

kr도메인 동적업데이트 시스템 설계 및 구현

정한라^o 서영진 송관호

한국인터넷진흥원

jhr^o@nida.or.kr, yjsuh@nida.or.kr, khsong@nida.or.krThe Design and Implementation of Dynamic Update System
for kr Domain NamesHanra Jeong^o Yungjin Suh Kwanho Song

National Internet Development Agency of Korea

kr도메인은 도메인이름체계상 “.” 루트(root)도메인 아래의 위치한 최상위 도메인(TLD, Top Level Domain)인 중 ccTLD(country code TLD)에 해당하는 도메인[1]으로 국제인터넷주소기관(ICANN, Internet Corporation for Assigned Names and Numbers) 산하의 인터넷할당번호관리기관(IANA, Internet Assigned Numbers Authority)으로부터 할당 받은 대한민국 대표 도메인이다. 이런, kr도메인은 한국인터넷진흥원(NIDA, National Internet Development Agency of Korea)내의 인터넷정보센터(KRNIC, Korea Network Information Center)에서 도메인등록관리시스템과 kr DNS (Domain Name Server)를 통해 안전하게 관리·운영되고 있다. 한국인터넷진흥원의 도메인등록관리시스템은 일반인이 등록한 kr도메인이름을 저장하고 관리하는 역할을 한다. 그리고 일정 시간 후 저장된 도메인이름을 대상으로 kr 존 파일(zone file)을 추출하고 이를 다시 kr DNS에 전송하는 역할을 담당한다. kr DNS는 전송된 존 파일을 검증하고 이상이 없으면 전송된 존 파일을 리로드(reloading)하여 등록 및 변경된 kr도메인이름에 대해 DNS(Domain Name System) 질의가 가능하도록 한다. 현재까지는 1일 3회에 한하여 kr 존 파일을 추출 반영하고 있다. 본 논문에서는 1일 3회 수행되는 배치(batch)작업 형태의 존 추출 프로세스를 5분 내외의 거의 실시간으로 이뤄지도록 하는 동적업데이트 시스템(Dynamic Update System)을 제안하고 그 설계 및 구현사항을 기술하고자 한다.

앞서 말한 것처럼 kr도메인은 우리나라 인터넷주소자원관리기관인 한국인터넷진흥원에서 관리 운영되고 있다. 그러나 일반인들이 kr도메인이름을 사용하기 위해서는 한국인터넷진흥원이 아닌 kr도메인 등록대행자를 통해서만 가능하다. kr도메인이름을 등록대행자를 통해 신청하면 그 데이터는 즉시 한국인터넷진흥원으로 전송된다. 한국인터넷진흥원은 전체 29개 등록대행자들과 안전하고 신속하게 도메인관련 데이터를 주고받기 위해 국제표준인 EPP(Extensible Provisioning Protocol)[2]에 기반한 통신프로그램을 사용한다. 이처럼 통신프로그램을 통해 전송된 데이터들은 패킷 및 데이터 자체의 무결성을 검증 후 도메인등록관리시스템의 데이터베이스에 저장된다. 이렇게 저장된 kr도메인이름은 Whois 서비스(<http://whois.nida.or.kr>)를 통해 즉시 조회가능하나 아직 kr네임서버에는 반영이 되지 않은 상태이므로 도메인을 이용한 서비스 및 DNS (Domain Name System) 질의는 불가하다. 1일 3회(8시, 12시, 18시), 도메인등록관리시스템은 그동안 들어온 데이터를 토대로 kr 존 파일을 생성하기 시작한다. 존 파일이 생성되면, 생성된 데이터를 master 네임서버로 전송한다. kr DNS는 master/slave 체계로 1대의 master 네임서버와 10대의 slave 네임서버들로 구성되어 있으며 master 네임서버는 내부에서만 접근 가능하다. master 네임서버는 등록관리시스템으로부터 넘어 온 존 파일에 대해 무결성 검사 후 이상이 없으면 네임서버 소프트웨어인 BIND 데몬의 reload 명령을 이용해 새로운 존을 적재하여 기존의 kr 존들을 갱신한다. 참고로, 현재 kr DNS에서 사용하는 네임서버 소프트웨어는 ISC(Internet Systems Consortium)에서 배포하는 BIND (Berkeley Internet Name Domain) 8 최신 버전[3]을 사용하고 있다.

BIND의 reload 명령은 master 네임서버로 하여금 새로운 존을 적재토록 하고 동시에 slave 네임서버들에게 notify 신호를 보내 존이 변경되었음을 알리도록 한다. slave 네임서버는 master 네임서버로부터 온 notify 신호에 대해서 일단 ACK 신호를 보낸 후, 갱신된 존에 대한 serial 번호를 요청한다. 그러면, master 네임서버는 변경된 존에 대한 serial 값을 slave 네임서버에게 보내고, slave 네임서버는 자신이 가지고 있는 해당 존에 대한 serial 값과 master 네임서버가 보내준 serial 값을 비교해서 master 네임서버의 serial 값이 클 경우, master 네임서버에 존 전송요청 메시지를 보내 새로운 존을 전송 받는다. serial 번호는 해당 존의 10자리 버전정보로 존이 얼마나 최신이나 아니냐를 판별하기 위해 사용된다. 존이 변경되면 serial 번호를 증가시켜 존이 최신임을 나타낸다. master 네임서버로부터 총 10대의 slave 네임서버로 존 전송이 끝나면 사용자가 등록 및 정보 변경한 kr도메인이름은 비로소 리졸빙이 가능하

다. 현재의 kr도메인이름 등록 및 변경 처리 프로세스는 앞서 기술한 것과 같이 상당한 시간을 필요로 한다. 즉, 일반인이 kr도메인이름 신청 및 정보 변경 시 도메인 등록DB에 저장되어 배치작업이 수행될 때까지의 시간, kr 존 파일이 추출되는 시간 master 네임서버의 존 리로딩(reloading) 시간, 각 존들을 master 네임서버에서 slave 네임서버들로 전송 되는 시간들을 기다려야만 한다

kr도메인에 대한 서비스 질과 고객만족도를 향상시키기 위해 한국인터넷진흥원에서는 오랫동안 동적 업데이트시스템 대한 연구와 테스트를 진행해 왔다 연구와 테스트에 오랜 기간 투자한 이유는 무엇보다도 네임서비스의 안정성을 고려하지 않을 수 없기 때문이다 현재는 1년여 이상 테스트베드에서 연구 및 테스트가 진행되어 만족할 정도의 안정성이 확보되었다

기존 도메인등록관리시스템과 동적업데이트 시스템의 차이점은 기존 시스템에 동적업데이트용 테이블(Request/Update Table) 및 업데이트 데몬들(Request/Update Deamon)이 새롭게 추가된 것이다. 변경된 처리방식은 다음과 같다 통신프로그램을 통해서 들어오는 도메인이름 신청 및 변경 요청 데이터는 한국인터넷진흥원 측의 통신 데몬에 의해 업무별조회/신규/변경 등)로 분류되어 기존 도메인 테이블과 새로 추가된 Request 테이블에 저장된다. 그리고 저장된 데이터는 동적업데이트 시스템의 주요 프로세스 중에 하나인 Request Process에 의해 10~20초 간격으로 Request 테이블에서 읽혀져서 master 네임서버로 보낼 데이터 형식으로 가공된 후 Update 테이블에 저장된다. 그러면, 동적업데이트 시스템의 또 다른 프로세스인 Update Process가 역시 10~20초 간격으로 Update 테이블의 내용을 읽어 와서 BIND의 nsupdate 명령을 이용해 master 네임서버로 변경 내용을 전송한다 전송 중 만약 에러가 발생하거나 master 네임서버로부터 에러 메시지를 받게 될 경우 트랜잭션은 Atomic 하게 롤백(roll back)되어 데이터의 일관성을 보장한다 전송된 내용에 이상이 없을 시 master 네임서버는 Update Process가 보낸 존 파일에 대해서 존 파일의 serial 값을 증가시킨 후 이미 메모리에 적재된 kr존 파일을 업데이트시키고, slave 서버로 존 업데이트에 대한 notify 신호를 보낸다. 그러면 slave 네임서버들은 곧바로 존 내용을 변경하여 kr도메인이름에 대한 정보 변경 절차를 마무리 짓는다 이때, master 네임서버에서 slave 네임서버들로 전송되는 데이터는 기존의 업데이트방식의 전체kr존 데이터가 아닌 kr존 중 일반사용자가 변경 요청한 일부 데이터다 master 네임서버는 BIND에서 제공하는 증진적 영역 전송(XFR, Incremental zone transfer) 방식으로 변경된 존 데이터만 slave 네임서버로 보내 존 전송 및 업데이트와 관련된 처리 시간을 단축시킨다[3] 그 결과 kr도메인 등록자는 도메인이름에 대한 등록 및 정보변경 신청 후 5분 내에 자신의 도메인을 기반으로 한 인터넷 서비스 및 비즈니스 활동을 할 수 있다 여기서 언급한 반영시간(5 분내)은 kr네임서버를 기준한 것으로 사용자 캐시네임서버의 경우에는 각 캐시네임서버 설정(보통 1시간마다 cache refresh)에 따라 어느 정도 차이가 있을 수 있다

그간 테스트베드에서 진행사항을 볼 때 동적업데이트 시스템은 안정성이나 성능 면에서 매우 우수한 시스템으로 평가된다. 그렇지만 애석하게도 실 서비스에 적용은 아직 시기상조이다 운영 환경의 개선이 필요하기 때문이다. 현재 kr네임서버는 BIND 8.x를 사용하고 있는데 동적업데이트를 적용하기 위해서는 master/slave 네임서버 모두를 최신의 multi-processing을 지원하는 BIND 9.x 버전으로 업그레이드 해야만 한다. BIND 8.x와 BIND 9.x의 주요 차이는 multi-processing을 지원하느냐 지원하지 않느냐다. BIND 8은 구동 및 운영 시 네임서버 데몬이 하나만 존재하여 모든 네임서비스를 처리한다 그러다보니 존 파일을 리로딩하면서 외부 질의에 대해서 응답을 못하는 상황이 벌어진다 그러나 multi-processing을 지원하는 BIND 9의 경우에는 named 데몬이 쓰레드(Thread) 형태로 여러 개 구동되어 리로딩과 외부 질의에 대한 응답을 동시에 처리 가능하다 뿐만 아니라 보안적인 측면도 강화되었다 동적업데이트 시스템을 도입할 경우 거의 매 시각 증진적 영역 전송 형태로 존 파일 업데이트가 이루어진다 이런 상황을 고려할 때 kr 네임서버의 BIND 9 업그레이드는 필수적이다 이에, 한국인터넷진흥원은 올 하반기 모든 kr 네임서버의 BIND 소프트웨어 버전을 BIND 9 최신버전으로 업그레이드 할 예정이다 또한, BIND 업그레이드가 마무리되면 동적업데이트 시스템을 실 서비스에 적용할 것이다 서비스 적용 시점은 12월 초로 예상된다.

참고 문헌

- [1] P. Mockapetris, Domain Names - Concepts and Facilities, RFC 1034, November 1987.
- [2] S. Hollenbeck, Extensible Provisioning Protocol (EPP), RFC 3730, March 2004.
- [3] P. Albitz and C. Liu, DNS & BIND, O'REILLY Press, 4th Edition, April 2001.