韓國國防經營分析學會誌
제 29 권, 제 1 호, 2003. 6. 30.

국방정보체계의 서비스 품질(QoS) 보장을 위한 정책기반(Policy-Based)네트워킹 적용에 관한 연구 (A study on the Application of Policy-Based Networking for QoS in The Defense Information System)

김 광 영, 이 승 종*

Abstract

Policy-based networking offers a network manager the ability to manage the network in a holistic and dynamic fashion rather than force a network manager to manage the network by dealing with each device individually. Policy-based networking is focusing on users and applications instead of emphasizing devices and interfaces. An important part of the policy-based networking is to simplify the task of administration and management for different disciplines.

The Defense Information System(DIS) of today are complex and heterogeneous systems. Operational needs are not a trivial task and Quality of Service(QoS) is not generally guaranteed. So, important data may be missed or congested by trivial data. Policy-based networking provide a way to support QoS and simplify the management of multiple devices deploying complex technologies.

This paper suggest implementation of policy-based networking in DIS to improvement of performance, and implementation is progressed step by step. Especially this paper is focusing on the providing QoS with policy-based networking using Lightweight Directory Access Protocol(LDAP) Server.

* 국방대학교 관리대학원

1. 서 론

오늘날 네트워크에서 정책기반(Policy-Based) 네트워킹의 중요성은 갈수록 증대되고 있다. IP네트워크에서 가상사설망(VPN: Virtual Private Network)이나 서비스 품질(QoS: Quality of Service) 등 사용자의 요구사항이 갈수록 다양해지면서 복잡해지고 있고 네트워크 장비 역시 수많은 제품이 시장에 나오고 있으며 장비 설치 시 설정은 복잡성을 더해가고 있다. 네트워크 관리의 핵심도 기존의 장비관리와 인터페이스 관리에서 사용자나 응용프로그램 중심의 관리, 정책저장소를 이용한 중앙집중식 관리의 개념으로 바뀌고 있다.

정책기반네트워킹은 현재의 네트워크에서 장비 설정에 관련된 관리자의 업무를 보다 간단하게 할 수 있으며 임무에 필수적인 응용프로그램의 수행능력을 예측할 수 있도록 하는 방법이다. 또한 중앙의 정책저장소를 이용한 중앙집중식 관리로 일관성 있는 정책의 적용과 트래픽의 중요도에 의한 차별적인 처리를 가능하게 한다[1].

첨단 정밀기술과 통신기술의 발달은 미래의 전장환경을 변화시키고 있으며 특히 정보화 기술의 발달은 무기체계의 실시간 전장지휘 및 통합 전투력 발휘를 가능하게 하였다. 오늘날의 전쟁은 전장상황을 종합적으로 판단하고 통제하면서 실시간 통합전력을 발휘하여 최소 희생으로 전쟁에서 승리하는 통합전장관리체계의 중요성이 강조되고 있으며 우리 군도 정보화 군 건설에 역점을 두고 21세기 새로운 전장개념에 적합한 자동화된 지휘통제시스템 도입을 지속적으로 추진하고 있다. 특히 각 군은 전술C4I체계를 구축하고 있으며 합참에서도 합동C4I체계를 구축계획을 추진 중에 있다.

자동화된 지휘통제시스템에서는 네트워크의 중요성이 더욱 커질 것이다. 또한 실시간 정보 전송을 위해 네트워크의 트래픽을 예측하고 필요한 대역폭을 확보, 제공하는 네트워크 관리자의 중요성도 더욱 커질 것이다. 그러나 네트워크 트래픽의 특성상 트래픽 예측이나, 모든 트래픽을 처리할 수 있는 네트워크를 구축하기 어렵고 군 특성상 다수의 전문적인 네트워크 관리자를 육성하기 어려운 것이 현실이다. 그러므로 정책기반네트워킹을 구현하면 정책관리도구를 사용한 자동화된 관리, 일관된 보안정책 수립, 네트워크 관리정책을 통해 트래픽을 분류하고 트래픽의 중요도에 따라 차등서비스를 제공하는 등, 네트워크의 효율적인 이용은 물론 장차전에서의 승리를 보장할 수 있을 것이다. 예를 들어 트래픽의 종류와 사용자, 상황에 따라 트래픽을 분류하고 분류된 트래픽에 따라 차별화된 서비스를 제공하므로 네트워크에서 트래픽 폭주가 발생하더라도 실시간대 전장상황을 관리, 지휘관에게 신속하고 신뢰성 있는 중요 의사결정 자료를 제공할 수 있는 것이다.

본 논문은 현재 국방정보망에서 차별화된 서비스를 제공하기 위한 방법을 제시하고 그 중 정책저장소로 LDAP(Lightweight Directory Access Protocol) 서버를 사용하여 QoS 구현을 위한 차등서비스 정책기반네트워킹 모델을 제시할 것이다. 또한 정책기반네트워킹을 국방정보통신망에 적용하기 위한 단계적 구축방안을 제시할 것이다. 본 논문은 국방정보통신망에 정책기반네트워킹을 도입함으로써 새로운 정보기술 환경에 적합한 저비용 고효율 국방정보통신망 구축에 기여하고자 한다.

2. 관련연구

2.1 차등서비스(DiffServ)

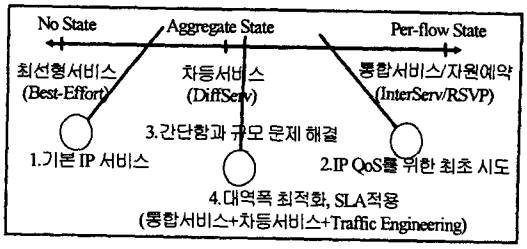
2.1.1 서비스 품질(QoS) 개념

상위수준의 추상적인 개념으로서의 QoS는 SLA(Service Level Agreement)에 명시된 전송 수준 특성 값에 따라 네트워크 서비스를 제공하는 능력을 말한다. 품질(Quality)은 서비스 능력, 지연(delay), 지터(jitter), 처리용량 (throughput), 패킷손실율로 표시할 수 있다. 네트워크 자원 수준에서 QoS는 서비스 제공자에게 트래픽에 우선권을 부여하고, 대역폭과 네트워크 지연을 통제할 수 있도록 하는 것이다. QoS는 높은 대역의 비디오 및 멀티미디어 정보를 지속적으로 전송해야 하는 경우에 특별한 의미를 가지며 다양한 레벨의 QoS를 지원하기 위해 Layer-2 또는 Layer-3 QoS 기술들이 연구되어지고 있다. IP네트워크에서 QoS는 통합서비스(InterServ: Integrated Service)와 차별화 서비스(DiffServ: Differentiated Service)로 구분된다.

2.1.2 차등서비스

1998년 IETF(Internet Engineering Task Force) DiffServ WG(Working Group)에서 제안된 이 모델은 <그림 2-1>에서 보듯이 QoS레벨로 보면 오늘날 인터넷과 같은 최선형서비스 제공과 통합서비스(IntServ) 모델에 의한 QoS를 보장하는 모델의 중간 위치에 있다.

이 모델에서는 우선적으로 QoS를 몇 개의 클래스로 분류하여 이 분류된 클래스에 따라 서비스를 보장하도록 하는 것이다. 이에 따라 IP 헤더의



<그림 2-1> QoS의 진자

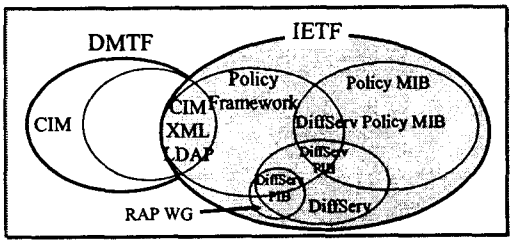
특정 필드(IPv4: Type of Service, IPv6: Traffic Class Field)에 마킹하여 DS(Differentiated Service)를 설정하게 된다. 이렇게 특정 값으로 설정된 DS값들에 의해 적절한 포워딩(PHB: Per-Hop Behavior)을 수행하도록 하는 구조이다.

본 논문은 차등서비스의 EF(Expedited Forwarding)와 AF(Assured Forwarding) PHB를 이용한 QoS 제공 방안에 대해 논의하였다. EF 서비스는 프리미엄서비스라고도 하며 낮은 지연과 낮은 지터의 특성을 가지고 있으며, 라우터의 큐(queue)에서 새로운 패킷이 도착하기 전에 버퍼에 있는 전송되는 특징을 나타낸다. AF는 사용자들로부터 받은 다양한 패킷에 대해 다양한 수준의 전송을 보장하는 서비스로 WFQ(Weighted Fair Queueing)가 AF 트래픽 통제에 유용하게 사용될 수 있다. AF에는 4종류의 클래스가 정의되어 있으며 각각의 DS노드에는 AF 클래스별로 일정량의 포워딩 자원(버퍼 공간, 대역폭)이 할당되어 있다. 각 AF에는 사용자나 서비스 제공자에 의해 정의된 3가지의 폐기우선순위가 적용되므로 AF의 PHB수는 총 12가지가 된다. 혼잡 상황 시 패킷의 폐기우선순위에 따라 AF 클래스 내에서 상대적인 중요성이 결정되어진다. DS 노드는 혼잡 시 낮은 폐기우선순위가 높은 폐기우선순위에 비해 패킷 손실이 덜 발생되도록 방지하는 역할을 한다.

본 논문에서는 AF의 1번 클래스를 사용하여 3가지의 폐기우선순위를 부여하는 방법을 적용하였다.

2.2 정책기반네트워킹(Policy-Based Networking)

정책기반네트워크 표준 모델은 IETF와 DMTF (Distributed Management Task Force)에서 별도의 표준을 개발하고 있으나 <그림 2-2>와 같이 하나의 표준으로 통합되고 있으며 두 표준화 단체는 공통의 표준을 만들기 위해 노력 중이다[15].



<그림 2-2> 표준화 동향

2.2.1 정책의 정의

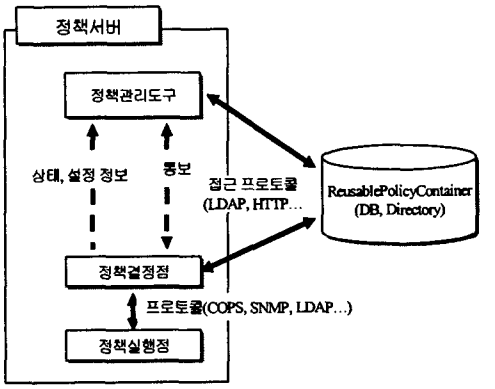
네트워크에서 정책이란 어떤 사용자, 애플리케이션, 호스트가 어떤 자원이나 서비스를 어느 조건에서 사용할 수 있는지를 결정하는 것이라 할 수 있다. 정책은 기업이 추구하는 목표와 SLA에 의해 결정되어지고 네트워크 관리자에 의해 설정되어 LDAP 서버나 데이터베이스와 같은 저장소에 입력되는 것으로 시스템의 작동 상태를 통제할 수 있는 것이다[10]. 정책은 다양한 방법으로 구분될 수 있으나 일반적으로 상위수준정책과 하위수준정책으로 구분할 수 있으며 사용하는 목적에 따라 IETF에서는 다음과 같이 분류하였다[11].

- 동기 정책(motivation policies)
- 설정 정책(configuration policies)
- 인스톨 정책(installation policies)
- 에러와 이벤트 정책(error and event policies)
- 사용자 정책(usage policies)
- 보안 정책(security policies)
- 서비스 정책(service policies)

일반적인 네트워크 정책에는 QoS와 보안 등이 있으며 시간, 사용자 식별, 선불통화카드나 토큰 등도 정책이 될 수 있다.

2.2.2 정책기반네트워킹(Policy-Based Networking)

IETF와 DMTF에 의해 정의된 정책기반구조는 <그림 2-3>과 같이 4가지의 기본 구성 요소로 이루어져 있다.

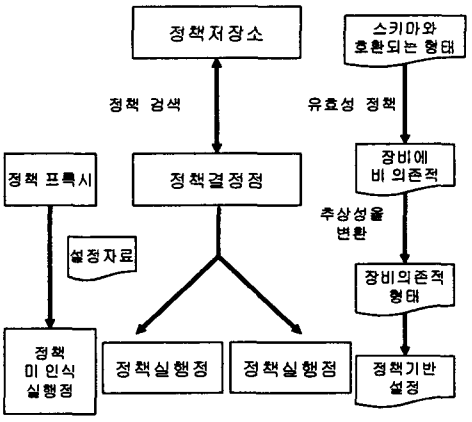


<그림 2-3> IETF/DMTF 정책기반구조

정책관리도구(Policy Management Tool)는 관리자에 의해 사용되는 구성 요소로 네트워크에서 사용될 정책을 입력하는 부분으로, 사용자나 관리자로부터 상위수준(high-level)정책을 입력 받아 네트워크의 다양한 장비(device)에 적용할 수 있도록

보다 상세하고 정확한 하위수준(low-level)정책으로 변환시켜주는 일을 한다. 여기서 장비는 정책실행점(PEP: Policy Enforcement Point)에서 입력 받은 여러 정책들을 실행하는 부분이다.

정책결정점(PDP: Policy Decision Point)은 현재 관리되고 있는 정책실행점에 사용가능한 규칙 조합을 찾아내고 저장소로부터 그 규칙을 가져온다. 저장소로부터 가져온 규칙을 PEP가 이해할 수 있는 형태나 구문으로 변환시키며 네트워크의 현재 상태를 점검하고 애플리케이션 정책을 적용하는데 필요한 네트워크 상태를 검증한다. 또한 저장소를 모니터하거나 관리도구로부터 제공되는 통보를 주목하면서 정책의 변화를 계속 감시한다. <그림 2-4>는 정책결정점에서의 정책처리절차를 나타낸다.



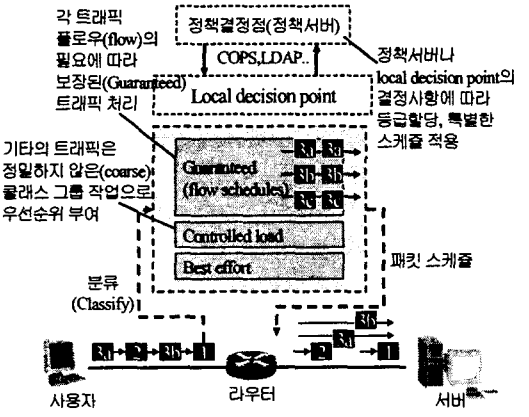
<그림 2-4> 정책결정점의 정책 처리절차

관리도구와 정책결정점간에는 정책저장소(ReusablePolicyContainer)를 통해 통신을 한다. 정책저장소는 관리도구가 생산한 정책을 저장하는 일을 하는데, 상위수준정책과 하위수준정책을 동시에 저장할 수 있다. 여러 업체들에 의해 생산된 다양한 장비간의 상호운용성을 보장하기 위해 저장소에 저장되는 정책은 IETF의 PFWG(Policy Framework Working Group)에서 정의한 정보 모델을 준수해야 한다. 정책실행점은 저장소와 직접 통신을 하지 않고 중간에 정책결정점을 경유하여 저장소와 정책에 관련된 정보를 획득하며 정책결정점은 저장소에 저장된 정책을 해석하여 정책실행점으로 전달해주는 책임을 맡고 있다[5][6].

관리도구와 정책결정점, 정책실행점, 저장소는 다양한 프로토콜을 사용하여 정책에 관련한 정보를 통신할 수 있다. 저장소와 어떤 프로토콜을 사용하여 통신을 할 것인가는 선택되는 저장소의 형태에 따라 달라진다. 현재 가장 많이 사용하고 있는 것은 LDAP을 사용하여 저장소와 정보를 주고받는 것이며 IETF에서는 LDAP v3를 표준으로 제안하였다.

정책실행점은 정책결정점이 정의한 정책을 실행하는 역할과 동작에 관련된 다른 정보나 상태를 모니터하여 적당한 위치로 보고하는 역할을 한다. 정책실행점은 패킷의 이동 경로를 따라 실행되는 컴포넌트로 인식되기도 한다.

정책실행점으로는 네트워크 라우터나 방화벽, 종단 호스트의 TCP/IP 처리 스택, 프락시, SOCKS 게이트웨이 등이 있다. 정책실행점 구성 요소들은 관리도구의 입력이 되는 정책에 의해 명세된 필요한 기능의 전달에 많은 부분을 의존하고 있다. <그림 2-5>는 정책실행점의 하나인 라우터에서 실제 정책을 변환하고 처리하는 방법을 나타내고 있다.



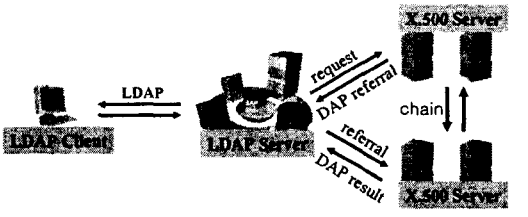
<그림 2-5> 라우터에서의 패킷처리

2.3 LDAP

LDAP은 관리도구가 표준화된 형태에 사용될 수 있는 정책을 쉽게 명세할 수 있도록 차별화서비스 정책을 지정할 수 있는 표준화된 방법이다. LDAP은 설정정보를 중앙사이트에 저장하고 관리도구는 중앙사이트에서 필요한 정보를 획득하여 저장소에 저장하고, 각 장비에서 실행 중인 에이전트는 정책이나 설정 정보를 저장소로부터 획득하여 정책을 장비에 맞도록 구현할 수 있도록 하는 프로토콜이다. 그리고 이러한 정보를 저장하는 저장소의 한 형태가 LDAP 프로토콜을 사용한 디렉토리 서버이다. LDAP 클라이언트는 대부분의 플랫폼에서 사용가능하고 새로운 프로토콜 개발이 필요 없으며 정책정보와 같은 레코드를 포함한 다른 형태의 레코드를 쉽게 저장할 수 있는 장점이 있다. 또한, 대부분의 조직에 필요한 인사 정보를 디렉토리 형태 정보로 저장할 수 있고 관리와 운용에 필요한 인사 정보를 체계적으로 저장하여 사용할 수 있는 장점이 있다.

2.3.1 LDAP 출현배경

LDAP은 최초 <그림 2-6>과 같이 X.500 DAP(Directory Access Protocol)로의 자원 요청없이 X.500 모델들을 지원하는 디렉토리 액세스(access)를 제공하기 위해서 제작되었다.



<그림 2-6> LDAP의 동작

이 프로토콜은 특별히 디렉토리들 상호간의 읽기/쓰기 액세스를 제공하는 처리응용(management application)들과 브라우저 응용들을 목표로 삼았으며, X.500을 지원하는 디렉토리와 사용될 때는 X.500을 위한 보완물로써 사용되었다. 그러나 X.500이 실제 적용하기 어렵고 규모면에서 대규모이며 개인용 컴퓨터 기반이 아니었기 때문에 LDAP은 점차 단순한 게이트웨이가 아니라 디렉토리 서비스 자체로 사용되기 시작했다. LDAP은 클라이언트 사용자를 위한 표준 'CAPI'가 만들어지면서 디렉토리 서비스의 핵심 프로토콜로 자리잡게 되었다. 더욱이 인터넷 웹의 성공은 URL(Uniform Resource Locator)을 지원하는 LDAP 개발을 선도하게 되어 웹브라우저를 통한 LDAP 접근이 가능하게 되었다[2].

LDAP이 정책기반네트워킹에서 X.500이나 다른 프로토콜보다 많이 사용되고 있는 것은 다음과 같은 장점을 가지고 있기 때문이다.

- 공개된 솔루션(open solution): LDAP은 공개된 표준이므로 누구라도 LDAP 서버나 클라이언트를 만들 수 있고 미래의 발전방향에 대해서 자유로운 의견을 제출할 수 있음
- 안전하고 확장 가능한 형태
- 표준 API를 사용한 프로그램
- 게이트웨이 서비스(gateway service)
- 업체 지원

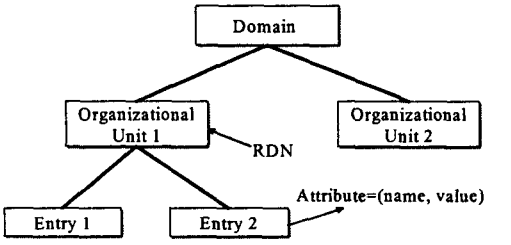
2.3.2 LDAP의 구성

LDAP은 디렉토리 접근 프로토콜이지만 프로토콜 이상의 의미를 내포하고 있다. LDAP은 크게 다음과 같은 세부분으로 정의할 수 있다.

- 데이터형태: 디렉토리 정보가 저장되고 사용되는 방법 정의
- 프로토콜: 클라이언트와 서버가 상호 통신하는 방법 정의
- API: 프로그램이 LDAP 서버와 상호 작용하는 방법 정의

LDAP의 가장 중요한 부분 중 하나가 데이터 형태이다. LDAP에서 데이터 형태는 모든 플랫폼에 수용가능하며 모든 문화에 수용 가능한 형태로 정의 되어있으며 각각의 엔트리는 범세계적인 이름스키마인 네임스페이스(namespace)에 속하도록 되어 있다.

LDAP 서버에 존재하는 데이터는 계층적이면서 관계적인 형태를 유지하고 있다. 즉, 서버의 엔트리는 루트 엔트리로부터 계층적이지만, 엔트리를 그룹화 할 수 있으므로 관계형식을 나타낸다고 할 수 있다. 기본적인 LDAP의 계층구조는 <그림 2-7>과 같다.



<그림 2-7> LDAP 데이터 형태의 기본구조

엔트리는 하나 이상의 값을 가진 애트리뷰트(attribute)로 이루어져 있으며 애트리뷰트는 이름/값의 구조를 가지고 있다. 각각의 엔트리는 식별자인 DN(Distinguished Name)에 의해 유일하게 식별될 수 있으며, DN은 상대식별이름인 RDN (Relative Distinguished Name)으로 구성되어 있다.

LDAP 서버는 한 스키마에서 객체 클래스(object class)와 객체 계층구조를 정의하고 있다. LDAP v3에서는 서로 다른 객체들과 구분 할 수 있도록 모든 요소에 세계적으로 유일한 OID (Object Identifier)를 부여하고 있으며 이것은 마치 호스트에 고유의 IP주소를 부여하는 것과 같은 것이다. IANA(Internet Assigned Numbers Authority)에서는 개인기업(private enterprise) 부분에 한하여 무료로 OID를 등록시켜주고 있으며 해당 OID의 하부 OID는 사용자 임의대로 사용할 수 있다. 이번 논문의 QoS 객체를 위해 IANA에 학교 이름을 등록하여 "14479, Korea National Defence University" 즉, 1.3.6.1.4.1.14479라는 OID를 할당 받아 사용하였다.

LDAP의 일반적인 프로토콜 모델은 서버(server)와 클라이언트(client) 형태의 프로토콜로 클라이언트는 서버로 필요한 작업을 요청하고 서버는 디렉토리에서 필요한 작업을 수행 후 클라이언

트로 결과 값을 응답하는 방식이다. 클라이언트와 서버는 다음의 3단계 과정을 통해 통신이 이루어진다[13].

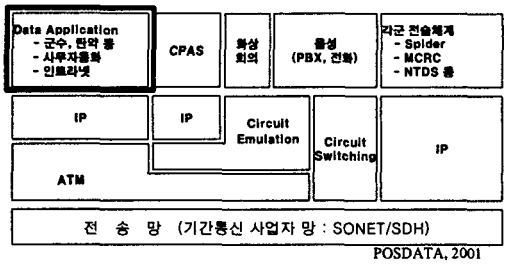
- 서버에 연결
- 서버와 일련의 동작 실행
- 서버와의 연결 종료

연결과 연결 해제는 TCP/IP의 표준 연결 설정 방법을 사용한다. LDAP은 디렉토리 접근 프로토콜이므로 디렉토리에서 엔트리의 저장 방법이나 검색 방법에 대한 정의는 하지 않으므로 디렉토리 서버 개발자들이 서버 개발 시 많은 융통성을 가지고 개발할 수 있는 장점이 있다.

3. 국방망 고찰

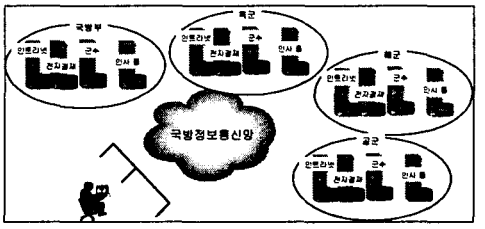
3.1 국방망의 구성 및 구조

국방망(국방인트라넷)은 국방정보통신망의 하위망으로 국방정보통신망의 네트워크의 부분집합이다. 국방정보통신망은 <그림 3-1>과 같이 기간통신사업자 망인 전송망 위에 ATM망이 있으며, 주요 지역간은 T3급으로 전송로가 구성되어 있다. 현재 운용 중인 국방망은 국방정보통신망 고도화 계획에 의거 ATM망으로 통합되었다. 현재 국방망은 전산업무 지원을 위해 각 군별, 각 부대별로 TCP/IP 기반의 인트라넷 웹서비스, POP3 기반의 전자메일 시스템, 전자결재 서비스, 지휘소자동화체계, 화상회의 시스템, 군수자원관리 시스템 및 탄약관리시스템, 야전제대인사업무 시스템, 자체 상황관리 시스템 등이 구축되어 있다[7].



<그림 3-1> 국방정보통신망 프로토콜 구조

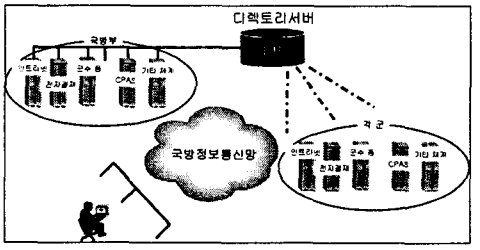
국방망 구조는 <그림 3-2>에서 보듯이 각 시스템마다 자체 데이터베이스로 사용자 정보를 구축하고 있으며 이러한 시스템은 각 군별로 분리되어 있다. 따라서 사용자 인증을 위한 사용자 정보는 각 군별, 각 부대별, 각 시스템별로 별도의 데이터베이스가 존재하고 있다. 그래서 사용자는 부대를 옮길 때마다 각 부대에서 제공하는 인트라넷, 응용체계 등의 서비스에 접속하여 사용자 정보를 등록해야 하는 번거로움이 있었다. 부대별 독립적으로 구축된 시스템은 전산자원의 낭비 및 관리자의 업무를 복잡하게 하였고, 네트워크 구축 및 확장에 따른 추가적인 비용 문제 및 급변하는 사용자의 요구에 적시적절하게 대처하지 못하고 있다.



<그림 3-2> 국방망 구조

그러나 <그림 3-3>과 같은 LDAP디렉토리 서버를 도입한 정책기반네트워킹은 전 군별로 사용자

정보를 하나의 LDAP 서버에 저장하여 네트워크 구축비용을 줄일 수 있고 관리자의 업무를 대폭 줄일 수 있으며 소수의 관리자로 대규모네트워크를 효율적으로 관리할 수 있다.



<그림 3-3> 디렉토리 서버를 이용한 국방망

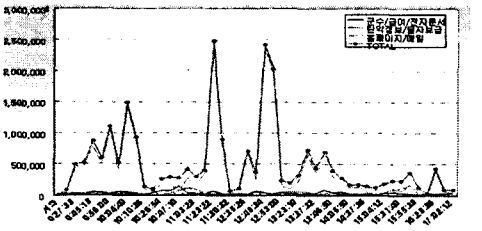
또한, 부대 전출입으로 인해 수시로 사용자 정보가 교체되는 환경에서도 한 데이터만 수정하면 되므로 항상 최신의 정보를 저장하여 제공할 수 있으므로 효율적인 시스템을 구축할 수 있는 것이다.

3.2 국방망 트래픽 분석

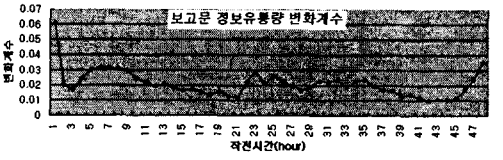
정책기반네트워킹은 정책을 통해 트래픽을 분류하고 각각 차별적인 서비스를 보장하는 방법이므로 정책기반네트워킹을 구현하기위해서는 정확한 네트워크 트래픽 분석 작업이 선행되어야 한다.

<그림 3-4>는 포스데이터가 평시 00사단 인트라넷에서 측정한 트래픽 분석자료로 그림에서 알 수 있듯이. 트래픽은 항상 동일한 것이 아니라 특정 시간에 인트라넷 홈페이지 접속과 전자우편 사용으로 인해 트래픽 집중현상을 나타내고 있다. 만약 네트워크가 트래픽이 집중하는 시간대에 필요한 대역폭 이상을 제공하지 않는다면 전체 네트워크가 마비될 수도 있을 것이다. 즉 중요한 지시나 보고 전송이 이 시기에 이루어진다면 네트워크는 필요한 서비스를 제공할 수 없을 것이다.

<그림 3-5>는 00사단 BCTP(Battle Command Training Program)시 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[6].



<그림 3-4> 00사단 트래픽 분석



<그림 3-5> 00사단 BCTP간 정보 유통량
(사단 → 군단)

평시와 훈련시의 트래픽 측정치에서 알 수 있듯이 현재의 국방망에서는 일부 서비스의 트래픽 증가나 특정시간대의 트래픽 증가로 인해 전체 네트워크의 사용이 제한되거나 중요정보 및 보고의 전달 지연이 발생할 수 있음을 알 수 있다. 트래픽 폭주 시의 데이터 유통량을 대비한 충분한 대역폭을 제공하면 되지만 그에 따르는 네트워크의 구축비용, 네트워크의 효율적인 이용 측면에서 바람직하지 않을 것이다. <표 3-1>과 같이 국방정보통신

망의 확장에 소요되는 예산은 갈수록 증가하고 있기 때문에 적정 대역폭만큼 쉽게 확장할 수도 없을 것이다[9].

또한, 트래픽 특성상 다양한 변수가 존재하기 때문에 정확한 정보유통량을 예측하기는 쉽지 않다. 특히 멀티미디어 데이터 등의 폭발적인 증가, 특정 상황에 따른 정보유통량의 급격한 변화, 정보화 환경의 급격한 변화 등은 정확한 정보유통량의 측정을 더욱 어렵게 하는 요소인 것이다.

<표 3-1> '02~'06 국방중기계획(국방정보통신망 확장예산)

'01 예산 (백만원)	중 기 계 획(백만원)					합계 ('02-'06)
	'02	'03	'04	'05	'06	
9,887	13,973	15,785	17,384	19,518	21,776	88,435

이러한 환경에서 정책기반네트워킹을 통한 트래픽의 선별적인 처리는 좋은 대안이 될 수 있을 것이다. 즉, 네트워크 대역폭을 초과한 트래픽 발생 시 네트워크가 마비되는 것이 아니라 미리 정해진 정책에 의해 트래픽을 분류, 차별적인 서비스를 보장하는 것은 전체 시스템의 효율적인 사용을 보장하고 임무에 필수적인 정보의 전송을 보장할 수 있을 것이다.

인터넷 등 상용망은 VoIP(Voice over IP), MPLS 기술을 도입한 VPN서비스, 유·무선 통합 등 네트워크 통합환경으로 진화하고 있다. 상용망의 네트워크 진화와 함께 국방망도 네트워크 통합환경으로 진화될 것이다. 현재 별도의 망으로 구축된 화상회의 시스템도 TCP/IP 기반의 화상회의 시스템으로 통합되고, 음성 서비스가 네트워크 서비스로 통합되어 VoIP형태로 제공될 것이고 각종 네트워크가 하나의 네트워크로 통합된 단일 네트워크로 발전되고 VPN서비스가 활성화 될 것이다. 통합 네트워크 구축 시 정책기반네트워킹은 보안, QoS 등의 서비스를 사용자가 설정한 정책에 제공할 수 있을 것이다[16].

3.3 정책기반네트워킹 구현을 위한 요구사항

지금까지 트래픽 분석, 네트워크 구성 및 구조 분석을 통해 국방망에 대해 알아보았다. 그 결과 국방망에 정책기반네트워킹을 도입하기 위해서는 다음과 같은 문제점과 요구사항이 도출되었으며, 이러한 문제들은 정책기반네트워킹을 도입을 통한 국방망의 효율성과 생존성을 증대시키기 위해 해결되어야 할 것이다.

(1) 국방망에서 사용되는 응용체계는 체계별로 별도의 시스템이 구축되어 있고 사용자 인증이나 정보저장을 위해 각기 다른 데이터베이스를 유지하고 있으므로 시스템 구축비용이 중복 투자되고 있다. 또한 부대내 사용자 정보변동 시 시스템별로 전 사용자 정보 데이터베이스를 변경시켜야 하는 등 관리자의 부가적인 노력을 많이 필요로 하는 시스템으로 구축되어 있다. 그러므로 각 군별, 각 부대별, 각 시스템의 사용자 정보를 하나로 통합하는 효율적인 방안에 대한 연구가 실시되어야 할 것이다.

(2) 효율적인 국방망 구축에 필요한 네트워크 대역폭 확보를 위한 체계적인 트래픽 측정이 실시되지 않았기 때문에 적절한 국방 네트워크 구축에 대한 객관적인 자료가 부족하다. 즉, 응용체계별,

사용자별, 시간대별 트래픽 측정에 대한 자료가 부족하여 차별화된 서비스 제공에 대한 대비가 부족하다. 그러므로 정책기반네트워킹 구현을 위해 체계적인 트래픽 측정 작업, 트래픽 분류 작업이 실시되어야 할 것이다.

(3) 정책기반네트워킹 도입에 필요한 응용 애플리케이션별 우선순위, 사용자별 우선순위, 그룹별 우선순위, 시간대별 우선순위 부여, 지연에 민감한 애플리케이션 구분/처리 등 세부적인 네트워크 정책이 수립되어야 한다.

(4) 각 응용체계의 통합, VPN 서비스 도입, 통합인증체계 구축 등 미래 네트워크 환경 변화에 대한 대비로 통합네트워크 구축에 대한 개념 정립이 필요하다.

4. 국방정보통신망에서의 정책 기반네트워킹 구축 방안

4.1 정책기반네트워킹의 역할

국방정보통신망에서 정책기반네트워킹의 역할은 사용자, 응용프로그램의 종류 등에 따라서 차별화된 서비스 등을 제공하는 것이다. 정책기반네트워킹 구축으로 국방정보통신망은 <표 4-1>과 같이 현재 네트워크 문제를 해결할 수 있을 것이다.

본 논문에서는 국방정보통신망에서 QoS 보장에 중점을 두고 정책기반네트워킹 구축에 관한 모델을 제시할 것이다.

4.2 QoS를 위한 정책기반네트워킹 구축 방안

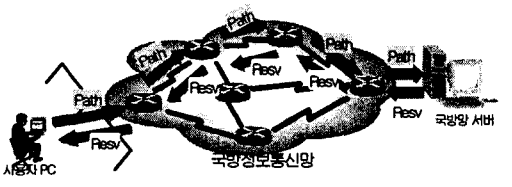
4.2.1 통합서비스를 이용한 정책기반네트워킹

<표 4-1> 정책기반네트워킹의 역할

현상 및 문제점	해결 방안
혼잡발생 시	정책에 의한 QoS 보장
네트워크 자원관리	정책에 의한 자원관리, 임무에 필수적인 응용프로그램 실행 보장
수동식 관리 방법	자동화된 관리
관리의 복잡성 및 이중화	정책, 규칙으로 관리하므로 간단함
네트워크 정책 일관성	일관된 정책적용
보안 통제	통합보안체계 구축 가능
데이터 분산	사용자 정보 등 중앙집중식 관리

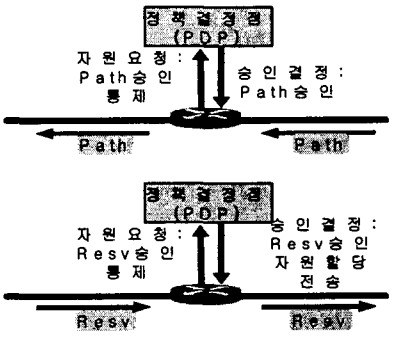
이 모델은 사용자와 서버 사이에 통합서비스의 신호 프로토콜인 RSVP(Resource Reservation Protocol)를 이용한 자원예약을 실시하여 사용자의 QoS를 보장하는 모델이다. <그림 4-1>과 같이 사용자는 자원예약 메시지를 서버에 보내고 서버는 사용자의 요구에 응답하게 된다. 이때 네트워크 라우터는 사용자의 요구사항(Path)을 검토하여 지원여부를 판단하여 그 결과(Resv)를 전송한다.

정책결정점과 정책실행점에서는 사용자의 요구를 기반으로 네트워크 자원, 사용자에게 적용된 정책을 기준하여 자원예약 사항의 승인여부를 결정한다.



<그림 4-1> 통합서비스 모델의 QoS 정책적용

네트워크 자원은 최초 부팅 시 접근통제목록(ACL: Access Control List)을 전송받아 트래픽을 분류하여 정책을 적용한다. <그림4-2>는 정책결정점과 정책실행점간 예약메시지 교환절차를 나타낸 것이다.



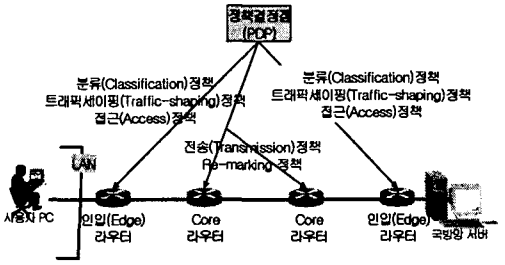
<그림 4-2> PDP와 PEP의 예약정보 교환

서버나 네트워크 자원(라우터)은 요구한 자원이 없을 경우나 사용자가 자원을 예약할 자격이 아닌 경우 등 에러메시지를 전송한다. 일단 예약된 자원은 상위 자원의 간섭이 없을 경우 할당된 자원을 계속 사용하는 것을 보장받는다.

정책실행점에서 RSVP 이벤트를 요청하는 프로토콜로 COPS나 LDAP, CORBA 등을 사용할 수 있다. 이 모델에서는 자원예약이 이루어지면 정해진 서비스를 보장받을 수 있지만 RSVP가 구현하기 복잡하고 대규모 시스템에서 적용하기 곤란하여 각 정책실행점간 자원예약에 소요되는 오버헤드(overhead)가 크다는 문제를 가지고 있다.

4.2.2 차등서비스를 이용한 정책기반네트워킹

차등서비스 모델은 통합서비스 모델과 달리 QoS를 위해 별도의 신호 프로토콜을 사용하지 않고 패킷 내에 포함시키는 묵시적인(implicit) 방법을 사용한다. 차등서비스 모델의 네트워크는 <그림 4-3>과 같은 방법으로 정책을 적용한다.



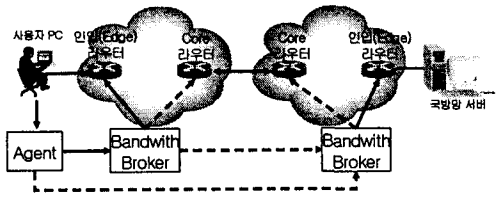
<그림 4-3> 차등서비스 모델의 QoS 정책적용

인입(edge) 라우터에서는 사용자 패킷정보를 보고 적용할 정책을 선정하여 DSCP에 마킹하며 코어(core) 라우터에서는 DSCP 코드표를 보고 독립적인 패킷전송을 실시한다. 만약 코어 라우터가 차등서비스를 지원하지 않는다면 패킷은 일반패킷과 동일하게 취급될 것이다. 차등서비스 모델은 인입 라우터가 트래픽 혼잡이 발생하는 지점이 되므로 인입 라우터의 역할을 분산시키면 네트워크 처리 속도를 향상 시킬 수 있을 것이다.

이 모델에서 <그림 4-4>와 같은 대역폭 중재자(BB: Bandwidth Brokers)는 네트워크 장비에 사용자의 정책을 설정하고 사용가능한 대역폭을 감시하는 역할을 한다. 또한 사용자의 서비스 요청을 장비가 이해할 수 있는 언어로 변환하고 현재 트래픽 사용량을 감시할 수 있다.

라우터는 각각의 링크로 대역폭 중재자의 가능한대역폭 용량에 대한 정보를 전송하고 EF 서비스의 처리용량을 할당할 수 있다.인입 라우터는 정책요청을 생성하고 대역폭 중재자에게 전송하는 역할을 한다. 대역폭 중재자는 요청된 내용을 검증하고

대역폭 사용량을 점검하여 해당 정책의 적용 여부를



<그림 4-4> 에이전트와 대역폭 중재자의 역할

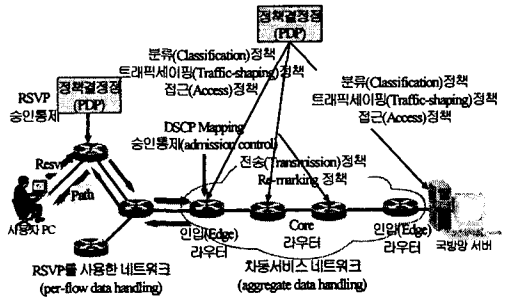
결정하여 사용자의 QoS를 보장한다.

차등서비스 모델은 통합서비스모델의 단점을 극복할 수 있지만 트래픽 용량의 예측, 다른 네트워크 자원의 사전 파악 등 자원관리의 복잡성의 문제점을 가지고 있다.

4.2.3 통합서비스와 차등서비스를 복합한 정책 기반네트워킹

이 모델은 통합서비스와 차등서비스의 단점을 극복하고 장점을 활용하기 위해 두 모델을 복합해서 운용하는 방법이다. RSVP는 지연이나 대역폭에 민감한 소리나 비디오 종류의 애플리케이션 QoS 보장을 위한 승인통제(admission control)를 위해 사용하고 차등서비스는 통합된 트래픽 흐름(flow)의 CoS(Class of Service) 제어를 위해 사용하는 것이다. <그림 4-5>는 복합모델에서 QoS를 보장하기 위한 정책의 적용방법으로 구현이 복잡하는 등 국방망에 적용하기에는 부적합하다고 할 수 있다.

본 논문에서는 현재 국방인트라넷에 구축된 LDAP 서버를 활용할 수 있는 차등서비스 모델을 제안하고자 한다. 이 모델은 구현이 비교적 용이하며 각 정책실행점에서 독립적으로 패킷을 통제할 수 있으므로 각 군별 독립적으로 QoS를 적용할 수 있다.



<그림 4-5> 복합모델의 QoS 정책적용

국방정보통신망 특성상 전체 네트워크를 동시에 정책기반네트워크로 구축하기는 어려우므로 정책실행점간 독립성을 보장하여 점진적으로 차등서비스망 네트워크로 변환시킬 수 있는 장점도 있다.

4.3 차등서비스 모델을 적용한 국방정보통신망에서의 QoS 보장 모델

이 절에서는 QoS를 위한 정책기반네트워킹을 구축할 수 있도록 LDAP 스키마를 정의하고 구현 모델을 제시할 것이다.

4.3.1 표준 QoS 정책 스키마 정의

가. QoS 애트리뷰트

차별화된 서비스를 제공하기 위해 차등서비스를 적용한 QoS 클래스는 <표 4-2>와 같이 정의할 수 있다. PHB에 따라 EF 및 AF의 1개 클래스를 사용하고 3종류의 폐기우선순위를 고려하였으며 현재의 최선형서비스(default)는 정책이 적용되지 않은 패킷이나 서비스 품질보장이 필요 없는 데이터 패킷에 적용할 수 있을 것이다.

관리도구에 의해 각 IP 패킷별로 DSCP 코드표가

<표 4-2> QoS 레벨과 DSCP 코드표

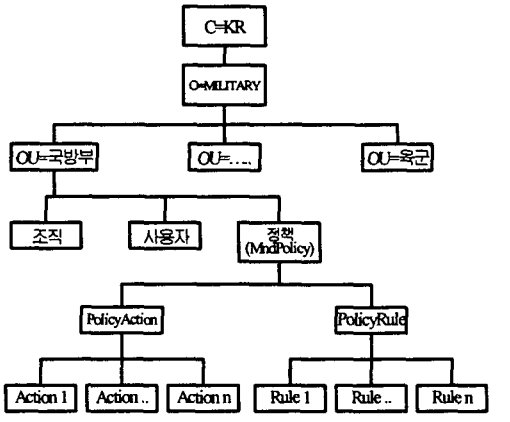
QoS 레벨		대역폭 (%)	우선 순위	DSCP 코드표
EF Class		50	0	10111000
AF	A Class	30	1	00101000
	B Class		2	00110000
	C Class		3	00111000
Default DSCP		20	4	00000000

부여되면 실제 망에서는 DSCP 코드에 따라 필요한 QoS를 지원해 주어야 한다. 네트워크의 라우터는 차등서비스가 지원되어야 한다. 이때 관리도구는 트래픽 모니터링 도구(대역폭 중재자 등)를 이용해 사용자가 해당 서비스를 지원받고 있는지를 감시하는 등 네트워크 상태를 지속적으로 관리자에게 보고할 수 있어야 한다.

나. MndPolicy 객체 클래스

본 논문에서 정의하는 QoS 정책객체는 IBM의 QoS 모델과 IETF와 DMTF의 정책에 관련한 표준화 모델을 참고로 하였다. 정책객체를 현재 국방표준 LDAP 스키마에 적용하면 <그림 4-6>과 같은 스키마가 될 것이다[8].

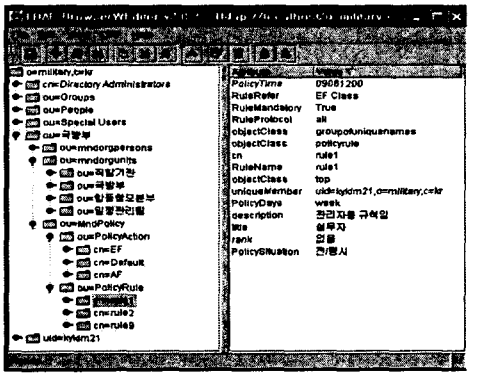
정책스키마는 PolicyAction과 PolicyRule 2개의 하위 클래스를 가진 스키마로 관리도구는 정책에 따라 PolicyRule을 생성하여 LDAP 서버에 저장한다. 사용자가 서버에 최초 사용자 등록을 할 때 등록되는 사용자의 정보에 따라 정책관리도구는 정책에 따라 사용자를 적절한 정책으로 분류하여 사용자 정책에이전트로 전송한다. 이후 사용자 로그인 시 관리도구는 해당 사용자의 정책객체를 검색하여 알맞은 정책을 적용, 차별화된 서비스를 제공하게 되는 것이다.



<그림 4-6> QoS를 위한 국방망 LDAP 스키마

4.3.2 LDAP 디렉토리 서버 구현

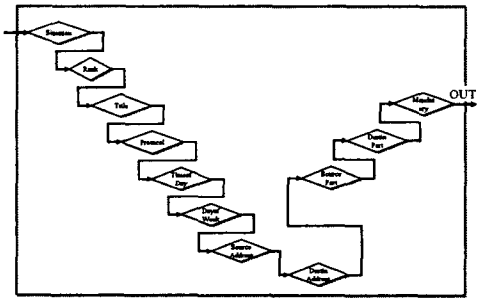
본 논문에서 구현한 LDAP 서버는 'Sun™ ONE Directory Server 5.1'로 윈도우즈 환경에서 사용하였다. LDAP 브라우저는 JAVA SDK를 이용한 공개용 'LDAP Browser/Editor 2.8.2'를 사용하였다.



<그림 4-7> QoS 스키마를 적용한 LDAP 서버

<그림 4-7>은 MndPolicy객체를 적용한 LDAP 서버를 구현한 것이다.

국방망에서 네트워크 정책은 <표 4-3>과 같이 사용자, 애플리케이션, 사용시간별로 부여할 수 있고 사용자는 다시 직책, 계급, 부대 등으로 분류할 수 있다. 애플리케이션은 전자결재, 전자우편, HTTP 등 프로토콜별로 사용시간은 전시, 평시, 훈련시, 평시는 일과를 기준으로 일과 내/외/야간으로 구분하여 정책규칙을 각각 생성할 수 있을 것이다. 정책관리도구는 <그림 4-8>과 같은 처리 알고리즘을 사용하여 입력된 정책에 따라 자동적으로 정책규칙(PolicyRule)을 생성할 수 있을 것이다.



<그림 4-8> 정책처리 알고리즘

정책생성 시 정책을 적용하는 네트워크 장비 성능은 접근통제 리스트와 필터의 수, 즉, 처리 절차의 복잡성에 의해 영향을 받을 수 있으므로 처리 절차를 단순화하는 것이 정책의 신속한 적용에 필요한 요소이다. 따라서 알고리즘을 단순화할 수 있도록 하는 것이 좋다.

해당 서비스 등급으로 분류된 정보는 LDAP 서버에 기록되며 사용자가 정책콘솔을 통해 서버에 로그인 시 사용자 정보를 기반으로 하여 LDAP 서버로부터 규칙을 검색, 정책에 명시된 서비스(PolicyAction)를 제공해 주어야 한다.

4.3.3 정책분배 프로토콜로서의 LDAP 고찰

정책분배 프로토콜은 SNMP, COPS 등 다양한 프로토콜이 있으며 구현하는 시스템에 적합한 프로토콜을 선정하면 된다. 본 논문에서는 정책전송 프로토콜로 LDAP을 사용하였다. LDAP은 서버에 대한 접근, 검색에 최적화된 프로토콜로 표준화 단체에서 디렉토리 접근 프로토콜로 표준화가 진행 중이며 많은 업체에서 지원하고 있다. 그러나 단점으로 시스템이 빈번한 트랜잭션을 수행하는 경우 처리시간이 지연되는 경우도 있다. 또한 LDAP은 디렉토리의 빈번한 변경이 있는 경우 그 변경 사항을 정책에이전트에게 통보하는 기능을 효과적으로 지원하지 않는다. 따라서 정책에이전트는 서버의 변경 사항을 알기 위해서 빈번한 폴링(polling)을 수행하게 되고 폴링은 불필요한 오버헤드를 발생시켜 시스템 성능을 저하시키는 요인이 될 수 있다. <표 4-3>은 LDAP과 다른 프로토콜을 비교한 것이다. 국방망은 사용자 변경의 횟수, 즉, 트랜잭션 발생이 적고, 개방된 망이 아니라 폐쇄된 망이므로 통합된 관리가 용이하다. 또한 중앙저장소를 지원하는 등 다른 프로토콜보다 효과적으로 사용될 수 있으므로 LDIF를 사용하는 LDAP을 정책분배 표준 프로토콜로 사용하였다.

본 논문에서는 정책검색과 적용의 오버헤드를 최소화하기 위해 정책객체를 최소화 하였고, LDAP 서버의 스키마도 기존 사용자 스키마를 반영하면서 국방망 특성을 고려하여 새로운 스키마를 정의하였다. 또한 국방망 특성상 최초 정책이 설정되고 사용자 등록이 되면 정책변경이나 사용자 정보 변경, 신규 추가 등의 트랜잭션이 빈번하지 않으므로 해당 사용자 정책은 사용자 PC의 정책에이전트에 저

장하는 방법을 제안하였다. 이 방안은 중앙의 정책 서버에서 정책을 검색하고 전송하는데 소요되는 시간을 줄일 수 있으므로 신속한 정책적용이 될 수 있는 것이다.

<표 4-3> 정책분배 프로토콜 비교

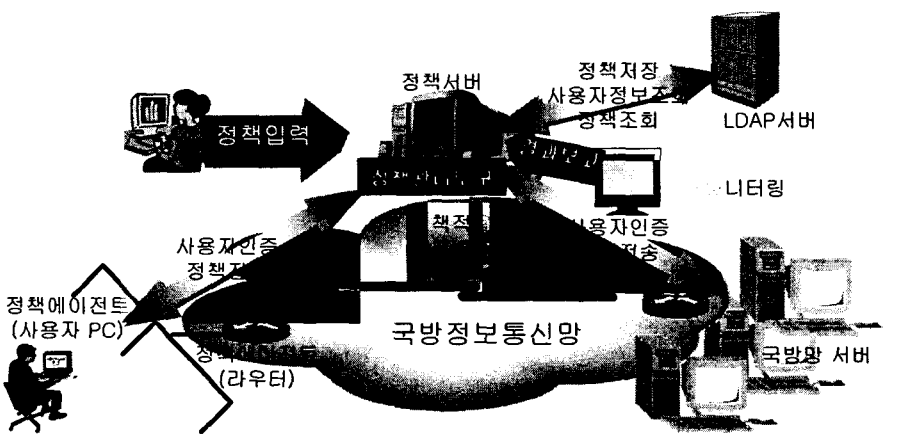
범 주	관리 프레임워크	스크립트	LDAP	COPS	SNMP	웹 서비
콘솔 복잡성	높음	높음	낮음	낮음	낮음	높음
에이전트 복잡성	낮음	없음	중간	중간	중간	낮음
에러 통제	높음	저조	지원	높음	높음	높음
지연	낮음	낮음	중간	낮음	낮음	낮음
중앙 저장소	가능	없음	있음	없음	없음	없음
표준	소유권	소유권	표준	표준	표준	아님
성숙도	다양함	높음	높음	낮음	높음	높음

4.3.3 정책기반네트워킹 구현 모델

<그림 4-9>는 본 논문에서 제안하는 국방망에서의 정책기반네트워킹 구현 모델이다. LDAP 서버는 기존에 국방인트라넷 인증시스템 구축 시 사용된 시스템을 사용하고 별도의 정책서버를 설치하며 네트워크 라우터는 차등서비스를 지원하는 라우터이어야 한다. 또한 정책에이전트를 사용자 PC, 네트워크 장비, 국방망 서버에 설치한다. LDAP 서버는 국방망(국방부)에 주 서버를 각 군별 사본을 만들어서 일정한 주기로 동기화 작업을 실시하는 모델을 제안한다.

정책기반모델에서 정책관리도구로 적정 QoS를 위한 정책기반네트워킹의 구현 절차는 다음과 같다.

우선 정책관리도구는 관리자에 의해 입력된 정책에 따라 정책규칙(PolicyRule)과 정책행동(PolicyAction)을 생성하여 LDAP 서버에 저장한다.



<그림 4-9> 국방망에서의 정책기반네트워킹 구현 모델

(1) 사용자는 개인 PC를 이용하여 시스템(정책에이전트)에 로그온하여 사용자 등록절차를 실시한다. 관리자는 등록된 사용자의 정보를 확인하여 인증을 실시한다.

(2) 등록된 사용자는 사용자 PC의 정책에이전트를 통해 시스템에 로그온을 실시한다. 정책관리도구는 LDAP 서버로 사용자 정보를 조회하고 인증을 실시한다. 이때 사용자의 모든 정책관련 정보를 사용자 정책에이전트로 전송하여 저장시킨다.

(3) 정책에이전트(사용자 PC)는 해당 사용자의 QoS 정책을 검색하여 사용자가 이용하려는 애플리케이션의 형태에 따라 정책을 적용, DSCP 코드표에 표시한다. 정책관리도구는 정책이 변경될 경우 해당 사용자 정책에이전트로 통보하여 변경된 사항을 다시 기록한다.

(4) 중앙의 정책관리도구는 사용자 에이전트로부터 획득한 사용자 정보를 네트워크 인입 라우터의 정책에이전트로 전송하며 DSCP 코드표에 따라 해당 QoS를 보장한다.

(5) 인입 라우터 정책에이전트는 전송된 정보에 따라 가입자가 해당 서비스를 받고 있는지에 대해 검사(traffic conditioning)를 실시한다.

(6) 네트워크에서 패킷은 지속적인 성능 모니터링을 통해 연결종료 요청이나 상위 패킷에 의한 중단이 아닌 경우 해당 QoS를 보장 받는다.

4.4 국방정보통신망에서 정책기반 네트워킹 구축 절차

현재 상용망에서도 정책기반네트워킹이 연구되고 있고 표준화가 진행 중이지만 표준화 미비 등의 이유로 완전한 정책기반네트워킹을 구현하기는 어려운 시점이므로 국방정보통신망에 정책기반네트워킹을 구축하기 위해서는 단계적인 구축방법이 적용되어야 할 것이다.

<표 4-4> 정책의 적용 대상 분류

정책	세부 분류
상황	전시, 평시, 훈련시, 긴급(CERT 보고)
사용자	계급, 직책, 부대
시간	일과 시간, 일과 이후, 평일, 공휴일
애플리케이션	일반적인 웹 서비스,
	임무에 필수적인 차등서비스(지휘소자동화체계, 군수/탄약관리 시스템, 각 군 전술체계 등)
	지연(음성)에 민감한 서비스
	동영상(원격 교육) 서비스

* CERT: Computer Emergency Response Team

4.4.1 1단계: 정책기반네트워킹 개념 연구

국방정보통신망에 정책기반네트워킹을 구축하기 위해 가장 먼저 해야 할 일은 어떤 목적을 가지고 어떤 방식으로 정책기반네트워킹을 구축할 것인지에 대한 종합계획을 수립하는 것이다. 이 단계에서는 다음과 같은 사항들을 고려해야한다.

- 정책기반네트워킹 적용 애플리케이션 선정
- 적용할 도메인 종류, 도메인 규모 설정
- 다른 관리 시스템과의 통합 방법
- 정책결정점에 관한 정의 및 위치
- 비 정책기반 장비에 대한 처리
- 정책의 세분화 범위
- 정보시스템의 관리자 및 시스템 설치 장소
- 정책의 유효성에 관한 결정 방법 선정

4.4.2 2단계: 네트워크 정책수립 및 표준화

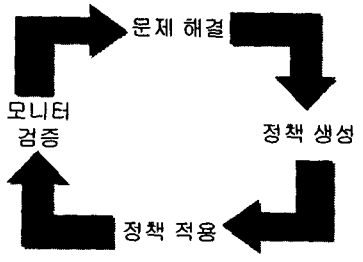
네트워크 분석을 토대로 트래픽 종류별 어떤

정책을 적용할 것인지에 대한 정책이 수립되어야한다. <표 4-4>와 같이 애플리케이션의 종류, 사용자에 따른 정책적용 방안, 사용시간에 따른 네트워크 처리에 관한 정책이 수립되어야 할 것이다. 또한 수립된 정책에 따라 네트워크에서 어떻게 트래픽을 처리 할 것인지에 관한 모델을 선정해야 할 것이다. 또한 대역폭이나 지연, 에러에 민감한 애플리케이션을 식별해서 정책을 적용할 수 있도록 해야 할 것이다.

다음으로 인터넷 표준을 기초로 하여 국방표준 LDAP 스키마를 작성해야 할 것이다. 현재의 국방정보통신망은 각 군별 독립적으로 체계를 개발, 운용하고 있지만 정책기반네트워킹을 구축하기 위해서는 국방표준 LDAP 스키마가 확정되어야 할 것이다.

4.4.3 3단계: 시범체계 선정 및 구축

정책기반네트워킹을 시범적으로 적용할 망을 선별해서 시험 적용하는 단계이다. 먼저 국방인트라넷을 중심으로 정책기반네트워킹을 구현하는 것이 바람직할 것이다. 국방인트라넷은 현재 LDAP 서버가 운용 중이고 통합인트라넷을 구축할 계획을 수립, 추진 중이므로 먼저 국방인트라넷부터 시험 운용하는 것을 제안한다. <그림 4-10>과 같은 순환 절차를 거쳐 정책기반네트워킹을 확대 적용해야 할 것이다. 국방인트라넷의 애플리케이션 중에서도 TCP/IP 기반의 애플리케이션인 사무자동화, 인트라넷, 군수, 인사관리 등의 네트워크를 대상으로 적용해야 할 것이다.



<그림 4-10> 정책적용의 순환절차

4.4.4 4단계: 전군 통합 정책기반네트워킹 구축

각 군과 국방인트라넷망의 통합으로 TCP/IP 기반의 각 군 애플리케이션인 사무자동화, 인트라넷, 군수, 인사관리 등의 네트워크를 통합, 운영하는 단계이다. 각 군별로 운영 중인 인트라넷 망과 자원관리 시스템을 통합하기 위해서는 국방표준 LDAP 스키마를 적용해야 할 것이다. 통합된 네트워크에서 LDAP 서버는 국방망에 주 서버를 두고 각 군은 보조 서버를 두어 운영하며 주 서버와 보조 서버는 일정 기간이나 이벤트 발생 등 특정 조건을 설정하여 동기화 시키는 방법을 사용, 최신의 정보를 공유해야 할 것이다.

4.4.5 5단계: 국방정보통신망 통합에 따른 정책기반네트워킹 구축

군에서 운용 중인 전체 네트워크를 통합하는 단계로 전술체계, CPAS(Command Post Automation System)체계, 각 망관리체계, 통합인증체계 등을 하나의 정책기반네트워킹으로 구축하는 것이다. 이 단계에서는 전화교환망, 위성망, M/W망, 각 군 전술C4I체계망, 화상회의 시스템 등이 하나의 LDAP 서버를 이용하여 정책기반네트워킹을 구축하는 것으로 필요하다면 상용망과의 연동도 고려해야 할

것이다. 이 시기는 국방정보통신망이 하나의 망처럼 완성되는 단계가 될 것이다.

5. 결 론

본 논문에서는 자동화된 네트워크 통합관리 및 사용자 정보 등 데이터 통합 관리, 효율적인 QoS 보장을 위해 정책기반네트워킹을 적용한 국방정보통신망 구축의 필요성과 단계적인 구축방안에 관해 제안하였다. 우리 군이 저비용 고효율의 국방정보체계 구축을 위해서는 정책기반네트워킹 도입이 필수적이라고 생각한다.

미래전은 정보전, 네트워크 전쟁이 될 것이다. 미래전에서 승리하기 위해서는 네트워크를 통해 중요정보를 실시간으로 의사 결정권자에게 보고하고 그 처리 내용을 신속, 정확하게 실무부대로 하달해야 할 것이다. 이때 네트워크에서 적보다 우위의 네트워크를 구축해야 할 것이다. 수많은 정보로 인해 네트워크가 마비되어 중요한 정보가 유실되거나 지연되는 일이 없도록 하기 위해서는 정책기반네트워킹을 통한 차별적인 서비스 제공, 즉 트래픽 폭주나 혼잡 시 중요한 정보는 다른 정보보다 우선권을 가지고 지연 없이 신속히 처리되도록 하는 네트워크를 구축해야 할 것이다.

정책기반네트워크는 통합인증체계 구축, 망관리 통합, VoIP 통합 망 구축 등 다른 분야에도 활용할 수 있는 등 미래의 통합 국방정보통신망 구축에 핵심기술이 될 것으로 판단되므로 적극적인 도입 전략이 필요하다.

참 고 문 헌

[1] Dave Kosiur, Understanding Policy-Based Networking, Wiley, 2001.

[2] Mark Wilcox, Implementing LDAP, Wrox, 2000.

[3] Uyless Black, MPLS and Label Switching Networks, Prentice Hall Series, 2001.

[4] Verna, Policy-Based Networking, New Riders, 2001.

[5] 이태공, 국방 정보 기반구조에 필요한 정보유통량 분석, 국방대학교, 2000.

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

[7] 포스데이터, "WDM발전방향 및 응용전망, "제2회 국방정보화기술심포지엄 신기술동향, 2001.

[8] 쌍용정보통신, "LDAP기반의 국방 통합 인트라넷 구축 전략," 제2회 국방정보화기술심포지엄 신기술동향, 2001.

[9] 국방전산소, 국방정보화 기획문서, 국방전산소, 2001.

[10] A. Westerinen외 9명, "Terminology for Policy-Based Management," RFC 3198, 2001.

[11] B. More외 3인, "Policy Core Information Model - Version 1 Specification," RFC 3060, 2001.

[12] G. Good, "The LDAP Data Interchange Format (LDIF)," RFC 2849, 2000.

[13] T. Howes외 2인, "Lightweight Directory Access Protocol (v3)," RFC 2251, 1997.

[14] Y. Snir외 4인, "Policy QoS Information Model," draft-ietf-policy-qos-info-model-04.txt, 2001.

[15] Distrbuted Managemant Task Force, CIM Policy Model(White Paper), 2002.

[16] ENTERASYS Networks, Directory Enabled Networking-A Technology Guide(White Paper), 2002.