(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.
H04L 12/22 (2006.01)

(45) 공고일자 2007년08월28일
(11) 등록번호 10-0751991
(24) 등록일자 2007년08월17일

(21) 출원번호 10-2002-0028933
(22) 출원일자 2002년05월24일
심사청구일자 2006년03월02일

(65) 공개번호 10-2002-0090160
(43) 공개일자 2002년11월30일

(30) 우선권주장 09/866,259 2001년05월25일 미국(US)

(73) 특허권자 잘링크 세미콘덕터 브이.엔. 아이엔씨.
미국, 씨에이 92612, 아이르빈 슈트 100, 121 이노베이션 드라이브

(72) 발명자 익, 제임스 칭-샤우
미국, 씨에이 92691, 미션 비에조, 24682 베스타

린, 창화
미국, 씨에이 91745, 하씨엔다 하이츠, 2248 컨츄리칸윤로드

(74) 대리인 이건주

(56) 선행기술조사문헌
JP2000354034 A US5944823 A

심사관 : 김병균

전체 청구항 수 : 총 14 항

(54) 보안기능이 개선된 데이터 네트워크 노드

(57) 요약

데이터 전송 네트워크상에서 데이터 스위칭 노드에서 데이터 패킷을 안전하게 전송하는 장치 및 방법이 제공되어 있다. 상기 데이터 스위칭 노드는 스위칭 엔트리들의 스위칭 데이터베이스를 유지한다. 각각의 스위칭 엔트리는 활성화시에 스위칭 엔트리의 변경을 방지하는 변경 보호 기능을 갖는다. 데이터 네트워크 노드들의 동적 토폴로지 발견은 데이터 스위칭 노드의 개개의 물리통신포트들에 연관된 토폴로지 발견 제어 플래그에 의해 디세이블될 수 있다. 미지의 수신지 플러드 데이터 트래픽은 디세이블된 토폴로지 발견을 갖는 물리통신포트들로 반복 전송되지 않거나 또는 물리통신포트들로 이런 미지의 수신지 데이터 트래픽을 반복 전송하는 것을 억제한다. 적대적 MAC ADDR 공격 사건을 검출하고 방지하며 보고하는 한편, 우호적 환경 및 적대적 환경 모두에서 동작할 수 있는 데이터 스위칭 노드로부터 여러 이점들이 유도된다.

대표도

도 1

특허청구의 범위

청구항 1.

보안기능이 개선된 데이터 스위칭 노드로서,

다수개의 통신포트들;

데이터 네트워크 노드 식별자와 통신포트간의 연관관계를 특정하는 다수개의 스위칭 엔트리들을 갖는 스위칭 데이터베이스;

각각이 하나의 스위칭 엔트리에 연관되어 있는 다수개의 스위칭 엔트리 보호 플래그들; 및

스위칭 데이터베이스 업데이트 과정을 실행하는 제어기를 포함하며,

상기 보호 플래그가 설정된 경우에는 보호된 스위칭 엔트리를 변경하기 위하여 적대적 데이터 네트워크 노드에 의한 공격이 방지됨으로써, 이에 의해 데이터 스위칭 노드가 우호적 데이터 네트워킹 환경 및 적대적 데이터 네트워킹 환경 모두에서 안전하게 동작하는 것을 특징으로 하는 보안기능이 개선된 데이터 스위칭 노드.

청구항 2.

제1항에 있어서, 상기 통신포트들이 포트 식별자들에 의해 스위칭 엔트리내에 표시되어 있는 것을 특징으로 하는 보안기능이 개선된 데이터 스위칭 노드.

청구항 3.

보안기능이 개선된 데이터 스위칭 노드로서,

다수개의 물리통신포트들;

데이터 네트워크 노드 식별자와 통신포트간의 연관관계를 지정하는 다수개의 스위칭 엔트리들을 갖는 스위칭 데이터베이스;

각각이 하나의 통신포트에 연관되어 있는 다수개의 토폴로지 발견 디세이블 플래그들; 및

데이터 전송 네트워크 토폴로지 업데이트 과정을 수행하는 제어기를 포함하며,

토폴로지 발견 디세이블된 물리통신포트에 연관되어 있는 통신포트를 지정하는 스위칭 엔트리를 적어도 하나 추가하기 위한 적대적 데이터 네트워크 노드에 의한 공격이 방지됨으로써, 이에 의해 데이터 스위칭 노드가 우호적 데이터 네트워킹 환경 및 적대적 데이터 네트워킹 환경 모두에서 안전하게 동작하는 것을 특징으로 하는 보안기능이 개선된 데이터 스위칭 노드.

청구항 4.

보안기능이 개선된 데이터 스위칭 노드로서,

다수개의 물리통신포트들;

각각이 데이터 네트워크 노드 식별자와 통신포트간의 연관관계를 지정하는 다수개의 스위칭 엔트리들을 갖는 스위칭 데이터베이스;

각각이 하나의 통신포트에 연관되어 있는 다수개의 토폴로지 발견 디세이블 플래그들;

전역 미지 수신지 플러드 제어 플래그; 및

페이로드 데이터 유니트(PDU) 전송 과정을 실시하는 제어기를 포함하며,

상기 스위칭 데이터베이스내에 저장되지 않은 수신지 데이터 노드 식별자를 갖는 수신된 PDU는 재설정된 토폴로지 발견 디세이블 플래그를 갖는 물리통신포트들로만 반복 전송됨으로써, 이에 의해 상기 물리통신포트들에 연결되어 있는 적대적 데이터 네트워크 노드들이 미지의 수신지 데이터 트래픽을 도청하는 것을 방지하는 것을 특징으로 하는 보안기능이 개선된 데이터 스위칭 노드.

청구항 5.

보안기능이 개선된 데이터 스위칭 노드로서,

다수개의 물리통신포트들;

각각이 데이터 네트워크 노드 식별자와 통신포트간의 연관관계를 지정하는 다수개의 스위칭 엔트리들을 갖는 스위칭 데이터베이스;

각각이 하나의 통신포트에 연관되어 있는 다수개의 미지의 수신지 플러드 제어 플래그들; 및

페이로드 데이터 유니트(PDU) 전송 과정을 실시하는 제어기를 포함하며,

상기 스위칭 데이터베이스내에 저장되지 않은 수신지 데이터 노드 식별자를 갖는 수신된 PDU는 재설정된 미지의 수신지 플러드 제어 플래그들을 갖는 물리통신포트들로만 반복 전송됨으로써, 이에 의해 상기 물리통신포트들에 연결되어 있는 적대적 데이터 네트워크 노드들이 미지의 수신지 데이터 트래픽을 도청하는 것을 방지하는 것을 특징으로 하는 보안기능이 개선된 데이터 스위칭 노드.

청구항 6.

데이터 전송 네트워크상에서 데이터 트래픽을 전송하는 데이터 스위칭 노드의 스위칭 데이터베이스를 안전하게 업데이트 하는 방법으로서, 상기 방법은,

데이터 스위칭 노드의 소스 물리통신포트상에 수신된 데이터 트래픽으로부터 소스 데이터 네트워크 노드 식별자를 추출하는 단계;

각각이 데이터 네트워크 노드 식별자와 통신포트간의 연관관계를 지정하는 다수개의 스위칭 엔트리들을 갖는 스위칭 데이터베이스에게 질의하며, 상기 질의는 상기 추출된 소스 데이터 네트워크 식별자를 키(Key)로서 사용하는 단계;

만일 상기 소스 데이터 네트워크 노드 식별자에 대응하는 스위칭 엔트리가 스위칭 데이터베이스에서 발견되지 않는 경우, 스위칭 데이터베이스에 신규한 스위칭 엔트리를 추가하는 단계; 및

만일 발견된 스위칭 엔트리에 연관된 스위칭 엔트리 보호 플래그가 재설정되는 경우, 상기 추출된 소스 데이터 네트워크 노드 식별자에 대응하는 것으로 발견된 스위칭 엔트리의 통신포트 내역을 변경하는 단계를 포함하며,

이에 의해, 상기 데이터 스위칭 노드에 의해 처리되는 데이터 트래픽의 방향변경(Redirection)을 방지하는 것을 특징으로 하는 방법.

청구항 7.

데이터 전송 네트워크에 연관되어 있는 데이터 스위칭 노드의 스위칭 데이터베이스내에 유지되고 있는 데이터 전송 네트워크 토폴로지 정보를 안전하게 업데이트하는 방법으로서, 상기 방법은,

데이터 스위칭 노드의 소스 물리통신포트상에 수신된 데이터 트래픽으로부터 소스 데이터 네트워크 노드 식별자를 추출하는 단계;

각각이 데이터 네트워크 노드 식별자와 통신포트간의 연관관계를 지정하는 다수개의 스위칭 엔트리들을 갖는 스위칭 데이터베이스에게 질의하며, 상기 질의는 상기 추출된 소스 데이터 네트워크 노드 식별자를 키로서 사용하는 단계; 및

만일 상기 소스 데이터 네트워크 노드 식별자에 대응하는 스위칭 엔트리가 스위칭 데이터베이스에서 발견되지 않으며 또 연관된 토폴로지 발견 디세이블 플래그가 재설정되는 경우, 스위칭 데이터베이스에 신규한 스위칭 엔트리를 추가하는 단계를 포함하며,

이에 의해, 적대적 데이터 네트워크 노드가 소스 물리통신포트에 연결되는 것이 방지되는 것을 특징으로 하는 방법.

청구항 8.

제7항에 있어서, 상기 토폴로지 발견 디세이블 플래그는 상기 소스 통신포트에 연관되는 것을 특징으로 하는 방법.

청구항 9.

제7항에 있어서, 상기 토폴로지 발견 디세이블 플래그는 상기 데이터 스위칭 노드의 모든 물리통신포트에 연관되는 것을 특징으로 하는 방법.

청구항 10.

데이터 스위칭 노드에 대한 미지의 수신지를 갖는 데이터 트래픽을 전송하는 보안기능이 개선된 방법으로서, 상기 방법은,

데이터 스위칭 노드의 소스 물리통신포트상에 수신된 상기 미지의 수신지 데이터 트래픽으로부터 소스 데이터 네트워크 노드 식별자를 추출하는 단계;

각각이 데이터 네트워크 노드 식별자와 통신포트간의 연관관계를 지정하는 다수개의 스위칭 엔트리들을 갖는 스위칭 데이터베이스에게 질의하며, 상기 질의는 상기 추출된 소스 데이터 네트워크 노드 식별자를 키로서 사용하는 단계;

만일 상기 데이터 스위칭 노드에 연관된 전역 미지 수신지 플러드 제어 플래그가 재설정되는 경우, 상기 데이터 스위칭 노드의 다수개의 물리통신포트들 각각으로 상기 수신된 데이터 트래픽을 반복 전송하는 단계; 및

만일 전역 미지 수신지 플러드 제어 플래그가 설정되는 경우, 설정된 토폴로지 발견 디세이블 기능을 갖는 물리통신포트들을 제외하고 다수개의 물리통신포트들 각각으로 상기 수신된 데이터 트래픽을 반복 전송하는 단계를 포함하며,

이에 의해, 설정된 토폴로지 발견 디세이블 플래그를 갖는 물리통신포트에 연결된 적대적 데이터 네트워크 노드가 미지의 수신지 데이터 트래픽을 감시하는 것을 방지하는 것을 특징으로 하는 방법.

청구항 11.

제10항에 있어서, 미지의 수신지 데이터 트래픽을 반복하며, 상기 방법은 상기 소스 통신포트로의 데이터 트래픽 반복전송를 억제하는 단계를 더 포함하는 것을 특징으로 하는 방법.

청구항 12.

제10항에 있어서, 상기 각각의 물리통신포트는 연관된 미지의 수신지 플러드 제어 비트를 더 포함하며,

상기 방법은, 상기 연관된 미지의 수신지 플러드 제어 비트가 설정되어 있는 통신포트들로의 데이터 트래픽 반복전송를 억제하는 단계를 더 포함하는 것을 특징으로 하는 방법.

청구항 13.

데이터 스위칭 노드에 대한 미지의 수신지 데이터 트래픽을 전송하는 보안기능이 개선된 방법으로서, 상기 방법은,

데이터 스위칭 노드의 소스 물리통신포트상에 수신된 상기 미지의 수신지 데이터 트래픽으로부터 소스 데이터 네트워크 노드 식별자를 추출하는 단계;

각각이 데이터 네트워크 노드 식별자와 통신포트간의 연관관계를 지정하는 다수개의 스위칭 엔트리들을 갖는 스위칭 데이터베이스에게 질의하며, 상기 질의는 상기 추출된 소스 데이터 네트워크 노드 식별자를 키로서 사용하는 단계;

만일 상기 물리통신포트에 연관된 미지의 수신지 플러드 제어 플래그가 재설정되는 경우, 상기 데이터 스위칭 노드의 다수개의 통신포트들 각각으로 상기 수신된 데이터 트래픽을 반복 전송하는 단계; 및

설정된 미지의 수신지 플러드 제어 플래그를 갖는 물리통신포트들을 제외하고 다수개의 물리통신포트들 각각으로 상기 수신된 데이터 트래픽을 반복 전송하는 단계를 포함하며,

이에 의해, 설정된 연관 토폴로지 발견 디세이블 플래그를 갖는 물리통신포트에 연결되어 있는 적대적 데이터 네트워크 노드가, 미지의 수신지 데이터 트래픽을 감시하는 것을 방지하는 것을 특징으로 하는 방법.

청구항 14.

제13항에 있어서, 미지의 수신지 데이터 트래픽을 반복하며, 상기 방법은 상기 소스 통신포트로의 데이터 트래픽 반복전송를 억제하는 단계를 더 포함하는 것을 특징으로 하는 방법.

명세서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 데이터 전송 네트워크에 있어서의 데이터 스위칭 기술에 관한 것으로, 특히 보다 향상된 네트워킹 보안특성을 제공하는 방법 및 장치에 관한 것이다.

데이터 전송 네트워크상에서 데이터를 전달함에 있어서, 데이터 스위칭 노드는 상호연결된 데이터 링크들을 통하여 데이터 트래픽의 흐름을 지시하는데에 사용된다. 각각의 데이터 링크는 하나의 포트 식별자(Port Identifier)를 갖는 물리통신포트를 통해 데이터 스위칭 노드에 연결된다.

전달될 데이터는 일반적으로 데이터 패킷, 프레임, 셀 등과 같은 페이로드 데이터 유니트(Payload Data Units; PDU)로 나뉘어진다. 상기 각각의 PDU는 라우팅(Routing) 정보와 페이로드를 포함한다. 상기 라우팅 정보는 일반적으로 PDU 헤더(Header)에 유지된다. 라우팅 정보는 예를 들어, 'Media Access Control ADDResses'(MAC ADDRs)를 포함한다. 상기

MAC ADDRs는 고유한 것으로서 데이터 네트워크 노드에 연관된 데이터 네트워크 인터페이싱 장치와 관련이 있다. 상기 네트워크 인터페이싱 장치의 예로는 네트워크 인터페이스 카드(Network Interface Card; NIC)가 있다. 따라서, 하나의 MAC ADDR은 하나의 데이터 네트워크 노드 식별자를 나타낸다고 말할 수 있다. 라우팅 정보내의 MAC ADDR의 실례는 소스(Source) 및 수신지 주소(Destination Addresses)로 알려진 것과 관계가 있다.

데이터 스위칭 노드들은 연결되어 있는 데이터 네트워크 노드들의 동적인 토폴로지 발견(Topology Discovery)를 위하여 MAC ADDR 정보를 활용하며 동시에 특정 수신지 MAC ADDRs로 데이터 트래픽을 전송하기 위하여 MAC ADDR 정보를 활용한다. 이러한 데이터 스위칭 노드는 스위칭 데이터베이스를 유지하고 또한 "계층 2 스위칭"을 실행한다고 한다. 계층 2는 개방형 시스템 상호접속(Open Systems Interconnection: OSI) 프로토콜 스택을 참조하여 기술되는데, 그의 세부사항은 데이터 스위칭 및 전송 기술분야에서 이미 잘 알려져 있는 것으로서 본 명세서에서 참조로서 포함된다.

스위칭 데이터베이스에 관한 예시로는 스위칭 데이터베이스 엔트리들을 갖는 조사표를 들 수 있는데, 각각의 엔트리는 MAC ADDR과 포트 식별자(Port IDentifier: PortID) 사이의 연관관계를 지정한다. 상기 스위칭 데이터베이스내에 유지되는 하나의 MAC ADDRs를 지정하는 어느 수신된 PDU는, 대응하는 데이터베이스 엔트리에 지정된 PortID로 전환된다.

스위칭 데이터베이스 없이도, 데이터 스위칭 노드는, PDU가 이미 수신되어 있는 물리통신포트를 제외하고는 PDU에 연관된 모든 물리통신포트들로 각 PDU를 동시전송하는 하나의 허브(hub)와 같이 행동한다. 이러한 동시전송동작은 또한 "플러드(flooding)"로서 알려져 있다. 상기 스위칭 데이터베이스의 존재는, 수신된 PDU들이 스위칭 데이터베이스에 존재하지 않는 미지의 수신지(Unknown Destination) MAC ADDRs를 가져가는 경우에 대한 플러드의 발생률을 줄인다.

토폴로지 발견으로서 알려진 과정인데, 하나의 스위칭 데이터베이스를 구성함에 있어서 데이터 스위칭 노드에 연관된 제어기가 각각의 물리통신포트에 수신된 PDU들의 소스 MAC ADDRs를 추출한다. 만일 상기 MAC ADDR:PortID 쌍이 스위칭 데이터베이스에서 발견되지 않는다면, 상기 제어기는 상기 스위칭 데이터베이스내에 엔트리를 생성함으로써, 새로운 MAC ADDR:PortID 연관관계를 저장한다. 이러한 스위칭 데이터베이스를 구축하는 능력은 또한 데이터 네트워크 노드들의 동적 발견기능을 제공한다. 상기 데이터 네트워크 노드들의 동적 발견기능은 데이터 스위칭 노드에 연결되어 있는 데이터 네트워크 세그먼트들에 대하여 최근들어 부가된 기능이다. 상기 데이터 네트워크 노드들의 동적 발견 및 상기 스위칭 데이터베이스의 구축으로 인해, 이러한 데이터 스위칭 장치의 "플러그-앤-플레이(plug-and-play)" 동작이 제공된다. 만일 상기 동작 및 구축이 제공되지 않는다면, 데이터 전송 네트워크내에서 상호연결된 데이터 네트워크 노드들에 대한 절대적인 지식뿐만 아니라 사람들간의 상호작용이 광범위하게 필요하게 될 것이다.

상기한 플러그-앤-플레이 동작은 흔히 확대되는데, 데이터 스위칭 노드에 연관되어 있는 데이터 전송 네트워크의 서로 다른 세그먼트들에게 데이터 네트워크 노드들이 연결되는 경우, 상기 데이터 스위칭 노드는 데이터 네트워크 노드들의 이동을 추적할 수 있게 된다. 엔트리내에 지정된 MAC ADDR를 갖는 PDU가, 엔트리내에 지정된 PortID와 상이한 PortID를 갖는 상이한 물리통신포트로부터 수신되는 경우, 상기 MAC ADDR과 PortID간의 연관관계는 상기 스위칭 데이터베이스내에서 변경된다. 이 경우, 새로운 PortID는 상기 엔트리내에 저장되어 있는 이전의 PortID 내역위로 단순히 덮어쓰기 된다.

상기한 플러그-앤-플레이 기능은, 데이터 네트워크 노드들이 연관되어 있는 데이터 네트워크내에서 이동할 경우, 스위칭 데이터베이스의 구성 및 재배열시에 연관된 데이터 전송 네트워크에서 데이터 네트워크 노드들을 발견함에 있어 사람이 관여해야할 것을 감소시킨다. 그렇지만, 상기 플러그-앤-플레이 기능에 의해 데이터 네트워크 노드는 적대적 MAC ADDR 공격에 노출된다. 예를 들어, 이 경우만으로 한정되지는 않는데, 데이터 스위칭 노드가 두 개의 데이터 전송 네트워크들간의 연결성을 메워줄 때, 이런 경우 적대적 환경에 대한 노출이 존재한다.

예를 들면, 적대적 환경에서, 적대적 데이터 네트워크 노드는 데이터 스위칭 노드의 자동 스위칭 데이터베이스 재배열 기능의 이점을 취함으로써 특정 MAC ADDR에 할당된 트래픽을 감시(Spy)할 수 있다.

예시적인 하나의 각본에 따르면, 상기한 적대적 데이터 네트워크 노드는 공격할 예정인 데이터 네트워크 노드의 MAC ADDR에 대응하는 소스 MAC ADDR을 갖는 데이터 패킷을 데이터 스위칭 노드를 향해 송출한다. 상기 데이터 스위칭 노드는 데이터 네트워크 노드의 이동을 등록함과 아울러, 적대적인 데이터 네트워크 노드가 연관되어 있는 물리통신포트에 대응하는 PortID로써 PortID 내역을 덮어쓰기 함으로써 상기 MAC ADDR에 대응하는 스위칭 데이터베이스 엔트리를 변경한다. 그 다음, 공격당한 데이터 네트워크 노드의 MAC ADDR에 할당된 모든 PDUs는 데이터 스위칭 노드에 의해 적대적 데이터 네트워크 노드로 전송된다. 상기 MAC ADDR 공격은 공격받은 데이터 네트워크 노드의 기능을 이어받는 적대적 데이터 네트워크 노드만큼 광범위하게 될 수도 있다. 이러한 사건은 현재 고도로 발달된 데이터 스위칭 장치의 의도적인 동작에 따른 것이며, 검출되지 않은 채로 진행할 수도 있다.

따라서, 적대적 MAC ADDR 공격사건을 검출하고 방지하며 또 보고하는 한편 데이터 스위칭 노드들이 우호적 환경 및 적대적 환경 모두에서 동작할 수 있도록 하게 할 필요가 있다.

발명이 이루고자 하는 기술적 과제

본 발명의 일측면에 따라서, 보안기능이 개선된 데이터 스위칭 노드가 제공된다. 상기 데이터 스위칭 노드는 스위칭 데이터베이스 엔트리들을 갖는 스위칭 데이터베이스를 유지한다. 각각의 스위칭 데이터베이스 엔트리는 대응하는 엔트리 보호 플래그(Entry Protection Flag)를 갖는다. 각 엔트리 보호 플래그는, 대응하는 스위칭 데이터베이스 엔트리의 편집을 선택적으로 억제하는데 사용되며 동시에 상기 데이터 스위칭 노드가 우호적 데이터 네트워킹 환경 및 적대적 데이터 네트워킹 환경 모두에서 안전하게 동작하게 하는데 사용된다.

본 발명의 또 다른 측면에 따라서, 보안기능이 개선된 데이터 스위칭 노드가 제공된다. 상기 데이터 스위칭 노드는 다수의 물리통신포트들간의 데이터 트래픽, 특히 물리통신포트들을 통해 도달가능한 데이터 네트워크 세그먼트들에 연결된 데이터 네트워크 노드들간의 데이터 트래픽을 전송한다. 각각의 물리통신포트는 연관된 포트 식별자(이하, PortID라 한다)를 갖는다. 상기 데이터 스위칭 노드의 데이터 네트워크 토폴로지 발견기능은 그 각각이 하나의 PortID에 연관되는 토폴로지 발견 디세이블(disable) 플래그들의 사용을 통해서 한 PortID씩 디세이블 될 수 있다. 상기 토폴로지 발견 디세이블 기능에 의해 적대적 데이터 네트워크 노드가 데이터 전송 네트워크에 참여하는 것이 방지됨으로써, 이에 의해 데이터 스위칭 노드가 우호적 데이터 네트워킹 환경 및 적대적 데이터 네트워킹 환경 모두에서 안전하게 동작할 수 있다.

본 발명의 다른 태양에 따르면, 안전이 보장된 데이터 스위칭 노드가 제공된다. 미지의 수신지를 갖는 데이터 트래픽을 수신할 때, 데이터 스위칭 노드는 선택적인 플러드 제어 메카니즘을 이용하여 상기 데이터 트래픽을 전송한다. 상기 선택적인 플러드 제어 메카니즘이 가동될 때, 상기 데이터 트래픽은 소스 물리통신포트 및 이네이블된 토폴로지 발견 디세이블 기능을 갖는 PortID를 제외하고는 모든 물리통신포트들에 플러드된다. 상기 선택적인 플러드 제어 메카니즘에 의해 적대적 데이터 네트워크 노드들이 미지의 수신지 데이터 트래픽을 도청하는 것을 방지함으로써, 이에 의해 데이터 스위칭 노드는 우호적 데이터 네트워크 환경 및 적대적 데이터 네트워킹 환경 모두에서 안전하게 동작할 수 있다.

적대적 MAC ADDR 공격 사건을 검출하고 방지하며 보고하는 한편, 우호적 환경 및 적대적 환경 모두에서 동작할 수 있는 데이터 스위칭 노드로부터 여러 이점들이 유도된다.

발명의 구성

본 발명의 특징 및 여러 장점들을 더 잘 이해하기 위하여 본 발명의 바람직한 실시예들을 이하 첨부한 도면을 참조하여 단지 예시적인 방법으로 더 상세하게 기술할 것이다.

이하 첨부된 도면을 참조하여 본 발명의 실시예들을 더욱 상세히 기술한다. 도면에 있어서 동일한 요소들에 대해서는 동일한 참조부호를 사용함을 유념하여야 할 것이다.

도1은 우호적 데이터 네트워킹 환경 및 적대적 데이터 네트워킹 환경 모두에서 동작하는, 상호연결된 데이터 네트워크 요소들을 보여주는 네트워크 구성의 개략도이다.

제어기 101을 갖는 데이터 스위칭 노드 100은 스위칭 데이터 베이스(SWitching DataBase; SW DB) 102를 유지한다. 도2, 도3 및 도4를 참조하여 상세하게 설명된 상기 SW DB 102는 데이터 스위칭 노드 100에 연결되어 있는 데이터 네트워크 세그먼트의 현재 구성(토폴로지)을 저장한다. 상기 SW DB 102내에 저장된 토폴로지 정보는, 어느 데이터 네트워크 노드 104가 어느 물리포트 106을 통하여 도착할 수 있는가를 설명해준다. 데이터 네트워크 세그먼트가 하나 이상의 데이터 네트워크 노드를 가질 수 있기 때문에, 하나 이상의 데이터 네트워크 노드 104는 물리포트 106과 연관되어 있는 방식으로 데이터 네트워크 노드가 구성된다.

개개의 데이터 네트워크 노드들 104는 데이터 네트워크 노드 104-B에 나타낸 바와 같이 예를 들어 네트워크 케이블 108과 같은 전용통신링크를 통하여 개개의 물리통신포트 106에 접속한다. 본 발명은 도1에 나타낸 바와 같이 데이터 스위칭 노드 100에 연결되어 있는 버스 네트워크 세그먼트(Bus-Network Segments) 110과 링 네트워크 세그먼트(Ring-Network Segments) 112 등에 동등하게 적용된다.

데이터 스위칭 노드 100은 우호적 데이터 네트워킹 환경 및 적대적 데이터 네트워킹 환경에서 모두 동작하는 것으로 보여진다. 특히, MAC ADDR X를 갖는 데이터 네트워크 노드 104-A, MAC ADDR Y를 갖는 데이터 네트워크 노드 104-B, MAC ADDR W를 갖는 데이터 네트워크 노드 104-C 등은 우호적인 것으로 간주되며, MAC ADDR Y를 갖는 데이터 네트워크 노드 104-E 브로드캐스팅(Broadcasting)은 적대적 컴퓨터로서 간주된다.

도2는 본 발명의 일실시예에 따른 스위칭 데이터베이스 엔트리 보호 기능을 가지며, 또 데이터 스위칭 노드에 의해 유지되는 스위칭 데이터베이스의 세부사항을 도시하는 개략도이다.

상기 SW DB 102의 예시적인 실시는 통상 200에 나타낸 조사표이다. 상기 조사표 200은 로우(Row) 스위칭 데이터베이스 엔트리들 202를 포함한다. 각각의 엔트리는 MAC ADDR, 연관 PortID 및 플래그(Flag)로도 알려진 스위칭 데이터베이스 엔트리 보호 지시자를 저장한다.

도2에 나타낸 바와 같이, 상기 조사표 200은 도1에 나타낸 네트워크 구성을 포함한다. 엔트리 202-0은 MAC ADDR X를 가지며 동시에 물리통신포트 106-1에 연결되어 있는 도1의 데이터 네트워크 노드 104-A에 해당한다. 엔트리 202-1은 MAC ADDR Y를 가지며 동시에 물리통신포트 106-2에 연결되어 있는 도1의 데이터 네트워크 노드 104-B에 해당한다. 엔트리 202-2는 MAC ADDR W를 가지며 동시에 물리통신포트 106-3에 연결되어 있는 도1의 데이터 네트워크 노드 104-C에 해당한다. 엔트리 202-3는 MAC ADDR Z를 가지며 동시에 물리통신포트 106-3에 연결되어 있는 도1의 데이터 네트워크 노드 104-D에 해당한다.

당 기술분야에서, 각각의 엔트리 보호 상태 플래그는 데이터베이스 엔트리 보호 비트로 볼 수 있다. 각각의 엔트리 보호 상태 플래그는, 보호 비트가 설정된 경우에, 연관된 스위칭 데이터베이스 엔트리 202가 보호된다는 것을 설명하는 것이다. 또, 각각의 엔트리 보호 상태 플래그는, 보호 비트가 재설정된 경우에, 연관된 엔트리 202가 보호되지 않는다는 것을 말하는 것이다. 특히, 도2는 엔트리들 202-1 및 202-3에 대하여 설정된 엔트리 보호 비트를 나타낸다. 상기 설정된 연관된 보호 비트들을 갖는 보호된 스위칭 데이터베이스 엔트리들은 변경될 수 없다. 따라서, MAC ADDR과 PortID간의 연관관계를 고정시킬 수 있다.

만일 적대적 데이터 네트워크 노드 104-E가 PortID N상의 MAC ADDR Y를 갖는 PDU의 전송을 시도하는 경우, 데이터 스위칭 노드 100의 제어기 101은 SW DB 102를 참고하여 2부터 N까지의 PortID 연관관계를 변경하기 위하여 MAC ADDR Y에 해당하는 엔트리 202-1의 변경을 시도한다. 그러나, 이러한 시도는 설정된 엔트리 보호 비트에 의해 방지된다. 실패된 시도는 잠재적 방해 사건으로 검출되며 예를 들어 경보 발생법(Alert Generation Method)이나 경보 전달법(Alert Dissemination Method) 등의 당업계에 잘 알려진 방법을 이용하여 보고된다.

상기 스위칭 데이터베이스 엔트리 보호 기능은 동등하며, 조작자에 의해 규정된 스위칭 테이블내에 수동적으로 설정된 스위칭 데이터베이스 엔트리의 고유의 보안 규정을 제공한다. 상기 조작자에 의해 규정된 스위칭 테이블에는 데이터 네트워크 노드와 데이터 스위칭 노드간의 연관관계가 명백하게 정의되어 있다.

엔트리 보호 상태 플래그는 예를 들어 관리 콘솔(Management Console)과 같은 제어 인터페이스에 의해 설정될 수 있다. 다른 방법도 있는데, 이 방법은 보호된 엔트리들 형태의 스위칭 데이터베이스 102에, 예를 들어, 하드 드라이브, 소거 및 프로그램 가능 읽기용 기억장치(消去-可能-用記憶裝置, Electronically Erasable and Programmable Read Only Memory, E(E)PROM)등의 보안기능이 개선된 영구 기억장치를 로딩(loading)하는 것을 포함한다.

이상에서 나타낸 바와 같이, 만일 SW DB 102내의 엔트리가 보호되는 경우에도, 엔트리들 202-2 및 202-3에 나타낸 바와 같이, 서로 다른 MAC ADDRs가 동일한 PortID에 연관되는 것을 막지 못한다. 데이터 스위칭 노드 100의 물리통신포트 106이 다중노드 데이터 네트워크 세그먼트(112, 110)에 연결되어 있는 경우, 하나 이상의 MAC ADDR가 하나의 PortID에 연관될 수 있다.

일반적으로, 상기 조사표 200에서의 기억장치의 한도로 인하여 한정된 개수의 엔트리들만이 저장될 수 있다. 만일 새로운 소스 MAC ADDR이 데이터 스위칭 노드 100에 수신되는 경우에는, 조사표 200으로 최대 개수의 엔트리들이 도달한 후, 최초로 사용된 엔트리 또는 최후에 사용된 엔트리 중 어느 하나가 SW DB 102로부터 제거됨으로써 새로운 MAC ADDR이 수용된다. SW DB 102내 합법적인 엔트리들을 결국 폐기하고마는 데이터 스위칭 노드 100에 의해 기억되는 위조 MAC ADDRs를 갖는 다수의 PDUs의 전송을 통하여, 적대적 데이터 네트워크 노드 104-E는 데이터 스위칭 노드 100을 통과하는 데이터 트래픽의 감시를 시도할 수 있다. 이 과정은 SW DB 102 중의 합법적인 MAC ADDRs의 "플러시(Flushing)"로 알려져 있다.

합법적인 라우팅 엔트리들이 폐기되는 경우, 폐기된 라우팅 엔트리들에 대응하는 합법적인 MAC ADDRs 수신지를 갖는 PDUs는, 적대적 데이터 네트워크 노드에 연결되어 있는 물리통신포트를 포함하는 모든 물리통신포트로 플러드된다. 이에 의해, 적대적 데이터 네트워크 노드는 데이터 스위칭 노드 100에 의해 처리되는 데이터 트래픽을 감시할 수 있다.

도3은 본 발명의 일실시예에 따른 각각의 물리통신포트에 대한 제어기능을 가지며, 동시에 데이터 스위칭 노드에 의해 유지되는 스위칭 데이터베이스의 세부사항을 보여주는 개략도이다.

토폴로지 발견 디세이블 기능(Topology Discovery Disable feature)은 제어 비트(또는 플래그)를 이용하여 실시될 수 있다. 상기 각각의 제어 비트는 하나의 PortID에 연관된다. 이와는 다른 실시들이 가능하며 도시한 관형상의 표시 300에 한정되지 않는다. PortID 3에 대하여 행해진 것처럼 토폴로지 발견이 특정 PortID에 대하여 디세이블되는 경우, 상기 PortID에 연관된 추가적인 스위칭 데이터베이스 엔트리들이 SW DB 102에 추가되는 것이 방지된다.

예를 들어, 토폴로지 발견은 네트워크 설정에 사용될 수 있으며, 또 특정 PortID에 연관된 SW DB 102로의 부가적 변경을 방지하도록 디세이블될 수 있다. 디세이블된 토폴로지 발견기능을 갖는 물리통신포트상의 데이터 스위칭 노드 100에 부가적인 소스 MAC ADDRs가 수신되는 경우, 경보가 발생될 수 있다.

본 발명의 또 다른 실시예에 따르면, 토폴로지 발견 제어에 의해 물리통신포트에 연관된 MAC ADDRs는 PortID당 하나를 기본으로하여 실시된 상한까지 동적으로 추가될 수 있다. 이에 의해, 제어된 양의 발견이 가능하지만 SW DB 102내의 모든 합법적인 엔트리들의 플러시를 방지할 수 있다.

도시한 미지의 수신지 플러드 제어 기능은 통신포트에 의한 제어 비트(또는 플래그)로서 실시될 수 있으나 이것에 국한되지 않는다. 제어 비트가 설정된 경우에는 미지의 수신지 플러드 제어 기능이 이네이블되며, 제어 비트가 재설정되는 경우에는 미지의 수신지 플러드 제어 기능이 디세이블된다.

상기 미지의 수신지 플러드 제어 기능은 선택된 통신포트로 PDU를 반복 전송하는 것을 방지하는데 사용된다. 이 기능은 선택된 통신포트들에 연결되어 있는 적대적 데이터 네트워크 노드들이 미지의 수신지 데이터 트래픽을 도청하는 것을 방지한다.

도4는 본 발명의 일실시예에 따른 데이터 스위칭 노드의 제어기능을 보여주는 개략도이다.

본 발명의 또 다른 실시예에 따르면, 제어 기능은 데이터 스위칭 노드의 모든 물리통신포트에 대한 보안 자원을 실행하는 전역범위(Global Scope)를 갖는다.

상기 전역 제어 기능(Global Control Feature)은 통상 전역 토폴로지 발견 제어 비트를 포함하며 400에 도시되어 있다. 상기 전역 토폴로지 발견 제어 비트가 설정되지 않은 경우, 스위칭 데이터베이스 엔트리들은 SW DB 102에 자동적으로 추가될 수 있다.

물론 관리 콘솔에 의해 추가된 스위칭 데이터베이스 엔트리들에는 영향을 미치지 않는다. 상기 전역 토폴로지 발견 제어 비트가 재설정되는 경우, 토폴로지 발견 제어는 상술한 바와 같이 한 포트씩 실행된다.

도4A에 나타낸 전역 미지 수신지 플러드 제어기능(Global Unknown Destination Flood Control Feature)은 토폴로지 발견 디세이블 기능과 관련하여 사용되며 하기의 이점을 갖는다.

특정 물리통신포트에 연결되어 있는 모든 데이터 네트워크 노드들을 발견한 이후에, 미지의 수신지를 갖는 PDUs를 그 통신포트로 플러드할 필요가 없는데, 이는 통신포트에 연결되어 있는 모든 데이터 네트워크 노드들을 알 수 있기 때문이다. 이것은 물리통신포트로 이런 PDUs를 반복 전송시에 PDU 처리량을 줄인다.

본 발명의 또 다른 실시예에 따르면, 이상에서 제시된 모든 제어 기능은 도4에 나타낸 바와 같이 단일의 제어 비트에 의해 활성화될 수 있다.

도5는 본 발명의 일실시예에 따라서 데이터 스위칭 노드에서의 MAC ADDR 공격의 검출, 방지 및 보고를 실시하는 보안기능이 개선된 PDU 전송과정을 보여주는 흐름도이다.

단계 500에서 소스 PortID를 갖는 소스 물리통신포트로부터 PDU를 수신함으로써 보안기능이 개선된 PDU 전송 과정이 개시된다. 단계 502에서, 데이터 스위칭 노드 100에 연관된 제어기 101은 라우팅 정보를 위하여 상기 수신된 PDU의 헤더를 검사하고 적어도 소스 MAC ADDR을 추출한다. 단계 504에서, 소스 MAC ADDR에 근거하여 SW DB 102에게 질의한다.

상기 단계 504에서 소스 MAC ADDR에 대응하는 스위칭 데이터베이스 엔트리가 SW DB 102에서 발견되는 경우에는, 단계 506으로 과정이 넘어가서 상기 PortID가 엔트리에 저장하였으며 상기 소스 PortIDs가 일치하는지 여부를 결정한다.

만일 단계 506에서 PortIDs가 일치한다고 결정되면, PDU를 전송하면서 과정이 단계 508로 진행된다.

만일 단계 506에서 PortIDs가 일치하지 않는다고 결정되는 경우에는 단계 510으로 진행하며, 이 단계에서 엔트리가 보호되고 있지 않다는 것으로 사실이 확인된다면, 단계 512로 가서 스위칭 데이터베이스 엔트리의 변경을 시도한다.

만일 단계 510에서 스위칭 엔트리가 보호되고 있는 것으로 발견되지 않는다면 엔트리는 단계 512에서 변경되며, PDU를 전송하면서 과정이 단계 508로 넘어간다.

만일 단계 510에서 스위칭 엔트리가 보호되고 있는 것으로 발견된다면, 과정은 단계 514로 진행하고 경보가 발생된다. 상기 과정에서 PDU가 폐기된 다음, 단계 500으로부터 재개됨으로써 과정이 지속된다.

만일 단계 504에서 소스 MAC ADDR에 대응하는 스위칭 데이터베이스 엔트리가 SW DB 102에서 발견되지 않는 경우, 단계 515 및 단계 516에서 실행되는 토폴로지 발견이 소스 PortID에 대하여 억제되는지 여부를 조건으로 하여, 과정은 SW DB 102로 새로운 엔트리를 추가하는 것을 시도한다.

만일 토폴로지 발견이 전체 데이터 스위칭 노드 100에 대하여 전역적으로 디세이블되는 경우에는, 과정이 단계 514에서 재개되고 경보가 발생된다. 만일 토폴로지 발견이 전체 데이터 스위칭 노드 100에 대하여 전체적으로 디세이블되지 않는 경우에는, 토폴로지 발견 제어가 소스 PortID에 대하여 실시된다.

단계 516에서 만일 토폴로지 발견이 소스 PortID에 대하여 이네이블 되는 경우, 단계 518에서 SW DB 102에 새로운 엔트리가 추가되며, PDU를 전송하면서 단계 508로 과정이 지속된다.

단계 516에서 만일 토폴로지 발견이 소스 PortID에 대하여 억제되는 경우, 과정은 단계 514에서 재개되고 경보가 발생된다.

PDU를 전송시에, 제어기 101은 PDU 라우팅 정보를 감시하며, 이에 의해 적어도 수신지 MAC ADDR을 추출할 수 있다. 상기 과정은 단계 520로 가서, 수신지 MAC ADDR에 근거하여 SW DB 102에게 질의한다.

상기 SW DB 102가 수신지 MAC ADDR에 대응하는 스위칭 엔트리를 포함하는 경우, 상기 PDU는 단계 522에서 상기 엔트리에 지정된 PortID로 전송된다. 상기 단계 522에서의 PDU 전송에 후속하여, 단계 500에서 상기 과정이 재개된다.

만일 SW DB 102가 수신지 MAC ADDR에 대응하는 스위칭 엔트리를 포함하지 않는 경우, 모든 물리통신포트를 포함하는 포트 플러드 리스트가 단계 524에서 발생된다. 그 다음, 단계 526에서 상기 포트 플러드 리스트로부터 소스 PortID가 제거된다. 단계 527에서, 포트 미지 수신지 플러드 제어 비트(Port Unknown Destination Flood Control Bit)가 설정되어 있는 모든 PortIDs이 또한 상기 포트 플러드 리스트로부터 제거된다.

전역 미지 수신지 플러드 제어 기능이 활성화되어 있다는 것을 조건으로 하여, 이 조건을 단계 528에서 확인한 다음, 만일 단계 532로 가게 되는 경우에는 PDU가 반복되어 포트 플러드 리스트내의 물리통신포트들로 플러드된다.

만일 전역 미지 수신지 플러드 제어기능이 이네이블된 경우, 디세이블된 토폴로지 발견을 갖는 모든 포트들은 단계 532에서 모든 물리통신포트들로 플러드되기 이전에 단계 530에서 포트 플러드 리스트로부터 제거된다.

남아있는 플러드 리스트내의 모든 포트들로 PDU가 플러드되는 것에 이어, 과정이 단계 500으로부터 재개된다.

발명의 효과

본 발명의 엔트리 보호 플래그는, 대응하는 스위칭 데이터베이스 엔트리의 편집을 선택적으로 억제하는데 사용되며 동시에 상기 데이터 스위칭 노드가 우호적 데이터 네트워킹 환경 및 적대적 데이터 네트워킹 환경 모두에서 안전하게 동작하게 하는데 사용된다.

본 발명의 토폴로지 발견 디세이블 기능에 의해 적대적 데이터 네트워크 노드가 데이터 전송 네트워크에 참여하는 것이 방지됨으로써, 이에 의해 데이터 스위칭 노드가 우호적 데이터 네트워킹 환경 및 적대적 데이터 네트워킹 환경 모두에서 안전하게 동작할 수 있다.

본 발명의 선택적인 플러드 제어 메카니즘에 의해 적대적 데이터 네트워크 노드들이 미지의 수신지 데이터 트래픽을 도청하는 것을 방지함으로써, 이에 의해 데이터 스위칭 노드는 우호적 데이터 네트워크 환경 및 적대적 데이터 네트워킹 환경 모두에서 안전하게 동작할 수 있다.

본 발명에서 제시된 실시예는 단지 예시적인 것이며 당업계의 업자는 상술한 실시예에 대한 변경이 본 발명의 요지를 벗어나지 않고서 가능하다고 인정할 것이다. 또한, 상기 본 발명의 범위는 오직 첨부하는 청구항에 의해서만 정의된다.

도면의 간단한 설명

도1은 우호적 네트워킹 환경 및 적대적 네트워킹 환경 모두에서 동작하는 상호연결된 데이터 네트워크 요소들을 도시하는 네트워크 구성의 개략도.

도2는 본 발명의 일실시예에 따른 스위칭 데이터베이스 엔트리 보호기능을 갖는, 데이터 스위칭 노드에 의해 유지되는 스위칭 데이터베이스의 세부사항을 도시하는 개략도.

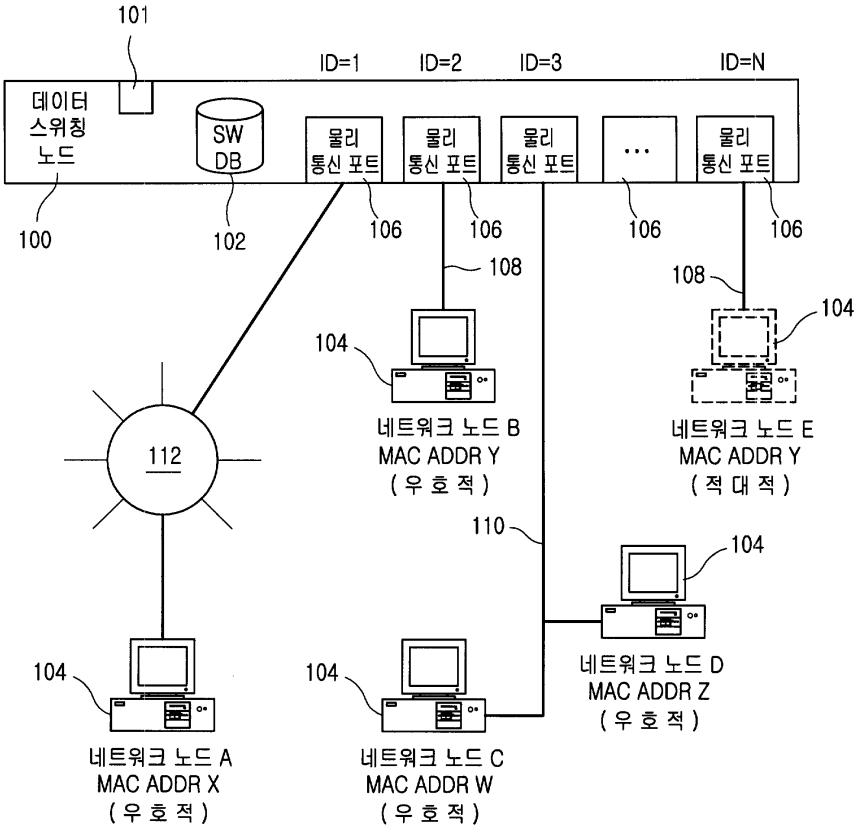
도3은 본 발명의 일실시예에 따른 각각의 물리통신포트에 대한 제어기능을 갖는, 데이터 스위칭 노드에 의해 유지되는 스위칭 데이터베이스의 세부사항을 도시하는 개략도.

도4는 본 발명의 일실시예에 따른 데이터 스위칭 노드의 제어기능을 도시하는 개략도.

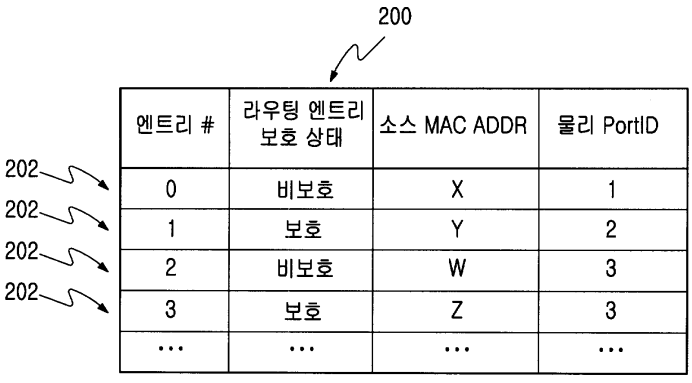
도5는 본 발명의 일실시예에 따른 데이터 스위칭 노드에서의 MAC ADDR 공격을 검출하고 방지하며 보고하는 보안기능이 개선된 PDU 전송과정을 보여주는 흐름도.

도면

도면1

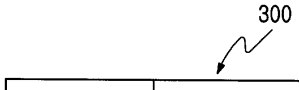


도면2



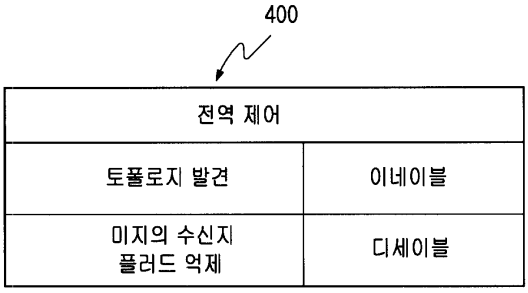
엔트리 #	라우팅 엔트리 보호 상태	소스 MAC ADDR	물리 PortID
0	비보호	X	1
1	보호	Y	2
2	비보호	W	3
3	보호	Z	3
...	...	...	...

도면3

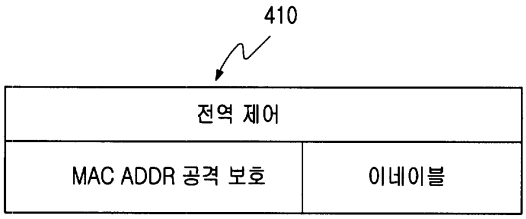


물리 PortID	토폴로지 발견	미지의 수신지 플러드 억제
1	이네이블	이네이블
2	이네이블	디세이블
3	디세이블	이네이블
...	...	...
N	...	...

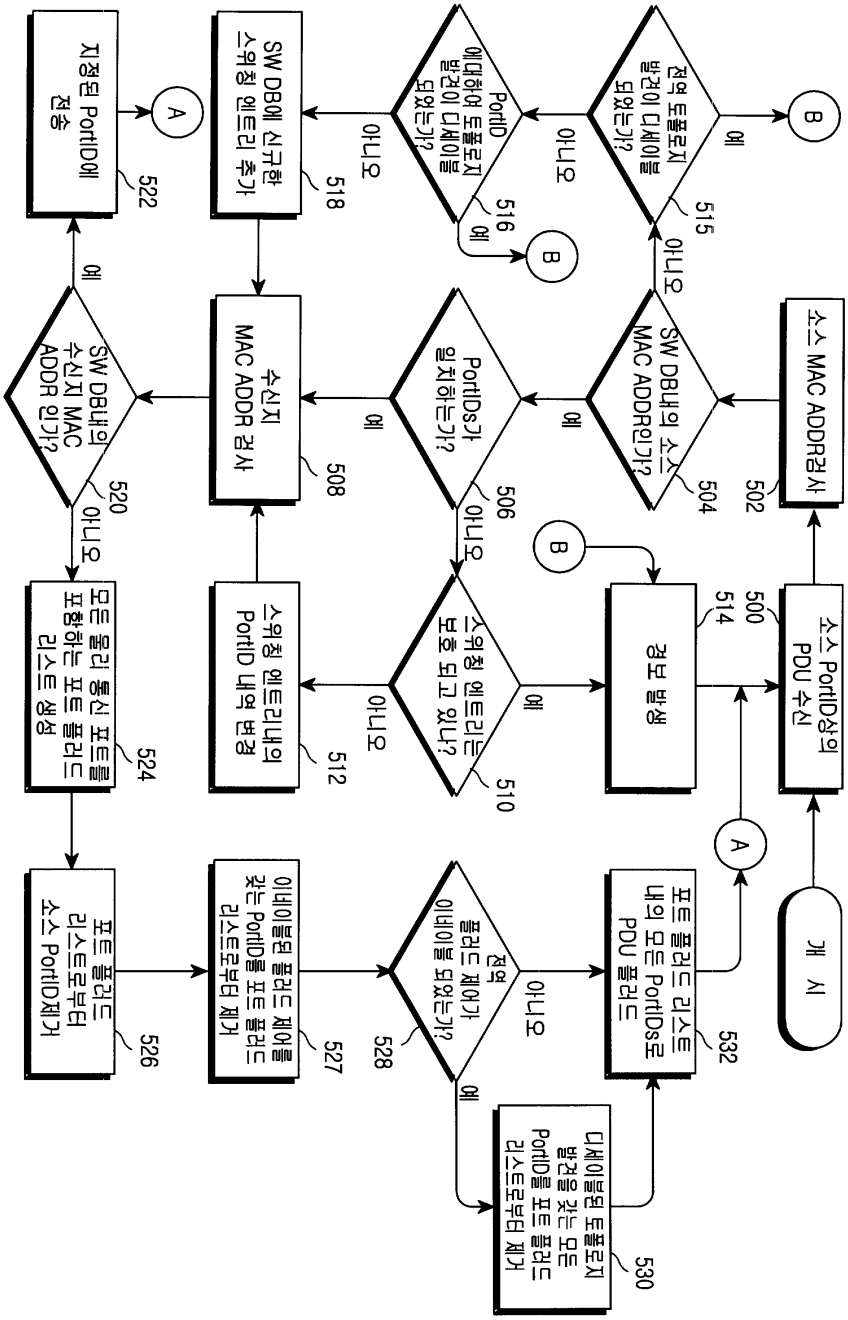
도면4a


400
전역 제어
토폴로지 발견
이네이블
미지의 수신지
플러드 억제
디세이블

도면4b


410
전역 제어
MAC ADDR 공격 보호
이네이블

도면5


개 시
소스 PortID상의 PDU 수신
소스 MAC ADDR검사
502
SW DB내의 소스 MAC ADDR인가?
504
예
아니오
전역 토폴로지 발견이 디세이블 되었는가?
515
예
아니오
B
PortID 에대하여 토폴로지 발견이 디세이블 되었는가?
516
예
아니오
B
PortIDs가 일치하는가?
506
예
아니오
B
스위칭 엔트리는 보호 되고 있나?
510
예
아니오
경보 발생
500
514
스위칭 엔트리내의 PortID 내역 변경
512
수신지 MAC ADDR 검사
508
SW DB에 신규한 스위칭 엔트리 추가
518
SW DB내의 수신지 MAC ADDR 인가?
520
예
아니오
지정된 PortID에 전송
522
A
모든 물리 통신 포트를 포함하는 포트 플러드 리스트 생성
524
포트 플러드 리스트로부터 소스 PortID제거
526
이네이블된 플러드 제어를 갖는 PortID를 포트 플러드 리스트로부터 제거
527
전역 플러드 제어가 이네이블 되었는가?
528
예
아니오
디세이블된 토폴로지 발견을 갖는 모든 PortID를 포트 플러드 리스트로부터 제거
530
포트 플러드 리스트 내의 모든 PortIDs로 PDU 플러드
532
A