□ 研 究 論 文 □

韓國國防經營分析學會誌

제 30 권, 제 1 호, 2004. 6. 30.

MPLS와 DiffServ를 이용한 국방전산망 데이터 트래픽 QoS 보장 방안 (A DISN's Data Traffic QoS Assurance Scheme using MPLS and DiffServ)

김 성 순, 이 승 종*

Abstract

Today's Internet is providing a single service which is so-called "best-effort service". Now, multimedia and real-time applications are not only demanding large bandwidth but also requiring high QoS. For this, MPLS and DiffServ technology can be adopted to support more scalability and QoS for data traffic engineering. The DISN(Defense Information Systems Network) supports CBR service for voice traffic and VBR service for data traffic which is best-effort service.

We propose how to adopt MPLS and DiffServ technology to support traffic engineering and guarantee QoS in the DISN. A traffic analysis according to prioritized traffic classes is done using OPNET simulation tool for assuring QoS. The result shows that low priority packets are delayed a little bit, but high priority packets are transferred more efficiently than without traffic engineering.

(**Keyword** : MPLS, DiffServ, QoS)

* 국방대학교 관리대학원

1. 서 론

최근 TCP/IP 기반의 인터넷 프로토콜이 컴퓨터 통신망의 실질적인 표준으로 확고히 자리 잡게 되면서 인터넷은 세계적인 공중 데이터망으로 성장하게 되었다[1]. 특히 인터넷이 본격적인 상업망으로 전환되기 시작하고, 고속 모뎀, 케이블 모뎀, ADSL (Asymmetric Digital Subscriber Line) 등의 다양한 고속 액세스(Access) 장비, 인터넷 컴퓨터 및 홈 네트워킹(home networking) 가전제품들이 보급됨에 따라서 인터넷의 수요가 폭발적으로 증가되고 있다. 하지만 현재 사용되고 있는 IP 기반 인터넷은 고속의 데이터 전송, 확장성, Best-effort 서비스에 따른 인터넷 QoS(Quality of Service) 측면에서 심각한 문제점이 제기 되었다. 이러한 문제점을 해결하기 위해서 빠른 스위칭(switching)을 제공할 수 있는 기존의 교환 기술을 이용한 데이터 링크 계층에서의 교환 전송 방식을 제안하고 있다.

세계적인 각 기업들은 이에 대한 독자적인 기술을 개발 중이며 IETF는 MPLS 워킹 그룹을 조직하여 이런 독자적인 기술들을 종합한 표준 프로토콜을 개발 하였다. Ipsilon사에 의해서 처음으로 데이터링크 계층 전송 방식이 대두되었던 초기에는 네트워크 계층 프로토콜로 IPv4와 IPv6에 초점을 맞추었으나 MPLS는 다른 모든 네트워크 계층 프로토콜을 사용할 수 있도록 확장되었고 또한 하부 물리적인 망으로 LAN, ATM 그리고 Frame Relay 등 모든 전송 방식에 대해서도 사용할 수 있도록 확장되었다.

MPLS는 현재 이용되고 있는 라우팅 프로토콜을 포함한 다양한 통신 프로토콜 및 서비스를 그대로 이용할 수 있으며 QoS 보장, 트래픽 엔지니어링 등의 장점을 가지고 있다[2].

MPLS는 인접한 라우터들과 협상하는 레이블 분배 프로토콜(Label Distribution Protocol)을 이용하여 IP 패킷을 전송하기 위한 LSP(Label Switched Path)를 설정한다. 설정된 LSP로 짧고 고정된 길이의 레이블을 이용하여 동일한 FEC(Forwarding Equivalence Class)에 속하는 IP 패킷을 전달하는 방식으로 기존 라우터의 IP 패킷 전달 방식인 LPM(Longest Prefix Match)방식에 비해서 전달 속도를 향상 시킨다[2].

이와 같이 레이블을 이용한 단순한 전달 방식에 의해서 고속화의 달성은 쉽게 이루어질 수 있지만 QoS 제공이 가능하기 위해서는 부가적인 기능을 필요로 한다. 특히 서비스 클래스에 따라서 서비스 처리를 차별화 하는 IETF에서 연구 중인 IntServ와 DiffServ를 지원하는 것이 중요한 이슈가 되고 있다. IntServ는 RSVP(ReSource Reservation Protocol)라는 자원예약 신호 프로토콜을 이용하여 모든 라우터가 특정 패킷 흐름(flow)마다 자원을 예약하고 할당한다[3][4]. 이 때문에 라우터는 각 패킷 흐름별로 유지해야 하는 연결 상태 정보의 양이 많아져 방대한 저장 공간이 필요하게 되고 이로 인하여 처리부하가 증가하게 된다. 특히, 인터넷 백본 라우터의 경우 전송 속도가 빠르고 연결된 패킷 흐름의 수가 많기 때문에 라우터가 유지해야 하는 상태 정보의 양이 더욱 증가하게 되어 확장성의 문제가 발생한다. 이러한 문제를 보완하기 위해 제안된 DiffServ는 패킷을 클래스(Class)별로 분류, 처리하여 트래픽과 확장성 문제를 해결한다[5].

인터넷의 고속전송 및 QoS 보장의 필요성은

ISP 뿐만 아니라 ATM 백본 기반의 군 독자망인 국방전산망 역시 네트워크에서 트래픽 혼잡이 발생하더라도 실 시간대의 각종 상황자료를 필요로 하는 지휘관들에게 빠르고 신뢰성 있는 의사 결정을 지원하기 위하여 필요하다.

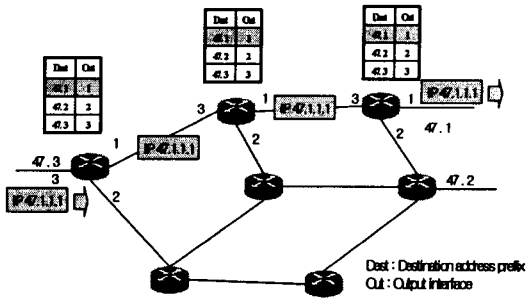
본 논문에서는 현재 Best-effort 서비스만을 지원하는 TCP/IP 기반의 국방전산망에서 MPLS기술과 DiffServ기술을 적용하여 군 기능별 QoS를 보장하기 위한 방안을 제시하여 차세대 국방전산망 구축에 기여하고자 한다. 이를 위해 논문에서는 서비스 클래스 매핑 제안과 이를 근거로 군 기능별 MPLS와 ATM 서비스 클래스로의 매핑을 제안한다. 또한 국방전산망에 MPLS와 DiffServ기술을 적용했을 때 실제로 QoS를 보장하는지 여부를 검증하기 위해서 시뮬레이션을 실시하였다.

2. MPLS와 DiffServ 관련기술

2.1 MPLS

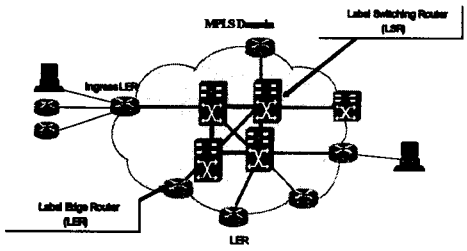
2.1.1 MPLS 개요

기존 라우터에서 포워딩 동작은 각 IP 패킷 헤더를 검사하여 다음 홉을 결정한 후 다음 홉으로 패킷을 전송하는 방식을 따른다. 이러한 방식은 각각의 패킷마다 수행되어야 하며, 또한 라우팅 경로 내의 모든 라우터에서 수행되어져야 하므로 트래픽 처리에 효과적이지 않다. <그림 2-1>은 전통적인 IP 라우팅 운용의 예이다.



<그림 2-1> 전통적인 IP 라우팅 운용

이러한 기존 라우터의 전송 방식과 달리 MPLS는 짧고 고정된 길이의 레이블을 이용하여 3계층(네트워크 계층)을 거치지 않고 패킷을 포워딩 할 수 있게 하였다. 따라서 MPLS는 단순한 포워딩 과정을 통해 기존의 IP 포워딩에 비해 망에서의 전달 속도를 증가시킨다. 이러한 MPLS의 단순 포워딩 과정은 3계층의 라우팅과 2계층의 스위칭 기능 결합을 통해 이루어진다. 즉 MPLS 망의 입구(Ingress)에서 3계층의 라우팅 정보를 바탕으로 패킷이 어떤 FEC에 속하는지 구분한 후, 각각의 FEC마다 레이블을 할당하고 FEC에 해당하는 패킷들에 대하여 할당된 레이블 값을 각 패킷에 캡슐화(Encapsulation)하여 다음 홉으로 전송한다. 레이블된 패킷을 수신한 다음 노드는 더 이상 3계층 정보를 분석할 필요 없이 레이블된 패킷의 레이블 값만을 검사하여 패킷 전송 처리를 수행하므로 망에서의 처리 속도를 빠르게 할 수 있다[6]. <그림 2-2>는 MPLS 망의 구조를 나타내고 있다.



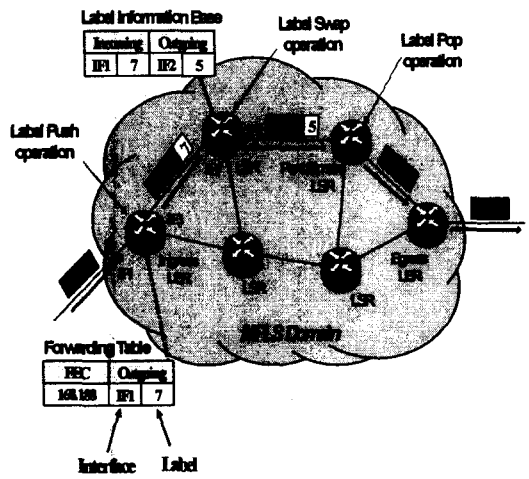
<그림 2-2> MPLS 망 구조

2.1.2 MPLS 주요 기능

MPLS는 라우팅과 패킷 포워딩을 분리하기 때문에 2계층의 스위칭 기술을 이용하여 기존의 3계층 라우팅에 비해 빠른 패킷전달을 제공할 수 있다. 또한 MPLS는 3계층과 독립적으로 수행되므로 다양한 3계층 프로토콜(예, IPv4, IPv6, IPX, Appletalk 등)을 지원 할 수 있으며, 다양한 2계층 장비(예, Ethernet, frame relay, ATM 등)상에서도 동작한다. MPLS의 주요 특징을 알아보면 레이블 스위칭에 의한 빠른 패킷 전달, 효과적인 명시적 라우팅, 트래픽 엔지니어링, QoS 라우팅 및 제약 기반 라우팅이라 할 수 있고, MPLS의 핵심 요소는 특정 데이터 흐름에 레이블을 대응하는 레이블 바인딩(label binding), 입력 레이블을 출력 레이블로 변경하는 레이블 교환(label swapping), 레이블 바인딩 정보를 인접 노드에게 전파 하는 레이블 분배(label distribution)라 할 수 있다[7].

가. MPLS 패킷 전달

일반적으로 IP 프로토콜 상에서 라우터가 패킷을 다음 홉으로 전달하기 위해서는 패킷들을 FEC로 분류하고 각각의 FEC를 다음 홉으로 사상하는 기능이 모든 라우터에서 수행되어야만 한다. 그러나 MPLS 에서는 패킷이 전달되는 경로인 LSP가 설정되어 있는 경우에 이러한 일들이 MPLS 망에 들어갈 때 한번만 발생한다. 즉, 어떤 한 FEC에 속하는 패킷을 레이블이라고 하는 식별자가 그 패킷에 삽입되어 레이블된 패킷이 되고, 이 레이블된 패킷을 받은 LSR은 네트워크 계층의 헤더를 조사할 필요 없이 곧바로 그 레이블 값을 인덱스로 사용하여 다음 홉을 결정한다. 레이블 스위칭에서는 레이블 삽입(label push), 레이블 교환(label swap), 레이블 삭제(label pop)와 같은 세 가지 연산이 사용된다[7]. <그림 2-3>은 MPLS에서 레이블을 이용한 패킷 전달 과정이다.



<그림 2-3> MPLS 패킷전달 과정

<그림 2-3>에서 각 입구 LER과 LSR들은 3계층 라우팅 프로토콜 동작에 의해 생성된 라우팅 정보를 바탕으로 FEC에 대한 정보를 담고 있는 FIB(Forwarding Information Base)를 구성하게 된다. 또한 입구 LER과 LSR들은 레이블 스위칭을 위해 각 FEC마다 레이블을 할당하게 되는데, 이러한 레이블 할당 및 해지를 위해 각 라우터에는 LDP가 동작해야 한다[8]. 각 LER 및 LSR은 LDP 동작을 통해 레이블 스위칭에 필요한 LIB(Label Information Base)를 생성한다. LIB 구성 요소로는 각 FEC에 해당하는 입력 인터페이스, 출력 인터페이스, 입력 레이블, 출력레이블로 이루어져있다. 이와 같이 각 MPLS 라우터에 의해 생성되는 FIB와 LIB는 실제 패킷이 MPLS 망으로 입력되어 전송될 때, 고속의 패킷 스위칭에 필요한 정보들이다.

<표 2-1>과 <표 2-2>는 FIB 테이블과 LIB 테이

블을 나타낸다.

<표 2-1> FIB 테이블

Destination IP	Next Hop Address	Net Mask	Destination Port	Interface	FEC
168.188.1.1	168.189.1.5	168.189	21(예:FTP)	Interface 1	168.188

<표 2-2> LIB 테이블

Input Port	Input Label	Output Port	Output Label
Interface 1	7	Interface 2	5

입구 LER과 LSR에서 세부적인 패킷 전달과정을 살펴보면 다음과 같다[2].

- 입구 LER에서의 패킷 전달과정

  우선 패킷이 MPLS 망의 입구 LER로 입력되면 입구 LER은 입력된 패킷의 헤더를 검사하고 3 계층 라우팅 정보를 기반으로 이미 구성되어진 FIB를 참조하여 입력된 패킷이 어떤 FEC에 속하는지를 판단한다. 입력된 패킷의 FEC가 결정 되면, 그 FEC에 해당하는 출력 레이블을 패킷에 캡슐화 한다. 이렇게 출력 레이블로 캡슐화된 패킷을 레이블된 패킷이라고 하며, 레이블된 패킷은 해당 출력 인터페이스로 전달되어 다음 홉으로 전송된다.

- LSR에서의 패킷 전달과정

  입력 인터페이스로부터 레이블된 패킷이 입력되면, 입력된 패킷의 레이블 값을 검사한다. 그리고 LIB를 참조하여 입력 레이블에 해당하는 출력 레이블 및 출력 인터페이스 결정하여 입력 패킷의 레이블을 출력 레이블로 교체하여 해당 출력 인터페이스로 전달하여 다음 홉으로 레이블된 패킷을 전송 한다.

나. FEC와 레이블

FEC는 특정 LSR에서 같은 방식으로 처리되는 3계층 패킷의 집합을 의미한다[7]. 예를 들어 목적지가 같은 IP 패킷들 또는 같은 서비스로 처리되는 패킷들은 하나의 FEC로 볼 수 있다. 이러한 FEC는 레이블이라고 하는 짧고 고정된 길이의 식별자와 대응된다. 레이블은 하나의 데이터 흐름을 간략한 형태로 표현한 것이며, 라우터에서 해당 패킷에 대해 전송 결정을 내리기 위한 정보로 사용되므로 패킷 헤더의 축소된 의미라 할 수 있다. 하나의 레이블 값은 두 개의 이웃한 MPLS 노드 사이에서만 의미가 있다. 이것은 레이블 값을 지역적인 의미로 국한함으로써, 두개의 MPLS 노드만 있어도 MPLS 동작을 할 수 있고, 두 개 이상의 MPLS 노드가 존재할 때에는 한 쌍의 MPLS 노드 사이에서 사용된 레이블 값은 다른 쌍의 MPLS 노드에서 사용된 레이블 값과 무관하게 사용될 수 있다는 장점이 있다. 이렇게 지역적인 의미로 사용하도록 함으로써, 레이블의 사용 및 관리를 보다 간단하게 할 수 있다. 레이블은 2계층 헤더 내(예를 들어 ATM 의 VPI/VCI)에서도 표기 할 수 있으며, MPLS의 경우에는 <그림2-4>에서 도시된 그림과 같이 MPLS Shim 헤더를 사용하여 표기한다[6][9].

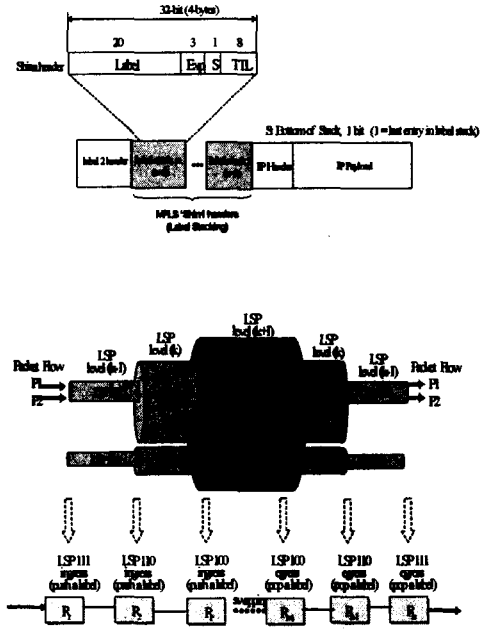
Label	EXP	S	TTL
20	3	1	8

Label : Label value　　S : Bottom of Stack
EXP : Experimental Use　　TTL : Time to Live

<그림 2-4> MPLS Shim 헤더

다. MPLS 계층구조

MPLS에서는 레이블 스택을 사용하여 다중 계층 구조를 갖는 라우팅을 지원할 수 있다. LSP안에 또 다른 LSP를 가짐으로써 LSP 터널 구조를 형성하는 것으로, 모든 패킷 전달 결정은 스택의 맨 위에 있는 레이블 값에 기초한다. <그림 2-5>는 LSP안에 또 다른 LSP를 갖는 다중 계층 구조와 레이블 연산을 보여주고 있다[10].



<그림 2-5> LSP 다중 계층 구조

2.1.3 MPLS 시그널링 프로토콜

MPLS에서는 레이블 할당 및 분배를 위한 프로토콜로서 두 가지를 정의하고 있다. 첫 번째는 기존의 라우팅 프로토콜이나 제어 프로토콜 속에 FEC와 레이블의 바인딩 정보를 포함시키는 피기백하는(Piggybacking) 방식이며, 두 번째는 MPLS에서 새로이 정의된 LDP프로토콜이다[7].

LDP 프로토콜은 LSR이 네트워크 계층의 라우팅 정보를 데이터 링크 계층의 스위치된 경로로 직접 매핑 함으로써 네트워크 상에 LSP를 설정할 수 있도록 정의된 프로시저와 메시지들의 집합이다[8]. LDP 메시지는 크게 다음과 같이 구분될 수 있다.

- Discovery 메시지 : 네트워 안에 LSR의 존재를 알려주거나 유지하기 위해서 사용되는 메시지
- Session 메시지 : LDP를 발생시키는 LSR들 간에 세션(Session)을 설정하고 유지하거나 해제하기 위하여 사용되는 메시지
- Advertisement 메시지 : FEC에 대한 레이블 매핑을 생성, 변경, 혹은 삭제하기 위하여 사용되는 메시지
- Notification 메시지 : 에러 및 유용한 정보를 알려주기 위하여 사용되는 메시지

그리고 레이블을 할당하는 방식으로 다음의 네 가지 경우가 있다.

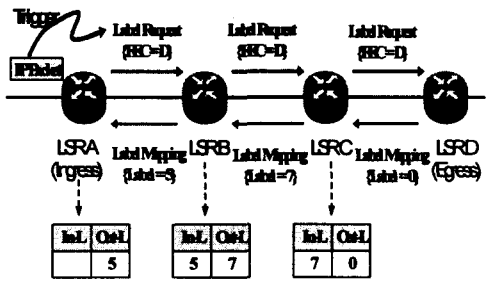
- 상위 LSR 레이블 할당(Upstream Label Allocation) : 상위 LSR이 레이블을 할당하여 하위 LSR에게 전달함으로써 LSP를 설정하는 방식
- 요구시 상위 LSR 레이블 할당(Upstream Label on Demand Allocation) : 하위 LSR이 레이블을 요구했을 때 상위 LSR이 레이블을 할당하여 하위 LSR에게 전달하여 LSP를 설정하는 방식

- 하위 LSR 레이블 할당(Downstream Label Allocation) : 하위 LSR이 레이블을 할당하여 상위 LSR에게 전달함으로써 LSP를 설정하는 방식.
- 요구시 하위 LSR 레이블 할당(Downstream Label on Demand Allocation) : 상위 LSR이 레이블을 요구했을 때에 하위 LSR이 레이블을 할당하여 상위 LSR에게 전달함으로써 LSP를 설정 하는 방식

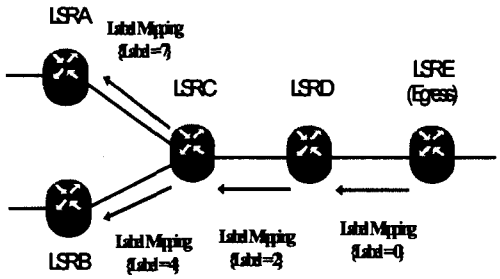
LDP 메시지를 언제 트리거(trigger) 할 것인지에 대한 방식으로 크게 두 가지로 정의 될 수 있다.

- 데이터 기반 트리거(Data-driven-trigger) : 한 LSR이 IP 패킷을 받았을 때 자동적으로 다음 LSR에게 LDP 메시지를 보내어 LSP를 설정하는 것.
- 제어기반 트리거(Control-driven-trigger) : 한 LSR이 라우팅 정보가 변경되었을 경우에 모든 이웃하는 LSR에게 LDP메시지를 보내어 LSP를 설정하는 것.

데이터 기반 트리거 방식과 제어 기반 트리거 방식은 각각 <그림 2-6> 과 <그림 2-7>과 같다 [7][8].



<그림 2-6> 데이터 기반 트리거 방식



<그림 2-7> 제어기반 트리거 방식

2.2 DiffServ

2.2.1 DiffServ 구조

DiffServ 모델은 1998년 IETF WG에서 제안 됐으며, 서비스 보장은 우선적으로 QoS를 몇 개의 클래스로 분류하고 이 분류된 클래스에 따라 서비스를 보장하도록 하는 것이다. 이에 따라 우선적으로 IP 헤더의 특정 필드(IPv4 : ToS, IPv6 : Traffic Class Field), 즉 DiffServ 필드에 표시하여 차등적인 서비스 값을 설정하게 된다. DiffServ 구조는 이렇게 특정 값으로 설정된 차등적인 서비스 값들에 의해 적절한 포워딩을 수행하도록 하는 구조이다[5].

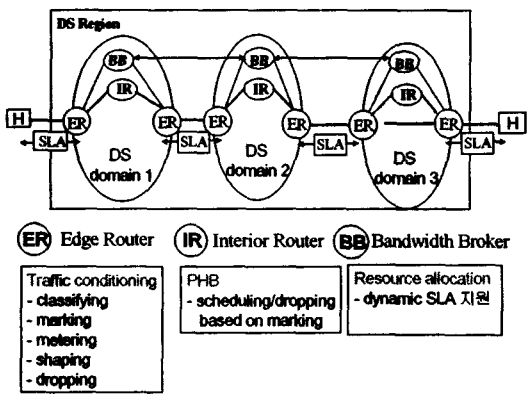
DiffServ 제공 능력을 갖는 DiffServ망(혹은 DS 도메인)은 여러 ISP망으로 구성될 수 있다. ISP를 연결하는 링크 사이의 경계에 경계 라우터(edge router)가 존재하며, 또한 DiffServ망과 non-DiffServ망이 연결되는 위치에도 경계 라우터가 존재하게 된다. DiffServ 구조는 여러 ISP에 걸친 양 종단간(end-to-end) 서비스(Inter-domain Service)와 하나의 ISP 망에서 시작되고 끝나는 Intra-domain 서비스의 두 형태를 지원한다. 따라서 일반 개인 뿐 아니라 ISP 망 자체가 DiffServ망의 사용자가 될 수 있다. DiffServ의 망 구조는 다

음과 같은 세 가지 기능요소로 구성된다[2].

- DiffServ byte와 패킷전달 기능
  (PHB : Per-Hop Behavior)
- 트래픽 조절 기능(Traffic Conditioning)
- 서비스 수준 협약
  (SLA : Service Level Agreement)

DiffServ 망의 기본 구조와 구성 요소는 <그림 2-8>과 같다. DiffServ망의 사용자는 먼저 DiffServ망의 관리자와 서비스 사용을 위한 협약을 체결한다. 이것은 서비스 수준 협약(SLA)이라는 쌍방간에 합의된 내용이어야 한다. DiffServ망의 사용자는 이러한 SLA에 의해서 DiffServ망을 통해 전달하고자 하는 패킷 흐름의 집합체를 정의하게 된다.

DiffServ망의 경계 라우터(Edge Router)는 이와 같이 정의된 패킷 흐름의 집합체에 대하여 트래픽 분류와 조절(conditioning) 기능을 수행한다. 패킷 조절 기능에는 트래픽 분류에 따른 패킷의 표시(mark), 흐름의 측정(meter), 그리고 쉐이핑(shaping)과 폐기 기능(dropping)을 포함한다.

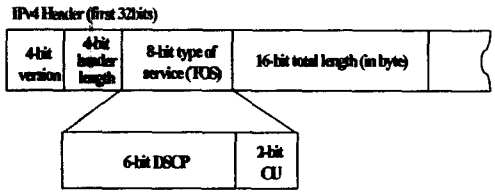


<그림 2-8> DiffServ망 기본구조

DiffServ망의 내부 라우터(Interior Router)에서는 이와 같이 경계 라우터에 의해서 표시된 코드에 의해서 단순히 패킷을 전달하게 된다. 이러한 내부 라우터에서의 패킷 전달 기능을 DiffServ에서는 PHB라는 용어를 사용하고 있다[5].

2.2.2 DiffServ byte

DiffServ망의 경계 라우터는 IP 패킷이 중간 내부 라우터에서 어떠한 방식으로 전달될지를 구분하여 이것을 IPv4의 TOS 필드 혹은 IPv6의 Traffic Class 필드에 표시하게 된다. DiffServ에서는 이 필드를 DiffServ byte, 그리고 DiffServ byte에 표시되는 값을 DSCP라고 부른다. 현재 RFC 2474에서 정의하고 있는 DiffServ byte의 포맷은 <그림 2-9>와 같다[11].



DSCP : Differentiated Services Code Point
CU : Currently Unused

<그림 2-9> DiffServ byte 포맷

<그림 2-9>에서 보는 바와 같이 6bit가 DSCP로 할당되었다. 이 코드 값은 패킷이 경유하는 라우터에서 패킷이 전달되는 순서(즉 패킷 스케줄링)와 버퍼 할당과 같은 패킷 전달 방식을 결정하게 된다. DiffServ byte는 DiffServ 표준화의 초기 논의 과정에서 6bit 중 한 개의 bit를 IN bit로 따로 규정하여, 패킷이 약속된 서비스 프로파일(profile)에 맞는지(In-profile)와 맞지 않는지(Out-of-profile)를

나타내도록 사용하려다가 6bit의 DSCP내에 묵시적으로 규정하기로 하였다. CU bit는 앞으로 명시적 혼잡 표시(Explicit Congestion Notification)와 같은 용도를 위해 예비한 필드이다. DiffServ byte는 패킷이 다른 도메인에 전달되면서 재 기록 될 수도 있다.

DiffServ망 내부의 라우터는 패킷 전달 메커니즘으로 다양한 버퍼 관리 및 패킷 스케줄링 기능을 제공한다. ISP 관리자는 이들을 잘 선택 구성하여, 특정의 몇 가지 패킷 전달방식을 제공하게 된다.

2.2.3 PHB(Per-Hop Behavior)

PHB는 라우터에서 패킷이 받게 되는 공통된 전달 방식을 규정한 것이며, 특정한 DiffServ 행동 집합에 적용되는 DiffServ 노드의 외부에서 관찰 가능한 전달 행동에 대한 기술이다[5]. PHB는 라우터의 내부 구현 메커니즘은 어떤 구현 기술을 사용하든지 상관하지 않으며 외부에 드러난 패킷 흐름의 입출력 동작만을 규정하고 있다[2].

가. DE(Default) PHB

DE PHB는 현재 인터넷 라우터에서 널리 사용되고 있는 패킷 전달 방식인 Best-effort 전달 방식을 정의하고 있다. 이 방식에서 패킷은 입력된 순서대로 출력되고, 손실이 일어날 수도 있다. 지연은 가능한 최소화되고 대역폭은 가능한 많이 이용된다. DE PHB는 DiffServ를 지원하지 않는 사용자를 허용하기 위함이다. DE PHB에 해당하는 DSCP는 '000000'이다[11].

나. Class Selector PHB

Class Selector PHB는 현재 사용하고 있는 IP 우선순위(precedence) 필드와의 호환성을 위해 정의되었다. 현재 IP 헤더의 ToS 필드는 3bit의 IP precedence bit와 4bit의 ToS bit로 구성되어 있다[12]. 현재 인터넷에서 IP precedence 값이 보편적으로 사용되고 있지 않지만 일부 라우터와 ISP 망에서 부분적으로 이용되고 있기 때문에 DiffServ망에서도 이미 사용 중인 값과의 호환성을 그대로 유지하기 위해서 Class Selector PHB를 정의하였다. 이 PHB에 해당되는 DSCP는 'xxx000'(x는 1이거나 0)이다[11].

다. Expedited Forwarding(EF) PHB

EF PHB는 라우팅 정보 갱신과 같은 망 제어 트래픽과 같이 우선순위가 가장 높은 전달 방식을 의미한다. EF PHB방식으로 패킷을 전달할 경우 라우터에서는 이 그룹 패킷의 출발률(departure rate)을 도착률(arrival rate) 보다 같거나 크게 설정하여 버퍼에서의 지연이 가능한 없도록 한다. EF PHB의 DSCP는 '101110'이다[13].

EF PHB를 이용하는 사용자는 그 만큼의 대가를 지불하면서 빠르고 보장된 서비스를 제공받게 되는데 마치 비싼 값을 지불하면서 비행기 1등석을 사용하는 승객과 같다고 할 수 있다. ISP망 사업자는 EF PHB를 토대로 프리미엄(premium) 서비스라고도 불리는 가상 전용선(Virtual Leased Line) 서비스를 실현할 수 있다[2].

라. Assured Forwarding(AF) PHB

사용자에 따라서 인터넷을 통해 IP 패킷을 전달할 때 어느 정도의 보장을 요구할 수가 있다. 어느 회사는 인터넷을 사용할 때 회사 내부의 각 사이트로부터의 합쳐진 트래픽이 망 사업자와 약정한 트래픽 프로파일을 초과하지 않는 이상 트래픽은 높은 확률을 가지고 전달된다는 보증을 원한다. 한편

때로는 약정된 트래픽 프로파일을 벗어나는 트래픽의 발생이 허용되는 것을 원할 수도 있다. 이러한 경우, 프로파일을 벗어난 과잉 트래픽은 프로파일을 준수한 트래픽보다는 낮은 수준의 패킷 전달 서비스를 받게 됨을 망 사업자와 사용자가 미리 이해하고 있다는 것을 전제로 한다. 즉, AF PHB는 네트워크의 혼잡 상황에서도 신뢰성 있는 서비스를 요구하는 가입자를 위한 서비스 클래스 이며, 혼잡 상황에서도 트래픽의 최소 성능 속도를 보장하는 PHB이다[14].

AF PHB에서 DiffServ망 사업자는 사용자에게 받은 패킷들을 여러 가지의 종류로 구분된 순서에 의해서 패킷 전달을 한다. AH PHB에서 패킷 전달 보장 순서는 패킷 전달의 순서를 결정하는 클래스와 혼잡(congestion) 발생시 패킷을 폐기하는 순서에 의해서 결정된다. 클래스는 이 그룹의 패킷 전달을 위해서 할당된 전달 자원에 의하며, 폐기 우선순위(drop precedence)는 이 그룹의 패킷에 할당된 버퍼의 크기에 따라 결정된다.

현재 AF PHB은 4개의 클래스와 3개의 폐기 우선순위로 구분하고 있다. <표 2-3>은 AF PHB에서 클래스와 폐기 우선순위에 따라 구분하여 할당되는 DSCP들을 나타내고 있다. AF PHB는 각 클래스 안에서 긴 기간의 체증은 최소화하는 반면 폭주를 일으키는 짧은 기간의 체증은 허용하도록 구현되고 있다[2].

<표 2-3> AF DSCP

Drop Precedence	Class 1	Class 2	Class 3	Class 4
Low	001010	010010	011010	100010
Medium	001100	010100	011100	100100
High	001110	010110	011110	100110

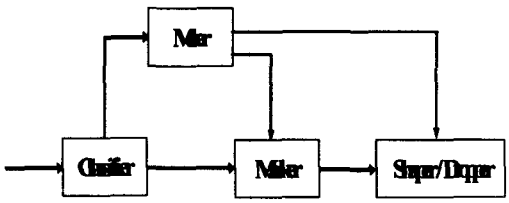
2.2.4 트래픽 조절(Traffic Conditioning)

사용자의 서비스 계약에 따라 DiffServ망의 경계 라우터는 DiffServ망 내에서 패킷을 어떻게 전달할 것인가를 결정하기 위해서 패킷을 분류하고 표시하는 기능을 수행한다. DiffServ 용어로는 이러한 기능을 트래픽 조절이라는 용어로 표현하고 있다. 트래픽 조절은 몇 가지 기능요소로 구성되는데 트래픽 분류(classification), 측정(meter), 표시(mark), 쉐이핑(shaping), 그리고 폐기(drop) 기능이 여기에 속한다. 다음은 트래픽 조절기능에 대한 설명이다.

- 트래픽의 분류 : 트래픽 분류는 다음의 두 가지 방법이 존재한다. 즉, DiffServ byte 외에 소스(source) 및 목적지 주소 필드 등 IP 헤더내의 필드에 근거하는 MF (Multi-Field) 분류와 단지 DiffServ byte만을 사용하여 분류하는 BA (Behavior Aggregate) 분류로 나뉜다.
- 트래픽 측정기(meter) : 트래픽 측정기는 SLA에서 약속한 트래픽 프로파일을 기준으로 패킷 흐름을 측정하여 그 결과를(즉, 프로파일 준수 또는 위반) 다음의 기능요소에 전달한다.
- 트래픽 표시기(marker) : 트래픽 표시기는 특정 패킷 전달 방식에 해당하는 코드를 DiffServ byte에 기록하여 패킷을 특정 BA에 속하도록 한다. 여기에서 BA는 동일한 DSCP를 갖고 DiffServ망으로 들어오는 패킷들의 집합을 BA라고 한다[5].
- 트래픽 쉐이퍼(shaper) : 트래픽 쉐이퍼는 BA의 트래픽 패턴을 미리 약속한 트래픽 프로파일에 준수하도록 조치를 취한다.

- 트래픽 폐기(drop) : 트래픽 폐기는 약정된 트래픽 프로파일(예, 패킷 도착률이나 버스트 길이)에 어긋나는 패킷에 대해서 패킷 폐기와 같은 적절한 조치를 취한다.

이들 구성 요소의 상관관계가 <그림 2-10>에 예시되어 있다[5].



<그림 2-10> 트래픽 조절의 논리적 도식

2.2.5 서비스 수준 협약(SLA)과 대역폭 브로커 (Bandwidth Broker)

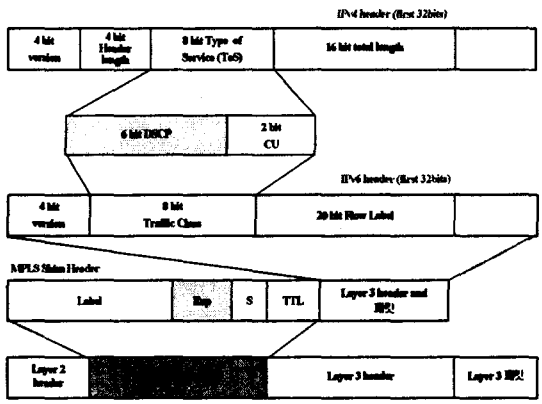
사용자는 DiffServ망의 사용을 신청할 때 자신의 트래픽과 원하는 서비스에 대한 사항을 DiffServ망의 관리자에게 알려준다. DiffServ망의 관리자는 이러한 사용자의 트래픽을 수용할 것인지의 여부를 결정한다. 이때 연결 수락 여부의 결정은 현재의 망의 상황과 사용자의 요구에 따라 정적으로 이루어질 수도 있으며, 동적으로 이루어질 수도 있다. 정적으로 이루어질 경우 상호 협약된 내용에 따라서 관리자의 수작업에 의해서 일정 시간 동안 미리 정해진 경로와 대역을 할당하게 된다. 이와 같이 사용자와 DiffServ망의 관리자 사이의 서비스 계약을 서비스 수준 협약이라 한다[15].

만약 DiffServ에 의한 서비스가 이루어질 경우 초기에는 이러한 정적인 방식으로 사용될 것이다. 하지만 이러한 서비스 협약이 동적으로 이루어질 경우 망의 부하나 가격 정책의 변화에 따라서 서비스 할당 내용이 달라질 수 있다. 이를 위해서는 RSVP와 같은 동적인 신호 프로토콜이 필요하게 된다. 그리고 DiffServ망의 자원을 관리하고 감시할 수 있는 노드가 필요한데 DiffServ에서는 이것을 대역폭 브로커라고 부르고 있다[15].

망의 경계 라우터는 이러한 신호 프로토콜에 의한 요청을 받았을 경우 연결 수락 여부 및 감시 기능에 대해서 대역폭 브로커에게 문의를 하게 되며 이후의 모든 트래픽 조절 기능에 대한 사항을 대역폭 브로커를 통해 전달 받게 된다. 각 DiffServ망에는 대역폭 브로커가 요구되며 각 대역폭 브로커는 서로 망 자원에 관련된 정보를 주고받을 필요가 있다. 한 가지 주의할 점은 SLA는 망 사업자와 사용자 사이의 협약 내용이며 IETF의 DiffServ 그룹에서는 SLA의 내용에 대해서는 규정하지 않는다[2]. 이에 따라 국방전산망에서 DiffServ를 적용하기 위해서는 군 특성상 동적 자원할당보다는 망구성시 관리자에 의한 정적 자원할당이 적합할 것으로 고려된다.

2.3 MPLS 망에서의 DiffServ지원

MPLS 망에서 DiffServ를 지원하기 위해서는 IP헤더에 있는 DSCP에 따라 DiffServ 클래스의 BA를 지원할 수 있도록 다른 기능을 추가 하여야 한다. <그림 2-11>은 DSCP와 MPLS 헤더와의 관계를 나타내고 있다.



<그림 2-11> DSCP와 MPLS 헤더 및 Layer헤더와의 관계

<그림 2-11>에서 보는 바와 같이 MPLS 망에서는 DSCP를 볼 수 없다. 따라서 MPLS 망에서 차등화 서비스를 지원하기 위해서는 DSCP가 MPLS 헤더의 EXP 필드(3bit)값으로 매핑이 이루어 져야 한다. MPLS 망에서 차등화 서비스를 지원하는 방법은 크게 두 가지로 나뉠 수 있는데, 하나는 E-LSP (EXP-inferred-PSC LSP)를 사용하여 차등화 서비스를 지원하는 방법과 다른 하나는 L-LSP (Label-inferred-PSC LSP)를 사용하여 차등화 서비스를 지원하는 방법이다[16].

이번 절에서는 MPLS 망에서 DiffServ를 지원하기 위한 기본 개념과 E-LSP와 L-LSP에 대하여 기술하였다.

2.3.1 기본개념

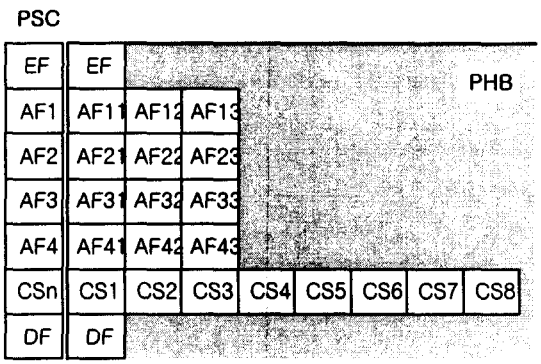
MPLS 망에서 일반 경로를 따라 데이터 흐름을 전송하기 위해서는 LSP를 설정해야만 한다. MPLS의 LSP는 MPLS 신호 프로토콜을 사용하여 설정된다. 입구 LER에서 각 패킷은 하나의 레이블에 할당되어 하향링크로 전송된다. 해당 LSP상에 존재하는 각 LSR은 각 패킷의 레이블을 보고 그 레이블에 해당하는 다음 홉으로 패킷을 전송한다. 입구 LER에서 그 패킷들은 자신들이 속한 BA에 해당하는 DSCP 따라 분류되고, 표시된다. 그리고 각 전송 노드에서 DSCP는 각 패킷에 해당하는 폐기 확률과 큐잉 처리 등을 결정하는 PHB를 선택하는데 사용된다.

차등화 서비스의 경우 AF PHB 그룹 에서 같은 클래스에 속한 3개의 PHB가 동일한 트래픽 흐름에 속하는 패킷에 할당될 수 있다. 이 경우 동일 흐름에 속한 패킷의 순서 유지를 위해 같은 클래스에 속한 3개의 PHB는 하나의 묶음으로 동일 LSP에 흘려보내야 한다. 이를 위해 순서 제약을 갖는 PHB의 묶음을 하나의 묶음으로 하는 새로운 PHB Scheduling Class(PSC)의 정의가 필요하고, 이에 대응하여 BA 묶음을 하나의 묶음으로 하는 새로운 Ordered Aggregate(OA)의 정의가 필요하다[2]. 즉, reordering이 발생하지 않는 PHB들의 조합을 여기서 OA로 정의하며, 하나의 OA에 속하는 여러 BA들의 조합 또는 여러 PHB들의 조합을 PSC(PHB Scheduling Class)로 정의한다[16].

따라서 OA와 PSC는 유사한 개념이며 MPLS 망의 LER은 패킷의 DSCP가 나타내는 PHB를 적절한 PSC로 변환하고, 패킷은 PSC와 FEC에 해당하는 LSP를 따라 전송된다.

2.3.2 PSC(PHB Scheduling Class)

<그림 2-12>는 차등화 서비스의 PHB와 차등화 서비스를 지원하기 위한 MPLS 망에서의 PSC 사이의 관계를 나타낸다[16].



<그림 2-12> PSC와 PHB의 관계

- DF PSC(Default PSC) : 차등화 서비스에서의 Default PHB이다.
- CSn PSC : 차등화 서비스에서 정의하고 있는 8가지의 Class Selector(CS) codepoint 들을 말한다. 여기서 n은 1에서 8가지이다.
- AFn PSC : 차등화 서비스에서는 독립적으로 포워딩하는 N개의 독립적인 AF (Assured Forwarding) 클래스에 대해 정의하고 있으며 각 AF 클래스내의 패킷들은 M레벨의 폐기 우선순위(Drop precedence)중에 하나를 가진다. AF class i에 속하며 j의 폐기 우선순위를 가지는 패킷에 대해 AF codepoint는 AFij로 나타낼 수 있다. 여기서 i는 1에서 N까지이며 j는 1에서 M까지이다. 현재는 N=3, M=4로 정의되어있다. 각각의 AF 클래스들은 서로 다른 스케줄링 처리를 받을 수 있으므로 각 AF 클래스는 하나의 PSC가 될 수 있으며 AFn으로 나타내어진다. 여기서 n은 1에서 4까지이다.
- EF PSC : 차등화 서비스에서 정의하고 있는 EF(Expedited Forwarding) PHB에 해당한다.

2.3.3 E-LSP(EXP-Inferred-PSC LSP)

E-LSP는 하나의 LSP를 사용하여 8개까지의 BA를 지원한다. E-LSP를 사용하기 위해서는 MPLS 망의 에지(edge)에서 DSCP 필드는 <그림 2-4>에 예시되어 있는 MPLS Shim 헤더 EXP 필드에 매핑되어야 한다. 즉 PSC와 폐기 우선순위 모두가 MPLS Shim 헤더의 EXP 필드에 표시된다. 이러한 LSP들을 E-LSP라 정의한다[16].

DSCP필드의 길이는 6bit이므로 8개 이상의 BA에 대해서 DSCP필드는 MPLS 레이블 스택 내에 있는 3bit 길이의 EXP 필드에 완전히 매핑 될 수 없다. E-LSP에서는 DSCP전체를 3bit EXP 필드에 매핑 시켜야 하므로 매핑 리스트를 벗어나는 상황에 적절한 조치를 취해야 하며 이러한 상황처리는 서비스 제공자의 지역 정책을 따른다[2].

2.3.4 L-LSP(Label-Only-Inferred-PSC LSP)

MPLS 망에서 차등화 서비스를 지원하기 위해 한 쌍의 <FEC, OA>당 하나의 LSP를 설립하여 차등화 서비스를 제공할 수 있다. 이 방법에서 LSR은 레이블된 패킷에 적용되어질 PSC를 레이블 값을 보고 판단한다. 또한 레이블된 패킷에 적용될 폐기 우선순위는 MPLS Shim 헤더내의 EXP 필드에 표시된다. 이러한 LSP들을 L-LSP라 정의 한다.[16]. RFC 3270에 정의된 PHB와 PSC/EXP 매핑 관계는 <표 2-4>와 같다.

PHB		PSC	EXP Field
DF	⇒	DF	000
CSn	⇒	CSn	000
AFn1	⇒	AFn	000
AFn2	⇒	AFn	001
AFn3	⇒	AFn	010
EF	⇒	EF	000

CSn : $1 \le n \le 8$
AFn : $1 \le n \le 4$

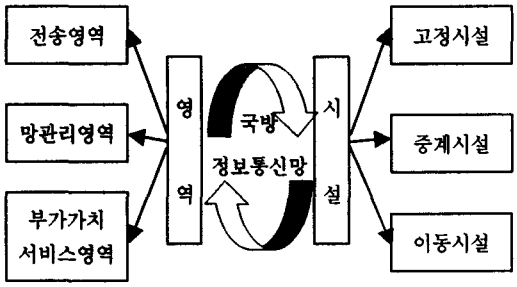
<표 2-4> PHB와 PSC/EXP 매핑 관계

3. 국방전산망 분석

3.1 국방전산망 정의

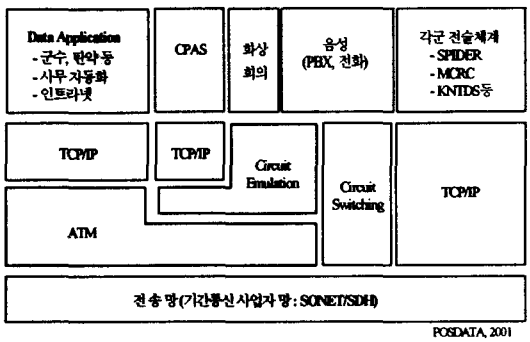
일반적으로 정보통신망이라 함은 전화, 데이터 교환, FAX 등과 같은 서비스를 다수의 이용자에게 제공하기 위한 단말장치, 교환기, 전송장치 등의 설비를 상호 연결해서 구성한 망을 가리킨다. 국방정보통신망은 국방정보통신망 통합 망관리체계 기본계획에서 '국방정보화기반 요소로서, 군사적인 목적으로 사용되는 정보통신망으로 미래전에 필요한 정보의 공유 및 종단 간 정보의 실시간 유통을 보장하는 전 군적 수준의 통합된 개념의 통신망'이라고 정의하고 있다. 국방정보통신망은 <그림 3-1>과 같이 전송, 망 관리, 부가가치 서비스의 3개영역을 전략/전술제대에 위치한 고정시설, 노드와 노드사이 혹은 고정통신망과 이동통신망을 연결하는 중계시설, 전술제대에서 운용하는 이동시설 등의 3개시설로 구성되어 양자를 연결해주는 역할을 수행한다[17].

국방전산망은 국방정보통신망 중 고정통신망에 속하며 <그림 3-2>와 같은 국방정보통신망 프로토콜 구조에서 화상회의, 각 군 전술 체계 등을 제외한 TCP/IP 기반의 데이터 애플리케이션(Application)인 국방인트라넷, 국방사무자동화체계, 기타 응용체계등 현재 사용자 PC에서 제공되는 서비스를 말한다[18].



<그림 3-1> 국방정보통신망의 영역 및 시설

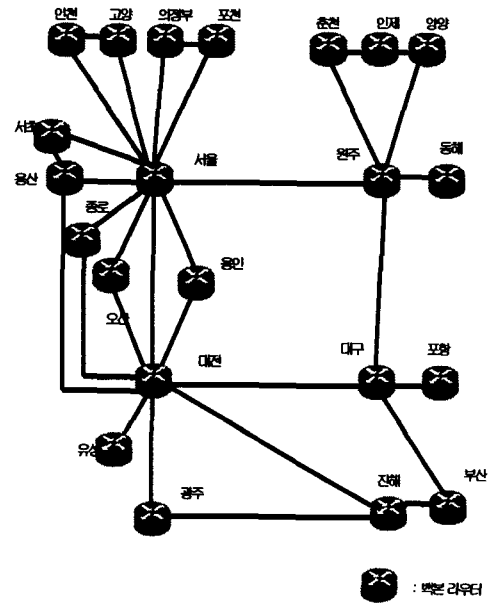
국방전산망은 국방정보통신망 중 고정통신망에 속하며 <그림 3-2>와 같은 국방정보통신망 프로토콜 구조에서 화상회의, 각 군 전술 체계 등을 제외한 TCP/IP 기반의 데이터 애플리케이션(Application)인 국방인트라넷, 국방사무자동화체계, 기타 응용체계 등현재 사용자 PC에서 제공되는 서비스를 말한다[18]. 본 논문은 위에서 정의한 국방전산망을 대상으로 MPLS와 DiffServ를 이용한 군 기능별 차등화된 서비스의 제공으로 중요 데이터 트래픽에 대해서 QoS를 보장하기 위한 방안에 대한 연구이다.



<그림 3-2> 국방정보통신망 프로토콜 구조

3.2 국방전산망 구성

국방전산망은 국방정보통신망의 일부분이며 국방정보통신망은 <그림 3-2>에서 알 수 있듯이 기간통신사업자 망인 전송망 위에 ATM 망이 있으며, 주요 지역간은 T3급으로 전송로가 구성되어 있다. 현재 국방전산망은 전산업무 지원을 위해 각 군별, 각 부대별로 TCP/IP 기반의 인트라넷 웹 서비스, 전자메일 서비스, 전자결재 서비스, 원격교육 시스템, 군수자원관리시스템 및 탄약관리시스템, 야전체대인사업무시스템, 상황관리시스템, 기타 부대에서 독립적으로 구축한 시스템 등으로 구성되어 있다. 국방정보통신망에서 전산데이터에 대한 처리를 담당하는 국방전산망은 육•해•공군의 모든 IP 트래픽에 대해서 라우팅 정보를 공유하기 위해 전군에 위치한 22개 ATM 교환노드의 ATM 교환기에 영내회선 OC3(155Mbps)를 이용하여 22개의 Cisco라우터로 백본 라우터를 구성하고 있으며, 단위부대의 LAN을 담당하는 라우터를 백본 라우터와 연결하여 국방전산망을 구성하고 있다[19]. <그림 3-3>은 국방전산망 ATM 백본 라우터 구성도 이다.



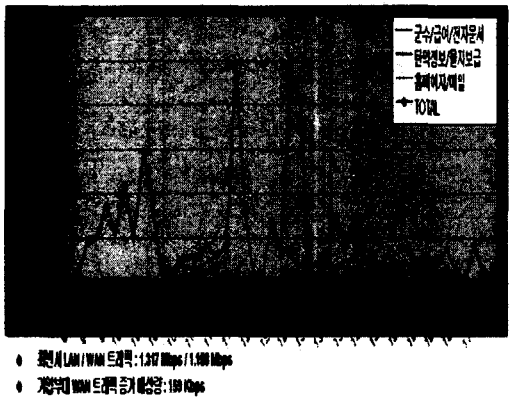
<그림 3-3> 국방전산망 ATM 백본 라우터 구성도

전군의 라우팅 정보를 공유하기 위한 백본 라우터 간에는 ATM 교환기를 통하여 Point-to-Point 방식으로 ATM PVC를 이용하여 연결되어 있으며 OSPF로 전군의 라우팅 정보를 공유하고 있다. ATM PVC 장애 발생에 따른 물리적인 백업경로는 별도로 구성되어 있지 않으며, ATM PVC의 자체적인 경로 재설정을 통하여 논리적으로 백업 경로가 구성되어 있다. ATM 교환기간 전용선은 T3(45Mbps)로 연결되어 있으며, T3 대역폭 중에서 약 35Mbps 정도가 CBR(Constant Bit Rate) 음성 용량으로 할당되어 있고, 데이터 트래픽은 10Mbps로 가변적인 대역폭을 할당하는 VBR(Variable Bit Rate)방식으로 구성되어 있다. CBR은 특성상 음성신호가 전혀 사용되지 않는 경우라도 대역폭을 항상 점유하게 되므로 ATM 교환기간에 구성된 T3 전용선의 대역폭을 비효율적으로 사용하게 된다

[19].

3.3 국방전산망에서 MPLS와 DiffServ 도입의 필요성

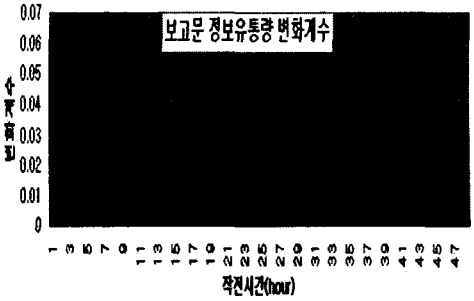
본 논문에서 국방전산망 관련 트래픽 분석은 타 기관에서 군 관련 프로젝트 수행 중 실시한 자료를 인용하였다.



<그림 3-4> 00사단 트래픽 분석

<그림 3-4>는 포스데이터(POSDATA)가 2001년 육군 00사단 인트라넷에서 측정한 트래픽 분석 자료이다. 그림과 같이 트래픽 유통량은 항상 일정한 것이 아니라 특정 시간에 인트라넷 홈페이지 접속과 전자우편 사용으로 인하여 트래픽이 집중되는 현상을 나타내고 있다. 현재의 네트워크는 대역폭 용량이상의 트래픽이 동일 시간대에 집중하면 전체 네트워크가 마비되거나 트래픽 전송이 지연될 수 있는 취약한 구조이므로, 중요한 데이터 전송이 이 시점에 이루어진다면 중요 데이터의 지연이나 손실이 발생할 수 있을 것이다[20].

<그림 3-5>은 육군 00사단 BCTP(Battle



<그림 3-5> 00사단 BCTP간 정보 유통량

Command Training Program)간 측정된 트래픽으로 인트라넷 트래픽과 마찬가지로 항상 일정한 트래픽이 발생하는 것이 아니라 특정 시간대, 예를 들어 중요 작전이 실시되고 있는 시점에 트래픽이 집중되는 현상을 나타내고 있다.

현재 Best-effort 서비스 구조인 국방전산망에서 일부 서비스의 접속률 증가나 특정시간대의 대역폭 초과 트래픽 발생은 전체 네트워크 사용 제한, 중요 명령 및 보고 등 정보 흐름이 지연되거나 손실될 수 있음을 나타낸다[21]. 이 트래픽 집중 시기에 우선순위에 기반을 두어 어떻게 트래픽을 효율적으로 처리할 것인가에 대한 방법이 QoS 보장기술이며, MPLS와 DiffServ를 이용하여 사용자에게 필요한 QoS를 제공할 수 있을 것이다.

우리 군은 현재 업무의 많은 부분을 인트라넷을 이용하고 있으며 앞으로도 인트라넷 등 네트워크를 이용하는 업무량은 더욱 증가할 것이다. 네트워크 중심의 환경에서 국방전산망의 효율적인 구축은 성공적인 임무 완수에 매우 중요할 것이다. 인터넷 같은 상용망에서는 트래픽 폭주, 혼잡 등으로 네트워크가 일부 지연되는 현상이 있어도 중대한 문제가 발생하지는 않을 수 있으며, 사용자에게 필요한 서비스 제공을 위한 대역폭 확보도 보다 쉽게 할

수 있을 것이다. 그러나 국방전산망은 우리나라의 국방, 즉, 국가안위와 관계되는 문제이므로 사소한 오차의 발생, 트래픽 지연이라도 중대한 오류를 발생시킬 수 있으며 네트워크 확장이나 대역폭 확보도 상용망보다 어려운 것이 현실이다. 예를 들어, 국방 CERT(Computer Emergency Response Team) 부서의 긴급 해킹 보고가 중요하지 않은 데이터 트래픽 때문에 지연되거나 유실된다고 하면 국방전산망의 마비, 심지어 국가 안보에 지대한 영향을 끼칠 수도 있는 것이다. 이러한 환경에서 군 기능별 차등화 서비스는 트래픽의 선별적인 처리에 좋은 대안이 될 수 있을 것이다. 즉, 네트워크에서 혼잡이 발생 했을 때 트래픽을 분류, 차별적인 서비스를 보장하고 특별한 기능의 중요 정보는 다른 트래픽보다 우선권을 주어 처리하는 시스템은 전체 시스템의 효율적인 사용을 보장하고 임무에 필수적인 정보 전송을 보장할 수 있는 것이다.

인터넷 등 상용망은 VoIP, VPN 서비스, 유·무선 통합 등 네트워크 통합 환경으로 진화하고 있다. 상용망의 네트워크 진화와 함께 국방정보통신망도 네트워크 통합 환경으로 진화될 것이다. 현재 별도의 망으로 구축된 화상회의 시스템도 TCP/IP 기반의 화상회의 시스템으로 통합되고, 음성 서비스가 네트워크 서비스로 통합되어 VoIP 형태로 제공될 수 있을 것이다. 또한, VPN 서비스가 활성화되고 유·무선이 하나의 네트워크로 통합된 단일 네트워크로 발전될 것이다. 이와 같이 진화된 국방전산망에서는 VoIP, VPN, 군 기능에 따른 차등화 서비스는 필수적으로 요구될 것이다.

TCP/IP 기반의 QoS 보장기술은 서론에서도 언급했듯이 IntServ, DiffServ기술이 존재한다. IntServ의 문제점 보완을 위해 DiffServ가 등장했으며, DiffServ 자체만을 생각했을 때 국방전산망에 적용하기에는 문제점이 따른다. DiffServ에서의 DSCP로 표시된 패킷들은 국방전산망의 백본인 ATM에서는 53byte의 고정 cell로 패킷들이 나누어지기 때문에 인식할 수 없다는 것이 그 문제이다. 그렇기 때문에 DiffServ의 DSCP로 표시된 PHB들은 MPLS의 PSC와 EXP 값으로 매핑이 이루어지고, MPLS의 EXP 값 또한 ATM에서 인식할 수 없기 때문에 ATM의 CLP(Cell Loss Priority) bit로 매핑이 이루어져야 한다[16]. 차등화 서비스를 위해 MPLS가 필요한 더 큰 이유는 MPLS에서 패킷 전달을 위한 레이블 값이 ATM의 cell전달을 위한 VCI/VPI값으로 직접 매핑이 가능하다는 것이다[8].

4. 국방전산망에서 QoS 보장방안

제 2장과 3장에서 살펴본 바와 같이 MPLS에서의 DiffServ 구현 방법에는 E-LSP와 L-LSP가 있으며, 국방전산망과 같이 ATM 백본을 위해서는 다시 ATM기반으로의 서비스 매핑이 필요하다.

서비스 클래스를 볼 때 DiffServ는 6bit의 DSCP 필드 값을 사용해서 패킷들을 최대 64개의 클래스로 구분할 수 있다. 그러나 실제로는 32개의 표준 PHB가 클래스로 사용될 수 있으며 이중에서 EF, AFx, BE등 6개의 클래스가 많이 사용된다. MPLS의 경우는 3bit EXP 필드를 사용하여 클래스를 표현하므로 최대 8개의 클래스를 사용할 수 있음을 의미한다. 그러나 실제의 경우에 있어서는 적게는 2개에서 많게는 8개까지의 클래스를 사용하고 있으며, 가장 일반적인 경우가 4개의 클래스를

사용한다. 즉, 서비스 클래스는 큐잉(queueing)과 스케줄링(scheduling)의 효율성을 고려하여 Gold, Silver, Bronze로 구분하며, Best-effort 클래스를 포함시키기도 한다. ATM의 경우는 CBR, VBR, UBR, ABR, GFR의 5가지 클래스로 구분하고 있다[2].

본 장에서는 국방전산망에서 네트워크의 전체적인 트래픽 증가로 인하여 중요 정보 및 보고의 전달 지연은 전력의 큰 손실이 될 것이기 때문에 트래픽의 폭주로 인하여 중요한 정보나 보고가 지연되지 않도록 군 기능별 우선순위에 따른 차등화된 서비스를 제공하기 위해서 먼저 DiffServ의 DSCP에 따른 PHB와 MPLS의 EXP 값의 매핑을 제안하고, ATM으로의 서비스 매핑을 위한 ATM CLP 값과 MPLS 서비스 클래스 매핑을 제안한다. 또한 실질적인 국방전산망에서의 적용을 위해서 MPLS 서비스 클래스와 ATM 서비스 클래스의 매핑과 군 기능별 우선순의 부여를 통하여 QoS 보장방안을 제안한다. 군 기능은 최소한의 분류로 정보, 작전, 인사, 군수, 기타로 가정한다.

4.1 서비스 클래스 매핑 제안

MPLS 망에서 차등화 서비스를 제공하기 위해서는 DiffServ의 DSCP 에 따른 PHB와 MPLS의 EXP 값의 매핑이 필요하다고 언급했다.

이는 국방전산망 내에서 ATM 백본을 거치지 않는 라우터 구간만이 있을 수 있기 때문에 고려해야 한다. 즉, 국방전산망에 MPLS와 DiffServ를 초기 도입할 때 백본 라우터 하나에 연결된 단위부대들과 백본 라우터를 가지고 있는 한 부대와의 가능한 매핑 제안이다. <표 4-1>은 DiffServ의 서비스 클래스와 MPLS의 EXP 값에 따른 서비스 클래스의 매핑 제안 이다.

<표 4-1>에서 DiffServ의 EF 패킷을 Gold 서비스에 할당 하였으며 EXP 값 3bit 에 대하여 '110'을 할당 하였다. 즉, Gold 서비스를 나타내는 앞 2bit는 '11'로 설정하였고 폐기우선순위를 나타내는 마지막 1bit는 폐기우선순위가 낮으므로 '0'으로 할당 하였다. AF 패킷 중 클래스 1, 2에 해당하는 패킷들은 Silver 서비스에 할당하였으며 EXP 값은 '100, 101'로 할당하였다. 앞 2bit는 Silver 서비스를 나타내는 '10'이다. AF 패킷 중 클래스 3,4에 해당하는 패킷들은 Bronze 서비스에 할당하였으며 EXP 값은 '010, 011'로 할당 하였다. DF 패킷은 Best-effort 서비스로 할당하고 EXP 값은 '001'로 할당 하였다[22][23].

<표 4-1> DiffServ의 DSCP와 MPLS의 EXP 값에 따른 서비스 클래스 매핑

DiffServ		MPLS	MPLS 서비스
PHB	DSCP	EXP 값	클래스
EF	101110	110	Gold
AF11	001010	100	Silver
AF12	001100	101	
AF13	001110	101	
AF21	010010	100	
AF22	010100	101	
AF23	010110	101	
AF31	011010	010	Bronze
AF32	011100	011	
AF33	011110	011	
AF41	100010	010	
AF42	100100	011	
AF43	100110	011	
DF	000000	001	Best-effort

이와 같이 서비스 클래스에 따라 EXP 값의 마지막 bit를 0 혹은 1로 결정한 것은 네트워크 혼잡이 발생할 경우 폐기 우선순위가 높은 패킷 흐름을 먼저 폐기 하도록 한 것이다.

<표 4-1>과 같은 방식이 E-LSP 방식이며, 이

방식은 ATM 백본을 거치지 않는 구간에서만 적용 가능하다. 이유는 ATM에서는 하나의 연결(connection)내의 패킷들에 대하여 서로 다른 스케줄링 및 큐잉 처리를 할 수 없기 때문이다. 그러므로 하나의 LSP에 최대 8개의 서로 다른 BA를 지원하는 E-LSP 방식은 ATM 백본구간을 고려했을 때 사용할 수 없으며 국방전산망 백본 구간에서는 L-LSP 방식을 사용해야 한다. <표 4-2>는 ATM 백본 구간에서 적용 가능한 서비스 매핑 제안이다.

<표 4-2> MPLS EXP 값과 ATM CLP 값에 따른 서비스 매핑

DiffServ		PSC	EXP	CLP	MPLS 서비스 클래스
PHB	DSCP				
EF	101110	EF	000	0	Gold
AF11	001010	AF1	000	0	Silver
AF12	001100	AF1	001	1	
AF13	001110	AF1	010	1	
AF21	010010	AF2	000	0	
AF22	010100	AF2	001	1	
AF23	010110	AF2	010	1	
AF31	011010	AF3	000	0	Bronze
AF32	011100	AF3	001	1	
AF33	011110	AF3	010	1	
AF41	100010	AF4	000	0	
AF42	100100	AF4	001	1	
AF43	100110	AF4	010	1	
DF	000000	DF	000	1	Best-effort

L-LSP 방식에서 폐기 우선순위를 나타내는 EXP 값은 ATM 구간에서는 알 수 없기 때문에 ATM 헤더의 CLP(1bit)를 이용하여 나타내야 한다. <표 4-2>에서 보는 봐와 같이 DiffServ PHB는 MPLS의 PSC/EXP 쌍으로 매핑이 이루어지고 MPLS의 EXP 값은 다시 ATM의 CLP 값으로 매핑이 이루어진다. 여기에서 EXP 값에 따른 3가지 우선순위는 1bit를 가지는 CLP 값으로 매핑이 이루어지므로 2가지 우선순위만을 나타낸다.

4.2 군 기능별 QoS 보장방안

국방전산망에서의 MPLS를 이용한 차등화서비스 적용 방안을 살펴보면 MPLS의 서비스 클래스를 ATM 서비스 클래스로의 매핑 또한 필요하다.

본 장에서 제안하는 구조는 기존 국방전산망에 할당된 백본에서의 데이터 트래픽 10Mbps에서 군 기능별 서비스 할당과 우선순위에 대한 제안을 하고 백본 간선 T3(45Mbps)전체에 대한 군 기능별 서비스 할당과 우선순위에 대한 방안을 제안한다.

4.2.1 기존 데이터 트래픽(10Mbps)에서의 QoS 보장방안

기존 데이터 트래픽 10Mbps에 대한 ATM 백본에서의 군 기능별 우선순위와 이론상 ATM 서비스로의 매핑은 <표 4-3>과 같이 제안한다. 기능별로 분류해보면 Gold 서비스는 정보, 작전, Silver는 인사, Bronze는 군수에 할당했으며, Best-effort는 기타에 할당 했다. 평시 서비스의 분류에서 Gold 서비스는 원격교육 시스템 및 상황관리 시스템 등에 할당할 수 있으며, Silver 서비스는 전자결재 서비스, 야전제대 인사업무 시스템 등에 적용할 수 있다. Bronze 서비스는 군수 자원관리 시스템, 탄약관리 시스템 등에 적용할 수 있고 Best-effort 서비스는 인트라넷 웹 서비스, 전자메일 서비스 등에 적용할 수 있다.

<표 4-3> 기존 데이터 대역폭(10Mbps)에 대한

군 기능별 MPLS서비스와 ATM 서비스로의 우선순위 매핑관계

군 기능	MPLS 서비스 클래스	우선 순위	ATM 서비스 클래스	대역폭 할당 예
정보 작전	Gold	0	VBR	10%
인사	Silver	1	ABR	25%
군수	Bronze	2	ABR	25%
기타	Best-effort	3	UBR/GFR	40%

<표 4-3>에서 제안한 것과 같이 정보, 작전 기능에 대해서는 VBR로 할당하였다. 이는 군 기능 중 정보, 작전 우선순위를 0순위로 가정하였기 때문이며, 정보, 작전 데이터 트래픽은 네트워크 혼잡이 발생하더라도 최소한의 대역폭을 유지 하도록 설정 하였다. 인사, 군수 기능에 대해서는 ABR 서비스를 각각 할당하였고, 평시 트래픽의 대부분을 사용하는 웹 서비스나, 이 메일 서비스는 Best-effort 서비스로 할당 하였다. Best-effort 서비스는 ABR 서비스를 받는 인사, 군수 트래픽이 발생하지 않을 때는 90%의 대역폭을 사용할 수 있다.

예를 들면, <표 4-3>에서의 대역폭 할당 예와 같이 대역폭을 할당 했을 때 정보, 작전 트래픽은 네트워크 혼잡이 발생하더라도 10Mbps의 대역폭 중 10%에 해당하는 1Mbps의 대역폭을 사용 할 수 있다.

4.2.2 백본 간선(T3)에서 VoIP 사용에 따른 QoS 보장방안

이번 절 에서의 제안은 VoIP기술이 실제 사용 가능했을 경우의 제안 방안 이다. VoIP기술은 높은 음성압축기술을 이용해 음성 트래픽의 양을 60% 정도 줄일 수 있다[19]. 3.2절에서 국방전산망 백본 간선 트래픽 45Mbps 중 35Mbps를 음성신호에 이용하고 데이터 트래픽은 10Mbps를 이용한다고 언급했다. 이에 대한 트래픽 재 할당은 음성 서비스에 대한 대역폭 할당은 20Mbps로 하고 나머지 25Mbps를 데이터 트래픽에 할당하는 방안을 제안한다. <표 4-4>는 ATM 백본 간선(T3)에서 VoIP 사용에 따른 군 기능별 MPLS 서비스와 ATM 서비스로의 매핑 제안 예이다.

이 제안은 음성 트래픽중 일부를 VoIP로 사용하여 현재 사용하고 있는 35Mbps의 음성 트래픽을 보장하고 나머지 데이터 트래픽의 대역폭을 확장하여 사용하며, 사용하는 데이터 트래픽에 대하여 군 기능별 QoS를 보장하기 위한 방안이다.

<표 4-4>에서 VoIP 서비스는 MPLS Gold 서비스, ATM CBR 서비스로 할당하여 항상 일정한 대역폭을 할당 받을 수 있도록 하였다.

<표 4-4> VoIP 사용에 따른 군 기능별 MPLS 서비스와 ATM 서비스로의 우선순위 매핑 관계

군 기능	MPLS 서비스 클래스	우선 순위	ATM 서비스 클래스	대역폭 할당 예
VoIP	Gold	0	CBR	24%
정보 작전	Silver	1	VBR	20%
인사 군수	Bronze	2	ABR	28%
기타	Best-effort	3	UBR/GFR	28%

즉, 대역폭 할당 예에서 대역폭 25Mbps 중 24%에 해당하는 6Mbps를 할당하면 이는 VoIP 압축기술 60%를 적용하였을 경우 15Mbps의 음성 대역폭을 사용하는 것과 같은 효과를 가질 수 있다. 정보, 작전 트래픽은 MPLS Silver 서비스, ATM VBR 서비스로 할당 하였다. 인사, 군수 트래픽은

MPLS Bronze 서비스, ATM ABR 서비스로 할당하였고, 기타 웹 서비스와 이 메일 서비스는 Best-effort 서비스로 할당하여 인사, 군수 트래픽이 발생하지 않을 경우 대역폭 사용 예를 적용했을 때 최대 14Mbps 까지 사용 가능토록 하였다. <표 4-5>는 <표 4-3>과 <표 4-4>를 비교하여 나타내었다.

<표 4-5> 각 방안 간의 서비스 클래스 비교

군 기능	MPLS 서비스 클래스		ATM 서비스 클래스		대역폭 할당 예	
	기존	재 할당	기존	재 할당	기존 데이터 대역폭 (10Mbps)	재할당 데이터 대역폭 (25Mbps)
VoIP 서비스		Gold		CBR		6Mbps
정보 작전	Gold	Silver	VBR	VBR	1Mbps	5Mbps
인사	Silver	Bronze	ABR	ABR	2.5Mbps	7Mbps
군수	Bronze		ABR	ABR	2.5Mbps	
기타	Best-effort	Best-effort	UBR GFR	UBR GFR	4Mbps	7Mbps

<표 4-5>에서 알 수 있듯이 VoIP 서비스를 고려할 때 백본 간선(T3)에서 VoIP 사용에 따른 QoS 보장방안이 더 효율적임을 알 수 있다. 한 가지 고려할 사항은 각각의 방안에 대하여 MPLS 서비스 클래스 변화가 있음을 알 수 있다. 즉, 군 기능별 PHB의 변화가 있음을 나타내고 있다. <표 4-6>은 기존 데이터 대역폭과 재 할당 데이터 대역폭에 간의 군 기능별 PHB와 MPLS 서비스 클래스 변화를 나타낸다.

<표 4-6> 군 기능별 PHB와 MPLS 서비스 클래스 변화

DiffServ		PSC	CLP	MPLS 서비스 클래스	기존 데이터 대역폭 예 (10Mbps)	재 할당 데이터 대역폭 예 (25Mbps)
PHB	DSCP					
EF	101110	EF	0	Gold	정보, 작전	VoIP
AF11	001010	AF1	0	Silver	인사	정보
AF12	001100	AF1	1			
AF13	001110	AF1	1			
AF21	010010	AF2	0			작전
AF22	010100	AF2	1			
AF23	010110	AF2	1			
AF31	011010	AF3	0	Bronze	군수	인사
AF32	011100	AF3	1			
AF33	011110	AF3	1			
AF41	100010	AF4	0			군수
AF42	100100	AF4	1			
AF43	100110	AF4	1			
DF	000000	DF	1	Best-effort	기타	기타

4.3 국방전산망과 화상회의망 간선 통합시 QoS 보장방안

국방전산망을 포함하고 있는 국방정보통신망에는 여러 가지 기반체계들이 있으며 이 절에서는 국방정보통신망 중 화상회의망을 국방전산망의 백본 간선 T3에 통합 하였을 때의 QoS 보장방안 제안과 비용 효율성 측면을 제시한다.

화상회의망은 각 작전사급 부대간 T1으로 연결되어 있으며, 국방정보통신망 ATM 교환기의 전용회선 서비스를 받고 있다. 현재 화상회의망은 T1간선 12회선으로 구성, 운영되고 있으며 12회선의 간선 중 11회선이 국방정보통신망에 통합 운영되고 있다[24].

먼저 화상회의망을 국방전산망의 백본 간선(T3)에 통합 하였을 때의 QoS 보장방안은 백본 간선

트래픽 45Mbps 중 25Mbps를 데이터 대역폭으로 할당하고 VoIP기술을 실제 사용 가능 하였을 경우로 가정한다. 즉, 이번 절에서 제안하는 방안은 4.2.2절에서 제안한 방안에 TCP/IP 기반으로 전환된 화상회의망을 통합하여 효율성 및 비용절감을 기대하기 위한 방안이다.

화상회의망은 VoIP와 같이 MPLS Gold 서비스, ATM CBR 서비스로 할당하였다. 이에 따라 화상회의를 포함한 백본 간선 트래픽(45Mbps)중 재 할당 데이터 대역폭(25Mbps)에 대한 군 기능별 MPLS서비스와 ATM 서비스로의 우선순위 매핑 관계는 <표 4-7>과 같이 나타 낼 수 있다.

<표 4-7> VoIP와 화상회의를 고려한 군 기능별 MPLS서비스와 ATM 서비스로의 우선순위 매핑 관계

군 기능	MPLS 서비스 클래스	우선순위	ATM 서비스 클래스	대역폭 할당 예
화상회의	Gold	0	CBR	6%
VoIP 서비스	Gold	1	CBR	24%
정보, 작전	Silver	2	VBR	20%
인사, 군수	Bronze	3	ABR	25%
기타	Best-effort	4	UBR/GFR	25%

<표 4-7>에서 알 수 있듯이 대역폭 사용 예와 같이 대역폭을 할당 했을 경우 화상회의는 25Mbps 중 6%에 해당하는 1.5Mbps의 대역폭을 할당받음으로써 기존 T1간선의 대역폭을 그대로 적용 받을 수 있으며, 인사, 군수 트래픽과 기타 트랙픽은 각각 6.25Mbps의 대역폭을 사용할 수 있다. 이는 <표 4-3> 기존 데이터 대역폭(10Mbps)에 대한 군 기능별 MPLS 서비스와 ATM 서비스로의 우선순위 매핑관계에서 대역폭 할당 예와 같이 할당한 인사, 군수에 대한 대역폭 각 2.5Mbps와 기타 트래픽 4Mbps 보다 더 높은 대역폭을 할당 받으므로 더 효율적임을 할 수 있다.

<표 4-7>과 같은 QoS 보장방안으로 화상회의망을 국방전산망의 백본 간선내로 통합 시킬 수 있으며 화상회의망을 위한 T1 간선 사용을 줄일 수 있다. 화상회의망을 위한 T1간선 임대료를 알아보면, 국방부가 한국통신에 실제 지불하는 전용회선 월간 임대료는 <표 4-8>와 같다[19].

<표 4-8> 실제 전용회선 월간 임대료(2002년 기준)

(단위 : 원)

구 분	56/64Kbps	T1	E1	T3
11~30Km	283,560	1,222,500	1,629,960	12,233,160
31~50Km	395,940	1,707,240	2,276,280	17,081,880
51~100Km	625,440	2,721,600	3,628,800	27,225,960
101~200Km	709,380	3,334,080	4,445,460	33,343,140

<표 4-8>를 기준으로 화상회의망에 사용되는 간선 12회선 중 국방정보통신망에 통합 운영되는 11회선에 대해서 KT에 지불하는 연간 회선 임대비용을 추정해 보면 백본 간선은 51~200Km의 균일 분포를 갖는다고 가정할 때 연간 임대료는 약 4억원으로 추정된다. 산출 방법은 <표 4-9>에 나타나 있다[19].

<표 4-9> 화상회의망에 사용되는 연간 간선 임대료

(단위 : 원)

구분	회선수	1회선당 월간 임대료	1회선당 연간 임대료	연간 총 임대료
T1	11회선	(2,721,600 + 2*3,334,080) / 3	37,559,040	413,149,440

국방전산망에서 MPLS와 DiffServ를 이용한 QoS 보장방안은 중요 트래픽을 보장함으로써 신속하고 생존성 있는 의사결정 자료를 전송할 수 있으며, 비용적인 측면에서도 국방비를 절약할 수 있는 방안이다.

그러므로 현재 인터넷과 마찬가지고 Best-effort 서비스만을 지원하는 국방전산망은 급속도로 발전하는 외부의 미래 네트워크 환경과 멀티미디어 환경에 대비하여 지속적으로 진화를 추진해야 하고, 반드시 QoS에 대하여 고려해야 한다.

하지만 현실적으로 MPLS와 DiffServ를 국방전산망에 적용하기 위해서는 백본의 ATM 교환기를 LSR의 역할로, ATM 교환기에 직접 연결된 백본 라우터를 LER의 역할을 수행하도록 변경하여야 한다. 국방전산망을 구성하는 ATM 교환기는 Alcatel 사의 장비를, 백본 라우터는 Cisco사의 장비를 사용하고 있으며 MPLS와 DiffServ 지원을 위해 ATM 교환기에는 MPLS 지원을 위한 모듈을 추가 탑재해야 하며, 백본 라우터로 사용되고 있는 Cisco사의 7200계열 라우터는 기본적으로 MPLS를 지원하기 때문에 DiffServ지원을 위한 모듈을 추가 탑재하거나 혹은 MPLS와 DiffServ 모두 지원가능한 장비로 교체해야 한다.

5. 시뮬레이션 및 분석

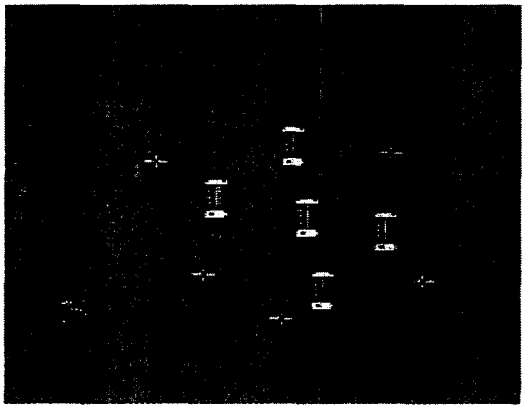
본 장에서는 제안하는 QoS 보장방안을 위한 MPLS와 DiffServ를 지원하는 망 구조와 MPLS와 DiffServ를 지원하지 않는 망 구조를 비교대상으로 네트워크 토폴로지(topology)를 구성하고 성능평가 및 분석을 한다. 성능평가는 시뮬레이션을 통하여 실시하였고, 시뮬레이션 도구로는 OPNET을 사용하였다.

본 시뮬레이션은 MPLS와 DiffServ를 이용했을 때 QoS를 보장하는지 여부에 대한 검증 방법이다.

5.1 시뮬레이션 네트워크 토폴로지 구성 및 모델링

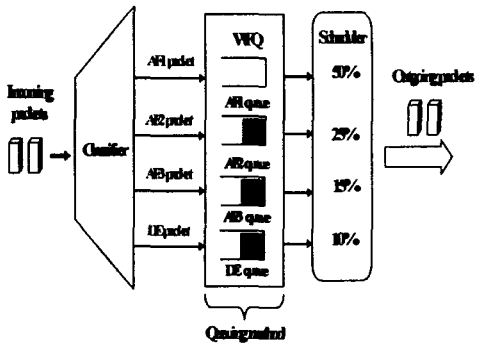
시뮬레이션 네트워크 토폴로지 구성은 성능을 측정하기 위한 모델로 <그림 5-1>과 같은 구조로 가정하였다. 이 모델은 국방전산망의 백본 네트워크를 간략화 한 것으로 백본 네트워크에서 QoS 제공 능력을 측정하기 위한 것이다. 이 모델의 단말은 송신측인 LER2에 연결된 작전, 군수, 기타로 구성하고 서버는 LER5에 연결된 육본으로 구성된다. 서버는 FTP 서버이다. 네트워크 링크(link) 용량 및 트래픽 발생량은 네트워크 혼잡 및 비 혼잡 상황을 연출하기 위해 임의로 설정 하였다. 백본 노드는 LSR1 ~ LSR6 이며, 단말은 FTP 트래픽을 혼잡상황에서는 10초당 853Kbyte씩, 비 혼잡 상황에서는 600Kbyte씩 발생시켜 서버인 육본으로 전송한다. LER2는 QoS 지원을 위한 트래픽 매핑을 지원한다. 단말, 서버와 LER사이는 T3(45Mbps), LER과 LSR사이는 OC3(155Mbps), 백본 링크(LSR

과 LSR)사이는 E1(2.048Mbps)으로 설정하였다. 작전, 군수, 기타에서 발생하는 FTP 트래픽들은 기존 라우팅 프로토콜인 OSPF에 의해 설정된 LER2 - LSR1 - LSR3 - LSR5 - LER5에 생성된 LSP를 지나 육본 FTP 서버로 전송된다.



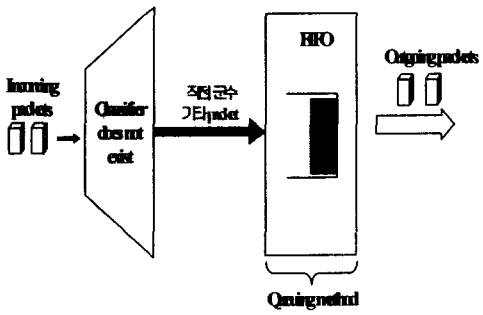
<그림 5-1> 시뮬레이션 네트워크 토폴로지 구조

MPLS와 DiffServ를 지원하는 망에서의 시뮬레이션을 위한 서비스 클래스 매핑은 작전, 군수, 기타에서 발생하는 트래픽에 대하여 소스주소와 목적지 주소에 따라 각각 AF1, AF3, DE로 설정 하였고, 서비스 우선순위는 AF1, AF3, DE순으로 하였다. 각 서비스를 제공하기 위한 큐잉(Queueing)방식은 WFQ(Weighted Fair Queueing)방식을 사용하였다. 이 방식에서 각 큐는 웨이트(weight)를 할당 받게 되며, 할당 받은 웨이트에 비례하도록 스케줄링이 이루어진다. 각 서비스에 대한 웨이트는 AF1, AF2, AF3, DE에 따라 각각 50, 25, 15, 10으로 설정하였다. <그림 5-2>는 WFQ 방식의 동작에 관한 것이다. <그림 5-2>에서 AF1 ~ DE 큐에 모든 패킷이 존재 할 경우에는 웨이트 값에 비례하여 50 : 25 : 15 : 10의 비율로 서비스가 이루어지며 시뮬레이션에서와 같이 AF2에 패킷이 없을 경우에는 AF2 큐에 할당된 웨이트가 나머지 큐에 균등하게 할당되어 약58 : 0 : 23 : 18의 비율로 서비스가 이루어진다.



<그림 5-2> WFQ 방식의 동작

성능측정을 위한 또 다른 모델은 <그림 5-1>의 구조는 동일 하지만 MPLS와 DiffServ를 제공하지 않는 망 구조이다. 이 구조에서의 큐잉 방식은 FIFO(First In First Out) 방식을 사용한다. <그림 5-3>은 FIFO 큐잉 방식의 동작을 나타낸다.



<그림 5-3> FIFO 큐잉 방식의 동작

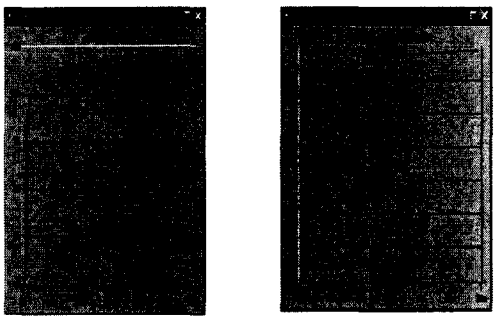
FIFO 방식은 하나의 큐에 모든 클래스의 트래픽을 저장하게 되며, 패킷의 클래스나 우선순위에 상

관없이 먼저 입력된 패킷을 먼저 서비스 하게 된다. 또한 FIFO 방식은 트래픽의 구분이 존재하지 않기 때문에 FIFO 방식을 사용하는 장비에서는 패킷 분류나 분류에 의한 표시와 관련된 기능은 필요 없게 된다.

5.2 시뮬레이션 결과 및 분석

시뮬레이션은 MPLS와 DiffServ를 지원하는 망과 지원하지 않는 망에서 단말인 작전, 군수, 기타에서 FTP 서버인 육본으로 FTP 트래픽을 전송하고 단말 각각에 대하여 upload response time과 queueing delay를 측정하여 성능 분석을 실시하였다. <그림 5-4>는 네트워크 혼잡과 비 혼잡 상황에서 대역폭 이용률을 보여주고 있다.

(X축 : 시뮬레이션 시간, Y축 : 대역폭 이용률)

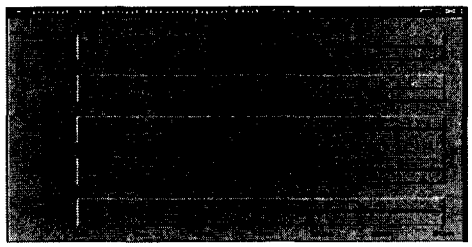


< 그림 5-4> 네트워크 혼잡과 비 혼잡시 대역폭 이용률
(왼쪽:네트워크 혼잡시,오른쪽:네트워크 비혼잡시)

<그림 5-4>의 왼쪽은 네트워크 혼잡시 백본인 LSR1 ~ LSR3의 링크 이용률이 100%가 됨을 나타내고 있으며, 오른쪽은 비 혼잡시 LSR1 ~ LSR3의 링크 이용률이 약 68%가 됨을 나타내고 있다.

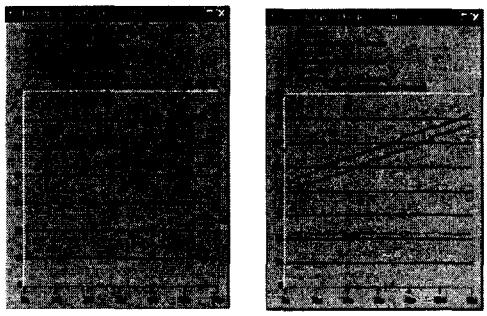
<그림 5-5>는 라우팅 프로토콜인 OSPF에 의해 설정된 경로인 LSP를 따라 패킷이 처리되는 것을 나타낸다.

(X축 : 시뮬레이션 시간, Y축 : 패킷처리량)



<그림 5-5> LSP를 통한 패킷처리

(X축 : 시뮬레이션 시간, Y축 : 응답시간)



MPLS와 DiffServ 미지원 MPLS와 DiffServ 지원

Object Name	Minimum	Average /W	Maximum
기타 <Engineer 1 / File Transfer>	26.9	48.1	64.5
군수 <Engineer 1 / File Transfer>	26.8	48.0	64.5
작전 <Engineer 1 / File Transfer>	26.6	48.0	64.4

MPLS와 DiffServ 미지원

Object Name	Minimum	Average /W	Maximum
기타 <Engineer 1 / File Transfer>	32.9	58.3	72.3
군수 <Engineer 1 / File Transfer>	28.7	53.6	67.5
작전 <Engineer 1 / File Transfer>	21.9	22.3	23.0

MPLS와 DiffServ 지원

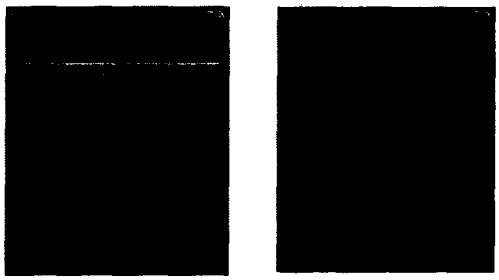
<그림 5-6> 혼잡시 upload response time측정결과 결과 비교

시뮬레이션 네트워크 토폴로지에서 LSP는 LER2 - LSR1 - LSR3 - LSR5 - LER5로 설정되었다. <그림 5-5>에서 보면 LSR1에서 LSR4로는

패킷 처리가 발생하지 않으며, LSP상의 다음 홉인 LSR3으로 패킷 처리가 발생하는 것을 알 수 있다.

<그림 5-6>은 혼잡시 MPLS와 DiffServ를 지원하지 않는 망과 지원하는 망에서의 upload response time 측정 결과이고, <그림 5-7>은 비 혼잡시 upload response time 측정 결과 이다.

(X축 : 시뮬레이션 시간, Y축 : 응답시간)



MPLS와 DiffServ 미지원 MPLS와 DiffServ 지원

Object Name	Minimum	Average /W	Maximum
기타 <Engineer 1 / File Transfer>	17.6	18.0	18.0
군수 <Engineer 1 / File Transfer>	17.6	17.8	17.8
작전 <Engineer 1 / File Transfer>	17.5	17.7	17.7

MPLS와 DiffServ 미지원

Object Name	Minimum	Average /W	Maximum
기타 <Engineer 1 / File Transfer>	21.2	25.2	25.2
군수 <Engineer 1 / File Transfer>	18.6	20.0	20.0
작전 <Engineer 1 / File Transfer>	15.4	15.6	15.6

MPLS와 DiffServ지원

<그림 5-7> 비 혼잡시 upload response time 측정결과 비교

<그림 5-6>과 <그림 5-7>의 결과에서 MPLS와 DiffServ를 지원하지 않는 망에서의 평균 upload response time을 보면 각각의 트래픽들에 대하여 동일한 서비스가 이루어짐을 나타내고 있으며, MPLS와 DiffServ를 지원하는 망에서 서비스 클래스가 높은 작전 패킷들은 MPLS와 DiffServ를 지원하지 않는망에서의 작전 패킷 보다 혼잡시에는 약 26초, 비 혼잡시는 약 2초가량 빨리 처리됨을 알 수 있다. 반면에 서비스 클래스가 낮은 군수 트래픽은 혼잡시 약 5초가량 늦게 처리되고, 비 혼잡시 약 2초가량 늦게 처리됨을 알 수 있다. 또한 Best-effort 서비스를 받는 DE 패킷들은 기존망보다 혼잡시 10초, 비 혼잡시 7초가량 늦게 처리됨을 알 수 있다.

이는 스케줄링시 할당된 웨이트에 따라 우선순위가 높은 트래픽을 우선 처리하고, 우선순위가 낮은 트래픽은 상대적으로 늦게 처리함으로써 기인하며, <그림 5-6>과 <그림 5-7>의 결과에서 네트워크 혼잡시나 비 혼잡시 모두 QoS가 보장되는 것을 알 수 있다.

(X축 : 시뮬레이션 시간, Y축 : 지연시간)

MPLS와 DiffServ 미지원 MPLS와 DiffServ지원

<그림 5-8> queueing delay 측정결과 비교

다음 <그림 5-8>은 혼잡상황에서의 MPLS와 DiffServ를 지원하지 않는 망과 지원하는 망에서의 queueing delay 측정결과 이다.

<그림 5-8>에서 나타난 queueing delay 역시

MPLS와 DiffServ를 지원하는 망이 더 짧은 delay를 나타내고 있다. 이와 같이 MPLS와 DiffServ를 이용하면 클래스별로 QoS 보장이 가능하며, 기존 망보다 더 효율적임을 알 수 있다.

6. 결 론

현재 Best-effort 서비스만을 지원하는 국방전산망은 빠르게 진화되고 있는 네트워크 환경과 멀티미디어 서비스 그리고 다양한 응용프로그램들의 등장으로 멀지 않은 미래에는 서비스의 질적인 향상과 높은 대역폭을 요구하게 될 것이다. 중요하다고 판단되는 데이터와 그렇지 못한 데이터들이 혼재하는 현재 네트워크 환경에서 중요하지 않은 데이터들에 의해 중요 데이터의 전송지연이나 손실이 발생하는 것은 큰 문제점이라 할 수 있다. 국방전산망 역시 이러한 문제점을 가지고 있다.

본 논문에서는 이러한 문제점을 해결하기 위한 방안으로 국방전산망에 MPLS와 DiffServ기술을 이용하여 군 기능에 따른 트래픽별 QoS 보장방안을 제안하였다. 먼저 기존 데이터 대역폭을 그대로 이용하면서 군 기능별 QoS를 보장하는 방안을 제안하였고, 국방전산망에서 VoIP기술이 적용되어 사용가능 했을 경우를 가정하고 백본 간선에서 VoIP 사용에 따른 QoS 보장방안을 제안하였다. 또한 화상회의망과 국방전산망의 간선통합시 QoS 보장방안을 제안하였다.

본 논문에서 제안하는 핵심은 국방전산망에서의 QoS 보장이며 MPLS와 DiffServ기술을 적용시킨 망에서의 QoS 보장여부에 대한 검증방법으로 시뮬레이션을 사용하였다. 시뮬레이션은 MPLS와 DiffServ를 지원하는 망과 지원하지 않는 망의 비교를 통하여 성능분석을 실시하였고 그 결과 MPLS와 DiffServ기술을 이용했을 때 우선순위가 낮은 패킷들의 처리는 지연되더라도 우선순위가 높은 패킷들의 처리는 기존 망에서보다 빨리 처리됨을 알 수 있었다.

결론적으로 국방전산망에서 QoS를 보장하기 위해서는 MPLS와 DiffServ기술을 도입해야 하며, QoS가 보장될 경우 보다 효율적인 국방전산망 운용이 가능 할 것이다. 즉, QoS 보장으로 화상 회의망과 같은 국방정보통신망내의 다른 체계 또한 동일한 네트워크를 통해서 서비스가 이루어질 수 있는 것이다. 이를 위해 QoS 보장기술에 대한 지속적인 연구는 필수적이며, 현실적으로 군 기능별 QoS를 지원하기 위해서는 국방전산망에 대한 정확한 트래픽예측에 대한 연구가 필요하고, 보다 더 효율적인 국방전산망 운용을 위해서는 향후 MPLS 망에서 VoIP지원 및 트래픽 엔지니어링에 대한 연구가 필요하다.

참 고 문 헌

[1] B. Davie, et al., "MPLS Technology and Applications", Morgan Kaufmann, 2000.

[2] 한국전자통신연구원, "MPLS LER에서 DiffServ 지원을 위한 IP 패킷 처리구조 연구", 연구보고서, 2000.

[3] L. Zhang, et al., "RSVP version 1 Functional Specification", RFC 2205, 1997.

[4] J. Wroclawski, "The Use of RSVP with IETF Integrated Services", RFC 2210, 1997.

[5] S. Shenker, et al., "An Architecture for

Differentiated Services", RFC 2475, 1998.

[6] E. Rosen, et al., "Multiprotocol Label Switching Architecture", RFC 3031, 2001.

[7] 한국전산원, "초고속 MPLS 기술분석, 서비스 수요 및 도입방안 연구", 연구보고서, 2003.

[8] L. Andersson, et al., "LDP Specification", RFC 3036, 2001.

[9] D. Tappan, et al., "MPLS Label Stack Encoding", RFC 3032, 2001.

[10] 김영탁, "DiffServ-aware-MPLS : a Promising Traffic Engineering for Next Generation Internet(NGI)", 제8회 정보통신응용기술워크숍, 2003.

[11] K. Nichols, et al., "Definition of the Differentiated Services Field(DS Field) in the IPv4 and IPv6 Headers", RFC 2474, 1998.

[12] ISI, "Internet Protocol", RFC 791, 1981.

[13] Jacobson, et al., "An Expedited Forwarding PHB", RFC 2598, 1999.

[14] Heinanen, et al., "Assured Forwarding PHB Group", RFC 2597, 1999.

[15] Y. Rernet, et al., "Requirement of DiffServ Boundary Router", Internet Draft<draft-bernet-diffedge-01.txt>, 1998.

[16] S. Davari, et al., "MPLS Support of Differentiated Services", RFC 3270, 2002

[17] 국방부, "국방정보통신망 통합 망관리체계 기본계획(Master Plan)", 2001.

[18] 국방부, "국방정보통신망(ATM) 보안 대책 연구", 2002.

[19] 국방부, "국방정보통신망 VPN 적용시 최적의 통신회선 구축방안 연구", 2002.

[20] 포스데이타, "WDM발전방향 및 응용전망", 제2회 국방정보화기술심포지엄 신기술동향, 2001.

[21] 김영호, "군 정보통신 유통량 예측 방안," 국방정보통신연구원, 2001.

[22] 김성순, 이승종, "국방전산망에서 ATM 기반 MPLS를 이용한 차등서비스 적용방안에 관한 연구", 한국정보처리학회 춘계학술발표대회, 2003.

[23] 김성순, 신현응, 이승종, "국방전산망에서 QoS 보장과 Traffic engineering을 위한 MPLS 적용방안에 관한 연구", 한국통신학회 하계학술대회, 2003.

[24] 국방부, "매가센터 지원을 위한 네트워크 개선방안 연구", 2001.