네트워크 보안 기능을 갖는 패킷처리 기반의 링크 통합 장비 설계

논 문

60P-3-9

The Design of a Link Aggregation Equipment Based on Packet Processing with Network Security Capability

신재흥[†] · 김홍렬^{*} · 이상하^{**} · 허용민^{***} · 이상철[§]

(Jae-Heung Shin · Hong-Ryul Kim · Sang-Ha Lee · Yong-Min Hur · Sang-Cheol Lee)

Abstract - The technology to build high speed network using low cost DSL in the areas where the cost to build high speed network is high and the network environment is not very accommodating is important in providing the high speed network that meets the user demand and utilizing the network resources in an efficient way. This study presents development of the link aggregation equipment that performs the access control and firewall functions for packet processing based LAN users. The equipments developed support up to 5 line link aggregation as opposed to current 2 line link aggregation. The equipments also allow the use of high speed network in the areas where the network environment is not very accommodating. Also, the fail-over function is added to each line to provide reliability and the self-security function is enhanced to protect the network from unauthorized use and prevents waste of network resources by authorized users.

Key Words : Link Aggregation, Access Control, Firewall, Fail-Over

1. 서 론

저렴한 xDSL(Digital Subscriber Line)과 같은 회선을 활용하여 네트워크 환경이 열악한 환경이나 일반 인터넷 서비스 이용자들이 고속 대역폭을 요구하는 상황이 발생할 경우, 이런 서비스를 제공하기 위해 현재 망에서 기존의 링크를 사용하여 사용자가 원하는 대역폭을 얻기 위한 방법으로 표준화된 링크 통합 기술을 적용할 수 있다. 이 링크 통합 기술은 여러 개의 물리적 포트를 모아서 고속으로 데이터를 처리할 수 있는 한 개의 논리적 포트로 만드는 것이다. 링크 통합에 속하는 포트들을 링크 통합 그룹이라고 부르고 한 포트를 지정해서 그 그룹의 주 포트(master port)로 사용한다.

그룹의 모든 포트는 같은 VLAN(Virtual LAN)에 속해야 하고, STP(Spanning Tree Protocol) 상태, 정적 멀티캐스트, 트래픽 통제, 트래픽 세그멘테이션(traffic segmentation), 802.1p 기본 우선순위(default priority) 설정 등이 모두 동일해야 한다. 포트 잠금, 포트 미러링, 802.1x 기능이 트렁크 그룹(trunk group)에 설정되어서는 안 된다. 통합된 링크는 모두 같은 속도여야 하고 전이중로 설정되어야 한다[1].

링크 통합의 장점은 통합 그룹에 속한 링크들은 서로 동

적으로 백업된다. 즉, 한 링크가 죽으면 나머지 링크들이 거의 순간적으로 트래픽을 접수하여 링크 사용률을 높인다. 또한 2개 이상의 링크는 연결된 링크를 모두 합한 값에 해당하는 대역폭을 지원하여 연결된 두 스위치 사이의 대역폭을 향상시켜 전체적으로 링크 성능을 향상 시킨다.

링크 통합을 하는 방법은 정적(기본 설정)과 동적인 IEEE 802.3ad(LACP)의 두 가지 방법이 있다. 정적은 링크 통합을 직접 설정해야 하고 통합된 포트 그룹의 동적 변화를 허용하지 않는다. IEEE 802.3ad(LACP)은 스위치와 다른 네트워크 장비 사이의 동적으로 통합된 링크를 협상하는데 사용된다[2][3][4][5].

링크 통합과 관련된 많은 제품들이 시장에서 유통되고 있다. 대만의 많은 기업에서 생산된 제품들은 가격 경쟁력은 있지만, 소용량 스위치 형태로 접근 통제 목록(Access Control List)와 링크 통합 기능이 매우 떨어지는 단점이 있다. 그리고 링크 통합과 관련된 많은 기술을 보유하고 있는 미국의 Cisco를 비롯한 고가의 장비 업체에서 생산된 제품은 기능이 매우 복잡하고 가격이 비싸서 제품 확산에 어려움이 있다.

장비를 생산하는 업체들은 주로 스위치 칩 업체에서 출시한 칩셋(chipset)을 사용하여 L2/L3 스위치 형태의 장비를 개발해 왔다. 이러한 장비는 이더넷(Ethernet) 스위치 기능에 중점을 두어 매우 제한된 수준의 접근 통제와 링크 통합 기능을 제공한다. 스위치 칩셋 제조업체인 Broadcom, Marvell 등에서 출시한 각 계층에 맞는 칩셋과 저가형 이더넷 스위치 칩 제조업체인 Realtek을 사용하여 링크 통합 장비를 개발하는 경우, 기본적인 스위칭 위주의 제한적인 성능과 기능을 제공하거나 가격이 매우 비싼 문제를 갖고 있다[1].

본 연구에서는 링크 통합 장비로 xDSL 장비와 같이 낮은 대역폭을 갖는 다중 회선을 사용하여 고속 통신환경을 제공

* 비 회 원 : 동서울대학 컴퓨터정보과 부교수 · 공박

** 비 회 원 : 동서울대학 정보통신과 부교수 · 공박

*** 비 회 원 : 동서울대학 디지털전자과 조교수 · 공박

§ 시니어회원 : 동서울대학 전기정보제어과 교수 · 공박

† 교신저자, 정회원 : 동서울대학 디지털방송미디어과 부교수 · 공박

E-mail : jhshin@du.ac.kr

접수일자 : 2011년 6월 21일

최종완료 : 2011년 7월 27일

하는 보드를 개발한다. 또한, 계층 2에서의 네트워크 보안을 강화하여 외부로부터의 침입을 방지하고, 내부 사용자의 네트워크 접근 통제 기능을 제공하여 제한된 네트워크 대역폭을 보다 효율적으로 사용할 수 있는 기능을 제공하도록 한다.

2. 링크 통합과 방화벽

2.1 링크 통합의 확장

계층적 네트워크 모델에서 각 계층은 대역폭 통합을 위한 계층이다. 대역폭 통합은 계층의 각 부분에서 요구되는 특정 대역폭을 고려하여 설계할 수 있는데, 두 스위치 간의 각 병렬 링크(parallel link)들을 하나의 논리적 링크로 결합하는 것이다. 네트워크 대역폭 요구에 대해 특정 스위치 사이의 링크를 결합하는 방법을 링크 통합이라고 한다. 링크 통합은 스위치들 사이의 전송 처리율(throughput)을 높이기 위해 여러 개의 스위치 포트를 결합할 수 있게 한다.

그림 1에서 PC1과 PC3은 응용(application) 개발을 위해 광대역이 필요하다고 가정하자. 네트워크 관리자는 접근계층 스위치인 S1, S2와 S3에 요구되는 대역폭의 증가를 결정하면, 계층적 구조에 따라 이들 접근계층 스위치들은 분배계층 스위치인 D1, D2 그리고 D4와 연결한다. 분배계층 스위치들은 핵심계층 스위치인 C1과 C2에 연결한다. 링크 통합은 각 스위치들의 특별한 포트에 특별한 링크를 결합하는 방법이다. 이와 같은 방법으로 네트워크의 특별한 부분의 대역폭 확대를 지원한다.

그림 1 링크 통합

Fig. 1 Link aggregation

2.2 방화벽

방화벽은 네트워크 게이트웨이 서버에 위치하고 있는 일련의 연관된 프로그램들로서, 다른 네트워크 사용자들로부터 사설 네트워크의 자원들을 보호해준다. 방화벽은 외부인이 자신의 공개되지 않은 자원에 접근하는 것을 막고, 내부인 접속해야 할 외부의 자원들을 통제하기 위해 내부망과 외부망 사이에 설치된다.

방화벽은 라우터 프로그램과 밀접하게 동작함으로써, 모든 네트워크 패킷들을 해당 목적지로 어떻게 전달할 것인지를 결정하기 위해 검사하고, 여과하고, 컴퓨터 사용자를 대신하여 네트워크에 요청을 해주는 프록시 서버(proxy server) 기능을 아예 포함하거나 또는 함께 상호 협력하여 동작한다.

방화벽은 네트워크의 다른 부분들과는 별개로, 특별히 지정된 컴퓨터에 설치되는 경우가 많은데, 이는 들어오는 요구가 사설 네트워크의 자원으로 곧바로 전달되지 않도록 하기 위한 것이다.

그림 2 방화벽

Fig. 2 Firewall

3. 패킷기반의 링크 통합과 방화벽 설계

3.1 링크 통합과 방화벽 개발

본 연구에서 개발하는 링크 통합 장비는 패킷 처리 기반의 xDSL과 같이 낮은 대역폭을 갖는 다중 회선을 사용하여 고속의 네트워크 환경을 제공하기 위해 다중 회선의 프레임 순차 순환대기(round-robin) 방식으로 시스템 분배 부하를 줄이고 빠른 프레임 단순화하여 전달하여 링크 통합을 제공할 수 있게 하였다.

또한, 계층2에서 네트워크 보안을 강화하여 외부로부터의 침입을 방지하고, 내부 사용자의 네트워크 접근 통제 기능을 제공하기 위해 각 계층의 패킷 헤더 필드를 처리하도록 하는 제한된 대역폭에서 네트워크 대역폭을 보다 효율적으로 사용할 수 있는 보드를 개발한다.

그림 3은 링크 통합을 위한 네트워크 구성도이다.

그림 3 링크 통합을 위한 네트워크 구성도

Fig. 3 Network configuration for link aggregation

3.1.1 하드웨어와 소프트웨어 구조

개발하고자 하는 링크 통합 장비의 하드웨어 블록도는 그림 4와 같다. 링크 통합 기능과 방화벽을 이용한 네트워크 접근 통제 기능을 고려한 설계가 필요하다. CPU는 RISC 기반의 CPU(MIPS 기반)를 사용하여 고속 링크 통합과 접근 통제 기능을 구현한다.

링크 통합 장비의 운영체제는 임베디드 리눅스를 기반으로 한다. 소프트웨어 블록도는 그림 5와 같이, 부팅 위한 부트로더(boot-loader)와 리눅스 커널로 구성되며, 리눅스 커널에는 네트워크 프로세서 구동을 위한 디바이스 드라이버(device driver)와 펌웨어, 링크 통합 처리를 위한 디바이스 드라이버, 접근 통제를 위한 디바이스 드라이버 등으로 구성된다.

링크 통합 기능은 네트워크 프로세서(processor)를 이용하여

그림 4 하드웨어 블록도

Fig. 4 Hardware block diagram

그림 5 소프트웨어 블록도

Fig. 5 Software block diagram

구현하며, 네트워크 프로세서는 네트워크 포트들로부터 들어오는 패킷을 트렁크 포트(trunk port)로 구성된 포트에 분배하여 전송한다. 각 트렁크 포트에 수신된 패킷은 네트워크 프로세서를 거쳐 네트워크 포트에 전송된다. 또한, 링크 통합을 수행하는 트렁크 포트의 링크 연결 여부를 감시하여 링크가 끊어졌을 경우, 해당 포트에 패킷을 전송하지 않도록 구성하여 오류 대체 작동(fail-over) 기능을 구현한다.

방화벽은 링크 통합 장비에 연결된 네트워크 설정과 구성을 변경하지 않고 지원되도록 한다. 방화벽 구성을 위한 접근 통제 정책 설정은 계층 2에서 VLAN ID, 계층 3에서 출발지 IP 주소, 목적지 IP 주소, 계층 4에서 출발지 TCP/UDP 포트 번호, 목적지 TCP/UDP 포트 번호를 제어할 수 있도록 한다.

위와 같이 링크 통합과 방화벽 기능을 수행하도록 개발된 보드는 아래의 그림 6과 같다.

그림 6 구현된 보드

Fig. 6 Implemented board

4. 실험 및 성능평가

본 연구를 통하여 개발된 링크 통합 장치의 성능을 입증하기 위하여 jperf ver 2.0.0을 사용하여 시험 하였다. 성능 시험을 위한 시스템 구성은 그림 7과 같다.

그림 7 성능 시험을 위한 시험 시스템 구성

Fig. 7 Test system configuration for performance testing

본 연구를 통해 개발된 보드를 이용하여 실험을 위한 장치 구성은 그림 8과 같다.

그림 8 실험을 위한 장치 구성

Fig. 8 Test equipment configuration

링크 통합에 대한 성능 측정을 위한 각 포트 구성은 아래의 표 1과 같다.

표 1 포트 구성

Table 1 Port configuration

1 포트	VDSL A pair만 이용하여 전송속도 측정
2 포트	VDSL A, B pair를 이용하여 전송속도 측정
3 포트	VDSL A, B, C pair를 이용하여 전송속도 측정
4 포트	VDSL A, B, C, D pair를 이용하여 전송속도 측정
5 포트	VDSL A, B, C, D, E pair를 이용하여 전송속도 측정

4.1 링크 통합 성능평가 결과

1번 포트를 이용하여 종포트(slave port)에서 주포트(master port)로 전송하였을 때(upload), 그림 9와 같이 18.60Mbps의 전송속도를 나타낸다.

그림 9 종포트에서 주포트로 전송(upload)(1번 포트)

Fig. 9 Transmission from slave to master on port 1(upload)

5번 포트를 이용하여 종에서 주로 전송하였을 때(upload)는 그림 10과 같이 81.50Mbps로 약 4.38배의 전송 효율을 나타냈다.

그림 10 종포트에서 주포트로 전송(upload)(5번 포트)
Fig. 10 Transmission from slave to master on port 5 (upload)

또한, 1번 포트를 이용하여 주포트에서 종포트로 전송하였을 때(download), 그림 11과 같이 37.30Mbps의 전송속도를 나타낸다.

그림 11 주포트에서 종포트로 전송(download)(1번 포트)
Fig. 11 Transmission from master to slave on port 1 (download)

5번 포트를 이용하여 주포트에서 종포트로 전송하였을 때(download)는 그림 12와 같이 93.00Mbps로 약 2.01배의 전송 효율을 나타냈다.

그림 12 주포트에서 종포트로 전송(download)(5번 포트)
Fig. 12 Transmission from master to slave on port 5 (download)

5. 결 론

저렴한 xDSL(Digital Subscriber Line)과 같은 회선을 활용하여 네트워크 환경이 열악한 지역이나 고속 네트워크를 구축하는데 많은 비용이 요구되는 지역에 고속 네트워크를 구축할 수 있는 기술은 소비자의 요구에 부응할 수 있으며, 네트워크 자원을 효율적으로 활용할 수 있기 때문에 매우 중요하다.

본 연구에서는 링크 통합 장비로 xDSL 장비와 같이 낮은 대역폭을 갖는 다중회선을 사용하여 고속 통신환경을 제공하는 보드를 개발하였다. 또한, 계층 2에서의 네트워크 보

안을 강화하여 외부로부터의 침입을 방지하고, 내부 사용자의 네트워크 접근 통제 기능을 제공하여 제한된 네트워크 대역폭을 보다 효율적으로 사용할 수 있는 기능을 제공하도록 하였다. 개발된 보드의 테스트 결과, 단일 라인을 사용하는 경우보다, 5개의 라인을 결합하여 실험한 결과, 다운로드(download)는 약 2배, 업로드(upload)는 약 4.38배의 전송 효율을 나타냈다.

참 고 문 헌

- [1] IEEE Std 802.1AX-2008 IEEE Standard for Local and Metropolitan Area Networks-Link Aggregation, IEEE Standards Association, 3 November 2008. <http://standards.ieee.org/getieee802/download/802.1AX-2008.pdf>.
- [2] Richard Foote, "Link Aggregation 802.3ad", Corporate Systems Engineering, June 22, 2001.
- [3] Water Thirion, "Link Aggregation Operations", jato Technologies, Inc., July 1998.
- [4] Ho-Young Lee, Soong-Hee Lee, Jong-Hyup Lee, Frame Distribution Methods for Link Aggregation between 10GbE Switches, Journal of Korea Information and Communications Society, Vol28, pp945~950, 2003. 12.
- [5] IEEE 802.3ad Link Aggregation(LAG) http://www.ieee802.org/3/hssg/public/apr07/frazier_01_0407.pdf
- [6] Higher Speed Ethernet Requirements http://www.ieee802.org/3/hssg/public/nov06/perkins_01_1106.pdf
- [7] <http://www.openmaniak.com/iperf.php#jperfer>

저 자 소 개

신 재 흥 (申在興)

1964년 10월 10일생. 1986년 한양대학교 전자공학과 졸업. 1997년 동 대학원 전자공학과 졸업(공학박사). 1997년~현재 동서울대학 디지털방송미디어과 부교수, 동서울대학 교수학습지원센터 책임교수

Tel : 031-720-2175

Fax : 031-720-2294

E-mail : jhshin@du.ac.kr

김 홍 렬 (金弘烈)

1964년 3월 2일생. 1986년 한양대학교 전자공학과 졸업. 1997년 동 대학원 전자공학과 졸업(공학박사). 2000년~현재 동서울대학 컴퓨터정보과 부교수

Tel : 031-720-2153

Fax : 031-720-2293

E-mail : rhkim@du.ac.kr

이 상 하 (李 相 夏)

1960년 6월 19일생. 1987년 울산대학교 전자계산학과 졸업. 2002년 아주대학교 대학원 컴퓨터공학과 졸업(공박). 1991년~1992년 (주)큐닉스컴퓨터. 1993년 ~1999년 (주)케이엔아이시스템. 2000년~현재 동서울대학 정보통신과 부교수

Tel : 031-720-2268

Fax : 031-720-2286

E-mail : shyi@du.ac.kr

허 용 민 (許 龍 珉)

1964년 3월 29일생. 1987년 한양대학교 전자공학과 졸업. 1996년 동 대학원 전자공학과 졸업(공박). 1996년~1999년 LG 정보통신 선임연구원. 현재 동서울대학 디지털전자과 조교수

Tel : 031-720-2176

Fax : 031-720-2263

E-mail : ymhur@du.ac.kr

이 상 철 (李 相 喆)

1952년 8월 13일생. 1977년 숭실대학교 전기공학과 졸업. 1991년 동 대학원 전기공학과 졸업(공박). 1981년~현재 동서울대학 전기정보제어과 교수

Tel : 031-720-2065

Fax : 031-720-2262

E-mail : sclee@du.ac.kr