2001 년 한국정보처리학회 추계 학술발표논문집 제 8 권 제 2 호

ATM 기반 MPLS LER 에서 패킷 필터링 기능을 지원하기 위한 포워딩 엔진 제어 기법

박재형 O, 윤현정, 전병천
한국전자통신연구원 네트워크연구소 인터넷기술연구부
e-mail : jhpark@etri.re.kr

A Control Scheme of Forwarding Engines for Supporting Packet Filtering in ATM-based MPLS LER

Jaehyung Park O, Hyun-Jeong Yun, Byung-Chun Jeon
Internet Technology Dept., Network Laboratory, ETRI

요 약

최근 인터넷의 급속한 사용 증가로 인해 전송 링크의 광대역 지원과 멀티미디어 트래픽의 QoS 보장 문제, 향상된 IP 서비스의 제공 문제 해결은 필수적이다. MPLS 기술은 IP 의 유연성과 확장성을 제공할 수 있는 패러다임의 하나이다. MPLS 망의 경계에 위치하는 LER 은 링크 계층 뿐만 아니라 IP 계층에서도 패킷을 전달해야 한다. 본 논문에서는 하드웨어 포워딩 엔진을 갖는 MPLS LER 에서, 패킷 필터링 기능을 지원하기 위해서 포워딩 엔진을 제어하기 위한 기법에 대해서 기술한다. 이러한 패킷 필터링 기능은 MPLS LER 에 firewall 기능을 제공하는데 응용될 수 있다.

1. 서론

오늘날 전자상거래, 음성 기반 응용 및 멀티미디어 서비스, WWW 등의 이용이 증가함에 따라 인터넷 트래픽의 양이 빠른 속도로 증가하고 있고, 또한 이들의 차등화 된 서비스 제공을 요구하고 있다. 이러한 요구사항을 충족시켜주기 위하여 단순히 링크의 속도만을 증가 시켜 주는 것이 아니라 향상된 IP 서비스를 제공해 주면서 QoS 를 만족시켜 줄 수 있는 네트워크 구성 요소의 필요성이 대두되고 있다[2].

이러한 요구 사항을 만족시켜 주기 위하여 MPLS (Multiprotocol Label Switching)는 IETF (Internet Engineering Task Force)에서 표준으로 채택되었다[3]. MPLS 도메인에는 에지에 존재하는 LSR(Label Switching Router)과 LER(Label Edge Router)두 가지의 라우터가 존재한다. MPLS 네트워크 도메인에는 크게 두 구성요소가 있는데, 도메인 에지에 존재하여 일반 IP 패킷에 레이블을 붙여 포워딩해 주는 LER (Label Edge Router)과 레이블과 입력 인터페이스에 따라 레이블 Swapping 과 포워딩을 수행하는 LSR (Label Switching Router)이 있다.

ATM 시스템을 기반으로 구성된 국가망에서 인터넷 서비스를 제공하기 위해서 개발 중인 MPLS LER 은 IP 패킷을 고속으로 처리하기 위해서 다수의 포워딩 엔진을 갖는 시스템으로[1] 하드웨어 포워딩 엔진은 입력되는 패킷의 헤더를 분석하여 출력하여야 할 인터페이스를 결정하여 전송한다.

네트워크에 존재하는 라우터에서 기본적인 firewall 은 특정 소스에서 유입되는 트래픽을 차단하거나 특정 목적지로 향하는 트래픽을 차단하는 기능에 의해서 제공된다[6]. 본 논문에서는 ATM 기반 MPLS LER 구조에 대해서 설명하고, MPLS LER 의 하드웨어 포워딩 엔진의 룩업 제어기의 테이블을 변경하여 IP 패킷 필터링 기능을 제공하는 방안에 대해서 기술한다.

2. ATM 기반 MPLS LER

2.1 ATM 기반 LER 구조

LER 은 MPLS 도메인의 LSR 과 연결되어야 하는 동시에 non-MPLS 도메인의 일반적인 IP over ATM 호스트 및 라우터, PPP 호스트와도 연결되어 연동하여야

한다. IP 도메인과 MPLS 도메인 사이에서 고속의 패킷 전달을 지원하기 위해서, LER 은 그림 1 과 같이 다수개의 하드웨어 포워딩 엔진을 갖는 구조로 이루어져 있다.

ACC 는 ATM Connection Controller 로서 ATM 프로토콜 및 자원을 관리하고, PIM 은 Processor Interface Module 로서 다수개의 프로세서와 스위치간의 데이터 채널을 지원한다. AIM 은 ATM Interface Module 로서 16 개의 STM-1 또는 4 개의 STM-4c 인터페이스를 지원한다. MIM 은 MPLS Interface Module 로서 LER 에서 MPLS 서비스를 지원하기 위해서 필요한 모듈로서 4 개의 622Mbps 의 포워딩 엔진으로 구성되어 있으며, AIM 과 같은 인터페이스를 갖는다.

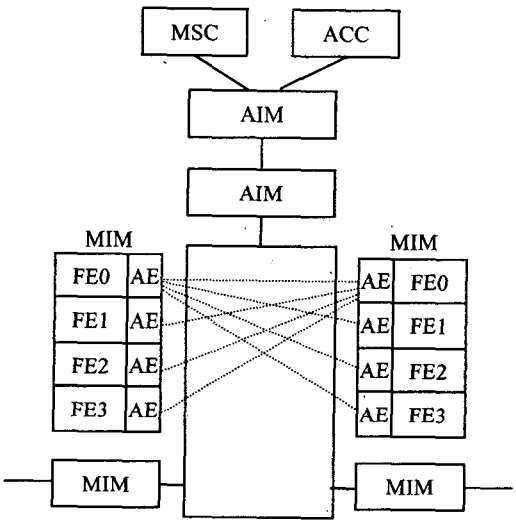

그림 1. LER 의 구조

MSC 는 RIP, OSPF, BGP, LDP 와 같은 라우팅 프로토콜을 수행하여 라우팅 정보와 레이블 정보를 유지한다[4]. 또한, IP 네트워크 인터페이스를 유지하고, 내부 스위치의 연결 자원들도 유지한다. 그리고, 각 포워딩 엔진의 룩업 테이블을 생성하여 포워딩 엔진에 전달하는 역할도 수행한다.

2.2 하드웨어 포워딩 엔진

하드웨어 포워딩 엔진[5]은 두 개의 기능으로 구분된다. 하나는 외부 ATM 인터페이스를 통해 입력되는 IP 패킷에 대해서 패킷 전달 수행하는 IP 패킷 포워딩 기능과 스위치로부터 들어오는 패킷에 대한 VC 머징 기능이다. 포워딩 엔진은 외부 ATM 인터페이스와 ATM 스위치 인터페이스, ATM SAR, IP 룩업 제어기, VC 머징 제어기로 구성되어 있다.

하드웨어 포워딩 엔진에서 IP 패킷 처리는 다음과 같은 순서로 이루어진다. 1) 입력된 패킷에서 IP 헤더를 추출하고, 2) 입력 인터페이스에 대한 패킷의 형태를 분석하고, 3) 헤더에 오류가 없는지 점검하고, 4) 룩업 제어기에 의해서 패킷이 전달되어야 할 인터페이스를 결정하고, 5) MPLS 의 LSP 로 전달될 경우 Label 을 검색하고, 6) 헤더를 변경하여 전달하는 과정으로 수행된다.

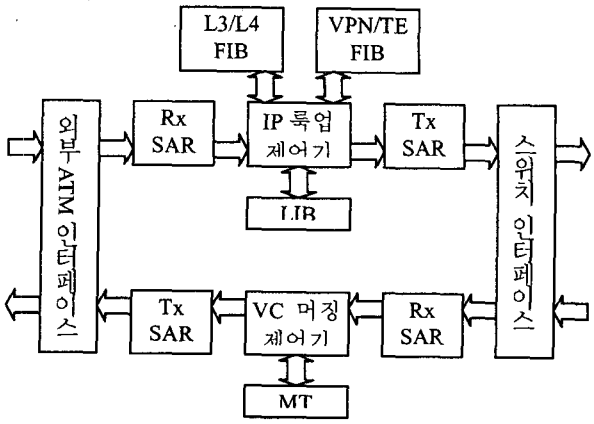

그림 2. IP 포워딩 엔진의 구조

이 과정에서 IP 룩업 제어기에는 네 가지 종류의 FIB 테이블이 있으며, 각각은 목적지의 주소만으로 구성된 L3 테이블과 출발지/목적지/포트로 구성된 L4 테이블과 VPN 용 FIB 테이블과 전용 회선 서비스 및 실시간 서비스를 위한 TE 용 FIB 테이블이 있다. 룩업 제어기는 L4 테이블, TE 테이블, L3 테이블 순서로 탐색하여 출력하여야 할 인터페이스를 결정한다.

3. 패킷 필터링 기능을 위한 포워딩 엔진 제어 기법

본 절에서는 MPLS LER 에서 라우팅 테이블 변경에 의한 하드웨어 포워딩 엔진의 포워딩 테이블 제어 방법에 대해서 기술하고, 패킷 필터링 기능을 제공하기 위한 포워딩 엔진을 제어하는 기법을 제시한다.

3.1 포워딩 테이블 변경

MPLS LER 에서 라우팅 테이블이 변경되는 경우는 ① 새로운 IP 를 갖는 인터페이스가 추가되거나, ② 정적 경로를 설정하거나, ③ 라우팅 프로토콜에 의해서 새로운 경로가 생성되거나, ④ 기존 인터페이스를 제거하거나, ⑤ 정적 경로를 삭제하거나, ⑥ 라우팅 프로토콜에 의해서 경로를 제거하는 경우가 있다. 이것은 크게 추가되는 경우와 삭제되는 경우 두 가지로 분류할 수 있다.

첫 번째, ①의 경우와 같이 새로운 인터페이스가 추가되는 경우의 절차는 다음과 같다.

1. IP 주소와 포트, vpi, vci 를 갖는 연결 설정 요구
2. IP 주소 중복성 및 포트, vpi, vci 의 중복성 검사 후 이미 존재하는 경우 Fail
3. 해당 포워딩 엔진의 외부 ATM 인터페이스 쪽의 Rx/Tx SAR 에 채널 Open
4. 해당 포워딩 엔진의 포워딩 테이블에 MSC 에 할당된 주소에 대해서 EFC 를 통해 MSC 로 전달될 수 있도록 추가
5. 다른 포워딩 엔진의 스위치 인터페이스 쪽의 Tx SAR 에 채널 Open
6. 다른 포워딩 엔진의 포워딩 테이블에 추가된 IP 주소에 대해서 5 번에서 Open 된 채널로 전달될 수 있도록 추가

7. 해당 포워딩 엔진의 스위치 인터페이스로 다른 포워딩 엔진에서부터의 스위치를 통한 연결이 설정되도록 Rx SAR 채널 Open
8. 7 번에서 Open 된 Rx 채널이 3 번에서 Open 된 Tx 채널로 전달될 수 있도록 머징 테이블에 추가

두 번째, ②와 ③의 경우와 같이 새로운 경로가 추가되는 경우의 절차는 다음과 같다.

1. Next hop 을 갖는 새로운 경로 추가 요구
2. 다른 포워딩 엔진의 라우팅 자원 중에 Next Hop 이 MSC 에 이미 존재하는 인터페이스인지 검사 후 존재하지 않으면 Fail
3. 존재한다면 각 포워딩 엔진에서 스위치로 향하는 Tx SAR 에 Open 된 채널을 검색
4. 다른 포워딩 엔진의 포워딩 테이블에 추가된 IP 주소에 대해서 3 번에서 검색된 채널로 전달될 수 있도록 추가

세 번째, ④의 경우와 같이 기존 인터페이스가 삭제되는 경우의 절차는 다음과 같다.

1. IP 주소와 포트, vpi, vci 를 갖는 연결 해제 요구
2. 해당 포워딩 엔진의 vpi, vci 에 해당하는 값을 갖는 외부 ATM 인터페이스 쪽의 Rx/Tx SAR 에 채널 Open 된 채널 해제
3. 다른 포워딩 엔진에서 해당 인터페이스로 연결을 위해서 스위치 인터페이스 쪽의 Tx SAR 에 채널 Open 된 채널 해제
4. 해당 포워딩 엔진의 포워딩 테이블에 MSC 에 할당된 주소에 대해서 EFC 를 통해 MSC 로 전달될 수 있도록 추가된 엔트리 삭제
5. 다른 포워딩 엔진에 추가된 머징 테이블 중 삭제될 IP 주소와 동일한 엔트리 삭제
6. 해당 포워딩 엔진의 스위치 인터페이스로 다른 포워딩 엔진에서부터의 스위치를 통한 연결이 설정되도록 Rx SAR 채널 Open 된 채널을 IP 주소로 검색하여 삭제
7. 다른 포워딩 엔진의 포워딩 테이블에 추가된 IP 주소에 대해서 추가된 엔트리 삭제

네 번째, ⑤와 ⑥의 경우와 같이 기존 경로가 삭제되는 경우의 절차는 다음과 같다.

1. Next hop 을 갖는 기존 경로 삭제 요구
2. 다른 포워딩 엔진의 라우팅 자원 중에 Next Hop 이 MSC 에 이미 존재하는 인터페이스인지 검사 후 존재하지 않으면 Fail
3. 존재한다면 각 포워딩 엔진에서 스위치로 향하는 Tx SAR 에 Open 된 채널을 검색
4. 다른 포워딩 엔진의 포워딩 테이블에 추가된 IP 주소에 대해서 3 번에서 검색된 채널로 전달될 수 있도록 추가된 엔트리 삭제

포워딩 엔진의 포워딩 테이블을 제어하기 위한 메시지는 다음과 같은 구조체에서 필요한 부분을 추출하여 구성할 수 있다. 그리고, out_ch 값이 0 일 경우에는 '폐기됨'을 의미한다고 정의한다.

```
typedef struct {
    unsigned int        msg_type; /* Add/Delete */
    unsigned int        sour_addr;
    unsigned int        sour_netmask;
    unsigned int        dest_addr;
    unsigned int        dest_netmask;
    unsigned int        sour_port;
    unsigned int        dest_port;
    unsigned int        out_ch;
    unsigned int        pkt_type;
    unsigned int        label;
    unsigned int        ttl;
} Data_Req;
```

다음 절에서는 IP 패킷 필터링 기능을 지원하는 방법으로 특정 입력 인터페이스에서 들어오는 패킷을 거부/허용하는 방법과 특정 출력 인터페이스로 나가는 패킷을 거부/허용하는 방법에 대해서 살펴본다.

3.2 특정 입력 인터페이스에 대한 IP 패킷 필터링

특정 입력 인터페이스에서 유입되는 패킷에 대한 필터링은 해당 포워딩 엔진에서의 거부 및 허용을 제어함으로써 가능하다. 그림 3 은 MPLS LER 에 유입되는 트래픽 중 인터페이스 ls01 에서 들어오는 패킷 중에서 출발지가 192.18.10/24 인 서브넷인 패킷만을 거부하는 경우를 나타낸다. 또한, ls00 에서 들어오는 패킷에 대해서 목적지가 193.20.16/24 로 향하는 패킷을 거부하는 경우를 나타낸다.

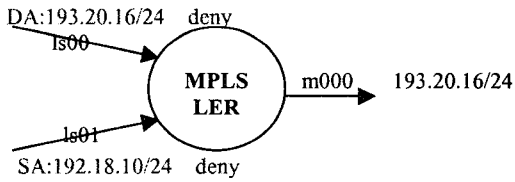

그림 3. 입력 인터페이스에 대한 거부의 예

입력 인터페이스의 패킷에 대해서 거부하는 경우는 인터페이스에 해당하는 포워딩 엔진의 L3/L4 테이블을 변경하면 된다. 테이블에 변경하는 절차는 다음과 같다(IN_DENY_FILTER).

1. 출발지(SA)를 포함하여 필터링을 할 경우에는 L4 룩업 테이블에 추가하고 처리방법을 버림으로 함.
2. 목적지(DA)만을 포함하여 필터링을 할 경우에는 L3 룩업 테이블에 추가하고 처리방법을 버림으로 함.

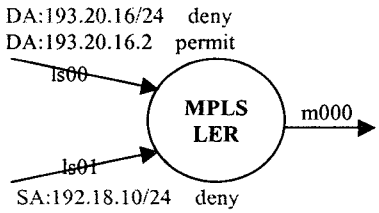

그림 4. 입력 인터페이스에 대한 허용의 예

그림 4 는 그림 3 의 상황에서 ls00 에서 들어오는 패킷 중 193.20.16.2 로 가는 패킷만을 허용하는 경우를 표현하는 것이다.

테이블 변경 절차는 다음과 같다(IN_PERMIT_FILTER).

1. 출발지(SA)를 포함하여 필터링을 할 경우에는 L4 룩업 테이블에 추가하고 새로운 경로가 추가되는 경우와 마찬가지로 수행.
2. 목적지(DA)만을 포함하여 필터링을 할 경우에는 L3 룩업 테이블에 추가하고 새로운 경로가 추가되는 경우와 마찬가지로 수행.

3.3 특정 출력 인터페이스에 대한 IP 패킷 필터링

특정 출력 인터페이스로 전달되는 패킷에 대한 필터링은 해당 포워딩 엔진을 제외한 다른 포워딩 엔진에서의 거부 및 허용을 제어함으로써 가능하다. 그림 5 는 MPLS LER 에서 나가는 트래픽 중 인터페이스 ls01 으로 나가는 패킷 중에서 목적지가 192.18.10/24 인 패킷만을 거부하는 경우를 나타낸다. 또한, ls00 으로 나가는 패킷에 대해서 출발지가 193.20.16/24 서브넷인 패킷을 거부하는 경우를 나타낸다.

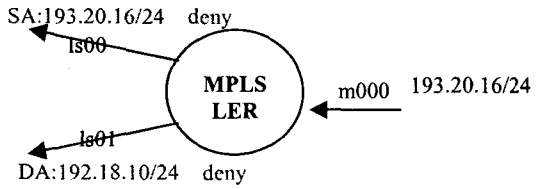

그림 5. 출력 인터페이스에 대한 거부의 예

출력 인터페이스의 패킷에 대해서 거부하는 경우는 인터페이스에 해당하는 포워딩 엔진을 제외한 다른 포워딩 엔진 전체의 L3/L4 테이블을 변경하면 된다. 테이블에 변경하는 절차는 다음과 같다(OUT_DENY_FILTER).

1. 출발지(SA)를 포함하여 필터링을 할 경우에는 L4 룩업 테이블에 추가하고 처리방법을 버림으로 함.
2. 목적지(DA)만을 포함하여 필터링을 할 경우에는 L3 룩업 테이블에 추가하고 처리방법을 버림으로 함.

그림 6 은 그림 5 의 상황에서 ls00 으로 나가는 패킷 중 출발지가 193.20.16.2 인 패킷만을 허용하는 경우를 표현하는 것이다.

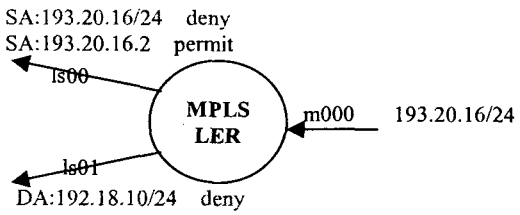

그림 4. 입력 인터페이스에 대한 허용의 예

테이블 변경 절차는 다음과 같다(OUT_PERMIT_FILTER).

1. 출발지(SA)를 포함하여 필터링을 할 경우에는 L4 룩업 테이블에 추가하고 새로운 경로가 추가되는 경우와 마찬가지로 수행.
2. 목적지(DA)만을 포함하여 필터링을 할 경우에는 L3 룩업 테이블에 추가하고 새로운 경로가 추가되는 경우와 마찬가지로 수행.

기술한 네 가지의 필터, IN_DENY_FILTER, IN_PERMIT_FILTER, OUT_DENY_FILTER, OUT_PERMIT_FILTER,를 이용하여 MPLS LER 에서 기본적인 IP 패킷 필터링 기능을 제공할 수 있다.

4. 결론

본 논문에서는 ATM 기반의 MPLS LER 시스템의 구조 및 포워딩 엔진의 구조에 대해서 설명하였다. 또한, 라우팅 테이블의 변경에 따른 하드웨어 포워딩 엔진의 포워딩 테이블을 변경하는 절차에 대해서 고찰하였으며, 기본적인 IP 패킷의 필터링을 지원하기 위해서 포워딩 테이블의 변경 절차에 대해서 제시하였다.

참고문헌

[1] [1] 한국전자통신연구원, "ATM 기반 인터넷 서비스 시스템(MPLS) 개발", 연구보고서, 2000 년 12 월.

[2] S. Keshave and R. Rharma, "Issues and Trends in Router Design", IEEE Comm. Mag., pp.144-151, May 1998.

[3] E. Rosen, A. Viswanathan, and R. Callon, "Multiprotocol Label Switching Architecture", IETF RFC3301, Jan. 2001.

[4] 윤현정, 류호용, 전병천, "ATM 스위치 기반 MPLS 시스템에서 연결 제어 구조", NCS, 2000 년 12 월.

[5] B. Choi, C. Choi, Y. Jeong, and J. Lee, "High-Performance IP Packet Forwarding Engine with *Pipelined Lookup Control*", *Proceeding of APCC2000*, pp.385-389,Oct. 2000.

[6] 홍진호, "시스코라우터: Configuration Guide with Routing Protocol", ㈜ 사이버출판사.