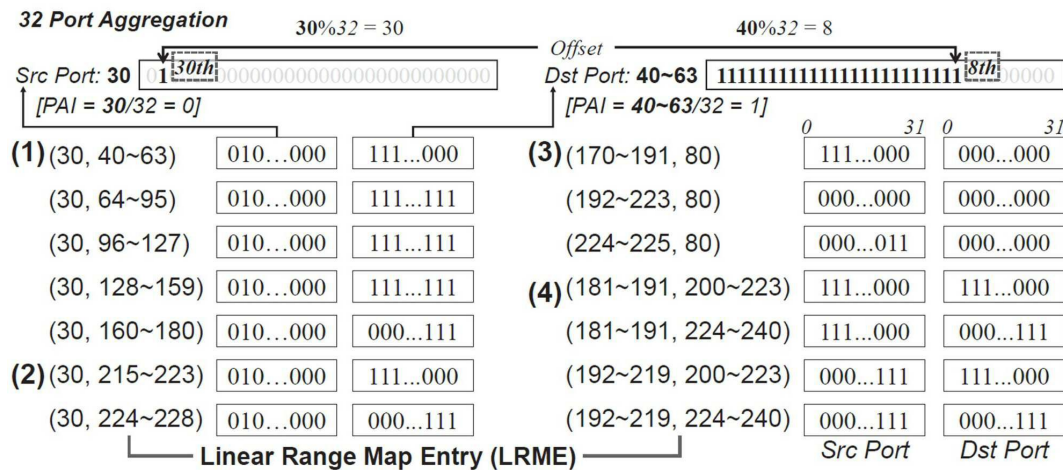
도면3



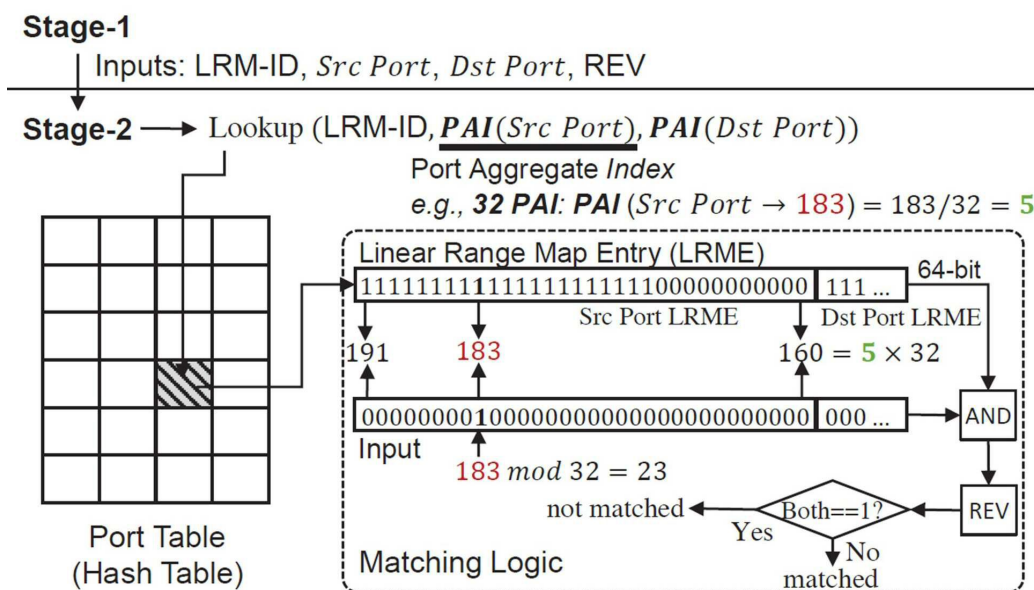
도면4



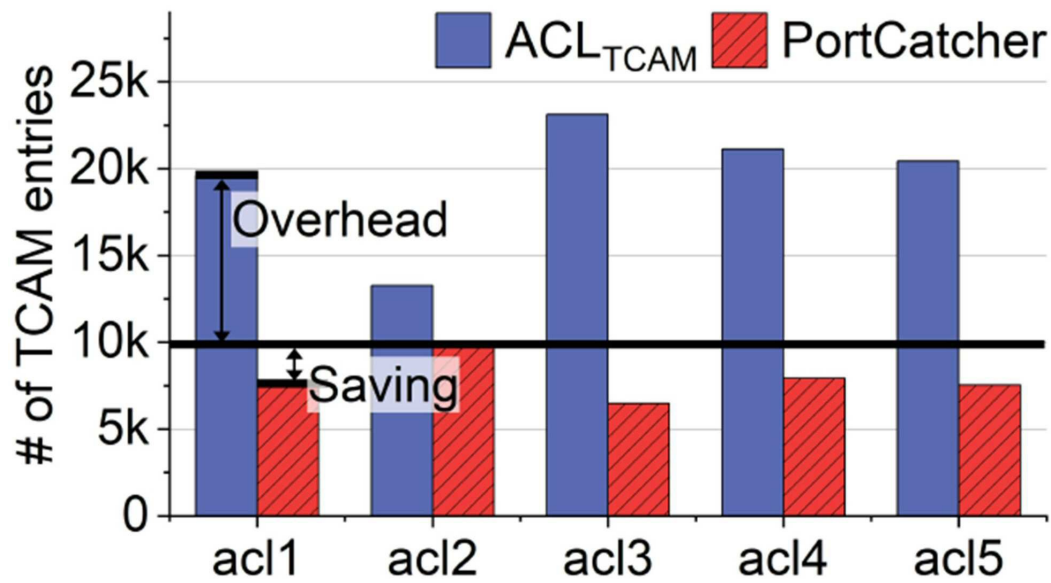
도면5



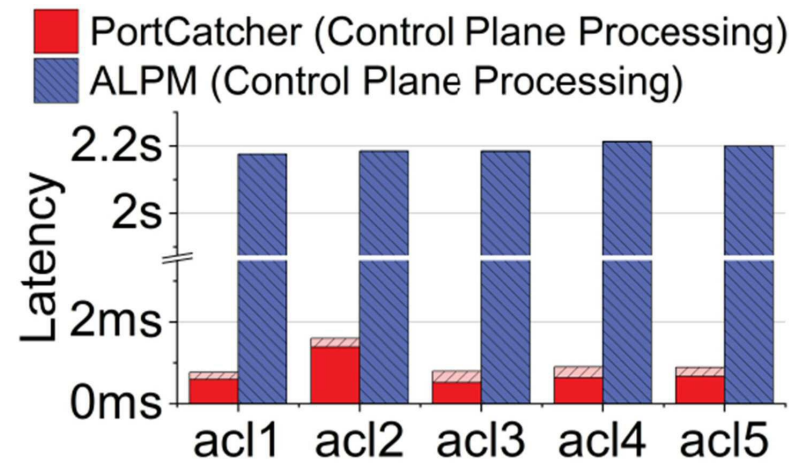
도면6



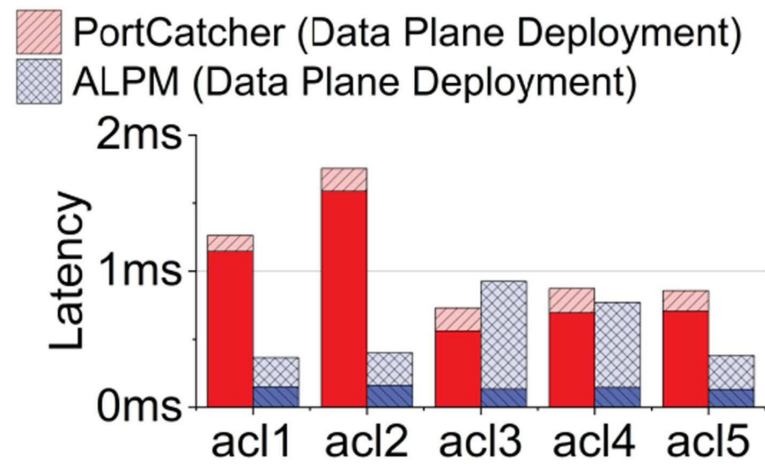
도면7



도면8

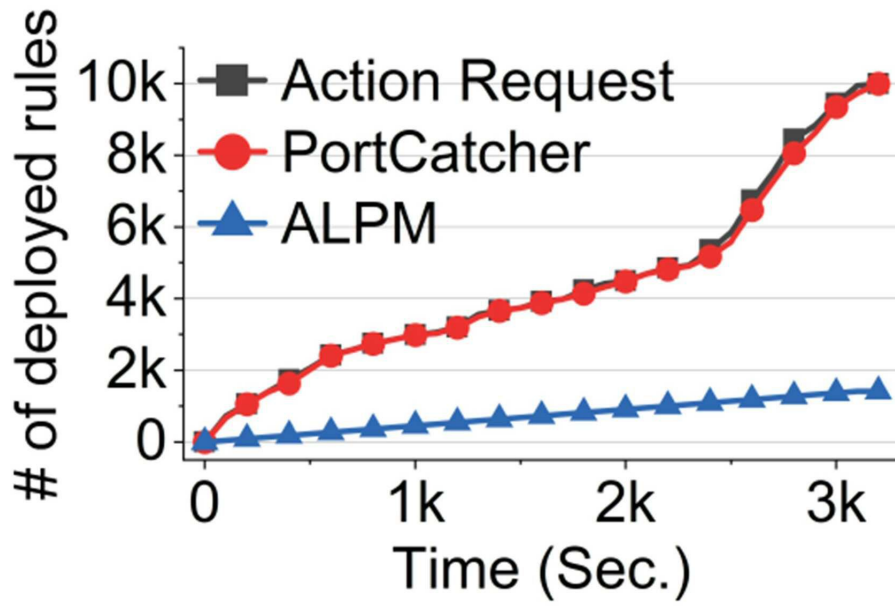


(a) Insertion

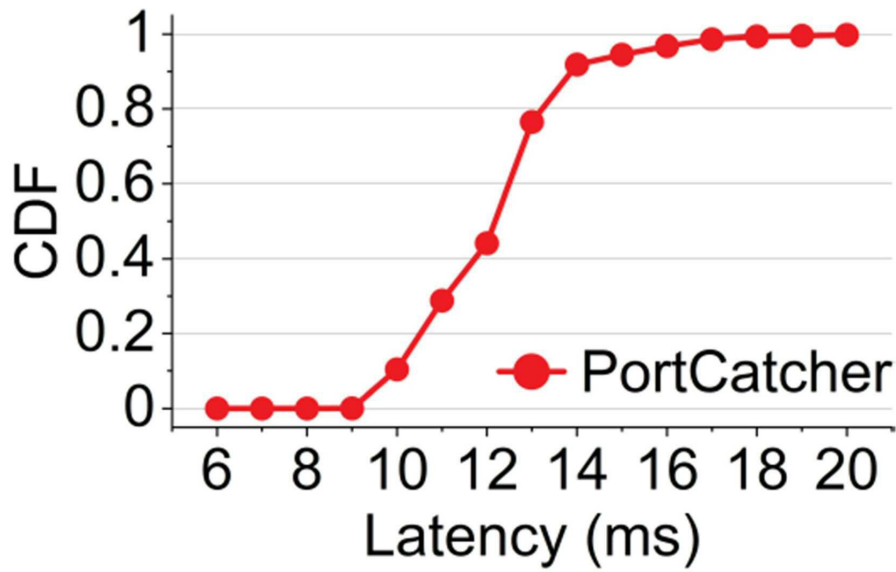


(b) Deletion

도면9



도면10



도면11

