대규모 IP 네트워크에서 정책기반의 네트워크 제어방법 연구

A Policy-based Network Control Methodology for Large-scale IP Network

오 준 석*, 손 춘 호, 김 기 응, 이 재 진
(Junsuk Oh, Choonho Son, Kieung Kim, Jaejin Lee)

Abstract : Many different types of network equipments are deployed in a large-scale IP network. In this operating environment, network service providers suffer from difficulty in controlling various equipments simultaneously in case network faults happen in their overall or regional network due to physical link failure or abnormal traffic. This paper presents a policy-based methodology to control many different types of network equipments at the same time in abnormal cases. The key idea is that NMS(Network Management System) keeps vendor-neutral control policies in normal times and that when an abnormal case occurs in network, NMS transforms the selected policy into vendor-specific control commands and enforces them to various equipments simultaneously.

Keywords: Network Control, Network Management, Internet Traffic Control, NETCONF

I. 서론

인터넷망은 서비스 제공자(Service Provider, 이하 SP)망, 기업망(Enterprise Network)및 개인가입자로 구성되어 있다. SP망의 규모가 커짐에 따라 다양한 기종의 망 장비가 놓이게 된다. 근래에는 액세스망의 고도화와 VoIP, VoD, IPTV, 파일공유 등 다양한 인터넷 서비스 도입으로 가입자당 점유 대역폭이 계속 증가하고 있다. 이와 더불어 인터넷망 고유의 보안 취약점으로 인하여 침해성 트래픽 또한 지속적으로 발생하고 있다. 이처럼 서비스 트래픽, 웜 및 DDoS(Distributed Denial of Service) 등의 공격성 트래픽의 증가는 SP들로 하여금 이벤트 발생시 효과적인 네트워크 제어 방안에 대하여 고민하게 한다. 한편, 인터넷기술이 진화함에 따라 인터넷 트래픽 제어 기술도 다양해 지고 있다. OSI 통신 계층별로 패킷의 헤더 정보를 기반으로 트래픽을 정적(Fixed) 또는 동적(Flexible)으로 필터링하고, 트래픽에 우선순위를 부여하거나 라우팅 경로를 변경시키는 기술들이 있다. 그러나 이러한 제어 기술들이 모두 표준화된 것은 아니라는 데에 문제점이 있다. 대규모 SP 망에는 여러 장비제조업체의 다양한 장비들이 놓이게 되는데 특정 제어기능을 지원하지 않는 장비가 있고 설령 제공한다고 하더라도 제어형식이 제각각 다르기 때문에 망을 관리해야 하는 SP 입장을 난처하게 만든다.

본 고에서는 대규모 인터넷 SP 네트워크에서 폭주 트래픽 발생시 이기종 장비를 효과적으로 제어하는 방법에 대하여 기술하고자 한다. 트래픽을 제어하는 방법으로는 망의 경계점에서 트래픽 출입을 제어하는 것과 망을 통과한 트래픽은 QoS제어와 경로(Path) 제어를 통해서 Drop이 발생하지 않도록 하는 방법이 있다. 본 고의 초점은 망의 경계점에서 트래픽을 제어하는 방법에 초점이 맞춰져 있으며 트래픽 제어기술, 정책 기반의 제어기술, 장비의 구성 변경기술 세 측면에서 기술 분석을 한 뒤에 네트워크 제어시스템의 Workflow 중심으로 제어방법에 대하여 기술하고자 한다.

* 책임저자(Corresponding Author)
논문접수 : 2008. 7. 25., 채택확정 : 2008. 8. 1.
오준석, 손춘호, 김기응, 이재진: KT 기술연구소
(jsoh@kt.com, choonho@kt.com, gekim@kt.com, jaejin@kt.com)

II. 관련연구

Schudel과 Smith는 인터넷 트래픽이 흐르는 평면을 Data Plane, Control Plane, Service Plane, Management Plane 등 네 가지로 구분하고 각각의 평면에 대한 트래픽 제어기술을 보안(Security)의 관점에서 기술하였다[1]. Data Plane은 End-to-End 사용자 데이터가 흐르는 평면으로 Interface ACL(Access Control List), Rate-Limit, Queuing 등의 기술로 트래픽을 효과적으로 제어할 수 있다. Control Plane은 라우팅 프로토콜이 주고받는 데이터가 흐르는 평면으로 장비와 장비간에 트래픽이 흐른다. 이 평면도 ACL 기술, IGP(Interior Gateway Protocol) 및 EGP(Exterior Gateway Protocol) 옵션 설정 등의 방법으로 트래픽 제어가 가능하다.

정책 기반의 네트워크 관리기술과 관련하여 IETF에서는 Policy Framework Working Group을 2004년 6월까지 운영하였으며[2], Policy Core Information Model 등의 표준화 작업을 완료하였다[3]. 여기에서는 Rule-set으로 구성되는 Policy의 데이터 모델 구조와 PDP(Policy Decision Point) 및 PEP(Policy Enforcement Point)와 같은 객체에 대하여 정의하고 있다.

장비의 구성(Configuration)을 변경(제어)하는 기술과 관련하여 IETF에서는 표준화가 진행 중에 있다. IP 네트워크 장비의 구성 변경은 주로 CLI(Command Line Interface)에 의하여 이루어진다. 이 CLI는 사람(운용자)를 위한 인터페이스이므로 텍스트 출력결과에 대한 판단능력이 없는 NMS(Network Management System)같은 응용프로그램이 사용하기에는 한계가 있다. IETF NETCONF(Network Configuration) Working Group에서는 응용프로그램이 XML기반으로 장비 구성을 제어하기 위한 프로토콜로서 NETCONF를 정의하였고[4], 2006년 12월에 표준화하였다[5]. 또한 IETF NETMOD(NETCONF Data Modeling Language) Working Group에서는 NETCONF가 주고받는 XML로 된 장비 구성 데이터 모델을 정의하고 있다[6].

III. 기술 분석

1. 트래픽 제어 기술

그림 1처럼 SP(Service Provider)의 인터넷망 경계점에는 국내 또는 해외의 다른 SP와의 접점 회선이 있고, 기업 또는 개인의 가입자회선이 있다. 망 경계점에 적용할 수 있는 보편적인 트래픽 제어 기술은 망경계장비의 인터페이스에 ACL(Access Control List)를 적용하거나 Rate-Limit 기술이 있다. ACL은 트래픽을 차단하는 기술이며 Rate-Limit은 전송율을 제한하는 기술이다. 이 두 기술은 Data Link 계층(Layer2) ~ Transport(Layer4) 의 헤더 정보 즉, MAC 주소, IP 주소, L4 Protocol 및 TCP/UDP 포트번호로부터 트래픽을 식별하여 차단(Deny) 또는 허용(Permit) 정책을 인터페이스에 적용할 수 있다. 이 두 기술은 대부분의 장비 기종에서 지원되고 있다.

트래픽 제어시 TCP/UDP 포트번호는 응용프로그램을 차단할 수 있는 정보이다. 그러나 곧 특정 응용프로그램이라는 등식은 성립하지 않는다. 예를 들어 근래에 트래픽 차단을 피하기 위하여 Well-known 포트-예를 들어 80포트-를 사용하는 P2P(Peer-to-Peer) 프로그램이 많이 개발되어 있다. 이처럼 점점 지능화되어 가는 응용프로그램(Application) 트래픽을 식별하기 위하여 패킷의 특정 비트열을 조사하는 FPM(Flexible Packet Matching)과 같은 고급 제어기술도 개발되어 있다[1]. 이것의 한계점은 특정 기종에만 적용될 수 있다는 것인데 점차 보편적인 제어기술이 되어야 할 것으로 판단된다.

이와 더불어 트래픽 식별 정보인 MAC주소, IP주소, TCP/UDP Port번호에 대한 사용정보 즉, MAC주소와 IP주소는 어떤 고객이 사용하는 것이며 TCP/UDP 포트번호는 어떤 응용프로그램이 사용하는 것인지 정보분석시스템으로 구축이 되어야 정확한 제어를 할 수 있다.

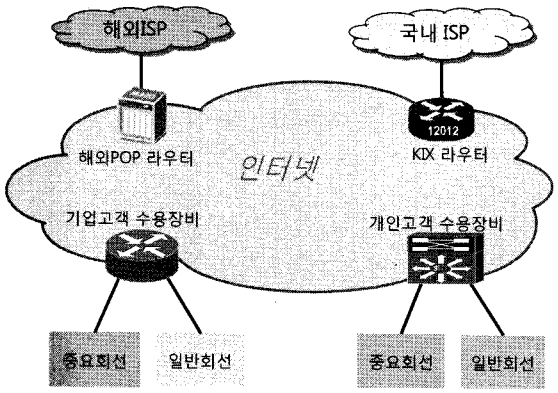


그림 1. 인터넷 가입자회선 및 망 경계회선 구분

2. 정책 기반 제어방법

트래픽으로 인한 망의 성능 장애가 광범위하게 발생했을 경우 다양한 이기종 장비를 신속하게 제어할 수 있어야 한다. 이를 가능하게 하는 것이 정책기반의 제어방법이다. 정책(Policy)은 룰(Rule)의 집합이며 룰은 조건(Condition)과 행위(Action)로 정의된다[3]. 예를 들어, A유형의 가입자회선에는 B유형의 트래픽만 허용한다라는 룰을 만들 수 있다. 대규모 망의 긴급상황에서 신속한 제어를 하기 위해서는 표 1의 예와 같이 모든 장비의 용도와 인터페이스 용도가 정확히 부여되어 있어야 한다. 장비용도와 인터페이스 용도를 룰의 조건으로 정할 수 있으며 행위(Action)으로는 인터페이스 ACL 또는 Rate-Limit를 정할 수 있다. 이때 MAC 주소, IP 주소, TCP/UDP 포트번호를 세부 행위 항목으로 부여할 수 있다.

표 1. 장비 및 인터페이스 용도 구분(예)

장비용도	인터페이스용도
기업고객수용장비	고속전용회선
	일반전용회선
	고속 메트로이더넷회선
	일반 메트로이더넷회선
개인고객수용장비	FTTH 회선
	ADSL 회선
	VDSL 회선
망 경계장비	해외ISP 회선
	국내ISP 회선

3. 장비 구성방법

네트워크를 제어하기 위한 최종 단계는 장비의 구성(Configuration) 정보를 변경하는 것이다. 장비의 구성정보를 변경하기 위한 방법으로는 표준 프로토콜인 SNMP(Simple Network Management Protocol), 장비기종별 CLI(Command Line Interface), XML기반의 NETCONF(Network Configuration Protocol)에 의한 것이 있다. 이 중에서 SNMP는 데이터 구조에 있어서 계층(Hierarchy)을 표현할 수 없고 전송 신뢰성이 부족한 UDP기반이라는 단점이 있어서 주로 감시용 프로토콜로 사용되고 있다. 그래서 라우터나 스위치 같은 인터넷 장비에 대한 구성 변경은 주로 CLI에 의해 작업된다. 이 CLI는 Text 기반이라서 사람과 상호작용이 편리한 반면, NMS(Network Management System)와 같은 응용프로그램이 장비를 제어하기에는 어려운 방식이다. 왜냐하면 CLI 입력 명령에 대한 출력 결과가 너무나 다양하고 예외상황에 대하여 정의된 에러코드가 없기 때문이다. 따라서 NMS가 CLI로 장비를 제어한다면 아주 제한적으로 명령어를 적용할 수 있다. 이러한 SNMP와 CLI의 단점으로 등장한 것이 NETCONF이다.

NETCONF는 4계층 구조를 갖는 프로토콜로서 전송(Transport) 계층, RPC(Remote Procedure Call) 계층, 운용(Operations) 계층, 콘텐츠(Contents) 계층으로 되어 있다[5]. 가장 하위 단의 전송 계층에서는 SSH(Secure Shell) 등의 인증과 데이터보안이 유지되는 프로토콜이 정의되어 있으며 장비 구성 변경을 위한 API(Application Programming Interface)를 원격에서 호출하기 위한 방법으로는 RPC를 사용하고, 그 상위 단의 운용 계층은 장비 구성을 변경하는 API(get-config, edit-config 등)를 정의하고 있다. 마지막으로 콘텐츠 계층에서는

실제 장비의 구성(Configuration)을 XML형태로 관리하고 있으며 DATASTORE로 불린다.

NETCONF는 기본적인 구성 변경 명령 외에 다양한 부가기능(Capability)을 정의하고 있다[5]. 대표적인 것이 Candidate, Rollback-on-error, Validation 기능이다. Candidate 기능은 장비의 메모리에서 실행 중인 실제 구성정보를 완전히 변경(Commit)하기 전에 테스트모드에서 운용해보기 위한 기능이며 Rollback-on-error는 구성정보 변경 중 에러가 발생할 경우 이전 상태로 복구하는 기능이다. 또한 Validation 기능은 구성 변경을 적용하기 전에 문법적 오류 등이 없는지를 확인해 보기 위한 기능이다.

장비를 제어함에 있어서 CLI 방식이건 NETCONF 방식이건 간에 Rollback-on-error 기능과 Validation 기능은 아주 중요한 필수기능이다. 그러나 NMS(Network Management System)에서 이 두 기능을 CLI 방식으로 개발한다고 하면 아주 복잡한 작업이 된다. 왜냐하면 모든 예외상황에 대한 케이스를 다 고려하여 Rollback을 위한 CLI 명령 절차를 만들어 놓아야 하고, 명령어 문법 오류에 대한 케이스 또한 고려하여 Validation 기능을 개발해야 하기 때문이다. 반면에 NETCONF의 경우는 이 어려운 기능을 장비의 부가기능으로 정의해 놓았다. 따라서 NMS에서는 장비의 해당 기능을 호출하고 리턴 값만 받으면 되기 때문에 개발 부담이 훨씬 줄어들게 된다. 그림 2는 CLI와 NETCONF 방식을 비교한 것이다. CLI의 경우는 NMS 개발부담이 큰 반면에 NETCONF의 경우는 장비 제조시 개발부담이 커지게 된다. 하지만 NETCONF 방식은 에러 처리를 분명하게 할 수 있고 표준안에서 정의하고 있는 다양한 부가기능을 제공할 수 있기 때문에 망관리 차원에서 바람직한 방향으로 판단된다.

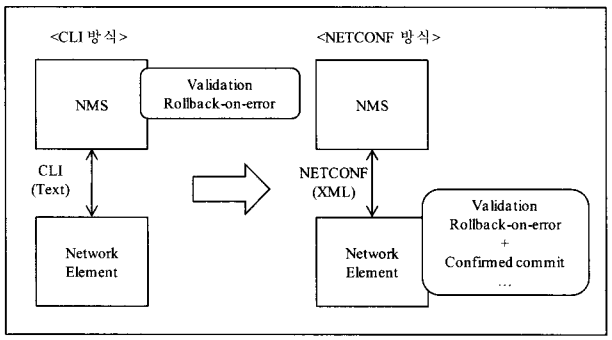


그림 2. CLI와 NETCONF 방식 비교

IV. 네트워크 제어 방법

앞서 분석된 세가지 기술 측면, 즉 트래픽 제어기술, 정책기반 제어방법 및 장비 구성방법을 고려하여 네트워크 제어 시스템의 Workflow를 정의하면 그림 3과 같다.

제어 정책 구성에서는 룰의 집합을 만드는데, 룰의 조건(Condition)에는 장비용도 및 인터페이스용도 등이 포함되고, 실행(Action)에는 인터페이스 ACL 및 Rate-Limit 트래픽 제어기술을 적용할 수 있다. 이때 제어기술의 실행(Action)의 매개변수(Parameter)로는 MAC주소, IP주소 및 TCP/UDP Port번호가 올 수 있다. 룰의 실행(Action) 부분을 구성하는 트래픽 제어기술과 매개변수는 장비기종에 상관없이 독립적인 내용이다.

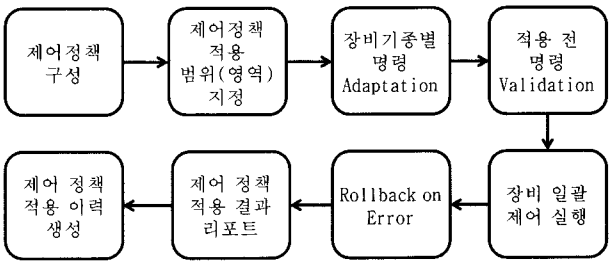


그림 3. 제어 시스템 Workflow

다음은 제어정책을 적용할 범위를 선택할 수 있어야 한다. 여기서 범위란 지리적 영역을 말한다. 각 영역마다 망의 경계회선들이 있으며 특정 제어정책을 제한적인 영역에 적용할 수 있어야 한다.

제어정책과 적용영역 범위가 정해졌으면 해당 장비에 명령이 내려갈 수 있어야 한다. 명령을 내린다는 것은 장비의 구성(Configuration)을 변경한다는 것을 의미한다. 장비마다 구성 문법(Syntax)이 제각각 다르기 때문에 NMS(Network Management System)에서는 장비 독립적인 제어정책을 장비기종의 OS(Operating System) 버전에 맞는 구성 명령으로 변환시켜주는 능력을 갖춰야 한다. 앞서 언급된 제어하고자 하는 IP주소나 TCP/UDP 포트번호 등은 장비기종과는 독립적인 매개변수이므로 이 매개변수를 NMS에 입력값으로 받아들이고 각 장비기종의 OS 구성 문법대로 명령을 생성시켜야 한다.

다음은 자동으로 생성된 장비기종별 제어 명령을 장비에 적용하기 전에 확인(Validation)하는 과정을 거쳐야 한다. 이는 장비의 구성을 변경하기 전에 한번 더 문법적 오류를 체크하기 위한 것이다. CLI 기반의 제어방식에서는 사람, 즉 운용자가 자동으로 생성된 구성 명령을 UI에서 직접 확인해 보는 방법 외에는 없다고 판단된다. 반면에 NETCONF 기반의 제어방식에서는 NETCONF의 Validation 부가기능을 호출함으로써 가능하다.

구성 명령에 대한 Validation 작업이 되었으면 제어대상 장비들에 대하여 일괄적으로 구성을 변경할 수 있어야 한다. 인터넷망의 비정상 상황을 해소하기 위하여 제어대상 장비들에 대하여 멀티쓰레드 또는 멀티프로세스 방식으로 신속한 제어를 할 수 있어야 한다.

다음으로 일괄 제어 작업을 하는 도중에 에러가 발생하면 원상태로 복구할 수 있어야 한다. 이것을 Rollback-on-error 기능이라고 부른다. CLI 기반의 제어방식은 이 기능에 대한 구현이 아주 난해하다. 왜냐하면 앞서 언급했듯이 CLI는 출력결과가 아주 다양하게 나타나기 때문이다. 따라서 CLI 방식은 입력에 대한 기대출력(Expected Output)을 미리 정의해 놓고 이 기대값에서 벗어나면 원상태로 복구할 수 있는 Rollback 명령을 생성해 놓아야 한다. 반면에 NETCONF 기반의 제어 방식에서는 NETCONF의 Rollback-on-error 기능을 사용하겠다고 선언함으로써 가능하다. 이와 더불어 NETCONF는 분산 트랜잭션과 같이 2-Phase Commit (또는 Confirmed Com-

mit) 기능을 지원할 수 있다. 이 기능을 활용하면 여러 장비를 동시에 제어할 때 한 장비에서 에러가 났을 때 모든 장비를 원상태로 복구시키는 것도 가능하다.

마지막으로 제어 정책에 대한 적용작업이 완료되었으면 제어대상 장비 각각에 대한 결과 리포트를 생성하여 운용자로 하여금 결과를 확인하게 하고 실패한 장비에 대하여 실패원인이 무엇인지 로그를 보여줄 수 있어야 한다. 명령 문법의 오류나 통신 장애 등의 원인을 정확히 분류하여 후속조치를 할 수 있는 환경을 제공해 주어야 한다. 적용 결과 리포트 기능과 함께 적용 이력을 관리하는 것도 적용된 제어 정책 해지 및 중복 제어 방지 차원에서 중요한 기능이다.

V. 결론

본 고에서는 대규모 IP 네트워크의 경계점에서 트래픽을 효과적으로 제어하기 위한 방법에 관하여 기술하였다. 트래픽 제어기술, 정책기반 제어방법 및 장비 구성방법 세가지 측면에서 기술 분석을 하였으며 이 기술을 활용한 네트워크 제어시스템의 Workflow를 제시하였다.

망 경계점으로는 가입자접점과 타 사업자와의 망 경계점이 있는데 이 경계점의 넘나드는 트래픽을 효과적으로 제어하기 위한 기술로서 정책 기반의 인터페이스 ACL(Access Control List)과 Rate-Limit 기술을 강조하였다. 제어기술과 더불어 트래픽 식별을 위한 MAC주소, IP주소, TCP/UDP 포트번호에 대한 사용정보와 정책 구성을 위한 장비용도 및 인터페이스용도 정보DB 구축은 네트워크 제어시스템의 필수적인 구성요소임을 나타내었다.

네트워크 제어의 최종 작업이 되는 장비 구성변경과 관련하여 CLI(Command Line Interface)방식과 NETCONF(Network Configuration) 방식에 대하여 비교 분석하였으며, NETCONF 방식은 NMS(Network Management System)의 향후 발전방향이 되어야 할 것으로 판단된다.

참고문헌

[1] G. Schudel and D. J. Smith, *Router Security Strategies- Securing IP Network Traffic Planes*, Cisco Press, USA, 2008.

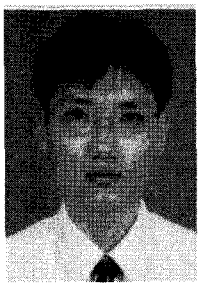
[2] IETF Policy Framework Working Group, http://www.ietf.org/html.charters/OLD/policy-charter.html

[3] B. Moore et al., "Policy Core Information Model", RFC 3060, IETF, February, 2001.

[4] IETF NETCONF(Network Configuration) Working Group, http://www.ietf.org/html.charters/netconf-charter.html

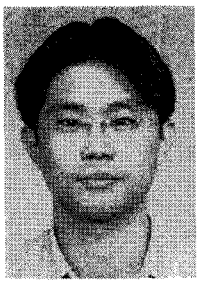
[5] R. Enns, Ed., "NETCONF Configuration Protocol", RFC 4741, IETF, December 2006.

[6] IETF NETMOD(NETCONF Data Modeling Language) Working Group, http://www.ietf.org/html.charters/netmod-charter.html



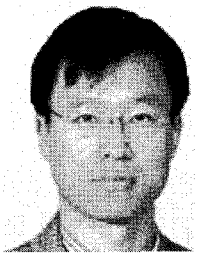
오준석

한국과학기술원 물리학과 학사
CMU/ICU 소프트웨어공학 석사
1997년 ~ 현재 KT 기술연구소 인터넷연구담당 선임연구원
<관심분야> 트래픽제어, MPLS VPN, QoS, 통신망운용관리



손춘호

연세대학교 컴퓨터과학과 학사
한국과학기술원 전산학과 석사
2006년 ~ 현재 KT 기술연구소 인터넷연구담당 전임연구원
<관심분야> 트래픽제어, QoS, 네트워크 모델링, 네트워크 보안



김기응

단국대학교 전자공학과 학사
단국대학교 전자공학과 석사
1989년 ~ 현재 KT 기술연구소 인터넷연구담당 수석연구원
<관심분야> 통신망운용관리, Multicast Network 관리기술, QoS, 트래픽제어

이재진

경북대학교 전자공학과 학사
경북대학교 전자공학과 석사
고려대학교 전자공학과 박사
1987 ~ 현재 KT 기술연구소 인터넷연구담당 상무
<관심분야> 인터넷 망관리, 네트워크 엔지니어링, 액세스 기술