

캐리어 이더넷 망에서 빠른 절체를 위한 선형 프로텍션 스위칭 기능 설계 및 구현

정회원 안계현*, 김광준*

Design and Implementation of Linear Protection Switching for Fast Restoration in Carrier-class Ethernet Networks

Kye-hyun Ahn*, Kwangjoon Kim* *Regular Members*

요약

고속 네트워크 장비에 네트워크프로세서의 사용이 보편화 되고 라우팅 기능과 패킷처리 기능을 분리하는 분산형 시스템 구조가 이용됨에 따라 대용량의 트래픽을 매우 빠르게 처리하는 향상된 성능을 보일 수 있으나, 제어 평면과 데이터 평면 사이에 추가 메시지 교환이 필요하여 시스템 내부 통신 지연이 증가하는 문제가 발생한다. 본 논문에서 제안한 구조는 이더넷 프로텍션 스위칭 기술에 필요한 패킷 처리 기능 블록들을 효율적으로 배치하여 설계함으로써, 메시지 교환에 따른 지연의 증가에도 불구하고 단일 링크의 장애 발생 시 50 msec급 수준의 빠른 절체 성능을 보인다. 이에 따라 높은 신뢰성과 수십 기가비트의 광대역 전송이 요구되는 캐리어 이더넷 시스템에 적합한 선형 프로텍션 스위칭 기술의 설계 및 구현 방안을 제공할 수 있다.

Key Words : Linear Protection Switching, Carrier-Class Ethernet

ABSTRACT

This paper proposes Ethernet linear protection switching technology in order to provide the SONET/SDH-like resiliency over Metro Ethernet Networks. The proposed design is made of an architecture with a control processor board and several data processing boards, where the control processor board is independent of data processing board, providing a flexible solution for carrier Ethernet system. However, it leads an increasing message delay between inter-processors. In this paper, we implement and confirm a restoration of failed transport connections withing 50 millisecond in spite of increasing message delay between the control processing board and data processing board providing carrier-class network survivability.

I. 서론

이더넷은 본래 거리가 짧은 LAN(Local Area Network)에서만 사용됐으나 기술의 발달로 WAN(Wide Area Network)에 도입되면서 메트로 이더넷이라는 이름으로 사용된다. 더욱이 L2 스위치에 라

우팅 기능을 추가한 이른바 L3 스위치 라우터가 등장하면서 이러한 추세는 더욱 가속화됐다. 메트로 이더넷은 상대적으로 저렴한 장비 가격, 효율적이고 증명된 기술 등을 바탕으로 안정성과 사용자가 원하는 다양한 속도의 대역폭을 제공할 수 있는 유연성 등의 장점을 갖는다.

※ 본 연구는 지식경제부 및 정보통신연구진흥원의 IT핵심기술개발사업의 일환으로 수행하였음. [2008-F017-01, 100Gbps급 이더넷 및 광전송 기술 개발]

* 한국전자통신연구원 네트워크연구본부 (khyun@etri.re.kr)

논문번호 : KICS2008-11-496, 접수일자 : 2008년 11월 11일, 최종논문접수일자 : 2009년 9월 7일

메트로 이더넷 포럼(MEF, Metro Ethernet Forum)에서는 이더넷의 장점 위에서 텔레콤 환경이 요구하는 수준의 성능을 제공하는 것으로 캐리어 이더넷의 개념을 정의하였다^[1]. 이에 덧붙여 전형적인 LAN 기반의 이더넷 기술을 코어망에 적용하기 위해 캐리어 이더넷 서비스가 제공해야하는 5가지 주요 속성을 규정하였는데, 표준화된 서비스, 확장성, 신뢰성, QoS(Quality of Service), 서비스 관리가 그것이다. 본 논문에서는 이들 속성 중에서 신뢰성(Reliability) 관점에서 캐리어급 성능을 제공하기 위한 프로텍션 기능에 대하여 다룬다.

프로텍션(Protection)이란 망 설비나 장비의 일부에 고장, 성능저하 등의 문제가 발생하여 정상적인 기능을 수행하지 못하게 되더라도 있더라도 사용자에게 미치는 영향을 최소가 되도록 하면서 망의 기능을 지속하도록 하는 자기 치료 특성(self-healing property)이다. 일반적으로 프로텍션 기법은 빠른 복구 시간과 효율적인 자원 이용을 위해 제어 신호 처리, 동시다발적 장애에 대한 복구 가능 여부 등을 고려하여 설계한다.

캐리어 이더넷 망을 위한 프로텍션 기능은 단일 워킹 전송 경로에서 하나의 장애(failure)가 발생했을 때 손상된 워킹 트래픽을 100% 보호(protect)할 수 있도록 구성되어야 한다. 장애가 발생한 후, 50 msec 이내에 절체가 완료되어 연결이 회복되어야 하며, 프로텍션 스위칭이 연속적으로 발생하더라도, 프레임이 순서대로 전달되어야 한다^{[2],[3]}.

본 논문에서는 이와 같은 요구 사항을 만족시키기 위하여 ITU-T(International Telecommunication Union-Telecommunication)에서 권고한 이더넷 프로텍션 스위칭(EPS: Ethernet Protection Switching) 기술을 기반으로 캐리어 이더넷 망에서 점대점 VLAN(Virtual LAN) 기반의 이더넷 가상 연결 서비스에 대하여 SONET/SDH 수준의 50ms 이내 빠른 프로텍션 스위칭 기능을 제공하는 기술을 설계하였다.

특히, 본 논문에서 제안한 설계 방법은 단일의 중앙 제어 보드와 다수의 데이터 처리 보드로 구성된 분산형 이더넷 시스템 구조를 고려함으로써 제어 평면의 독립성을 제공한다. 즉, 물리적으로 데이터 처리 보드의 종류나 개수가 달라지더라도 제어 보드에 보드 간 처리를 위해 필요한 API(Application Programming Interface)만을 추가함으로써 동일한 기능을 수행하는 이더넷 시스템을 구성할 수 있다.

본 논문의 구성은 다음과 같다. II장에서는 캐리

어급 이더넷을 위한 프로텍션 기술에 대한 요구사항과 후보 기술을 소개하고, III장에서는 이더넷 프로텍션 스위칭 표준 기술을 기술한다. IV장에서는 구현할 이더넷 시스템의 구조 특성과 이를 고려한 설계 및 구현 방안을 제안하고, 성능 시험을 통해 단일 링크 장애가 발생한 경우 소요되는 절체 시간을 측정하였다. 마지막으로 V장에서 결론을 맺는다.

II. 캐리어급 이더넷을 위한 프로텍션 기술

2.1 요구사항 기법

MEF에서는 메트로 이더넷을 위한 프로텍션 요구 사항을 제시하였는데^[2] 이들 중에서 주요한 몇 가지를 정리해보면 다음과 같다.

우선 가입자는 자신이 이용하는 이더넷 서비스를 위한 회선 복구시간(connectivity restoration time)과 SLS(Service Level Specification) 복구시간 등의 프로텍션 파라미터를 망 사업자에게 요구할 수 있어야 한다. 이때 프로텍션 파라미터는 각 플로우별 또는 서비스 그룹별로 정의되어야 한다. [2]에서는 가입자가 요구하는 절체 시간을 50 msec 이내, 200 msec, 2 sec, 5 sec과 같이 4종류로 나누어 선택할 수 있도록 하였다.

프로텍션을 위한 기법은 물리적인 링크 오류와 같은 장애뿐만 아니라 기준치를 초과하는 BER(Bit Error Rate), CRC(Cyclic Redundancy Check) 오류에 따른 성능 저하 상태, 노드 고장 등과 같은 장애 종류에 대해서도 이더넷 서비스 연결을 보호할 수 있어야 하고, 두 전송 경로 간 스위칭이 이루어지더라도 이더넷 서비스의 양 끝 단에서 항상 동일한 전송 경로를 선택하도록 프로텍션 기법을 설계해야한다. 또한 여러 계층에서 각각 자신의 계층에서 수행하는 프로텍션 기법을 독립적으로 운영할 수 있어야 한다. 상위 계층에서 수행하는 프로텍션 기법은 하위 계층의 프로텍션 기법과 함께 동작할 수 있도록 설계되어야 하며, 이를 위해 프로텍션 기법은 Hold-off time을 지원해야 한다. 덧붙여 복구/비복귀(Revertive/non-revertive) 모드와 복구 시간(Wait to Restore time) 설정, 특정 전송 경로의 강제 스위칭 또는 스위칭 금지를 시킬 수 있는 운용자 제어 명령 등을 지원해야한다.

워킹 경로와 이를 보호하기 위해 설정한 프로텍션 경로는 서로 동일한 망 자원을 공유하지 않아야 한다. 이런 특성을 자원 다양성(Resource Diversity)이라고 하는데, 어느 정도의 다양도를 허용할지는

정책에 따라 결정할 수 있도록 한다. 또한 프로텍션 경로에서 본래의 서비스 품질을 어느 수준까지 보존할 것인지도 네트워크 관리자가 정의할 수 있어야 한다.

추가적으로 ITU-T SG13 G.8031 표준안³⁾에서는 점대점 이더넷 가상 연결 서비스 (EVC: Ethernet Virtual Connection)에 대하여 단일의 장애가 발생하였을 때, 데이터 트래픽을 보호 할 수 있어야 하고, 전환 시간 (Transfer time)은 현재 대표적인 코어망 기술인 SONET/SDH가 제공하는 50 msec 이내이어야 하며, 워킹 경로와 프로텍션 경로의 연결 상태는 주기적으로 모니터링 되어야 하는 등의 요구 사항을 명시하고 있다. 전환 시간은 복구 절차 수행에 따라 트래픽이 우회 경로로 전송되도록 처리하는데 소요된 시간을 나타낸다⁴⁾.

2.2 후보 기술 분석

일반적으로 프로텍션 기법들을 분류할 때, 복구 모델을 기준으로 프로텍션 스위칭 기법과 리라우팅 (Rerouting) 기법으로 구분할 수 있다.

먼저 프로텍션 스위칭 기법은 정상 상태에서 서비스를 전달하는 워킹 경로를 설정할 때, 보호 경로도 함께 설정한다. 이때 보호 경로를 위한 자원도 미리 할당된다. 따라서 장애가 발생했을 때, 기 설정된 보호 경로로의 스위칭만을 수행하므로 신속한 복구가 가능하다. 하지만 보호경로를 위한 자원이 미리 할당되어야 하므로 망 자원의 효율성이 떨어지고, 미리 설정해놓은 보호 경로 상에서 장애가 발생하는 경우 장애 복구에 실패할 수 있다.

리라우팅 기법은 장애가 발생하고 이를 감지한 이후, 복구를 위한 우회 경로를 설정한다. 자원의 이용률이 좋고 연속적인 장애 발생에도 대응할 수 있으나, 우회 경로를 설정하기 위한 시간이 필요하다는 단점이 있다.

전형적인 이더넷 기술의 경우, 장애가 발생한 이후에 새로운 전송 경로를 결정하기 위하여 STP(Spanning Tree Protocol)를 운영할 수 있다. 그러나 STP는 Listening, Learning과 관계된 지연 시간으로 인해 우회경로를 통해 트래픽을 전달하는데 최소 30 sec 이상이 요구된다. 이러한 STP의 단점을 극복하기 위하여 802.1s Multiple STP와 802.1w Rapid STP를 표준화하였다. 하지만, RSTP도 1~10 sec 정도의 시간을 소요한다^{5),6)}. 즉 xSTP 기반으로 프로텍션 기능을 수행하는 것은 새로운 우회 경로를 설정하기 위한 시간을 요구함에 따라, SONET

이 제공하는 50 msec 이내 정도의 빠른 장애 복구 시간을 보장하기 위해서는 새로운 링크 보호 기술이 필요하다.

이를 위해 ITU-T에서는 이더넷 기반의 프로텍션 스위칭 기술에 대한 표준화 작업을 수행하여 G.8031/Y.1342 Ethernet Protection Switching (EPS) 권고안³⁾을 작성하였다. 해당 표준안에 포함된 이더넷 프로텍션 스위칭 기술에 대하여 다음 장에서 설명한다.

III. 이더넷 프로텍션 스위칭 기술

3.1 프로텍션 스위칭 기능 모델

ITU-T에서는 이더넷을 기반으로 VLAN 기반의 점대점 이더넷 서비스 연결을 구성하는 두 개의 종단(endpoint)간 단일 링크를 보호하기 위한 EPS (Ethernet Protection Switching) 기술을 표준화하였다. EPS 기술을 이용한 보호 대상은 점대점 이더넷 가상 연결 서비스 (EVC)이다.

EVC는 데이터가 전달되는 망의 전송 기술에 상관없이 두 개 이상의 UNI(User Network Interface)을 연결하는 이더넷 서비스를 가리킨다. 캐리어 이더넷 망에서 제공하는 서비스들은 전송 경로 및 서비스 품질 등이 EVC를 단위로 관리되며, 점대점 방식의 E-Line 서비스, 점대 다중점 방식의 E-Tree 서비스, 다중점대 다중점 연결인 E-LAN 서비스로 구분된다. 본 논문에서 설계하는 프로텍션 스위칭 기능은 E-Line 서비스를 고려한다. E-Line 서비스는 두 개의 UNI로 이루어지며, 망으로 유입되는 모든 서비스 프레임은 UNI와 UNI가 가지는 VLAN ID와 EVC 간 맵핑 테이블을 참조하여 결정한다. 또한 EVC에 따라 출력 포트도 결정한다.

EVC에 대한 단일 전송 링크를 보호하기 위한 프로텍션 스위칭 모델은 1+1과 1:1 구조를 지원한다.

1+1 구조는 하나의 트래픽 신호를 두 개의 경로 (working transport entity와 protection transport entity)를 사용하여 항상 중복 전송하는 방법이다. 워킹 경로와 보호 경로가 합해지는 지점에서 어떤 경로로부터 수신된 트래픽을 수락, 포워딩 할 것인지 결정한다. 이 경우, 하나의 전송 경로로부터 다른 전송 경로로의 스위칭은 수신측에서 경로 자원을 up/down하는 이벤트로 처리한다.

반면 1:1은 정상 트래픽 신호가 두 개의 경로 중 어느 하나를 선택하여 송수신을 하는 방법이다. 즉 보호 경로를 이용한 트래픽 전송은 장애가 발생하

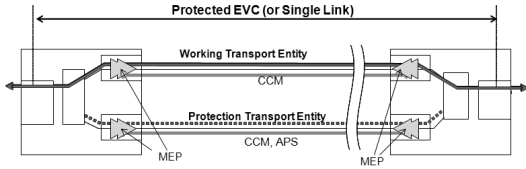


그림 1. 1:1 프로텍션 스위칭 모델

였을 때에만 수행한다. 이때, 양 끝단에서 동시에 보호 경로로 스위칭을 하기 위해서는 상호동작을 수행해야하며, 이를 위해 APS(Automatic Protection Switch) 프로토콜을 사용한다.

그림 1은 1:1 구조를 갖는 프로텍션 스위칭에 대한 기능 모델을 도시한 것이다. 연결 상태를 감시하기 위한 CCM(Connection Check Message) 메시지와 양끝단에서 동일한 엔터티로 스위칭을 하기 위한 APS 메시지 등 이더넷 OAM (Operations, Administration and Maintenance) 메시지가 단일 링크 내에서 교환된다.

양 끝단에 위치한 중단점은 단일의 EVC에 대하여 “Head end” 또는 “Tail end”로서 기능을 수행한다. “Head end”는 정상 트래픽을 복사(copy)하여 요청이 있을 때 보호 경로에게 전송하는 브리지(Bridge) 기능을 수행한다. “Tail end”는 워킹 경로와 보호 경로 중에서 어느 하나를 선택하여 트래픽을 수신하는 셀렉터(selector) 기능을 수행한다. 양쪽 방향 모두 보호되는 양방향(Bidirectional) 전송에서는 양쪽 끝단에서 브릿지와 셀렉터 기능을 모두 제공한다.

3.2 자동 보호 절체 프로토콜

자동 보호 절체(Automatic Protection Switch) 프로토콜은 이더넷 OAM PDU(Payload Data Unit) 종류 중의 하나인 APS OAM PDU를 이용하여 자신의 요청(Request)/상태(State) 정보, Bridged signal, Request signal에 대한 정보를 상호 전달함으로써 프로텍션 스위칭을 처리할 때 양 끝 단이 동일한 전송 경로를 선택하도록 지원한다.

APS PDU는 백업 전송 경로만을 이용하여 전달되며, 최초 EVC가 설정될 때 APS 프로토콜의 동작을 위해 한 번씩 주고받으며, 이후 정상 상태에서는 생성되지 않는다.

임의의 한 끝단에서 상호 교환하는 APS PDU를 이용하여 그림 2와 같이 프로텍션 스위칭 알고리즘을 수행할 때 자신의 요청뿐만 아니라 상대방 끝단에서 APS를 통해 전송된 요청도 입력이 될 수 있

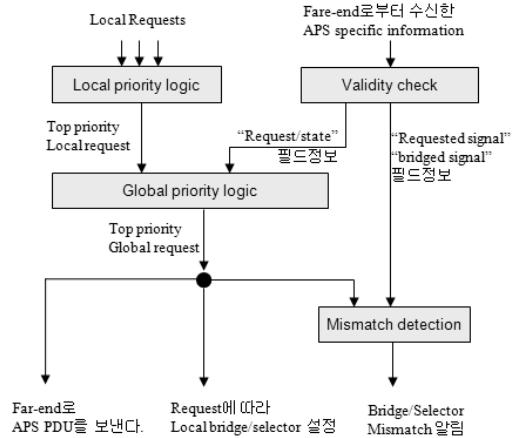


그림 2. 1+1/1:1 선형 프로텍션 스위칭 알고리즘 원리^[3]

으며, 이에 따라 보호 도메인 전체에서 우선순위가 가장 높은 요청에 따라 프로텍션 스위칭 알고리즘이 동작할 수 있다.

따라서 프로텍션 스위칭이 일어날 수 있는 경우는 전송 경로에 대한 신호 전달 오류(Signal Fail)가 인지되었거나, 네트워크 운영자가 직접 스위치를 지시하는 명령을 입력하였을 때, 그리고 수신한 자동 보호 절체 프로토콜이 스위칭을 요청했을 때이다. 추가적으로 복귀(Revertive) 모드인 경우에 스위칭을 일으켰던 원인이 해소된 이후에 트래픽이 본래의 워킹 경로로 되돌아가려 할 때에도 스위칭이 일어날 수 있다.

IV. 이더넷 프로텍션 스위칭 기능 설계 및 성능 시험

4.1 캐리어 이더넷 시스템 구조

4.1.1 하드웨어 구조

캐리어 이더넷 시스템은 지능형 멀티미디어 액세스 기능을 갖는 캐리어급 이더넷 가입자를 수용하는 시스템으로서, 높은 신뢰성과 경제성을 보장하고 다양한 서비스 기능을 수용할 수 있는 메트로 이더넷 망과 액세스 플랫폼의 특성을 고려하여 다음과 같이 설계한다.

시스템에 수용되는 모든 보드는 AdvancedTCA의 PICMG3.0 규격을 준수하여 설계하고, 시스템 용량의 확장 또는 축소 설치 등을 고려하여 하드웨어를 기능별로 모듈화 한다.

ATCA 기반 시스템의 하드웨어 구조는 시스템의 용량과 지원 가능한 슬롯의 수의 따라 5-슬롯 ATCA

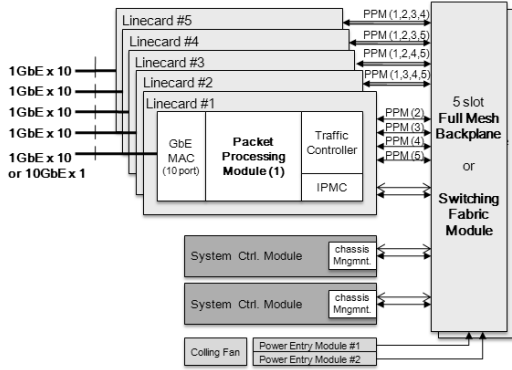


그림 3. 하드웨어 구조

보드 수용 시스템과 14-슬롯 ATCA 보드 수용 시스템으로 구분할 수 있는데, 본 논문에서 구현한 캐리어 이더넷 시스템은 5-슬롯 풀 메쉬 구조를 기본으로, 슬롯당 10Gbps를 지원하도록 설계하여 50Gbps까지 지원하는 구조를 갖는다. 스위치 보드와 14-슬롯 듀얼 스타 구조를 활용하는 경우에는 100Gbps 이상의 시스템 용량을 구현할 수 있다.

그림 3은 본 논문에서 설계한 캐리어 이더넷 시스템(CCE)의 하드웨어 구조도이다. 시스템 하드웨어의 논리적인 구조는 시스템 제어(SCM) 보드, 패킷 처리 및 정합 기능(PPM) 보드, 패킷 스위치 기능(SFM) 보드, 백플레인 기능 보드, 전원공급 및 냉각 기능 모듈로 구성된다. 패킷 스위치 기능 보드는 160Gbps 시스템 용량을 위해 사용하며, 패킷 처리 및 정합 기능(PPM) 보드는 50Gbps 시스템과 160Gbps 시스템에서 공용으로 사용할 수 있도록 설계하였다. 5개의 슬롯을 지원하여 슬롯 당 10Gbps를 지원하도록 설계되었으며, 시스템 제어 기능과 상위 소프트웨어 구현을 위한 2개의 SCM 카드를 지원한다. 시스템 내에 쿨링팬이 내장되어 있으며, 두 개의 -48V 전원 모듈을 지원한다.

4.1.2 소프트웨어 구조

본 논문에서 구현한 캐리어 이더넷 시스템의 소프트웨어는 패킷 처리 보드 내에 마이크로 엔진에서 상대적으로 고속 패킷 처리가 가능한 마이크로 코드 블록과 Xscale CPU에서 처리하는 코어 컴포넌트(Core Component)가 구성되어 있고, 이에 덧붙여 중앙 제어 프로세서 보드와 메시지를 송수신하기 위한 보드 간 통신 수단으로서 CP-PDK(Control Plane Platform Development Kit)가 구성된다. 이에 따라 L2 스위치 기능 등을 마이크로 코드로 처리하

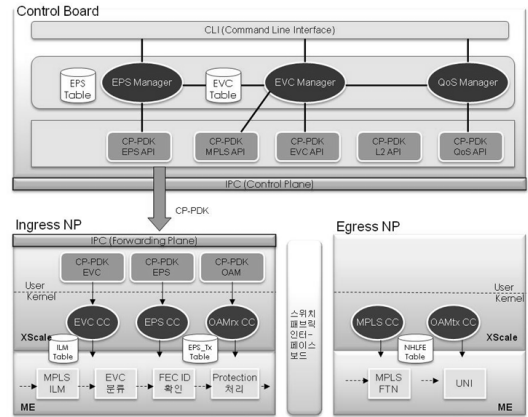


그림 4. 소프트웨어 구조

고 향후 고성능의 패킷 처리를 위한 추가 기능이 요구될 경우에도 하드웨어 변경 없이 마이크로 코드의 추가만으로도 쉽게 기능 확장이 가능한 구조를 제공할 수 있다. 또한 제어 보드에는 이더넷 시스템을 제어하고 시스템 운영자의 입력력 인터페이스를 처리하기 위한 기능, 캐리어 급 이더넷 서비스를 제공하기 위한 서비스 관리 및 상위 프로토콜 기능을 C 코드로 구현한다.

이를 기반으로 설계한 캐리어 이더넷 시스템의 소프트웨어 기능 블록 구조는 그림 4와 같다.

제어 프로세서에서 사용자 인터페이스(CLI: Command Line Interface)를 통해서 입력된 명령은 EPS 매니저, EVC 매니저, QoS 매니저 기능 블록들을 거쳐 CP-PDK에서 제공하는 API를 호출한다.

IPC 계층에서는 CP-PDK CP에서 구현된 API 명령을 IPC의 전달 메커니즘을 통해서 라인카드의 포워딩 플레인(CP-PDK FP)으로 전달된다. 라인카드에는 제어프로세서의 각각의 매니저에 일대일로 연결되는 코어 컴포넌트 블록이 존재하고 해당 블록으로 전달된 메시지를 이용해서 라인카드의 XScale 코어와 마이크로 엔진 사이에 공유되는 테이블을 설정한다.

라인카드에서 구동되는 소프트웨어 블록은 테이블 구성에 따라서 패킷을 처리하는 마이크로 블록과 테이블을 관리하고 예외처리 기능을 수행하는 코어 컴포넌트 기능으로 구분된다. 마이크로 블록은 Intel IXP MEv2 명령어 집합으로 작성된 어셈블리 코드로 구현되며 다수의 마이크로 블록이 모여서

IXP2800 네트워크 프로세서 내부의 16개의 마이크로 엔진에 맵핑되어 구동된다. 코어 컴포넌트는 XScale에서 수행되며 C 언어로 구현되었다. 각각의 코어 컴포넌트는 일대일 혹은 일대 다수로 연결된 마이크로 블록을 제어하고 해당 마이크로 블록에서 발생시킨 예외 등을 처리하는 기능을 수행한다.

라인카드에는 입력기능을 담당하는 네트워크 프로세서와 출력기능을 담당하는 네트워크 프로세서가 존재하고 이들 사이의 통신은 PCI 버스의 인터럽트 기능을 이용해서 수행된다. 코어 컴포넌트에서는 PCI 버스의 통신기능을 투명한 계층으로 인식하여 잉그레스(Ingress)/이그레스(Egress)의 위치에 관계없이 각 코어 컴포넌트 사이의 메시지를 처리하는 메커니즘이 구현되어 있다.

CCE50의 코어 컴포넌트(Core Component)는 리눅스 커널 계층에서 리눅스 커널 쓰레드(thread)로 맵핑되어 기능을 수행한다. 라인카드에서 시스템 애플리케이션을 초기화 하는 블록에서는 각 소프트웨어 모듈을 순차적으로 초기화 하여 커널 쓰레드에 각 컴포넌트를 맵핑하여 기능을 수행시킨다. 각 쓰레드는 실행엔진(Execution Engine)에 맵핑되고 실행엔진은 쓰레드에 맵핑되어 메시지 이벤트를 처리한다.

4.2 설계 및 구현 방안

상기와 같은 하드웨어와 소프트웨어 구조 특성을 갖는 캐리어 급 이더넷 시스템에 이더넷 프로텍션 스위칭 (EPS) 기술을 구현하기 위한 설계 방안은 다음과 같다.

4.2.1 전송 기술

캐리어급 이더넷 서비스인 E-Line과 E-LAN을 제공하기 위하여 MPLS(Multi Protocol Label Switching) martini Draft의 응용인 VPLS(Virtual Private LAN Service)와 VPWS(Virtual Pseudo-Wire Services)를 이용하여 EVC를 구현하고, 메트로 망에서의 전송 경로는 MPLS LSP(Label Switched Path)를 사용하여 구현하였다. MPLS 기술을 사용함에 따라 보호 경로를 통해 데이터 전송을 보장할 수 있고, 빠른 속도(wire-speed)로 워킹 경로로부터 보호 경로로 트래픽을 스위칭 할 수 있다. 보호 전송 경로는 EVC 설정 시 운영자에 의하여 입력되도록 구현하였으며, VPLS 생성 및 이와 관련된 LSP 설정에 필요한 시그널링 프로토콜은 본 논문에서는 다루지 않는다.

본 시스템에 유입되는 패킷은 자신이 속한 EVC를 확인하여, 해당 EVC가 약속한 전송 품질, 프로텍션 스위칭 적용 여부 등의 서비스를 보장받도록 처리된다. 이를 위해 필요한 EVC 및 UNI 등의 정보들은 일괄적으로 중앙 제어 보드에서 유지하도록 설계한다.

데이터 처리 보드로는 자신에게 속한 포트에 대한 UNI 정보가 변경되는 이벤트가 발생한 경우에 제어 보드로 해당 사실 및 변경된 정보를 알리는 한편 패킷 처리에 필요한 일부의 UNI, EVC 정보들은 제어 보드로부터 내려 받아 참조하도록 설계한다. 본 논문에서는 물리적인 포트 당 하나의 UNI를 설정하는 것을 가정하였다.

4.2.2 장애 인지 기능

워킹 경로와 보호 경로의 연결성을 모니터링 하기 위한 이더넷 OAM의 CCM 기능 모듈은 최소 3.3 msec 이상의 주기에 따라 빠르고 빈번하게 지속적으로 수행해야하기 때문에 프로세싱의 부담을 감소시키기 위하여 마이크로 엔진 내에 구현하였다. 또한 CCM의 주기를 EVC마다 차별적으로 설정할 수 도록 설계하였다.

EVC의 연결에 대하여 기 설정한 CCM 주기의 3.5회 구간동안 CCM PDU가 수신되지 않은 경우, 해당 경로에서 장애가 발생한 것으로 인지하도록 설정하였다. 장애 발생을 인지한 CCM 기능 모듈은 해당 EVC에 대한 프로텍션 스위칭이 수행되도록 제어 프로세서 보드 내에 구현한 EPS 매니저에게 장애 발생 이벤트를 알린다.

4.2.3 이더넷 프로텍션 스위칭 기능

제어 보드에 위치한 EPS 매니저는 발생한 이벤트(장애 발생/복구 등)에 따라 APS 알고리즘을 수행하며, 상대방 장치에게 전송할 APS PDU 생성 및 보호 경로로의 절체 또는 원래 경로로의 복구 등을 결정한다.

전송 경로의 스위칭이 결정된 경우, EPS 매니저는 제어 보드에 위치한 EVC, UNI 등의 정보를 갱신하고 변경된 정보를 참조하는 데이터 처리 보드들에게 전달한다. 데이터 처리 보드에 위치한 패킷 포워딩 관련 테이블 정보가 수정되고, 이에 따라 EVC에 속한 패킷들이 결정된 연결 경로를 이용하여 송수신하도록 브릿지/셀렉터 기능을 수행함에 따라 성공적인 프로텍션 스위칭이 이루어진다.

또한 APS 프로토콜 처리는 제어 보드에 구현하

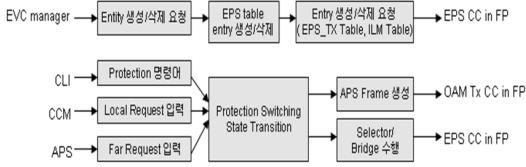


그림 5. 기능 수행 흐름도

지만, APS PDU는 이더넷 OAM PDU 중의 하나이므로 상대방 장치에게 APS PDU를 전송하기 위한 실질적인 PDU 생성 및 전달은 데이터 처리 보드 내 이더넷 OAM 기능 블록에서 수행하도록 설계한다. 이를 위해 EPS 블록은 APS PDU를 구성하기 위한 APS 정보를 OAM 코어 컴포넌트에게 전달한다.

그림 5는 앞서 기술한 방안 에 따라 설계한 이더넷 프로텍션 스위칭 기능의 수행 흐름도이다.

제어프로세서와 데이터 처리블록은 전형적으로 하나의 보드 상에 구현되어 왔으나, 본 구현에 사용하는 캐리어 이더넷 시스템은 이들을 물리적으로 개별적인 보드로 개발하고, 두 보드 사이의 메시지 전송을 위해서 ForCES 프로토콜을 사용하였다. ForCES 프로토콜은 인텔에서 제공하는 CP-PDK를 사용하며, CP-PDK에서 제공되는 ForCES 기반의 API를 사용하여 제어평면(Control Plane)과 데이터 평면(Data Plane) 사이의 독립성을 보장한다. 이렇게 제어평면과 데이터평면을 분리함으로써 제어평면은 그 종류에 무관하게 필요한 API들을 정의하고 지원함으로써, 다양한 데이터평면의 구현 보드에 사용이 가능하다.

반면, 프로텍션 스위칭을 수행하기 위한 APS 프로토콜 처리 블록과 전송 경로의 스위칭이 발생하는 데이터 포워딩 기능 블록이 서로 다른 보드에 위치하기 때문에, 이들 간 정보 교환을 위한 오버헤드 시간이 증가한다. 예를 들어 라인카드에 위치한 OAM CC(Core Component)에서 CCM 메시지 미수신에 따라 장애를 인지한 후 제어평면에 위치한 EPS 매니저에게 장애 발생 정보를 전달할 때, 또한 EPS 매니저의 처리 결과에 따라 EVC의 전송 경로의 스위칭 명령이 라인 카드로 전달할 때 등 보드 간 통신을 위한 처리 시간이 추가된다.

프로텍션 스위칭 기법의 절체 시간의 최소화를 위한 관점에서는 단일 보드 내에 해당 기능을 구현하거나, EPS 매니저의 기능을 라인카드 안에 구현하는 것이 보다 효과적일 것이다. 하지만 이를 위해서는 각각의 라인 카드가 동일한 시스템 내 다른

라인 카드를 통과하는 모든 EVC 정보, 전송 엔티티에 대한 상태 정보 등을 관리해야하므로 단일의 데이터 처리 보드에서 관리해야하는 정보량이 크게 증가하고, 또한 서로 다른 보드가 가지는 테이블들이 임의의 시각에 동일한 정보를 유지하기 위한 견고한 정보 관리 기법이 필요하다.

4.3 성능 시험

본 논문에서 설계한 이더넷 프로텍션 스위칭 기술이, 제어 보드와 데이터 처리 보드 간 통신을 요구하는 구조임에도 불구하고, 빠른 절체 시간을 제공하는 것을 확인하기 위하여 다음과 같이 성능 시험을 수행하였다.

제안한 기술이 구현된 캐리어 이더넷 시스템(CCE: Carrier-Class Ethernet system) 6개를 이용하여 그림 6과 같이 가상의 메트로 이더넷 망을 구성하고, 이들 중 CCE 1번과 CCE 6번에 가입자 장비를 직접 연결하여 이들 간 E-Line 서비스를 설정하였다.

CCE 1번, 2번, 3번, 6번을 연결하는 워킹 전송 경로를 설정하고, 보호 경로로는 CCE 1번, 4번, 5번, 6번을 연결하는 LSP를 설정하였다. 이에 따라 가입자 A로부터 유입되는 데이터 프레임은 메트로 이더넷 망을 거쳐 원격에 위치한 가입자 B로 전달된다. 프로텍션을 수행하는 보호 도메인을 CCE 1번과 CCE 6번을 연결하는 전송 경로 전체로 설정하기 위하여 CCE 1번과 CCE 6번에 MEP (MEG End Point)을 설정하였다.

성능 시험을 위하여 CCE 1번에 가입자 장비로서 이더넷 프로토콜 분석기를 연결하고, 가입자 B를 목적지로 하는 이더넷 프레임은 1 msec마다 주기적으로 발생시킨 후, 수신측 B에 도착하는 패킷들을 계속적으로 모니터링하면서 이더넷 서비스 연결 상태를 판단하였다.

장애가 발생하지 않은 정상 상태에서 가입자 A

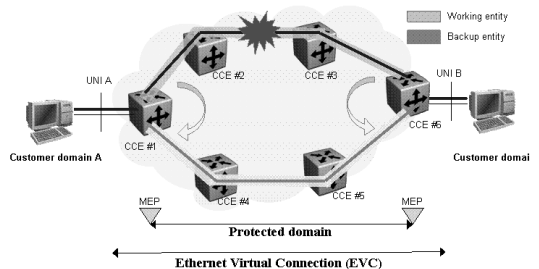


그림 6. 프로텍션 스위칭 실험 구성도

#	Status	Time (s)	Time Offset	Length	Source	Destination	Protocol	Info
832	S	0.319163	10023	124	198.19.1.2	198.19.1.1	IP	Unknown (0x72)
833	S	0.329197	10034	124	198.19.1.2	198.19.1.1	IP	Unknown (0x72)
834	S	0.339191	9994	124	198.19.1.2	198.19.1.1	IP	Unknown (0x72)
835	S	0.349195	10004	124	198.19.1.2	198.19.1.1	IP	Unknown (0x72)
836	S	0.359200	10005	124	198.19.1.2	198.19.1.1	IP	Unknown (0x72)
837	S	0.715309	356189	60	00:0b:0c:0d:0e:14	00:08:00:00:00:01	Ethernet II	
837	S	0.715311	356189	124	198.19.1.2	198.19.1.1	IP	Unknown (0x72)
839	S	0.909913	9975	124	198.19.1.2	198.19.1.1	IP	Unknown (0x72)
840	S	0.909953	10040	124	198.19.1.2	198.19.1.1	IP	Unknown (0x72)
841	S	0.919942	9989	124	198.19.1.2	198.19.1.1	IP	Unknown (0x72)
842	S	0.929968	10026	124	198.19.1.2	198.19.1.1	IP	Unknown (0x72)
843	S	0.939977	9989	124	198.19.1.2	198.19.1.1	IP	Unknown (0x72)
844	S	0.949978	10003	124	198.19.1.2	198.19.1.1	IP	Unknown (0x72)

그림 7. 프로텍션 스위칭 수행 전후시간에 수신된 데이터 정보

가 송신한 데이터 프레임이 목적지 B에 약 1 msec 간격마다 수신되는 것을 확인한 후, 워킹 경로에 위치한 CCE 2번과 CCE 3번 사이의 연결선을 강제적으로 끊어서 장애를 발생시켰다. 이후 수신측 B에 도착하는 패킷들의 도착 시간, 이전 패킷과의 수신 시간 간격, 패킷 형식 등의 정보를 분석하여 장애 발생 시 구현한 프로텍션 스위칭을 통해 보호 경로로의 전환 시간을 계산하였다.

그림 7은 실험을 통해 얻은 가입자 B에서 수신한 패킷들에 대한 정보를 수집한 화면이다.

가장 첫 번째 항목은 수신하는 패킷의 순번이고, Time(Rel.)은 수신한 시각, Time(Delta)는 이전에 수신한 패킷과의 시간 간격을 나타낸다.

836번째 패킷까지는 약 1 msec 정도의 간격으로 데이터 프레임이 도착하였다. 워킹 경로에 장애가 발생한 이후 837번째 패킷은 약 35.61 msec가 지난 후에 수신되었다. 또한 이 패킷은 데이터 프레임이 아닌 이더넷 OAM 기능 중의 하나인 AIS(Alarm Indication Signal) PDU이다. AIS PDU는 장애를 감지한 CCE 6번이 해당 서비스 경로를 따라 장애가 인지되었음을 알리기 위해 전달하는 메시지이다. 즉 CCE 6번에서 가입자 B에게 AIS PDU가 전달된 것이다.

AIS PDU 다음으로 도착한 패킷(839번째)은 본래 송신지 A에서 보낸 이더넷 데이터 프레임으로 약 27.46 msec가 지난 후에 수신되었다. 해당 데이터 프레임은 워킹 경로에서 장애가 감지된 이후, CCE 1번과 CCE 6번에서 프로텍션 스위칭을 수행하여 보호 경로를 통해 전달되었다.

이에 따른 전환 시간을 계산해보면 보호 경로를 통해 전달된 첫 번째 패킷의 도착시간과 워킹 경로를 통해 전달된 마지막 패킷의 도착 시간 사이의 간격인 63.07 msec가 전체 복구 시간(Restoration time)이다. 이 시간 중에서 장애 발생을 인지하는데 소요된 시간은 최대 CCM 주기의 3.5배인 11.66

msec이므로, 이를 제외한 나머지 시간, 51.41 msec가 보호 경로로 프로텍션 스위칭을 수행하는 데에 소요된 시간이라고 판단할 수 있다.

동일한 시험을 다수 시행해 본 결과, 약 50 msec 정도의 절체 시간 성능을 얻을 수 있었다. CCM 주기를 10 msec로 증가시킨 시험 결과에서도 모두 45 msec 이내에서 절체가 완료되었다. CCM 주기를 3.3 msec로 설정하는 것보다 10 msec로 증대시킨 경우에 보다 짧은 스위칭 시간을 나타내는 이유는 프로텍션 스위칭을 위한 AIS PDU 처리와 CCM 처리가 동일한 OAM 마이크로 블록에서 동작함에 따라 프로세싱 지연에서 차이가 발생한다고 판단된다. 하지만 빠른 장애인지로 인하여 전체 복구 시간은 CCM 주기가 짧은 경우에 더 좋은 성능을 보인다.

또한, 본 논문에서 설계한 구조는 데이터 포워딩을 담당하는 라인카드와 중앙 제어 기능을 수행하는 제어 프로세서 보드 사이에 정보 교환을 위해 CP-PDK를 사용한다. 이를 통한 보드 간 통신에 수 msec의 지연이 발생함을 확인하였다. CP-PDK가 아닌 별개의 보드 간 통신 채널을 이용한다면 프로텍션 스위칭에 소요되는 시간을 보다 단축시킬 수 있을 것으로 기대된다.

V. 결 론

본 논문에서는 메트로 망에서 캐리어급 서비스가 요구하는 높은 신뢰성을 제공하기 위하여 SONET/SDH 수준의 빠른 절체가 가능한 이더넷 선형 프로텍션 스위칭 기술을 설계하였다. MEF와 ITU-T에서 규정한 이더넷 가상 연결 서비스를 지원하며, 이더넷 OAM 기능과 연계하여 연결 상태 모니터링 및 장애 인지 등을 수행한다. 또한 ITU-T G.8031 표준 문서 기반의 APS 프로토콜을 수행한다.

특히, 제어 평면과 데이터 평면이 물리적으로 서로 다른 보드에 위치한 분산형 시스템 구조를 갖는 캐리어급 이더넷 시스템 특성을 고려하여 프로텍션 스위칭 기술의 구성 요소를 효율적으로 배치함으로써 보드 간 메시지 교환에 따른 지연의 증가에도 불구하고 빠른 절체 시간을 제공할 수 있도록 설계하였다.

설계한 기술을 캐리어급 이더넷 시스템 내에 구현하여 가상의 메트로 이더넷 망을 구성하고 단일 링크 장애에 대한 전환 시간 성능을 시험하였다. 이를 통해 50 msec 수준의 빠른 절체가 이루어지는

것을 보임으로써, 본 논문에서 설계한 프로텍션 스위칭 기법이 신뢰성 관점에서 캐리어 급 요구 사항을 만족시킬 수 있음을 확인하였다.

참 고 문 헌

- [1] Metro Ethernet Forum, "Carrier Ethernet-the Technology of Choice of Access Networks," *MEF White paper*, March, 2006.
- [2] MEF 2, "Requirements and Framework for Ethernet Service Protection in Metro Ethernet Networks," *MEF Technical Specifications*, Feb., 2004.
- [3] ITU-T Recommendation G.8031(2006), "Ethernet Protection Switching"
- [4] ITU-T Recommendation M.495 (1988), "Transmission restoration and transmission route diversity: Terminology and general principles"
- [5] Gary Holland, "Carrier Class Metro Networking: The High Availability Features of Riverstone's RS Metro Routers," *Riverstone Networks technology white paper #135*, 2002.
- [6] ATRICA, "Layer 2 vs. Layer 3, Which one fits Metro Networks Better," *ATRICA White paper*, 2002.
- [7] ATRICA, "Providing Carrier-Class Protection for Metro Optical Ethernet Networks," *ATRICA White paper*, 2002.
- [8] ITU-T Recommendation Y.1731 (2006), "OAM Function and Mechanisms for Ethernet Based Networks"

안 계 현 (Kye-hyun Ahn)

정회원



1996년 2월 전북대학교 컴퓨터 공학과

1998년 2월 전북대학교 컴퓨터 공학과 석사

2003년 2월 전북대학교 컴퓨터 공학과 박사

2003년 8월~현재 한국전자통신연구원

신연구원 네트워크연구본부 선임연구원

<관심분야> 이더넷, 네트워크 프로토콜

김 광 준 (Kwangjoon Kim)

정회원



1981년 2월 서울대학교 물리학과

1983년 2월 서울대학교 물리학과 석사

1993년 6월 미국 Ohio State University 물리학과 박사

1984년 3월~현재 한국전자통신연구원

신연구원 네트워크연구본부 광

전송기술연구팀 팀장 (책임연구원)

<관심분야> 광전송, Optical Networks, WDM