Access-Control List 가 MPLS GE 성능에 미치는 영향에 대한 연구

김광현*, 박승섭**
*경남정보대학 컴퓨터정보계열
**부경대학교 전자컴퓨터정보통신공학부
e-mail:kkh@kit.ac.kr

A Study for Effect of Access-Control List to MPLS GE Performance

Kwang-Hyun Kim*, Seung-Seob Park**
*Subdivision of Computer Inforamtion, Kyungnam College of Inforamtion & Technology
**Electronics, Computer and Telecommunication Engineering, Pukoung National University

Abstract

Multiprotocol Label Switching is an initiating IETF that integrated Layer2 information network links(bandwidth, latency, utilization) to Layer 3(IP) with a particular autonomous system(or ISP) in order to simplify and improve IP-packet exchange. MPLS gives network operators a grate deal of flexibility to divert and route traffic around link failures, congestion, and bottlenecks. The MPLS has advantages that will be able to solve existing problem of Network that ISP have had IP, QoS, Gigabit forwarding and traffic engineering. The purpose of this study is to measure Access-list and the capacities of PE Router that would operate as MPLS. Many ISP using MPLS service to handle high-speed internet traffic with apply to firewall in future.

1. 서론

최근 TCP/IP 기반의 인터넷 프로토콜이 컴퓨터 통신망의 실질적인 표준으로 확고히 자리 잡게 되면서, 인터넷은 수천 만 명의 사용자를 연결하는 세계적인 공공 데이터 망으로 성장하게 되었다. 특히 인터넷이 본격적인 상업망으로 전환되기 시작하면서 급격하게 양적인 팽창을 거듭하고 있으며, 더욱이 멀지 않은 미래에는 정보 통신 기술과 컴퓨터, 지능형 전자 제품들이 보급됨에 따라서 인터넷의 수요가 폭발적으로 증가될 것으로 예상되고 있다.

최근 이와 같은 인터넷의 새로운 변화를 수용하면서 고속화 (High-Speed)와 QoS (Quality of Service)를 제공할 수 있는 차세대 인터넷 망으로 진화하기 위한 하나의 움직임으로써 IP와 고속 멀티 서비스 ATM (Asynchronous Transfer Mode) 교환 기술의 통합이 활발히 진행 중에 있다.

이처럼 IP와 ATM의 고속 멀티 서비스 교환 기술을 이용하여 기존의 LAN (Local Area Network) 트래픽 및 인터넷 트래픽을 고속으로 처리하고 다양한 부가 서비스를 제공할 수 있는 방식으로 IETF (Internet Engineering Task Force)의 MPLS (Multi-Protocol Label Switching) 기술이 있다. MPLS 기술은 기존의 라우팅 방식을 기반으로 ATM의 고속 멀티 서비스 교환 기능을 결합하여 IP 패킷을 전달하는 방식으로써 대규모의 망에서 고속의 데이터 전송과 함께 다양한 부가 서비스 제공을 목적으로 한다.

그러므로 MPLS는 IP 기반에서 ATM의 고속 멀티 서비스 교환 기능을 수용함으로써 기존의 IP가 지니고 있는 많은 제약 사항을 해결할 수 있으며, 기존의 망에서 제공할 수 없었던 고속 서비스와 다양한 부가 서비스를 창출할 수 있기 때문에 망 사업자들로부터 차세대 인터넷으로 진화할 수 있는 새로운 핵심 기술로 평가 받고 있다.

본 논문에서는 현재 국내 초고속 국가망의 MPLS-VPN의 Edge 장비로 채택되어 사용되고 있는 CISCO 사의 ESR(Edge Service Router) 1000Serise 장비를 이용하여

MPLS Network의 구성 요소 중 고객 서비스의 중심이 되는 PE(Provider Edge)의 성능 중에서 패킷별 보안의 핵심이 되는 Access-List 가 Router 성능에 미치는 영향에 대하여 시험망을 구축하여 측정 결과를 비교 분석 하였다. 2장에서는 MPLS Network 의 성능이 중요한 이유에 대하여 기술 하고 3장에서는 성능분석을 위한 시험망 구성을 위한 장비 및 일반적인 MPLS Network 에 대하여 설명하고 4장에서 ACL(Access-List) 적용 전후의 성능 분석 결과에 대하여 설명 하였다.

2. 시험목적

MPLS 망이 도입된 이유 중 한 가지는 인터넷 트랙픽이 폭발적으로 증가하고 있기 때문이다. 인터넷의 이러한 추세에 따라 많은ISP(Internet Service Provider) 들이 등장하게 되었는데, 이들의 당연한 관심은 "어떻게 한정된 network resource를 효과적으로 이용하여 고객들의 트래픽을 전송할 것인가"이다. 기존의 IP routing 방식은 주로 목적지를 찾아가기 위해 최단거리 중심으로 packet의 next hop을 결정하게 되어 있으므로 망의 트래픽이 폭주하는 곳이 있는 반면, 한가한 곳도 동시에 존재할 수 있다. Client-Server 환경에서 어떤 server의 사용률이 매우 높고, client는 전세계에 분산되어 있다고 생각해보면 문제점이 좀더 명확해질 것이다. 기존의 방식으로 이를 해결하려고 하면, 일시적으로는 congestion control mechanism에 의해 해당 TCP 모듈에서 전송률을 낮추게 될 것이며 극단적인 경우는 TCP connection이 끊어지는 경우도 있을 것이다. 장기적으로는 이러한 현상이 계속 발생한다는 것은 망의 용량이 부족하다는 것을 의미하며 이를 위해서는 bandwidth를 늘려야 할 것이다. 그러나, backbone 망을 운영하는 ISP 입장에서는 최단 거리는 아니지만, traffic을 분산할 수 있다면, 폭주 시에 발생하는 congestion control을 적용하지 않아도 되며, 망의 투자비용을 최소화하면서 고객의 만족을 추구할 수 있을 것이다. 비효율적인 자원 할당으로 인한 congestion 발생 시는 load balancing 기법을 적용함으로써 이를 극복할 수 있을 것이다. Load balancing의 목적은 효율적인 자원 할당을 통해 congestion 발생 가능성을 줄이며 자원 활용률을 최대로 높이는 것이다. Congestion 발생 빈도가 줄어들면 packet loss 율도 하락할 것이며 전체적으로는 망의 throughput의 증가가 있을 것이다. 결과적으로 이는 사용자가 더 좋은 질의 network service를 받을 수 있는 것을 의미한다.

본 고에서는 인터넷 트래픽의 향상과 고객측 으로부터 나오는 모든 패캣의 분석을 통하여 필요 없는 트래픽과 망 전체에 영향을 미치는 특정 패킷의 차단을 위해 TCP/IP 보안에 많이 적용되는 Access-List 가 MPLS 가 도입된 NETWORK에서 고객의 트래픽을 수용하는 PE Router 에서 장비 Performance 에 미치는 영향에 대한 시험 결과로서 전 세계 Router 마켓의 80% 이상을 차지하고 있는 CISCO 사의 QoS 기반 ESR 장비를 대상으로 성능 측정을 함으로서 보안의 중요성이 더욱 강조되고 있는 시점에서 가입자 망 END부분과 연결되어 있는 MPLS 네트워크의 PE 라우터에 MPLS 적용 전후의 보안적용에 대한 성능 비교는 매우 중요하다고 하겠다.

3. 시험환경

3.1 MPLS Network 의 일반 구성

MPLS는 layer 2 switching에 기반한 packet forwarding과 layer 3 routing의 장점을 결합한 형태로 packet기반 또는 cell기반의 network에서 packet전송을 위해 label을 이용하며 이더넷, Frame Relay, ATM, SONET과 같은 일반적인 Layer 2 protocol에 모두 적용하여 보다 빠른 성능의 Data 전달을 위하여 사용된다.

기존의packet forwarding에서는 packet의 목적지 IP 주소에 의해 전송하지만, MPLS에서는 망의 edge에서 IP 주소를 고정된 길이의 label에 mapping한 다음 이 label을 이용하여 packet을 forwarding 하기 때문에 H/W에 의한 고속 스위칭이 가능해 진다.

MPLS에서 Label을 부여하고 분배하는 것은 LDP(Label Distribution Protocol), RSVP, BGP 등의 protocol을 사용하며 label 분배 protocol에 따라 동적 또는 고정된 경로(LSP: Label Switched Path)를 따라 packet을 전송할 수 있다. 이 경로(LSP)는 송수신 경로상의 각 노드에서 가지는 label들의 sequence로 볼 수 있으며data가 전송되기 전에 미리 설정되어 있거나 (control-driven), 특정data flow를 보고 설정할 수 있다 (data-driven).

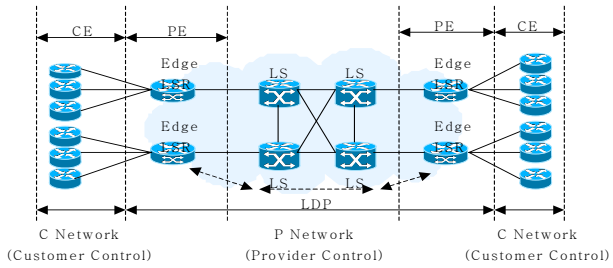


그림1 .MPLS Network 의 일반 구성

- LSR(label switch router) : label을 분배하고 label에 기반해서 packet을 전송하는 라우터 또는 스위치를 말한다.
- Edge LSR(LER) : MPLS network의 edge에서 label을 부여 또는 제거하는 라우터를 말한다.

3.2 시험 대상 장비

- Router 군
  - CISCO ESR 10008 1대 - CISCO ESR 10005 1대
  - Gigabit Ethernet Card 2개 - PRE Card 4 개
  - Gigabit Ethernet Card 2개
- 시험 대상 IOS Version : 12.0(17)SL1
- 시험 대상 Performance 측정 장비 : Smartbit 2000

4. 성능분석 결과

4.1 IP Performance 측정 (ACL 적용전)

4.1.1 시험 구성

ESR의 Architecture 특성상 622M 이상의 고속 모듈에서는 각 Interface마다 Output Queue가 2개씩 있는데, 2개의

Queue를 이용하여 최대의 성능을 얻기 위해서는 20개 Streams이상의 트래픽이 발생하여야 한다. 이와 같은 특징으로 상용망 에서의 실제 성능과 같은 환경하에 측정을 하기 위하여 본 시험에서는 90 개의 stream을 SMARTBIT 에서 단방향 및 양방향으로 발생하여 Gigabit Interface Module 의 성능을 측정하였다.

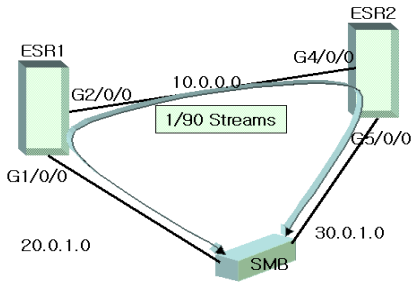


그림 2 Gigabit Ethernet Performance 측정 구성

4.1.2 시험 결과 및 분석

아래 시험 결과는 Smartbit에서 90개의 Stream을 Frame Size 64 Byte 에서1024 Byte 까지 변화를 주면서 발생시켰을 경우의 성능 시험 결과로서 256Byte 이상에서는 95 % 이상의 Performance 를 보이고 있다. 참고로 아래의 그래프 를 보면 ESR의 특성 즉 PRE Card 의 PXF 구조에 의한 Queuing 방식으로 1 Stream만으로 시험 하는 경우 작은Packet에 대해 성능 저하가 심한 것을 볼 수 있다.

표 1 Inbound Gigabit Ethernet Performance with ACL

구분	단방향(90 Stream)			양방향(90 Stream)		
Size	PPS	Mbps	Util (%)	PPS	Mbps	Util (%)
64	1,250,020	640.0	84.00	1,250,020	640.0	84.00
96	1,077,605	827.6	100.00	1,077,605,	827.6	100.00
128	844,611	864.9	100.00	844,611	864.9	100.00
256	400,648	820.5	88.46	400,648	820.5	88.46
320	359,203	919.5	97.70	363,378	930.2	98.84
512	228,107	934.3	97.08	228,107	934.3	97.08
768	152,442	936.6	96.10	152,442	936.6	96.10
1024	115,317	944.7	96.31	114,054	934.3	95.26

64 Packet 과 256 Packet에 대해 90 % 이하의 성능을 보이고 그외의 Frame Size에 대해서는 95 % 이상의 성능을 보인다.

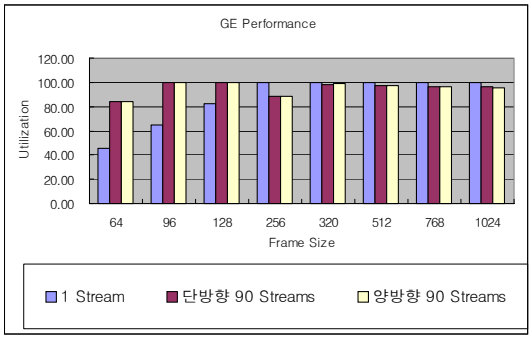


그림 3 Gigabit Ethernet Performance 결과 Graph

4.2 IP Performance 측정 (120 ACL 적용후)

4.2.1 시험망 구성 및 시험 환경

120개의 List를 갖는 Access-list를 선언 후 Router 의 Access-List 에 의한 Performance 영향을 알아 보기 위하여 90개 Streams중에서 하나의 Stream만 Access-list의 120번째에서 Accept 되게 하고 나머지 89개 Streams은 Drop 되도록 Access-list 구성하여 Inbound / Outbound 에 차례로 적용 후 성능 시험을 하였다.

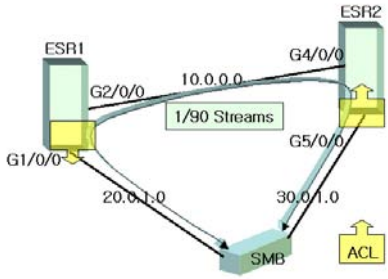


그림 4 GE with 120 ACL(Access Control List) Performance 구성도

4.2.2 Inbound ACL 적용 시험 결과

120개의 ACL을 GE Inbound 쪽에 설정 하였을 경우 96 bytes이하의 작은 Packet에 대해서 71 ~ 83 %의 성능 저하가 발생하였으나 128 이상에서는 추가적인 성능 저하는 없었다. 즉 ACL 에 의한 Performance 는 적은 Byte 에서는 그 만큼의 Header 조사 및 ACL 적용 여부를 판단하기 위하여 성능이 저하됨을 알 수 있다.

표 2 Inbound Gigabit Ethernet Performance with ACL

Size	PPS	Mbps	Util (%)
64	894,000	457.7	71.52
96	905,000	695.0	84.0
128	844,611	864.9	100.0
256	400,648	820.5	100.0
320	361,500	925.4	100.0
512	228,107	934.3	100.0
768	152,442	936.6	100.0
1024	114,054	934.3	99.00

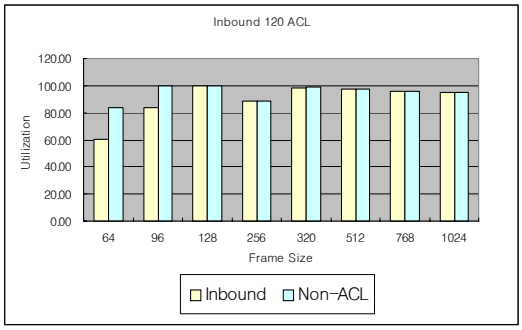


그림 5 Inbound GE Performance with ACL

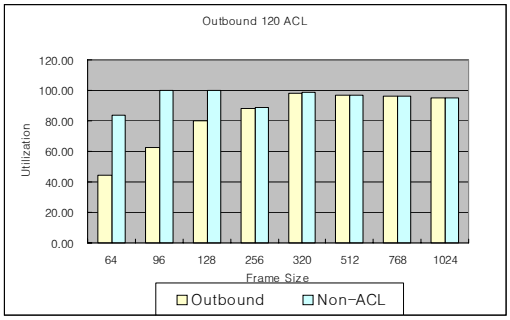
4.2.3 Outbound ACL 적용 시험 결과

120 ACL을 GE Outbound 쪽에 설정 하였을 경우 128 bytes 이하의 작은 Packet에 대해서 52 ~ 79% 성능 저하 발생 발생하였으나 256 이상에서는 추가적인 성능 저하는 발생하지 않았다. 즉 Inbound 에서 보다 성능 저하가 심한 이유는 Traffic 이 Outbound 로 나가기 위하여 라우터의 모든 Resource 를 사용하기 때문에 그만큼 성능이 떨어지는 현상을 발견 할 수 있다. 하지만 일정 Byte 이상

에서는 뚜렷한 성능 저하 현상을 발견 할 수 없었다.

표 3 Outbound Gigabit Ethernet Performance

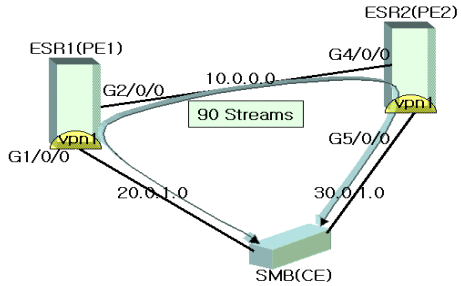
Size	PPS	Mbps	Util (%)
64	657,000	336.4	52.6
96	675,000	518.4	62.6
128	674,500	690.7	79.9
256	400,500	820.2	100.0
320	361,400	925.2	100.0
512	228,100	934.3	100.0
768	152,440	936.6	100.0
1024	114,054	934.3	99.0



4.3 GE with MPLS TEST(ACL 적용 전/후 비교)

4.3.1 시험망 구성 및 시험 환경

아래 그림과 같이 ESR 두대를 각각 PE! / PE2 로 설정하고 MPLS 를 enable한후 SmartBit을CE로 설정하여 하나의 Intranet VPN1을 구성하였고 Smartbit에서 90 Streams을 이용하여 양방향으로 트래픽 발생시켜 Gigabit Ethernet 의 Performance 를 측정하였다



4.3.2 시험 결과

Inbound ACL 적용 시, 64byte, 96byte의 performance 저하는 MPLS와는 무관하며, IP+ACL에서와 같이 Header 조사 및 ACL 적용 여부를 판단하기 위하여 성능이 저하되었으나 MPLS로 인한 추가 performance 저하는 발생하지 않았다. Outbound ACL 적용 시, 64, 96 byte 이하에서 performance 저하는 outbound ACL 처리를 위해 PXF pass를 추가로 거치기 때문으로 MPLS의 적용 시, IP보다 더욱 저하되었다.

구분	Non-ACL			Outbound 120 ACL			Inbound 120 ACL		
Size	PPS	Mbps	Util(%)	PPS	Mbps	Util(%)	PPS	Mbps	Util(%)
64	1,304,000	666.7	87.6	691,000	353.8	46.4	887,000	454.1	59.6
96	1,041,600	799.9	96.7	693,000	532.2	64.3	899,000	690.4	83.4
128	822,400	842.1	97.4	691,000	707.6	81.8	822,300	842.0	97.4
256	402,000	823.3	88.8	428,000	876.5	94.5	401,700	822.7	88.7
320	363,300	930.1	98.8	363,300	930.1	98.8	363,300	930.1	98.8
512	233,200	955.2	99.3	231,480	948.1	98.5	233,200	955.2	99.3
768	157,000	964.6	99.0	156,900	964.0	98.9	157,800	969.5	99.5
1024	119,270	977.1	99.6	119,270	977.1	99.6	119,270	977.1	99.6

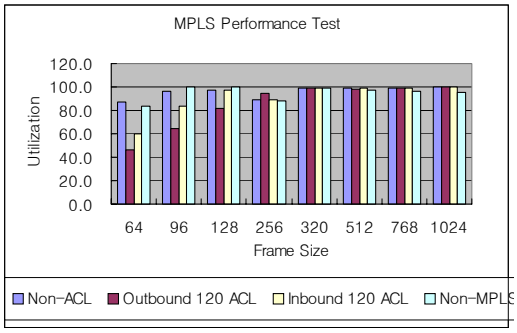


그림 8 GE with MPLS TEST 비교 Graph

5. 결론

향후 ISP 망의 MPLS 서비스는 다양한 Enterprise의 요구를 수용하면서 고품질 서비스를 보장하는 서비스로 발전하리라 생각되며, 이를 위해 가장 중요한 요소는 MPLS 망 장비의 Reliability, QoS 및 다양한 feature라고 할 수 있다.

MPLS 는 IP, QoS, Gigabit Forwarding, Network Scaling,과 Traffic Engineering 과 같은 기존에 ISP 들이 가지고 있던 Network 의 문제점을 개선 할 수 있는 장점이 있다.

본 논문은 향후 고속의 Internet Traffic 을 처리하기 위하여 여러 ISP들이 사용하게 될 것으로 예상되는 MPLS 서비스의 핵심으로 운영되고 있는 PE Router 의 Gigabit Ethernet 의 ACL 별 성능을 객관적으로 측정하는데 그 목적이 있었다.

향후의 과제는 현재의 MPLS기술에 Label 을 대신한 파장(Lambda)을 이용한 GMP- LS(Generalized MPLS) 의 상용화와 ISP 입장에서 고객의 서비스 극대화를 위한 QoS 별 효과적 트래픽의 배분에 있다고 할 수 있다.

참고문헌

[1] Vivek Alwayn, " MPLS Design and Implementation" CISCO Press, September 2001.

[2] Jim Guichard, Ivan Pepelnjak, "MPLS and VPN Architecture" CISCO Press, Octorber 2000.

[3] "CISCO 10000 Series Product Overview" CISCO Systems, May 2001.
-http://www.cisco.com/warp/customer/cc/pd/rt/10000/prodlit/c10sp_ds.htm

[4] S. Halabi, " Internet Routing Architecture", CISCO Press, 2000

[5] G.Swallow, "MPLS for Traffic Engineering, IEEE Communications, Vol.37,Dec 1999.