NGN 에서 COPS 를 이용한 정책(Policy) 기반 QoS 제어 메커니즘

*송성한, 김양중, 이동규, **정일영
한국외국어대학교 컴퓨터 및 정보통신공학과
e-mail : *s99king@hufs.ac.kr, **iychong@hufs.ac.kr

A Mechanism for Policy-based QoS Control on COPS Interface in NGN

Sung-Han Song, Yang-Jung Kim, Dong-Kyu Lee, Ilyoung Chong
Computer and Information Communication Engineering, Hankuk University of Foreign Studies

요 약

현재 NGN 망에서 강조되는 QoS 보장 기술은 인터넷에서 QoS(Quality of Service) 제공을 위해 해당 응용 서비스 마다 자원을 예약하거나 할당하는 기능을 수행하며, 이 때, 효율적인 종단간의 QoS 보장을 위해서는 전체적으로 자원관리를 할 필요가 생긴다. 정책(Policy) 기반 QoS 기술 관리는 이 경우에 수행이 된다. NGN 망에서의 정책 기반 QoS 기술을 위해서는 정책 기반 QoS 관리 기술 구조 및 프로토콜에 대한 총괄적인 이해가 우선되어야 한다. 즉, 정책 결정 및 정책 실행과 관련한 정책 기반 QoS 관리 기술 구조와 프로토콜 관련한 COPS(Common Open Policy Service)와 LDAP(Light Weight Directory Access Protocol)을 중심으로 이해가 되어야 하고, 이를 토대로 해서 정책 기반 QoS 관리 기술 서비스가 제공 될 수 있다.

1. 서론

NGN 망에서의 정책 기반 관리 기술은 단순히 QoS 관리뿐만 아니라 보안, 경로 제어 등을 위한 용도로 광범위하게 사용되므로, 정책 Policy 기반 관리 기술은 확장성 있는 구조를 가져야 하고, 그 구조와 사용 프로토콜에 대한 이해 및 응용하여 확장된 서비스를 지원할 수 있도록 개발 진행이 되어야 한다. NGN 망의 정책 기반 QoS 기술에서 정책이란 네트워크 자원을 관리 및 제어하기 위한 규칙의 집합이라 할 수 있다. 또한 지속적인 운용관리를 통해 구축된 지식 데이터를 기반으로 각 상황에 대해 조치한 여러 운용 관리 행위들 중에서 최상의 결과를 낸 행위의 집합을 정책이라고 할 수 있다.[1]

정책 기반 QoS 관리 시스템은 크게 정책 결정 관련한 PD-FE(Policy decision functional entity)와 TRC-FE(Transport resource control functional entity), 정책 실행과 관련한 PE-FE(Policy enforcement functional entity), 정책 저장 및 검색을 위한 각 Database, 그리고 NACF(Network attachment control functions)와 CPE, SCF(Service control functions)로 구성된다.[2][3] 그리고, NGN 망에서 정책 기반 QoS 기술을 제공하기 위해서는 이 기능들에서 통신을 담당하기 위한 프로토콜들이 필요한데, 이것이 바로 COPS(Common Open Policy Service)[4]와 LDAP(Light Weight Directory Access Protocol)[5]이다. COPS 는 PD-FE 와 PE-FE 사이 그리고 PD-FE 와 NACF 사이에서 정책 정보를 전달하기 위해서 필요하며, LDAP 은 사용자 DB 및 정책 DB 와 연동하여 PD-FE 나 PE-FE 가 정책 정보를 저장, 검색, 획득 하는데 필요한 프로토콜이다. 이러한 기능들 및 프로토콜을 중심으로 전체적인 정책 기반 QoS 관리 기술 구조의 시나리오 및 구체적인 구현 사항에 대해 설명하고자 한다.

2. 관련연구

본 절에서는 NGN 망의 정책 기반 QoS 기술의 전반적인 구조를 알아보고, 사용된 기능 및 프로토콜의 세부 사항에 대해 설명한다.

2.1. NGN 의 RACF 기반 QoS 제어 구조

NGN 망의 정책 기반 QoS 제어 구조의 전체적 구조는 그림 1 과 같이 나타낼 수 있다.

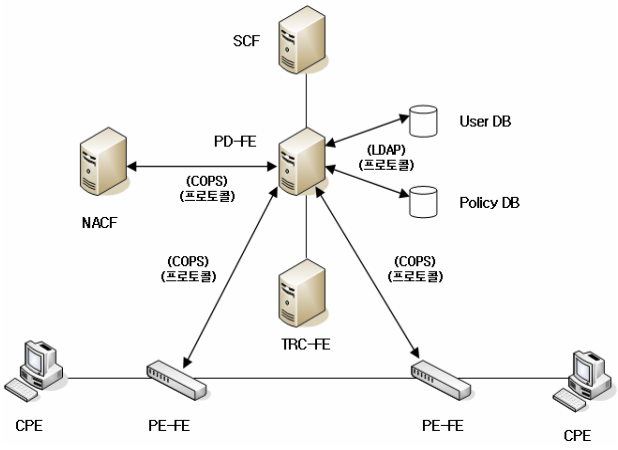

그림 1. NGN RACF 에서 정책 기반 QoS 제어 구조

- PD-FE: 정책 결정을 책임지는 일종의 정책 결정 포인트(PDP: Policy Decision Points)로써, 네트워크 정책 및 SCF 제공된 서비스 정보 와 접속네트워크의 NACF 로부터 제공된 전송계층 정보 그리고 TRC-FE 로부터 제공된 자원 제공 능력 정보를 기반으로 네트워크 자원 및 관리 기능을 제어하는 역할을 담당한다.
- PE-FE: 전송 계층의 PE-FE 는 일종의 정책 실행 포인트(PEP: Policy Enforcement Points)로써, CPE 와 접속 망 사이의 다른 패킷 네트워크 간의 패킷 전송을 위한 게이트웨이 역할 및 PD-FE 와의 연동으로 결정된 정책을 실행하는 역할을 담당한다.
- Database: Database 는 각각 사용자에 관한 사항을 저장하는 사용자 DB(User DB)와 정책설정에 관한 사항을 저장하기 위한 정책 DB(Policy DB)[6]로 나뉜다.
- NACF: NACF 는 사용자 정보를 기반으로 하여 접속망 관리에 대한 다양한 기능을 제공하는 역할을 담당한다.
- SCF: SCF 는 QoS 자원 제어 및 승인 제어를 요청하는 NGN 서비스 계층의 엔티티 역할을 한다.

2.2. LDAP 및 COPS 의 특징

LDAP 은 경량 디렉토리 접근 프로토콜(Light Weight Directory Access Protocol)의 약자로써 디렉토리 서비스를 지원하는 프로토콜이다.[7] 디렉토리 서비스는 네트워크에 연결된 망 장비 및 사용자, 서비스 등을 한곳에 모아두는 일종의 네트워크 데이터베이스 서비스로, 각 데이터베이스를 서버에 분산 수용할 수 있으며, 시스템 다운에 대비할 수 있고, 보안에 강하며, 공개적으로 표준화 되기 때문에 독자적 프로토콜에 종속되지 않는 등의 네트워크 운용 측면에서 편리성이 높다.

COPS 는 PD-FE 와 PE-FE 간에 정책 정보를 교환하기 위해 사용되는 TCP 기반의 질의-응답(query-and-response) 프로토콜이다.[8] COPS 는 프로토콜 자체의 변경 없이 다양하고 수많은 클라이언트를 지원할 수 있고, 인증 및 메시지 무결성을 위해 메시지 차원의 보안을 제공하는 등의 여러 장점이 있다.

2.3. LDAP 및 COPS 연동 시나리오

그림 2 는 LDAP 을 사용하여 현재 시스템에 적용한 연동 시나리오이다.

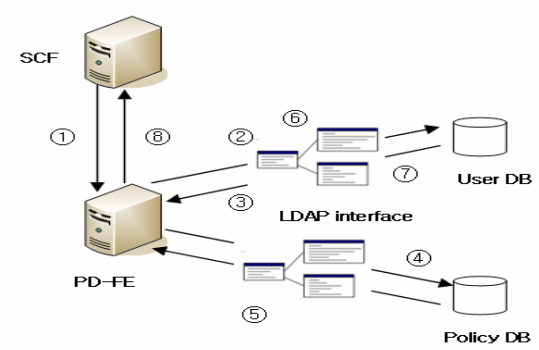

그림 2. NGN RACF 에서 LDAP 프로토콜 연동 시나리오

동작과정은 다음과 같다. 먼저, SCF 로부터 자원예약 메시지를 PD-FE 가 입력 받으면, PD-FE 에서 모든 메시지 필드 값을 LDAP 및 User DB 에 저장하고 LDAP 과 User DB 를 연동한다. 그리고, 저장이 완료되면, User DB 로부터 저장완료 메시지를 수신한다. TRCF 로부터 사용 가능한 스위치 포트를 수신하면, PD-FE 는 Policy DB 에 정책을 요청한다. Policy DB 로부터 PE-FE 및 스위치 포트, DSCP 관련 정책 정보를 수신하게 되면, PE-FE 로부터 자원 설정 관련 결과값을 설정 및 응답을 수신한다. 그리고 나서, User DB 에 저장하기 위해 LDAP 에 결과값을 송신한다. User DB 로부터 사용자에 대한 결과값 저장 정보를 확인 및 수신을 하면 최종적으로 SCF 로 자원 예약의 결과값 송신한다.

그림 3 은 COPS 프로토콜을 사용한 연동 시나리오이다. 다음과 같이 PD-FE 와 PE-FE 의 연동과 PD-FE 와 NACF 연동 관계로 나눌 수 있다.

동작과정은 먼저, SCF 로부터 자원예약 메시지를 PD-FE 가 입력 받으면, PD-FE 에서 모든 메시지 필드 값을 User DB 에 저장 후, 저장 완료 메시지를 수신한다. PD-FE 는 TRCF 에게 사용자가 요청한 Class 에 대해서 적당한 스위치포트를 요청하고, 사용 가능한 스위치포트 수신 후, Policy 서버에 적용할 정책을 요청한다. Policy 서버로부터 적절한 PE-FE 및 스위치포트와 같은 정책이 수신되면 PE-FE 로 자원(포트설정)예약을 요청한다. PE-FE 로부터 자원설정에 대한 결과값이 수신되면, PD-FE 는 NACF 로 네트워크 가입자의 정보 및 자원 승인 등의 확인을 요청한다. NACF

가 수신 후 문제가 없다면, 네트워크 가입자 정보 및 자원 승인 등의 확인 메시지를 PD-FE 로 전송한다. 최종적으로 PD-FE 는 사용자에 대한 결과값을 User DB 에 송신하고, 그에 대한 결과값을 DB 에 각각 저장된다. 확인 메시지가 전송되면, PD-FE 는 SCF 로 자원 예약의 결과값 송신한다. 그리고 최종적으로 PE-FE 에 적용되어 CPE 간의 데이터 송수신이 이루어진다.

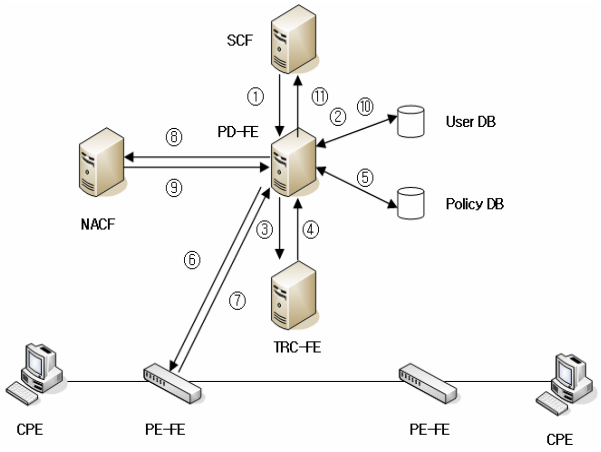

그림 3. NGN RACF 에서의 COPS 연동 시나리오

3. NGN RACF 에서 COPS 적용 QoS 제어 구현 구조

COPS 를 이용한 NGN RACF 에서 QoS 제어를 위한 메커니즘의 구현된 구조에서 크게 LDAP 이 사용된 PD-FE 와 DB 간의 인터페이스, COPS 가 사용된 PD-FE 와 PE-FE 간의 및 NACF 와 PD-FE 간의 인터페이스로 구분 된다.

3.1. PD-FE 와 db 간 LDAP 구현 메커니즘

현재 구현된 NGN 망의 정책 기반 QoS 기술 구조에서의 LDAP 은 사용자의 세부 정보가 저장되는 User Database 와 정책 정보가 저장되는 Policy Database 에서 사용된다. 아래의 표 1 은 각각 User database 와 Policy database 에서 사용되는 값들을 정의했다.

<표 1> User db 와 Policy db 에서 사용되는 주요 값

값	설명
Application ID	사용자 ID
Client Name	사용자 이름
Type of Service	서비스 형태
Class of Service	서비스 클래스
IP Address	IP 주소
Bandwidth	사용 대역폭

값	설명
Number	번호
Policy Name	정책 이름
Grade	등급 설정 내용
Port Number	포트 번호
Class Number	클래스 번호
Bandwidth	사용 대역폭

User database 에서는 연결되는 각 사용자에 대한 ID, 사용 IP 주소, 포트, 정책 값 등이 설정 및 저장되고, Policy database 에서는 정책을 적용하기 위한 정책 이름, 등급, 대역폭 등의 값이 설정 및 저장된다. 앞서 설명한 PD-FE 와 LDAP 간의 시나리오를 적용하여 테스트를 하면 LDAP 각 사용 데이터베이스에 관련 값들이 저장된다. 그림 4 는 User database 및 Policy database 연동 후 LDAP 서버에 저장되는 결과값이다. 'ldapsearch' 명령어를 사용하여 저장되는 결과를 확인 할 수 있다.

```
# my-domain
appl_id : bruce
name : Bruce william
Bandwidth : 3000
Serv_type : video
port : 20
In_time : 120
```

그림 4. LDAP 과 PD-FE 인터페이스에서 처리된 결과값 (예)

즉, PD-FE 는 LDAP 을 통해 각 database 에 관련 정보를 저장, 수정, 삭제, 참조 등을 진행하여 정책 기반 관리 기술을 적용한다. 이를 바탕으로 TRC-FE 및 PE-FE 등과 연동하여 정책이 적용된다.

3.2. PD-FE 와 PE-FE 간 COPS 구현 메커니즘

COPS 프로토콜을 사용하여 PD-FE 와 PE-FE 간에는 그림 5 와 같은 플로우로 구현이 된다. COPS 프로토콜이 사용되는 메시지로는 요청 메시지인 Req 메시지와 결정 및 처리를 담당하는 Dec 메시지로 구분된다.

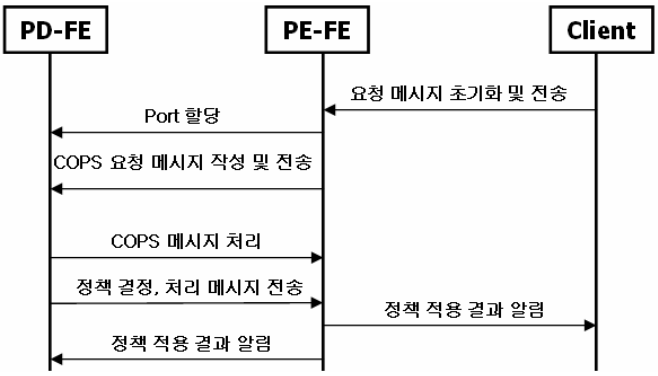

그림 5. PD-FE 와 PE-FE 간 COPS 구현 플로우

위의 세부적인 플로우를 기반으로 아래 그림 6 및 그림 7 과 같은 COPS 연동 프로그램에 사용되는 COPS 프로토콜의 Req 및 Dec 메시지 세부 인터페이스를 정의할 수 있다.

Req 메시지는 PE-FE 의 현 상태를 보고하고, 관련 요청 사항을 전송하는 역할을 한다. Dec 메시지는 Req 메시지에 대한 회신이나, 결정된 정책 전송 등의 역할을 갖는다. 메시지는 일반적 header, 핸들 값을 갖는 client handle, source 및 destination IP address 를 갖는 In-Int 및 Out-Int, 결정 사항을 저장하는 Decision 그리고, 에러 사항을 갖는 Error 필드 등을 갖는다.

Common Header	Client Handle	Context	IN-Int	OUT-Int	ClientSI(s)	LPDPDecision(s)	Integrity

그림 6. COPS 프로그램에 사용되는 Req 메시지 형태

Common Header	Client Handle	Decision	Error	Integrity

그림 7. COPS 프로그램에 사용되는 Dec 메시지 형태

3.3. NACF 와 PE-FE 간 COPS 인터페이스

NACF 는 NGN 서비스에 접속하기 위해 필요한 액세스 수준의 등록과 사용자 기능의 초기화를 제공하여 총괄적으로 액세스 망의 IP 주소 및 인증을 처리하는 기능을 수행한다. 그림 8 과 같은 프로그램을 위한 플로우를 통해 NACF 와 PD-FE 사이 인터페이스에 COPS 프로토콜이 적용된다.

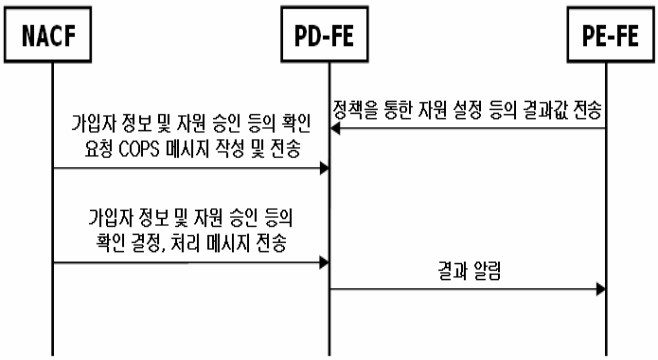

그림 8. NACF 와 PD-FE 간 COPS 제어 플로우

NACF 의 기능인 가입자 정보 및 자원 승인에 대한 요청 및 응답 메시지가 PD-FE 를 통한 COPS 메시지 형태로 처리가 된다. COPS 프로토콜의 요청 및 결정 응답 메시지 형태는 PD-FE 와 PE-FE 인터페이스 간의 연동에서 사용되는 메시지 형태와 동일하다..

3.4. COPS 기반 NGN RACF 를 통한 QoS 제어 특성

PD-FE 와 db 간 LDAP 구현 메커니즘을 사용한 가장 큰 이점은 분산적인 관리와 인증 및 보안이라 할 수 있다. 기존의 mysql 을 사용한 단순 database 는 표 1 에 나왔던 정책 및 사용자 database 가 일정의 기준이 없이 각 값 별로 나열이 되어 관리되었다. 물론, database 의 접근 역시 사용자의 id 만 알고 있으면 수정 등이 가능하여 인증 및 보안상의 큰 허점이 있었다. 하지만, LDAP 을 사용하면, LDAP 의 보안적 특징으로 단순 사용자 id 를 통한 접근 외에 시간의 제한, 특정 지정 ip 만의 접근 등을 설정, 사용이 가능하여 인증 및 보안상에 큰 장점을 가질 수 있게 된다.

PD-FE 와 PE-FE 간 COPS 구현 메커니즘을 사용했을 경우에는 기존의 단순히 각 기능들 사이에 정책을 넘겨주고 설정하는 차원을 넘어선 메시지 처리 기능을 지원한다. 즉, 결정 및 요청 관련 메시지 포맷을 COPS 형태의 요청(Req)메시지 및 응답 결정(Dec) 메시지로 구체적으로 설정하여 접근 인가 및 관련된 적절한 서비스를 제공할 수 있도록 한다. 그리고, COPS 프로토콜의 자신을 식별할 수 있는 특별한 객체로써의 접근을 통해, 프로토콜 자체의 다른 추가 변경 없이 다중의 클라이언트 즉, 여기서는 여러 PE-FE 들을 지원할 수 있도록 한다.

NACF 와 PD-FE 간의 연동 시에는 NGN 에서 현재 강조되고 있는 NACF 기능 처리를 위해서 COPS 가 굉장히 중요하다. 즉, NACF 의 중요 기능인 액세스 망의 인증처리를 위해 COPS 프로토콜의 인증 처리를 적용시킨다.

4. 결론

본 논문에서는 NGN 망에서의 정책 기반 QoS 관리 기술을 위한 각각의 기능들과 사용 프로토콜에 대해서 정의하고 구체적인 시나리오 및 메커니즘을 제안하였다.

기존의 LDAP 및 COPS 프로토콜을 고려하지 않았던 정책 기반 QoS 관리 기술에서는 여러 단점들이 있었다. PD-FE 에서 User DB 의 사용자 데이터 및 Policy DB 의 정책 데이터를 일반적인 DB 시스템으로 관리했던 방식은 효율적인 관리 및 보안적 측면에서 많은 취약점을 보여왔다. COPS 프로토콜을 적용하지 않았던, PD-FE 와 PE-FE 사이의 연동 역시, 효율적인 정책 적용 및 인증, 보안 처리 등에서 취약점이 있었다.

이를 보완하고 진보시키기 위해 LDAP 및 COPS 프로토콜을 적용시켜 두 프로토콜의 장점들을 이용할 수 있도록 하였다. 구체적인 메커니즘과 시나리오를 적용시켜 각 프로토콜이 적절하게 NGN 망에서 정책 기반 QoS 를 적용할 수 있도록 하였다. 또한, NACF 라는 기능을 추가시켜 COPS 프로토콜을 사용하여 PD-FE 와 NACF 사이에 사용자 인증을 지원할 수 있도록 하였다. 추가적인 LDAP 및 COPS 프로토콜, 그리고 NACF 기능의 연구를 진행하여 개발이 된다면, NGN 망에서의 정책 기반 QoS 관리 기술은 더욱 효율적으로 적용 될 수 있을 것이다.

참고문헌

[1] B. Moore et. al., “Policy Core Information Model - version 1 specification,” IETF RFC3060, Feb. 2001.

[2] Recommendation Y.2111 (formerly Y.RACF) Resource and admission control functions in Next Generation Networks, http://www.itu.int

[3] Recommendation Y.2012 (formerly Y.NGN-FRA) Functional requirements and architecture of the NGN

[4] D. Durham, Ed.,J. Boyle, R. Cohen, and et. al.,"The COPS (Common Open Policy Service) Protocol," RFC 2748, January 2000.

[5] J. Strassner et. al., “Policy Core LDAP Schema,” IETF Internet Draft, Oct. 2002.

[6] Policy Core Information Model Extensions”, http://www.ietf.org/internet-drafts/draft-ietf-policypcim-ext-08.txt

[7] Timothy A. Howes Ph.D., Mark C. Smith, Gordon S. Good “Understanding and Deploying LDAP Directory Services, 2nd Edition”, Addison Wesley, 2003

[8] S . Herzog, Ed., J. Boyle, R. Cohen, and et. al.,"COPS usage for RSVP," RFC 2749, January 2000.