Journal of Korea Multimedia Society Vol. 7, No. 5, May 2004(pp. 721-736)

이동 IP 환경에서 인터넷 차별화 서비스 제공을 위한 정책기반 네트워크 관리 구조

강승완[†], 김태경[††], 유상조[†††]

요 약

휴대용 컴퓨터나 PDA등의 증가로 이동성에 대한 사용자의 요구가 점점 늘어나고 있으나 현재의 프로토콜은 자신의 IP 주소를 변경하지 않고 다른 네트워크로 이동할 경우 호스트의 새로운 위치로 IP 패킷을 전달할 수 없다. 이러한 문제를 해결하기 위해 IETF에서는 이동 IP라는 프로토콜을 제안하였다. 오늘날 인터넷은 최선형 서비스라 불리는 서비스를 제공하고 있다. 그러나 인터넷이 상업화됨에 따라 서비스 요구가 다양해지고 있으며 동시에 QoS에 대한 요구가 급증하고 있다. 정책기반 네트워크 관리는 IP 망을 대상으로 관리의 복잡성, QoS 및 보안에 있어서의 문제점을 해결할 수 있는 방안으로 제시하고 있다. 따라서 본 논문은 이동 IP 환경에서 인터넷 차별화 서비스를 제공하는 정책기반 네트워크 관리에 대한 네트워크 토폴로지 구성을 살펴보고 그들의 동작 절차와 구조를 제안하고, 정책 시나리오를 표현하기 위해 정책 클래스로 정책들을 나누어서 본 논문에서 제안하는 정책 언어를 사용하여 제시하였다. 또한 여러 가지 제어와 네트워크 동작 절차를 실행하기 위해 이동 IP 환경에서 인터넷 차별화 서비스를 제공하는 정책기반 네트워크 관리를 구현하였다.

Architecture of Policy-Based Network Management for Providing Internet Differentiated Service on Mobile IP Environment

Seung-Wan Kang[†], Tae-Kyung Kim[††], Sang-Jo Yoo[†††]

ABSTRACT

Because of increasing the notebook computer and PDA, users' requirement with respect to mobility is growing more and more. However, current IP protocol is not changed IP address and can not deliver IP packets on new location of host in case moving another network. To solve this problem, the IETF has proposed mobile IP. Today users want to be provided suitable QoS in the internet since demand of services is variety. The policy-based network management is method which can solve various problems of QoS, security, and complication of management in IP networks. This paper presents the network topology constitution, operation procedure and architecture of policy-based network management for providing internet DiffServ on mobile IP environment. In this paper we propose policy classes of policy-based DiffServ network management on mobile environment and create policy scenarios using the proposed policy description language to represent the policy classes. Finally, we implemented a policy-based DiffServ network management system on mobile IP environment.

Key words: mobile IP(이동 IP), policy based networks(정책기반네트워크), QoS(서비스 품질)

※ 교신저자(Corresponding Author) : 유상조, 주소 : 인천광역시 남구 용현동(402-751), 전화 : 032)860-8304, FAX : 032)865-0480, E-mail : sjyoo@inha.ac.kr
접수일 : 2003년 10월 2일, 완료일 : 2003년 11월 24일
[†] 정회원, 인하대학교 정보통신대학원
(E-mail : wanis@hanmir.com)
[††] 정회원, 인하대학교 정보통신대학원
(E-mail : sh0408@hanmir.com)
[†††] 인하대학교 정보통신대학원 조교수
※ 본 논문은 한국과학재단 지역대학우수과학자지원연구(R05-2002-00125-0) 지원으로 수행되었음.

1. 서 론

오늘날 가정에서 혹은 회사에서 통신을 위해 인터넷을 사용하게 되면서 점점 더 많은 서비스들이 IP망에 제공될 수 있는 형태로 변경되고 있다. 또한 무선 통신에 새로운 인터넷 사용기술을 도입되면서 PDA 또는 무선랜 등 휴대가 간편한 노트북등에 연결하여 사용하는 이동 통신 사용자가 급증하고 있다. 고정된 지역에서 수행하던 통신이 이동 후 혹은 이동 중 통신을 원하는 사용자들이 늘어감에 따라 효율적이고 신뢰성 있게 데이터를 전송할 수 있는 요소 기술이 요구되고 있다. 따라서 유선망에 연결할 수 있는 무선 통신 장비를 가진 사용자들을 언제 어디에서나 투명하게 통신망에 접근할 수 있는 환경이 요구되며 현재의 인터넷에 접속하기 위해 필요한 인터넷 프로토콜은 호스트가 인터넷을 사용하기 위해서 접속되는 위치를 고정적으로 지정한다. 호스트가 IP 주소를 변경하지 않고 다른 서브넷으로 이동하면 호스트는 새로운 서브넷으로의 접속이 불가능할 뿐만 아니라 새로운 IP 주소 또는 라우팅 테이블이 없는 한 데이터 송수신이 불가능하다. 이러한 현재의 IP에서 단말기에 이동성을 제공하기 위해 IETF(Internet Engineering Task Force)에서는 이동 IP(mobile IP)[1]를 제안하였다.

이동 IP란 노드가 인터넷상에서 임의의 위치에 접속하더라도 자신의 고유주소로 전송되는 데이터그램을 수신할 수 있도록 IP 프로토콜을 확장한 것이다. 이동 IP에서는 도메인 이름과 주소와의 관계가 시간에 따라 변하기 때문에 IP층에서 노드의 이동에 대한 제어를 제공해 주어야 한다. 이러한 이동성 제공을 위해 각 노드들은 두 개의 인터넷 주소를 필요로 하게 된다. 하나는 홈 주소(home address)이고 다른 하나는 COA(Care-of Address)이다. 하나의 이동 노드(MN: Mobile Node)가 새로운 서브넷으로 이동했을 때, 외부 에이전트(FA: Foreign Agent)로부터 COA를 제공받는다. 그리고 MN은 새로 받은 COA를 홈 에이전트(HA: Home Agent)에 등록한다. 이를 통해 이후에 그 MN으로 오는 모든 데이터그램들은 HA에 의해 수집되고, HA는 이 데이터그램을 COA를 사용하여 FA로 캡슐화(encapsulation)을 통해 전달하게 된다. 만약 COA가 FA로 저장되어 있는 경우 이 데이터그램들은 FA에 의해서 역캡슐화(decapsulation)되고 최종적으로 MN으로 보내지게 된다.

오늘날의 인터넷은 최선형 서비스(best effort)라 불리는 단일 서비스만을 제공한다. 그러나 인터넷이 상업화됨에 따라 사용자의 서비스에 대한 요구가 다양해지는 동시에 서비스 품질(QoS: Quality of Service)에 대한 수요가 급증하고 있다[2]. 특히 멀티미디어 서비스가 보편화됨에 따라 실시간 처리가 필요하며 높은 대역폭을 요구하는 서비스가 다양해짐에 따라 인터넷에서 사용자 응용의 특성에 맞는 QoS를 제공하기를 원하고 있다. 인터넷 QoS는 네트워크를 통해 전달되는 패킷 플로우의 성능을 나타내는 것으로서 서비스의 가용성(availability), 지연 변이(delay variation), 처리율(throughput), 패킷 손실율(packet loss rate)등 몇 가지 성능 인자(metrics)로 표현된다. QoS의 주 목적은 사용자 트래픽에 대하여 종단간 QoS를 제공하는 것이다. 현재 IETF에서는 인터넷상에서 QoS를 보장하기 위한 방법들에 대한 표준화를 정의하였다. 그 중에서 가장 대표적인 것은 통합서비스(IntServ: Integrated Service)[3]와 차별화 서비스(DiffServ: Differentiated Service)[4]가 있다.

IntServ는 특정 사용자의 패킷 즉, 플로우(flow)에 특별한 QoS를 제공하기 위해서는 라우터에서 자원 예약의 반드시 필요하며 이를 위해 라우터에서 각 플로우별 상태를 유지해야 한다는 것이다. 그러나 플로우 수가 증가하면 플로우 상태 정보 양도 증가하므로, 상태 정보 저장을 위한 방대한 저장 공간이 필요하며 이를 관리하기 위한 처리 부하가 증가하게 된다. 따라서 이와 같은 구조는 확장성에 심각한 문제를 야기한다. 이러한 확장상의 문제를 해결하기 IETF는 DiffServ 모델을 제안하였다. DiffServ는 IP 네트워크에서 다양한 플로우가 몇 개의 서비스 클래스로 분류하여 중간 라우터에서는 이러한 서비스를 클래스별로 처리한다. DiffServ는 IntServ같이 모든 라우터에 대하여 플로우 상태 관리 및 시그널링(signaling)을 요구하지 않는다. DiffServ는 IP 헤더(header)의 TOS(Type of Service) 필드 중 6비트를 QoS를 정하는 부분으로 바꿨다. 이러한 방법은 모든 트래픽을 요구하는 QoS에 따라 나누고 이에 따라 트래픽을 집합화(aggregation)함으로써 스케쥴링 문제를 해결하였다. IPv4의 헤더에는 TOS 필드가 정의되어 있으며, 애플리케이션은 작은 지연, 높은 처리율, 낮은 손실율 등을 나타내기 위해 TOS 필드

를 사용하고 있다. 그러나 기존 라우터에서는 이와 같은 애플리케이션의 요구를 거의 무시하고 모든 패킷을 동일하게 처리하였다. Diffserv는 TOS 필드의 이름을 DS(Differentiated Service) 필드로 재명명하여 이를 다시 정의하고, PHB(Per-Hop Behavior)라 불리는 기본적인 패킷 전송 방법을 정의하고 있다. 결국 DiffServ 패킷의 DS 필드를 다르게 표시하고, 이 표시에 따라 패킷을 처리함으로써 몇 개의 차별화된 서비스 클래스를 생성하는 것으로서 기본적으로 상대적인 우선순위 기법이다.

그러나 이러한 유선망에서의 디자인된 모델은 이동 IP 네트워크 환경에서 부적합하다[5]. 이동 IP는 기존의 인터넷 서비스 형태인 최선형 서비스를 기반으로 제안되었기 때문에 사용자들이 요구하고 있는 음성, 화상이 지원되는 멀티미디어 응용과 원격 회의와 같이 사용자들 간에 실시간으로 상호 작용할 수 있는 환경에서 부적합하고 단순히 이동성을 지원하는 것만을 목표로 제안되었기 때문에 새로운 네트워크의 연결만을 보장할 뿐 데이터 대역폭이나 지연시간, 안정성 등과 같은 연결 후의 활동에 대한 보장을 하지 않는다. 또한 호스트의 이동성으로 인한 핸드오프 문제, IP 터널링 문제, 예약자원 낭비 등을 고려한 동적인 QoS 보장에 대한 문제가 있다. 현재 이동성이 있는 환경에서의 QoS 보장에 대한 연구는 여러 연구 기관과 대학에서 활발히 진행되고 있다.

이러한 IP 기반 네트워크의 확장은 네트워크 운용자로 하여금 다양한 종류의 서로 다른 트래픽 특성을 갖는 서비스의 효율적인 수용이라는 문제를 심각하게 고려하게 하고 있다. 기존의 IP 네트워크는 사용자들에게 차별화 된 서비스를 제공하지 못하고 있으며 네트워크를 이용한 서비스 제공자에게도 다양한 종류의 서비스 제공에 제한을 두고 있다. 또한 최근의 네트워크는 네트워크의 복잡화, 응용서비스의 다양화, QoS 제공 요구의 증가 등으로 인해 네트워크의 효율적 설계, 구축, 관리, 진화에 있어 해결해야 할 많은 어려운 문제들을 안고 있다. 또한 통신망을 관리하는 측면에서 통신사업자의 주요 운영정책과 사용자의 트래픽 변화에 따라 통신망에서 이를 효율적으로 관리하는 방안에 대한 연구가 요구된다. 또한 통신사업자들의 네트워크 환경은 여러 업체의 다양한 장비가 존재하고 모든 서비스들을 하나의 통합망(converged network)에서 제공하는 구조로 변하고 있다. 최근의 추세는 특정한 정책(policy)에 기반을 두어 이를 통신망 전체에 확산하여 통신망을 관리하는 기법이 고려되고 있다. IETF에서는 이를 위해 정책기반 네트워크 관리(PBNM: Policy-based Network Management)[6]기법을 제안하였다. 정책기반 네트워크 관리는 비즈니스 및 서비스 차원의 정책에 의해 정의하여 운용자는 손쉽게 통신망을 관리하고 네트워크 구성을 자동적으로 일관성 있게 유지 및 변경 시킬 수 있는 기법이다.

정책기반 네트워크 관리는 네트워크 운영자에게 자동화된 정책의 수립, 전달, 실행을 지원하는 망으로 현재 인터넷 QoS 및 보안과 관련하여 그 중요성이 커지고 있는 분야이다. 정책기반 네트워크 구축의 근본적인 목적이 '정보의 올바른 전송과 사용'에 있다면 그 중에 전송 부분의 품질에 크게 기여할 수 있는 개념이 바로 QoS이다. 정책기반 네트워크를 구축할 때 QoS를 도입하는 의도는 이제 적어도 특정 애플리케이션만큼은 보장 받고 싶은 서비스 품질이 있다는 것이다. 정책기반 네트워크 관리 기법은 새로운 비즈니스 모델을 세우면 이를 자동으로 네트워크에 반영시켜 줄 수 있도록 하는 방법으로써 제시된 기술이다. 새로운 요구사항이 발생하면 그에 따라 알맞은 정책을 세우고 정책을 실행할 수 있도록 도입된 장비인 정책 결정 점(PDP: Policy Decision Point)과 정책 실행 점(PEP: Policy Enforcement Point)를 통해 네트워크 인프라에 알맞은 정책을 적용, 관리하여 요구 사항이 성취될 수 있게 하는 것이다. 사업자는 새로운 요구사항이 생길 때마다 이를 반영하는 정책을 세우고 정책 관리 툴(policy management tool)을 이용하여 정해진 정책을 적용함으로써 그 정책에 따라 네트워크가 관리되도록 할 수 있는 것이다. 그러므로 정책기반 네트워크 관리를 통해 네트워크를 구성하는 각 네트워크 구성요소들의 정책들을 변화시킴으로써 네트워크 관리의 유연성을 제공할 수 있을 뿐만 아니라 적은 비용으로 대규모 네트워크를 관리할 수 있다. 정책기반 네트워크 관리는 현재의 네트워크에서 장비 설정에 관련된 관리자의 업무를 보다 간단하게 할 수 있으며, 임무에 필수적인 응용프로그램의 수행 능력을 예측할 수 있도록 하는 방법이다. 또한 중앙의 정책저장소(policy repository)를 이용하여 중앙 집중식 관리로 일관성 있는 정책의 적용과 트래픽의 중요도에 의한 차별적인 처리를 가능하게

한다.

본 논문에서는 이동 IP 환경에서 인터넷 DiffServ를 제공하기 위해 정책기반 네트워크를 적용함으로써 이동 IP 환경에서 DiffServ의 구성과 동작 절차 그리고 접근 제어, 이동 IP 동작, QoS 제어, 네트워크 모니터링 등의 정책 클래스들을 제안하고 이 클래스들을 바탕으로 여러 가지 시나리오를 바탕으로 전체적인 프레임워크을 작성하여 효과적으로 이동 IP 환경에서 인터넷 DiffServ 정책기반 네트워크를 관리할 수 있는 방안을 제시한다. 또한 실험실 규모에서 실제 이동 IP 환경에서의 인터넷 차별화 서비스를 제공하기 위한 정책기반 네트워크 구축 및 정책서버(policy server)를 개발하였다.

본 논문의 구조는 다음과 같다. 2장에서는 이동 IP 환경에서 DiffServ를 제공하기 위한 정책기반 네트워크를 소개하고 이들 동작 절차를 살펴본다. 3장에서는 본 논문에서 제안한 이동 IP 환경에서 정책기반 DiffServ 네트워크 관리 구조를 설명하고 정책 서버에서의 정책 클래스를 제안하고 이를 바탕으로 정책 시나리오를 개발하였다. 4장에서는 이동 차별화 서비스 네트워크에서 정책기반 네트워크 관리를 구현하였다. 마지막으로 5장에서는 본 논문에 대한 결론을 맺는다.

2. 이동 IP 환경에서 정책기반 차별화 서비스 네트워크

2.1 이동 IP 환경에서 정책기반 차별화 서비스 네트워크 구성

본 논문에서 제시한 정책기반 이동 차별화 서비스 네트워크 구성도는 그림 1과 같다. 백본망은 유선망과 똑같이 DiffServ를 지원하는 망으로써 모든 복잡한 기능, 상태 관리, 정책의 질의 및 수행 등에 관련된 상황을 담당하고 있다. FNER(Foreign Network's Edge Router), HNER(Home Network's Edge Router)와 CNER(Correspondent Network's Edge Router)는 DiffServ의 에지 라우터이다. 따라서 에지 라우터는 모든 패킷 흐름에 대한 트래픽 분류(classification)와 조절(conditioning) 기능을 수행한다. 패킷 조절 기능에는 트래픽 분류에 따른 패킷의 표시(mark), 흐름의 측정(meter), 그리고 쉐이핑(shaping)과 감시 기능(policing)을 포함한다. 또한

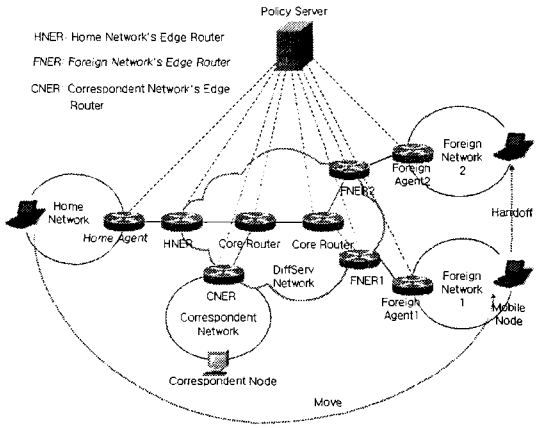

그림 1. 이동 IP 환경에서 정책기반 차별화 서비스 네트워크 구성

코어 라우터는 에지 라우터에서 마킹된 정보만을 이용하여 미리 결정된 클래스 별로 패킷 전달 기능만을 수행하게 된다. 서비스 클래스 별로 처리하기 때문에 라우터에서 고속의 패킷 전달을 할 수 있도록 하는 것을 기본으로 한다. 이를 위하여 망의 에지와 망의 코어에서의 역할을 분담하여 처리하는데, 망의 경계에서는 망에 들어가는 트래픽을 분류하여 조절하여 DSCP(DS Code Point)를 표시하고, 망의 코어에서는 이 DSCP와 관련된 PHB에 따라 패킷이 전달된다.

홈 네트워크(home network)와 외부 네트워크(foreign network)는 경계에 있는 에지 라우터와 연결되어 있다. 홈 네트워크는 HA를 포함한 네트워크로 보통 MN이 등록된 사설 네트워크 또는 사업자 네트워크이다. HA는 홈 네트워크에 있는 라우터로써 홈 네트워크에 접근한 MN을 확인하고 등록을 시키거나 또는 FA에 접근한 MN이 등록을 요청할 때 등록을 허락하고, MN이 상대 노드(CN: Correspondent Node)와 송·수신을 할 때 터널링(tunneling)을 하여 패킷을 MN까지 전달한다. 외부 네트워크는 FA가 포함된 네트워크로써 MN이 이동한 곳이다. FA는 외부 네트워크에 접근하는 MN를 확인하고 접근을 허락하거나 불허하고 그리고 접근이 허락된 MN에게 COA를 할당한다. 그리고 MN이 외부 네트워크에서 또 다른 외부 네트워크로 핸드오프(handoff) 하였을 때 이전 외부 네트워크가 미리 받아 있던 패킷을 터널링을 통해 MN이 후에 접속한 외부 네트워크에게 패킷을 전달하는 역할을 한다. 정책 서버는 MN의 사용자 프로파일(사용자 ID, IP 주

소 등)을 받아 그 프로파일을 바탕으로 사용자에게 알맞은 정책을 결정하고 구성하며 장비에 그 정책을 전송하여 사용자에게 최적의 서비스를 제공하려는 데 목적이 있다. 따라서 정책 서버는 이동 차별화 서비스 네트워크를 모니터링하고 이동 IP 동작, DiffServ의 동작을 제어하고 정책을 수립하고 저장하여 각각의 에지 라우터, 코어 라우터, HA와 FA에게 알맞은 정책을 분배하고 링크에 대한 자원을 할당하는 역할을 한다.

2.2 이동 IP 환경에서 정책기반 차별화 서비스 동작 절차

그림 2는 정책기반 이동 차별화 서비스 네트워크에서 MN이 외부 네트워크로 이동 하였을 때 정책 서버에 등록을 하고 동작하는 절차는 표현하였다(FA COA를 이용하였을 때의 동작 절차임을 가정한다.).

1) 등록 절차

(i) FA는 외부 네트워크에서 advertisement를 주기적으로 보낸다.

(ii) MN이 외부 네트워크에 접속하였을 때, MN는 FA가 보낸 advertisement를 수신하고 MN이 속해있던 HA에게 등록요청을 보내기위해 먼저 FA 등록요청을 전달한다.

(iii) FA는 이 정보를 수신하여 MN의 HA에게 등록요청 정보를 전달한다.

(iv) MN의 등록요청 정보를 수신한 HA는 MN의 프로파일(profile)을 통해 정책 서버에게 SLA (Service Level Agreement)를 요청한다.

(v) 정책 서버는 이벤트 검출(event detection) 기능을 통하여 새로운 MN의 인증을 거친 후, LDAP 프로토콜을 통하여 정책저장소해서 해당 MN에 대한 정보(QoS 정보 레벨, SLA 정보 등)를 요청한다.

(vi) 정책 저장소는 현재 기록되어 있는 MN의 정보를 LDAP 프로토콜을 통하여 정책 서버에게 전달한다.

(vii) 정책 서버는 에지 라우터와 코어 라우터 그리고 HA와 FA에게 MN의 정책 정보를 COPS 프로토콜을 통하여 전달한다.

(viii) 정책 정보를 수신한 HA는 MN이 보낸 등록요청을 허락하고 등록 응답 정보를 FA에게 보낸다.

(ix) FA는 등록 응답 정보를 MN에게 보낸다.

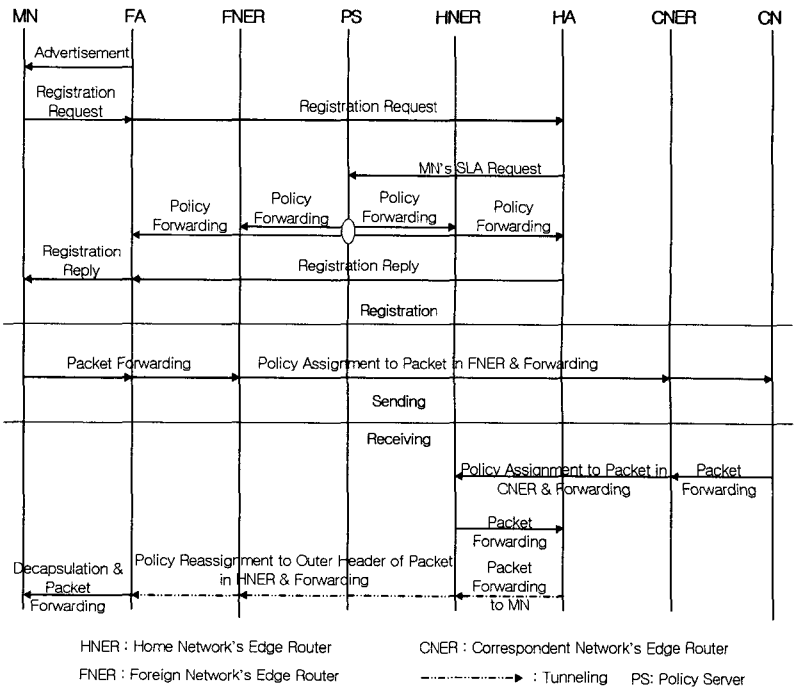

그림 2. 등록 절차 및 동작 절차

2) 데이터 전송 절차

가) MN가 송신 할 경우

(ⅰ) 이동 IP가 기본적으로 지원하는 삼각 라우팅(triangle routing)을 사용하여 MN는 FA를 거쳐 FNER(Foreign Network's Edge Router)에게 패킷을 전송한다.

(ⅱ) FNER은 외부 네트워크에 인접해 있는 에지 라우터로서 FA로부터 MN의 패킷을 수신한 FNER은 입력된 패킷이 어느 MN에서 온 것인가를 분류한다.

(ⅲ) 분류된 MN의 트래픽이 정책 서버와 계약한 트래픽 형태에 적합한지를 판단한다. 이때 패킷의 분류와 적합성 여부 검사는 정책 서버로부터 받은 정책 프로파일에 근거한다.

(ⅳ) 이러한 판단에 따라 코어 라우터에서의 패킷 처리 판단의 기준이 되는 DSCP를 설정하고 코어 라우터로 보내기 전에 트래픽의 쉐이핑이나 폐기를 수행한다.

(ⅴ) 입력된 패킷의 DSCP 값을 검사하여 어떤 PHB에 속하는 지를 결정한다. PHB는 라우터에서 클래스별 서비스 지원을 위해 정책 서버에 의해 결정된 정책에 따라 클래스 별 자원을 할당하고 우선순위에 따른 스케쥴링을 수행함으로써 실질적으로 구현된다.

(ⅵ) 그 PHB에 합당한 처리 규칙(MN의 정책)에 따라 패킷을 처리한 CNER(Corre-spondent Network's Edge Router)를 거쳐 CN에게 패킷을 전송한다. CNER은 상대 네트워크(Correspondent Network)에 인접한 에지 라우터이다.

나) MN가 수신 할 경우

(ⅰ) CN은 CNER에게 패킷을 전송한다.

(ⅱ) CNER은 위의 MN이 송신 할 경우의 FNER과 똑같이 패킷을 분류하고 MN의 트래픽이 계약을 위반하는지 여부를 판단한 다음 정책에 따라 해당하는 처리를 한다.

(ⅲ) 이러한 과정을 거친 트래픽은 DiffServ 네트워크 내부에서의 패킷 처리 규칙에 해당하는 PHB로 변환하여 코어 라우터와 HNER를 거쳐 HA로 전송한다.

(ⅳ) MN이 외부 네트워크로 이동하였을 경우, HA는 정책이 실행되어 온 패킷을 MN에게 보내기 위해 캡슐화하여 다시 HNER에 터널링으로 보낸다.

(ⅴ) CN의 정책이 할당되어진 패킷이 캡슐화하여 터널링으로 패킷이 보내졌기 때문에 CN의 정책은

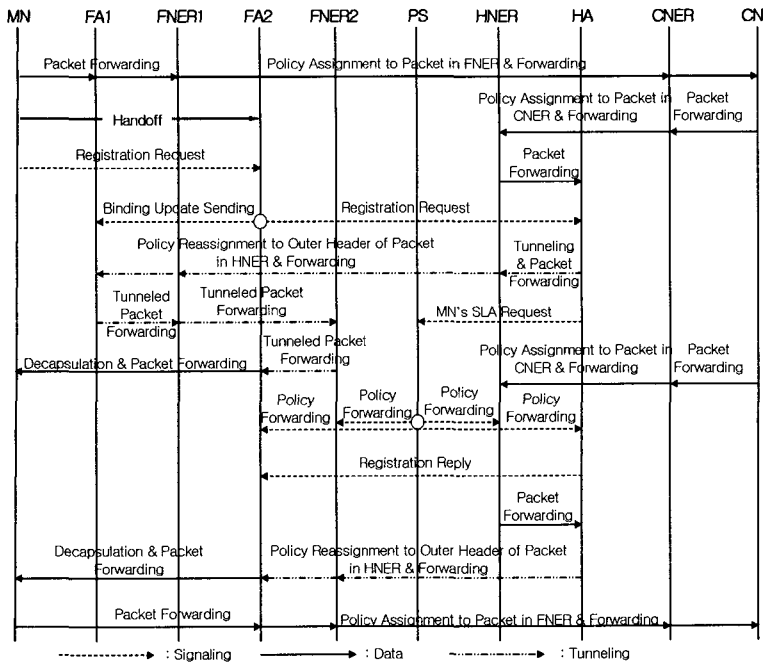

그림 3. 핸드오프시 등록 절차 및 동작 절차

캡슐화된 패킷의 안쪽 헤더(inner header)에 숨겨져 있다. 따라서 HNER은 캡슐화된 패킷의 바깥 헤더(outer header)에 다시 정책을 재할당하여 FNER을 거쳐 FA에게 패킷을 전송한다.

(vi) 캡슐화된 패킷을 받은 FA는 역캡슐화하여 최종적으로 MN에게 전송한다.

이동 IP는 이동성을 가지기 때문에 MN이 CN과 통신을 하는 중에 핸드오프가 발생하여 새로운 외부 네트워크로 접속을 할 수 있다. 그림 3은 핸드오프시 MN이 정책 서버에 등록하는 절차와 동작 절차를 나타내었다.

3) 핸드오프시 등록 및 동작 절차

(i) MN이 외부 네트워크1에서 CN과 송수신 하는 중에 외부 네트워크2로 핸드오프 하였다.

(ii-1) MN은 FA2의 advertisement를 수신하여 외부 네트워크2에 있음을 인지하고 MN은 HA에게 등록 요청을 보낸다.

(ii-2) 핸드오프 중에 CN은 CNER을 통해 MN으로 패킷을 보낸다.

(ii-3) 위의 동작 절차와 마찬가지로 CNER에서 패킷은 트래픽 조절기(traffic conditioner)를 거치고 나서 큐 매니저를 통해 해당하는 큐에 넣어주며 패킷 스케줄러가 각 서비스가 가지는 가중치에 따라 해당하는 서비스 즉, PHB에 따라 수행하여 패킷을 보낸다.

(iii-1) MN의 등록 요청을 가로챈 FA2는 HA에게 MN의 등록 요청을 전달하고 동시에 FA1에게 MN이 FA2로 이동하였음을 알리는 바인딩 업데이트 메시지(bind update message)를 보낸다.

(iii-2) CN에서 보낸 패킷은 HA까지 전달하여 캡슐화를 하고 터널링을 통해 HNER에게 보내어진다.

(iii-3) CN의 정책이 할당되어진 패킷이 캡슐화하여 터널링으로 패킷이 보내졌기 때문에 CN의 정책은 캡슐화된 패킷의 안쪽 헤더에 숨겨져 있다. 따라서 HNER은 캡슐화된 패킷의 바깥 헤더에 다시 정책을 재설정한 후 FNER1를 통해 FA1으로 패킷을 전송한다.

(iv-1) MN의 새로운 등록 요청을 받은 HA는 MN이 새로운 외부 네트워크로 이동하였음을 인지한 후 그 정보를 포함한 MN의 프로파일을 정책 서버에게 보낸다.

(iv-2) FA1은 바인딩 업데이트 메시지를 통하여 MN이 FA2로 핸드오프 하였음을 알고 캡슐화되어 온 패킷을 다시 FNER1과 FAER2를 거쳐 FA2로 전송한다.

(v-1) 정책 서버는 외부 네트워크2에 이동한 MN의 정책을 각각의 라우터들과 에이전트들에게 전송한다.

(v-2) FA2는 수신한 패킷을 역캡슐화하여 MN에게 전송한다.

(vi-1) HA는 FA2에게 등록 승인 메시지를 보낸다.

(vi-2) 이 때 CN에서 다시 패킷을 MN으로 보낸다.

(vii) CN에서 새롭게 보낸 패킷을 수신한 HA는 MN이 핸드오프하여 외부 네트워크2에 속해있음을 알고 있으므로 FA2로 패킷을 캡슐화하여 보낸다.

(viii) HNER은 캡슐화된 패킷의 바깥 헤더에 다시 정책을 재설정하고 FNER2를 거쳐 FA2로 전송한다.

(ix) FA2는 이 패킷을 역캡슐화하여 MN에 전송한다.

(x) MN이 CN에게 패킷을 전송할 시에는 핸드오프가 이미 지났으므로 FA2와 FNER를 거쳐 정책을 설정하여 CN에게 패킷을 전송한다.

3. 정책기반 이동 차별화 서비스 네트워크 관리

3.1 정책기반 이동 차별화 서비스 네트워크 관리 구조

본 논문에서 제안하는 이동 IP 환경에서 DiffServ를 제공하기 위한 정책기반 네트워크 관리는 단순히 네트워크 구성을 네트워크 운영자의 명령대로 바꾸는 것을 지원하는 것이 아니라, 네트워크상의 응용 서비스 제공, 가입자의 접근 제어, 네트워크 장비의 상태, 링크의 운용율, 서버 시스템 운용 스케줄 등 복합적인 네트워크 정책을 통합하여 운용하고 지원하는 관리 구조이다.

본 논문에서 제시한 정책기반 이동 차별화 서비스 네트워크 관리 구조는 그림 4와 같다. 정책 서버는 정책 응용 계층(policy application layer), 정책 제어 계층(policy control layer), 그리고 정책 전달 계층(policy delivery layer)으로 크게 3개의 카테고리로 나눌 수 있다. 정책 응용 계층은 정책 관리 툴로서

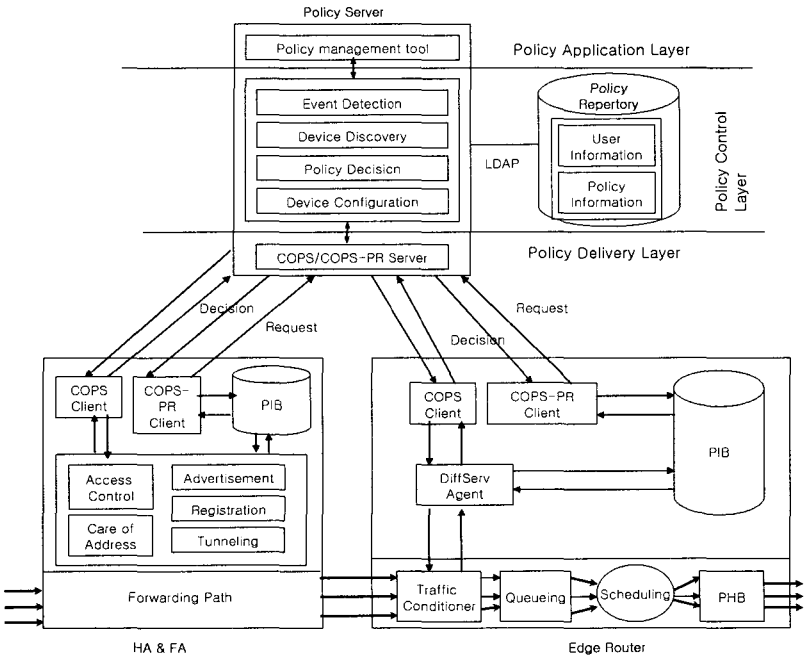

그림 4. 이동 IP 환경에서 정책기반 차별화 서비스 네트워크 관리 구조

정책을 지시하고 변경하고 디스플레이 하는 사용자 인터페이스를 제공한다. 또한 관리되고 있는 장치의 상태를 표시한다. 정책 제어 계층은 실제 정책을 결정하고 각 네트워크 장비에 결정된 정책을 전달하는 계층으로서 PDP에 해당한다. 정책 제어 계층은 이벤트 검출(event detection), 장비 발견(device discovery), 정책 결정(policy decision) 그리고 장비 구성(device configuration)으로 4가지 기능으로 나눌 수 있다. 이벤트 검출은 시스템 상태의 변화, 또는 운영자 또는 정책 저장소로부터의 정보 변화를 인지하여 이와 관련된 절차를 수행하기 위한 기능이다. 좀더 유연한 동작 및 관리 서비스를 제공하기 위해 정책 발견이 필요하기 때문에, 정책 서버는 장비가 구성을 요청할 때, 적용되는 수동적인 구성보다 적극적인 장비 구성을 하여야 한다. 따라서 정책 서버는 구성에 필요한 장비를 찾기 위해 네트워크 토폴로지 정보를 항시 알아야한다. 정책 결정은 이벤트 검출에 의해 트리거된 정책을 결정하는 기능으로 정책 저장소로부터 해당 정책을 받아 그 정보를 바탕으로 정책을 결정한다. 장비 구성은 장비 파리미터를 만들고 장비에 그 정보를 전달하는 기능이며 정책 서버로부터 장비의 타입(type), 큐(queue) 관리, 제어 프로토콜 등의 장비 특성 정보를 얻는다. 정책 전달 계층은 이 파라미터들을 COPS(Common Open Policy Service)[7]나 COPS-PR(COPS for Policy Provisioning)[8] 프로토콜을 이용하여 장비에 전송된다.

정책 저장소는 정책 정보을 저장하고 입출력하는 디렉토리 서비스(directory service) 저장 장치이다. 정책 저장을 통해 관리해야 할 데이터의 재사용과 기존 관리 정보의 갱신을 가능하게 한다. 정책 저장소와 정책 서버와의 통신은 표준화된 프로토콜인 LDAP(Lightweight Directory Access Protocol)[9]을 사용한다.

COPS는 네트워크 장비와 정책서버 사이에서 메시지를 신뢰적으로 교환하는 전송 프로토콜처럼 TCP를 이용하는 클라이언트-서버 프로토콜이다. COPS는 정책 서버와 네트워크 장비 사이에 정책과 관련된 정보를 주고받기 위해 디자인을 하였다. 네트워크 장비가 필요한 정책을 정책 서버에게 요청하고, 정책 서버는 네트워크 장비들에게 반영할 정책 정보를 수립하여 네트워크 장비에게 전송한다. 그러므로 네트워크 장비는 해당 정책 정보를 받아 장비들에게 반영한 후 정책 서버에게 결과를 통보한다. COPS-PR은 COPS를 확장한 프로토콜로써 DiffServ 정책 프로비져닝을 위한 기반이다. 이름 그대로 COPS-PR은 프로비져닝 모드에서 동작한다. COPS-PR 클

라이언트는 정책 서버에 연결하여 그들의 capability와 limitation을 보고하고 클라이언트에게 정책을 다운로드를 위해 최초의 정책을 요청한다. 정책 서버는 각 클라이언트의 요청을 처리하고 정책들과 네트워크 상태에 따라 네트워크 장비들에게 적합한 정책 구성 데이터를 다운로드한다.

HA와 FA 그리고 에지 라우터는 정책기반 네트워크에서 PEP에 해당하는 것으로 그림 4와 같은 구조를 가진다. 본 논문이 제안한 PEP의 구조는 단일의 COPS나 COPS-PR을 사용하는게 아니라 두개의 프로토콜을 같이 사용한다. COPS는 네트워크 상황에 따라 또는 가입자의 가입조건의 변화에 따라 동적으로 정책이 바뀌는 경우에 적절히 사용된다. 동적으로 이벤트가 발생하면 정책 서버는 즉시 정책을 결정하여 그 정책이 필요한 HA, FA나 라우터들에게 COPS 프로토콜을 사용하여 이를 전송한다. COPS-PS은 외부 이벤트 즉 SLA을 바탕으로 만들어진 파라미터로부터 네트워크 장비들의 정책 설정을 조절하기 위해 네트워크 장비가 부팅하여 최초로 정책 서버에 연결을 한 후 네트워크 장비에 대한 정책들을 미리 설정한다. 따라서 사용자의 패킷은 정책 요청의 기다림 없이 설정된 정책에 따라 즉각적으로 전송되어진다.

COPS-PR은 네트워크 장비를 제어하고 PEP에 정책 정보를 저장하기 위해 PIB(Policy Information Base)[10]라는 구조를 사용한다. 따라서 COPS-PR로 정책서버에서 받은 정책 구성 정보를 저장하기 위한 특별한 데이터베이스이다. PIB는 정책을 통해 네트워크 장비를 제어하는 기능이 포함되어 있지만 미리 구현되어 있는 기능을 사용하기 때문에 새로운 기능에 대해서나 갑자기 급변하는 네트워크 상황에 정책을 사용하지 못하는 단점을 가지고 있으므로 본 논문에서 COPS 프로토콜을 같이 사용하는 또 다른 이유이다.

HA와 FA는 COPS와 COPS-PR 클라이언트와 PIB를 포함하고 HA나 FA에 MN의 접근을 제어하며 Advertisement, 등록, 터널링과 COA를 제어하는 기능을 가진다. 에지 라우터는 HA 및 FA와 마찬가지로 COPS와 COPS-PR 클라이언트와 PIB를 포함하고 트래픽 조절기(traffic conditioner)에서 패킷을 분류, 마킹, 쉐이핑 등을 하여 큐잉(queueing)에 전달하여 해당하는 큐에 패킷을 넣어주면 패킷 스케줄러(packet scheduler)에서 각 서비스가 가지는 가중치에 따라 해당하는 서비스을 수행하여 PHB를 통해 각 서비스에 맞게 EF(Expedited Forwarding)나 AF(Assured Forwarding) 또는 BE(Best Effort)로 보낸다.

3.2 정책 클래스

정보 모델은 구현 전에 이해할 수 있도록 지식을 추상화한 것으로 사용자, 애플리케이션, 네트워크에 대한 지식뿐만 아니라 여러 사용자들이 그 지식들을 사용할 수 있도록 여러 지식 도메인들 간의 상호 작용하는 방법들에 대한 지식까지도 구조화한 것이다. IETF에서 표준화한 PCIM(Policy Core Information Model)은 정책 정보 핵심 모델로서 정책 정보 모델을 표현하기 위해 제시하는 객체 지향 정보 모델이다. PCIM은 애플리케이션들과 연관된 어떤 정책이든지 표현할 수 있도록 일반적이고 핵심적인 클래스들을 정의하였다. PCIM은 정책의 제어와 정책 정보를 표현하는 구조 클래스(structural classes)와 상호 연광성을 나타내는 연관 클래스(association classes)로 정의하고 있다[11].

따라서 본 논문에서는 PCIM을 바탕으로 이동 IP 환경에서 인터넷 차별화 서비스를 제공하는 정책기반 네트워크 관리의 정책 구조 클래스를 그림 5와 같이 나타내었다. 정책은 정책 규칙들의 집합(set)을 사용하여 적용되고, 각 정책 규칙은 조건들의 집합과 동작들의 집합으로 구성된다. 여러 정책 규칙들은 정책 그룹들과 결합되고, 이러한 그룹은 다른 그룹을 구성할 수 있다. PolicyGroup은 연관된 policyRule들의 집합이나, 연관된 PolicyGroup들의 집합을 위한 컨테이너를 의미하는 클래스이다. PolicyRule은 "주어진 조건(condition)을 만족하면 지정된 행동(action)을 취한다."와 같은 의미를 표현하기 위한 클래스이다. PolicyCondition은 정책 규칙에서 정책 조건을 나타내는 클래스로서 TimeofDaypolicyCondition은 가입자의 형태, 가입 조건에 따른 시간대에 대한 정책의 조건을 나타내고, CreditPolicyCondition은 가입자의 신용도에 따른 정책의 조건이다. SenderPolicyCondition은 송신자가 해당 트래픽을 수신할 수 있는 수신자를 지정해줄 수 있는 정책의 조건이고, UserIDPolicyConditiond은 사용자 ID를 기초로 접근을 허락하거나 불허하는 정책의 조건이다. 마지막으로 BiagreementPolicyCondition은 타

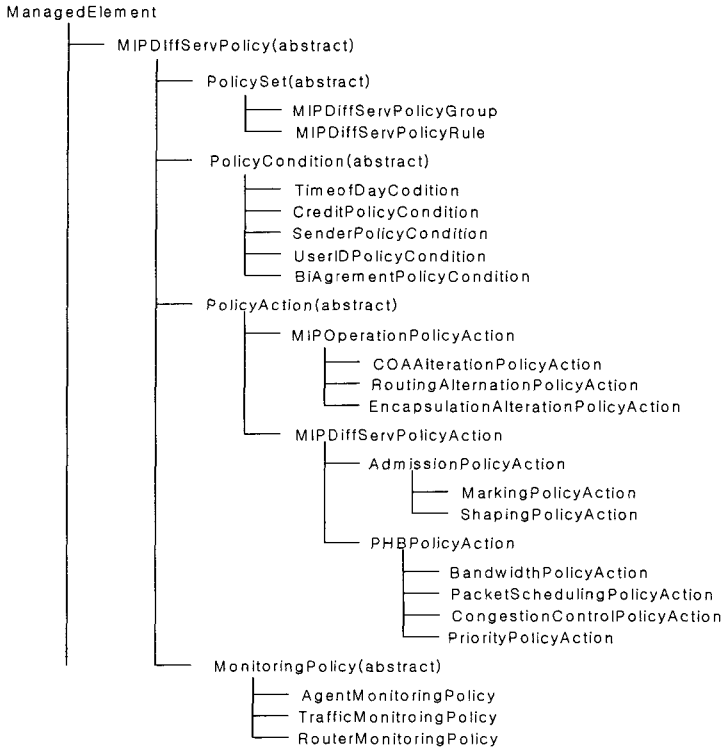

그림 5. 정책 구조 클래스

ISP(Internet Service Provider)로부터 서비스를 제공받는 MN이 현재의 ISP 망으로 이동하였을 때, 접근을 허용하거나 불허하는 정책의 조건이다. PolicyAction은 정책 규칙에서 조건을 0만족하면 수행하는 동작을 표현하는 클래스이다. 이 클래스는 이동 IP의 동작을 수행하는 MIPOperationPolicyAction과 이동 IP 환경에서 DiffServ를 MIPDiffServPolicyAction으로 두개의 서브 클래스로 나뉜다. MIPOperation PolicyAction은 이동 IP의 COA를 변경해주는 COA AlterationPolicyAction, 이동 IP의 라우팅을 변경시켜주는 RoutingAlterationPolicy-Action과 이동 IP의 캡슐화를 변경시켜주는 EncapsulationAlteration PolicyAction으로 나눌 수 있다. MIPDiffServPolicy Action은 크게 AdmissionPolicyAction과 PHB PolicyAction으로 구분한다. AdmissionPolicy Action은 개별적인 트래픽 플로우나 집합의 트래픽 클래스을 제어를 결정하기 위해 사용하고 Marking PolicyAction과 ShapingPolicyAction으로 나눌 수 있다. MarkingPolicyACtion은 패킷 헤더내의 DS 필드값을 적합한 DSCP로 할당하는 정책을 수행하고 ShapingPolicyAction은 트래픽의 속도를 조절하는 정책을 수행한다. PHBPolicyAction은 DSCP 값으로 패킷의 전달 방식을 결정하여 수행하는 정책이다. 이 정책은 트래픽 클래스에 예약된 대역폭을 할당해주는 BandwidthPolicyAction, 패킷의 전달되는 순서를 결정하는 Packet- SchedulingPolicyAction, 혼잡 제어 알고리즘을 제어하는 CongestionContorlPolicy Action과 패킷들의 우선순위를 결정하는 Priority PolicyAction으로 구분한다. MonitoringPolicy는 이동 IP 환경에서 정책기반 차별화 서비스 네트워크를 모니터링하는 정책들로서 HA와 FA를 모니터링하는 AgentMonitoringPolicy, 트래픽을 모니터링하는 TrafficMonitoringPolicy와 라우터의 행동을 모니터링하는 RouterMonitoring으로 나뉠 수 있다.

3.3 정책 시나리오

본 논문은 이들 정책 클래스를 가지고 정책 시나리오를 표현하기 위해 다음과 같은 정책 언어를 제안하였다. 그림 6은 정책 신택스(syntax)로서 이 신택스를 바탕으로 클래스들의 정책들을 표현하였다.

```
Title       policy name;
Subject     indicates policy;
Initiator   firstly invokes policy;
Target      executes policy;
On          event-trigger;
Policy      If
             condition;
            Then
             action;
```

그림 6. 정책 신택스

Title은 표현할 정책의 제목을 표시하는 곳이다. Subject는 정책을 지시하는 주체 즉, 관리자나 정책 서버를 가리킨다. Initiator는 맨 처음 정책을 지시하는 주체에게 정책을 청원하는 위치를 가리키고, Target은 주체에서 명한 정책을 실질적으로 실행하는 곳을 가리킨다. On은 event-trigger 즉, 어떠한 상황에서 이 정책이 발생하는 지를 나타내고, Policy에서 If는 정책의 조건(condition)을 나타내고 Then은 조건이 결정된 후 그것을 실행하는 행동(action)을 표현한다.

다음은 본 논문이 제시한 이동 IP 환경에서 정책기반 차별화 서비스 네트워크에서의 정책 클래스를 바탕으로 몇 개의 정책 시나리오 예를 보여주고 있다. 이 정책 시나리오들은 본 논문이 제안한 정책 언어를 사용하여 작성하였다.

1) 시간에 따른 접근 제어 정책(그림 7)

시간에 따른 접근 제어는 관리자가 가입자의 형태, 가입 조건에 따라 하루 중 또는 년 중 특정시간대에 네트워크 접근을 허용하거나 혹은 불허하는 정책이다. 이 정책의 예를 그림 7로 표현하였다. 즉, 가입자가 주중의 비즈니스 시간대(9시~17시)에만 네트워크 접근을 허용하는 예이다. MN이 HA 또는 FA에

```
Title       TimeOfDayAccessControlPolicy;
Subject     PolicyServer;
Initiator   HA || FA;
Target      HA || FA;
On          MNAccessRequest;
Policy      If
             (DayOfWeek == MonToFri)
             &&
             (TimeOfDay == 0900To1700);
            Then
             MNAccessAdmission;
```

그림 7. 시간에 따른 접근 제어 정책

접근을 하면 HA나 FA는 정책 서버에게 질의를 한다. MN이 주중의 비즈니스 시간대에 접근을 하면 정책 서버는 이동 단말의 접근을 허락하고 그 시간대가 아니면 접근을 불허하는 정책을 표현하였다.

2) 양방향 계약 접근 정책(그림 8)

HA와 FA의 동의 하에 MN의 접근을 허락하는 정책이다. 어떤 하나의 MN이 FA에 접근을 하였을 때, MN의 HA가 타 가입자망의 네트워크에 속하면, 정책서버는 타 가입자망과 계약을 맺고 있는 지를 확인하여 타 가입자망과 계약이 맺어 있으면, 타 가입자망에 속한 HA와 FA가 등록하여 MN이 서비스 받을 수 있도록 해주는 정책의 예이다.

```
Title       BiAgreementAccessControlPolicy;
Subject     PolicyServer;
Initiator   FA;
Target      HA && FA;
On          MNAccessRequest
            &&
            (HomeNetworkOfMN ≠ SameDimension);
Policy      If
             (HA && FA) == BiAgreement;
            Then
             MNAccessAdmission;
```

그림 8. 양방향 접근 제어 정책

3) 캡슐화 변경 정책(그림 9)

터널링을 위해 패킷은 캡슐화를 하는데 이 캡슐화 기법으로는 일반적으로 IP-in-IP 캡슐화 방법을 사용한다. 그러나 HA와 FA 사이에 네트워크 혼잡이 발생하면 IP-in-IP 캡슐화한 패킷은 패킷 지연이 발생한다. 그러므로 이 패킷 지연을 우려하여 패킷 사이즈를 최소로 캡슐화하는 최소 캡슐화 (minimal encapsulation)로 변경한다. 그림 9의 정책은 IP-in-IP 캡슐화 기법에서 최소 캡슐화 기법으로 변경하는

```
Title       EncapsulationAlterationPolicy;
Subject     PolicyServer;
Initiator   HA;
Target      HA && FA;
On          Network == Congestion;
Policy      If
             (HA && FA) == IPinIPEncapsulation;
            Then
             (HA && FA) ::= MinmalEncapsulation;
```

그림 9. 캡슐화 변경 정책

정책의 예이다. FA는 정책서버에게 정책을 문의하고, 정책서버의 이동 IP 관리자는 HA에서 FA로 네트워크 혼잡이 발생한다고 판단되고, FA가 최소화 캡슐화를 지원한다면, 캡슐화를 담당하는 HA에게 최소화 캡슐화로 변경하라는 정책을 전달하고 HA가 그 정책을 실행한다.

4) MN의 차별화 서비스 클래스구성 정책(그림 10)

이 정책은 MN에 DiffServ 클래스의 구성을 할당해주는 정책이다. MN이 FA에 접속하여 인증이 된 후, 정책 서버가 MN의 SLA를 확인하고 에지 라우터에 해당 노드의 클래스 관련 정책 구성 정보를 보내어 MN의 패킷이 FA를 거쳐 에지 라우터에 도착하면 정책 서버가 보내온 정책에 따라 MN의 패킷에 해당 클래스의 DSCP를 마킹한다. 그림 10은 DiffServ 클래스 중 EF로 할당되는 MN의 정책을 보여준다.

Title	MNEFConfigPolicy;
Subject	PolicyServer;
Initiator	EdgeRouter;
Target	Routers;
On	MN ∈ FA && ClassRequest;
Policy	**If** (Classification == EF) && (Metering == InProfile); **Then** (Marking ::= 101110) && (Shaping ::= (InputRate ≦ OutputRate)) && (PHB ::= EF);

그림 10. MN의 EF 구성 정책

5) MN의 클래스 강등 정책(그림 11)

MN이 높은 우선순위 클래스(예, EF 클래스)로 정책이 결정되어 패킷을 전송하고 있는데 만약 네트워크가 혼잡이 발생하여 MN의 패킷을 전송을 못하게 되면 이 혼잡 상황을 회피하기 위해 정책 서버가 정해진 정책에 따라 MN의 클래스 구성 정책을 한 단계 아래인 클래스 서비스로 강등하는 정책이다. 그림 11은 MN이 EF에서 AF의 gold 서비스로 강등되는 정책을 보여준다.

Title	MNEFDemotionPolicy;
Subject	PolicyServer;
Initiator	EdgeRouter;
Target	Routers;
On	Network == Congestion;
Policy	**If** (Classification == EF) && (Metering == InProfile) && (Marking == 101110) && (Shaping == InputRate ≦ OutputRate); **Then** PHB ::= GoldAF;

그림 11. MN의 EF 강등 정책

4. 이동 IP 환경에서 정책기반 차별화 서비스 네트워크 관리 구현

본 논문에서는 그림 12와 같은 실험실 규모의 이동 IP 정책기반 차별화 서비스 네트워크 테스트베드(testbed)을 구성하였다. 이 테스트베드는 현재 헬싱키 대학에서 구현해 놓은 Dynamics Mobile IP dynamics-0.8.1 리눅스 버전[12]을 컴파일하여 이동 IP 환경에서 정책기반 DiffServ 네트워크 관리 시스템을 구현하였다.

본 테스트 베드 구현을 위해 이동 IP 환경에서 정책기반 DiffServ 네트워크 관리을 위한 소프트웨어 구조는 그림 13과 같다. 크게 사용자 모드(user mode)와 커널 모드(kernal mode)로 구분된다. 사용자 모드는 정책 서버를 가리키며 커널 모드는 에이전트 데몬(daemon)을 가리킨다. 정책 서버는 각각의 노드들과 정책 정보를 주고받기 위해 COPS와 COPS-PR 프로토콜을 사용하여 에이전트 데몬들과 직접 통신을 하는데 각 에이전트 데몬들은 HA, FA와 라우터들 위에서 동작하면서 정책 서버에 정책을 질의하고 자신의 정보를 정책 서버에게 알려 정책 서버로부터 정책을 받아서 각 HA, FA 및 라우터들에 적용한다. 커널 모드는 리눅스의 커널을 나타내는 부분으로서 이 리눅스 커널에서 제공하는 QoS 부분을 이용하여 구현하였고 API를 이용하여 각 데몬들

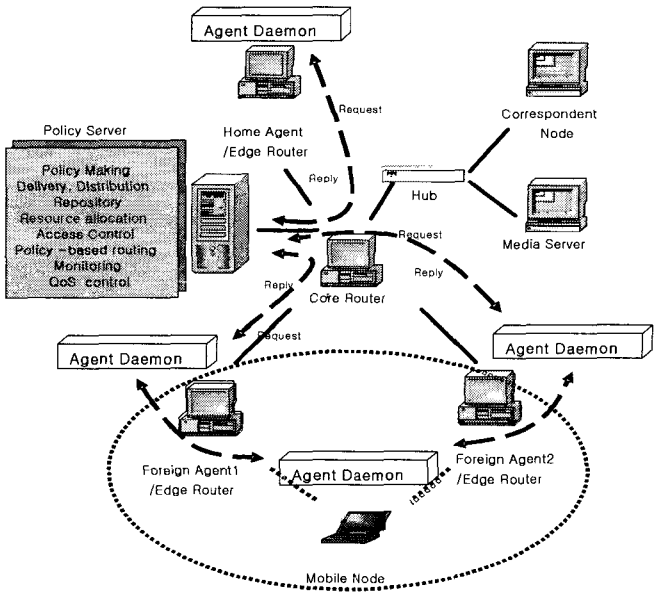

그림 12. 테스트베드

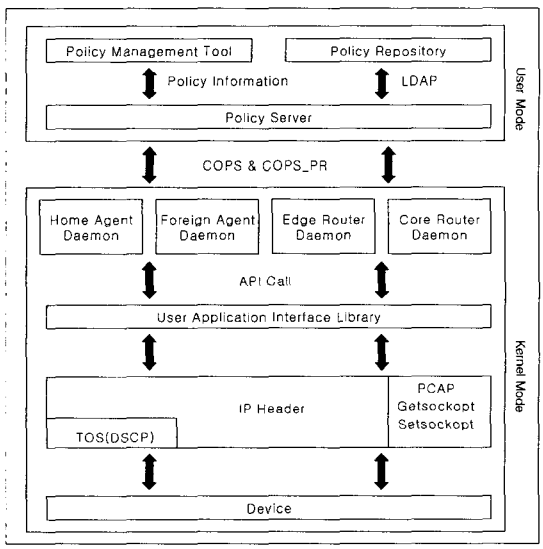

그림 13. 소프트웨어 구조

을 제어한다. 에이전트 데몬들은 이동 IP 소프트웨어에 의해 제공된 사용자 응용 라이브러리(user application library)로부터 개발되었고 정책을 실행하기 위한 커널에 위치하여 API를 사용하여 제어한다. 그리고 PCAP는 리눅스에서 패킷을 캡처하는 것을 제공해주는 라이브러리다. 따라서 이 PCAP를 사용하여 IP 헤더의 TOS 필드를 제어하여 이곳에 DSCP를 할당하여 이동 IP 네트워크에서도 DiffServ를 지원할 수 있는 환경을 만들었다.

그림 14는 개발된 정책 서버의 정책 관리 툴 GUI(Graphical User Interface)을 표현한 것이다. 이 정책 관리 툴은 정책을 지시하고 변경하고 디스플레이하는 사용자 인터페이스를 제공한다. 그리고 기존에 정의된 정책에 클래스에 대한 파싱(parsing) 기능과 정책 정의를 위한 편집 기능, 문맥 검사 기능 등도

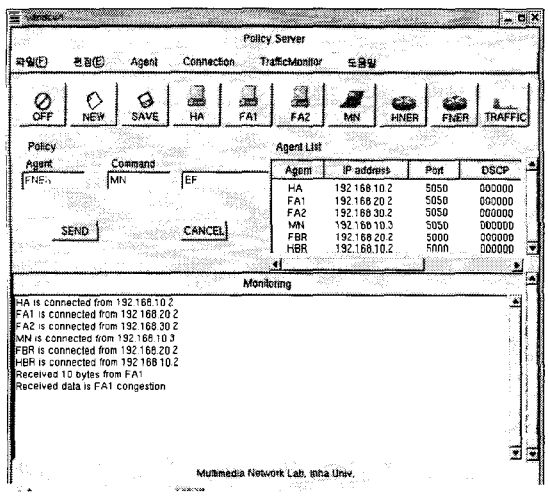

그림 14. 정책 관리 툴 GUI

포함한다. 또한 관리되고 있는 장치의 모니터링과 트래픽의 상태를 표시한다.

그림 15와 16은 콘솔 창에서 에이전트 데몬 명령 인터페이스를 보여준다. 정책 서버와 PEP가 질의와 응답으로 통신을 하여 정책 서버가 결정한 정책을 PEP에서 실행하는 것을 표현하였다. 에이전트 데몬은 원활한 명령 입력 및 모니터링을 위해 두개의 콘솔 창으로 구성하였다. 그림 15는 위의 정책 시나리오에서 캡슐화 변경 정책 시나리오 예를 PEP에서 그 정책을 전송하고(큰 콘솔 창), PEP가 정책 서버로부터 정책을 수신받아 동작을 하는 것(작은 콘솔 창)을 보여주고 있다. 즉, 네트워크가 혼잡할 때, MN가 이동 IP에서 기본 IP-in-IP encapsulation으로 동작을 하고 있으면 정책 서버 MN의 캡슐화를 minimal capsulation으로 바꿔주는 정책을 PEP에서 어떻게 명령을 보내고 어떤게 수신하여 모니터 하는지를 나타내었다.

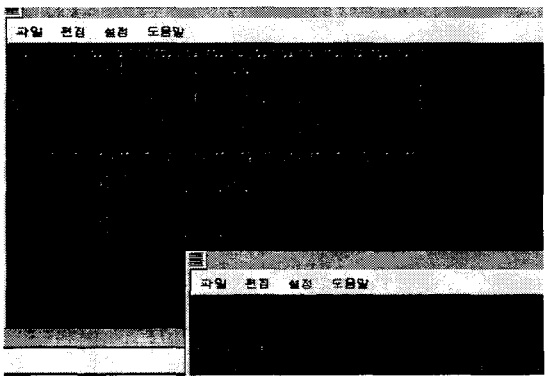

그림 15. 캡슐화 변경 정책을 이용한 에이전트 데몬 콘솔

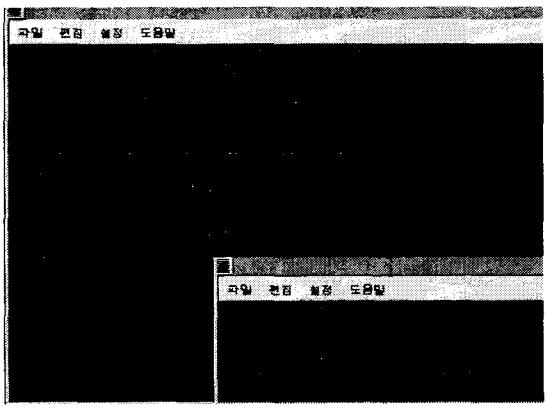

그림 16. MM의 클래스 구성 정책의 에이전트 데몬 콘솔

그림 16도 또한 위의 정책 시나리오에서 EF의 클래스 구성 정책을 기반으로 에이전트 데몬을 구성한 것이다. 이동 IP 환경에서 정책기반 DiffServ 네트워크에서 MN에 클래스를 구성하는 정책을 PEP에서 정책서버에 질의를 하고(큰 콘솔 창) 정책 서버가 EF 클래스 서비스를 결정하여 PEP가 정책을 수신받은 모니터링 창(작은 콘솔 창)을 보여주고 있다.

5. 결 론

본 논문은 이동 IP 환경에서 DiffServ를 제공하기 위한 정책기반 네트워크의 구성과 동작절차를 살펴보았다. 그리고 이동 IP 환경에서 정책기반 차별화 서비스 네트워크 관리 구조를 제안하였고 본 논문에서 제안한 정책 클래스를 바탕으로 정책 언어를 이용하여 이동 IP 환경에서 정책기반 차별화 서비스 네트워크에 알맞은 정책 시나리오를 제안하였다. 마지막으로 이동 IP 환경에서의 정책기반 차별화 서비스 관리를 실험실 규모에서 테스트베드를 구축하고 정책 서버와 정책 서버에 정책을 지시하고 변경할 수 있도록 제어하는 정책 관리 툴을 개발하였다.

앞으로 무선 이동망에서의 QoS 제공을 위한 정책기반 네트워크 관리에 대한 연구는 계속적으로 필요한 부분이다. 따라서 더 많은 효율적인 망 관리를 위해 정책 스키마 개발과 정책 시나리오 및 망 관리 구조 개선이 필요하다.

참 고 문 헌

[1] Charles E. Perkins, "IP Mobility Support for IPv4", RFC 3220, IETF, August 2002.

[2] R. Comerford, "State of the Internet: Roundtalble 5.0", IEEE Spectrum, Vol. 36, pp. 42-50, October 1999.

[3] R. Barden, D. Clark, and S. Shenker, "Integrated Service in the Internet Architecture: an Overview", RFC 1663, IETF, June 1994.

[4] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, and W. Weiss, "An Architecture for Differentiated Service", RFC 2475, IETF, December 1998.

[5] Dan Chalmers and Morris Sloman, "A Survey

of quality of Service in Mobile Computing Environment", IEEE communications Surveys, Second Quarter pp. 2-10, 1999.

[6] Mark L. Stevens and Watler J, Weiss, "Policy-based Management for IP Networks", Bell Labs Technical Journal, pp. 75-94, October-December 1999.

[7] D. Durham, ED, J. Boyle, R. Cohen, S Herzog, R. Raian and A. Sastry "The COPS(Common Open Policy Service) Protocol", RFC 2748, IETF, January 2000.

[8] K. Chan, J. Seligson, D. Durham, S. Gai, K. McCloghrie, S. Herzog, F. Reichmeyer, R. Yavatkar and A. Smith, "COPS Usage for Policy Provisioning", RFC 3084, IETF, March 2001.

[9] M. Wahl, T. Howes and S. Kille, "Lightweight Directory Access Protocol", RFC 2251, IETF, December 1997.

[10] R. Ed. Sahita, S. Hahn, K. Chan and K. McCloghrie, "Framework Policy Information Base", RFC 3318, IETF, March 2003.

[11] B. Moore, E. Ellesson, J. Strassner, A. Westerinen, "Policy Core Information Model -- Version 1 Specification", RFC 3060, IETF, February 2001.

[12] http://www.cs.hut.fi/Research/ Dynamics.

[13] Wang Changkun, "Policy-based Network Management", International Conference on Communication Technology Proceedings, Vol. 1, pp. 101-105, 2000.

[14] Leonidas Lymberopoulos, Emil Lupu and Morris Sloman, "An Adaptive Policy Based Management Framework for Differentiated Services Networks", proceedings of the Third International Workshop on Policies for Distributed Systems and Networks, pp. 147-158, June 2002.

[15] Ashish Mehra, Dinesh Verma and Renu Tewari, "Policy-Based DiffServ on Internet servers: The AIX Approach", IEEE Interent Computing, Vol. 1, pp. 75-80, September/ October 2000.

[16] Yuji Nomrua, Akira Chugo, Motomitsu Adachi and Masahito Toriumi, "A Policy Based Networking Architecture for Enterprise Networks", IEEE International Conference on Communications, Vol. 1, pp. 636-640, 1999.

[17] Paris Flekas, Panos Trimintzios, and George Pavlou "A Policy-Based Quality of Service Management System for IP DiffServ Networks", IEEE Network, Vol. 16, pp. 50-56, March/April 2002.

[18] Appan Ponnappan, Lingjia Yand, Radhakrishna Pillai. R, "A Policy Based QoS Management System for the InServ/DiffServ Based Internet", proceedings of the Third International Workshop on Policies for Distributed Systems and Networks, Vol. 1, pp. 159-168, June 2002.

강 승 완

2002년 2월 인제대학교 정보통신공학과 (공학사)
2002년 3월 ~ 현재 인하대학교 정보통신대학원 석사과정

관심분야 : 인터넷QoS, Mobile IP, Policy-based Network. Ad-hoc Network

김 태 경

2002년 2월 인하대학교 경영학부 (경영학사)
2002년 3월 ~ 현재 인하대학교 정보통신대학원 석사과정

관심분야 : 인터넷QoS, Mobile IP, Policy-based Network

유 상 조

1988년 2월 한양대학교 전자 통신학과(공학사)
1990년 2월 한국 과학 기술원 전기 및 전자공학과(공학석사)
2000년 8월 한국 과학 기술원 전자전산학과(공학박사)
1990년 3월~2001년 2월 한국통신 연구개발본부
2001년 3월~현재 인하대학교 정보통신대학원 조교수
관심분야 : 인터넷QoS, 초고속 통신망 구조, 멀티미디어 네트워킹, 트래픽 엔지니어링