66th IETF 회의 참가보고서

2006년 9월

경북대학교 통신프로토콜연구실

김동필 (dpkim@cs.knu.ac.kr)

김상태 (saintpaul1978@mail.knu.ac.kr)

하종식 (mugal1@dgssm.org)

윤성식 (tothepolaris@cs.knu.ac.kr)

주수경 (jusukyoung@hanmail.net)

요 약

본 보고서는 경북대학교 통신프로토콜 연구실원들이 66차 IETF 회의 참가 후 작성한 보고서이다.

본 보고서는 2006년 7월 9일부터 14일까지 캐나다 몬트리올에서 개최된 제66회 IETF 표준화 회의의 참가보고서이다. 여기서는 tsv, shim6, mipshop, rserpool, dccp Working Group에서 다루고 있는 내용과 이번 회의에서 발표된 의제와 차후 진행 사항 등에 대해 기고한다.

목 차

1. 서론

제66회 IETF (The Internet Engineering Task Force) Meeting이 2006년 7월 9일 부터 7월 14일까지 캐나다의 몬트리올에서 개최되었다.

IETF에서는 차기 인터넷 표준기술 규격을 제정하기 위해 8개 주제의 130여 개 Working Group에서 각각 회의가 이루어진다. 인터넷 구조의 발전과 인터넷의 원활한 실행을 위한 표준화와 관련된 네트워크 설계자, 기술자, 제조업체 그리고 연구원들에게 넓게 개방된 국제적인 공동체라고 볼 수 있다.

본 문서에서는 tsv, shim6, mipshop, rserpool, dccp Working Group에서 다루고 있는 내용과 이번 회의에서 발표된 의제와 차후 진행 사항 등에 대해 기고한다.

2. TSVWG

2.1 WG 개요

- Transport Area는 기존의 워킹그룹의 범위에 존재하지 않거나, 새로운 워킹그룹의 formation을 정당화하지 않는 transport topic을 다루는 RFC의 개발과 publication을 위한 제안을 받아들인다. TSVWG은 IETF의 그러한 work item을 개발하기 위한 포럼으로서 serve한다.

TSVWG 메일링·리스트는 그것들이 발생하는 경우, 그러한 work item들에 대한 open discussion forum입니다. The working group은 논의를 요구하는 active한 제안이 있을 경우 meeting을 가진다. The working group milestones은 현재 work item들과 그것에 연관된 milestone을 반영할 필요로서 업데이트된다.

(A) Stream Control Transmission Protocol (SCTP)의 Maintenance는 SCTP 스펙의 버그 수정과, 표준 track에 따르는 진행을 포함하고 있다. 이러한 work item은 또한 SCTP에 대한 소수의 module extension을 포함하고 있다. 현재, 이것들은 socket API와 threat 분석문서와 같은 SCTP-ADDIP, SCTP-AUTH and SCTP-PADDING을 포함하고 있다. 안정된 스펙을 유지하기 위해서 TSVWG 내의 SCTP의 추가적인 연구는 Area Director approval을 요구한다.

(B) Resource Reservation Protocol (RSVP)의 Maintenance는 RSVP스펙의 버그 수정과 표준 track에 따르는 진행을 포함하고 있다. 이러한 work item은 또한 RSVP에 대한 소수의 module extension 또는 특정 어플리케이션 시나리오를 address하기 위한 자문문서를 포함하고 있다. 안정된 스펙을 유지하기 위해서 TSVWG 내의 RSVP의 추가적인 연구는 Area Director approval을 요구한다.

(C) IP Differentiated Services (DiffServ) 메커니즘의 Maintenance는 대개 특정 어플리케이션 시나리오 내에서 DiffServ의 사용에 관한 자문 문서를 포함하고 있습니다. DiffServ에 관계된 다른 work item들은 Area Director approval을 요구한다.

(D) 선택된 다른 work item들은 보통 역사적인 이유 때문에 TSVWG에 존재한다. 이work item들은 TCP를 위한 extended statistics MIB, 그리고 TCP와 IP를 위한 the quick-start 메커니즘을 포함한다.

본 보고서에서는 SCTP 관련부분만 다루도록 한다.

2.2 WG 표준문서

2.2.1 완료된 RFC

1) Stream Control Transmission Protocol (SCTP) Checksum Change (RFC 3309) (34670 bytes) updates RFC 2960

- 기존의 Adler-32 checksum 방식이 error detection 에 취약하여 32 bit CRC checksum 방식으로 변경한다.

2) Transport Layer Security over Stream Control Transmission Protocol (RFC 3436) (16333 bytes)

- RFC 2960 및 RFC 3309에 정의된 SCTP 상에서, RFC 2246에 정의된 Transport Layer Security (TLS) 프로토콜의 사용법을 기술한다. TLS의 유저는, SCTP에 의해서 제공되는 특징, 즉 line blocking의 head를 회피하는 multiple stream의 지원, network level fault tolerance를 제공하는 multi-homing의 지원을 이용할 수 있다. 게다가 IP주소의 동적인 재구축을 지원하는 SCTP의 확장의 논의도 지원된다.

3) SCTP Partial Reliability Extension (RFC 3758) (50999 bytes)

- SCTP endpoint가 peer에게 cumulative ack point를 앞으로 이동시키라는 signal을 보내는 것을 가능하게 하는 SCTP 확장에 대해 기술한다. SCTP association의 양측이 이 확장을 지원하는 경우, 그것은 upper layer 프로토콜에 부분적으로 신뢰할 수 있는 data 전송 서비스를 제공하기 위한 SCTP implementation에 의해 사용된다. 이 문서는 , INIT 및 INIT ACK, 새로운 FORWARD TSN chunk type을 위한 새로운 파라미터로 구성된 프로토콜 확장에 대해 기술하고, 이 메카니즘에 의해서 upper layer에 제공할 수 있는, 부분적으로 신뢰할 수 있는 서비스의 하나의 예를 제공한다.

4) Stream Control Transmission Protocol (SCTP) Specification Errata and Issues (RFC 4460) (215405 bytes)

- 6 개의 상호 운용적 사건과 5 년의 구현, 테스팅, SCTP 이용을 경험하는 동안에 발견된 문제를 편집한 것이다.

2.2.2 진행중인 Internet Draft

1) Stream Control Transmission Protocol (SCTP) Dynamic Address Reconfiguration (draft-ietf-tsvwg-addip-sctp-15.txt)

- SCTP 의 시나리오 확장을 위해, 존재하는 association 의 IP 주소정보의 형태 변경, 멀리 떨어져있는 primary path 의 설정, association 설정동안 adaptation layer 정보의 교환 등이 추가된다.

이러한 확장으로 인해, 물리적인 인터페이스 카드를 추가/삭제할 수 있는 계산적인 또는 네트워킹 플랫폼에 대해 기존의 association 의 인터페이스를 늘리는 우아한 메소드를 제공할 수 있다. IPv6 에 대해서는 기존의 association 의 renumbering 을 가능하게 한다. 또한, peer 가 primary 목적지주소를 설정하는 것을 요구하는 메소드를 제공하는데, 하나의 주소가 삭제되는 경우나 엔드포인트가 패킷을 받도록 준비된 주소에 대한 정보가 미리 정의되어있는 경우 유용하다. 마지막으로 이러한 특징은 엔드포인트가 association 설정 중에 정보교환을 허락함으로써 수정하지 않고 SCTP 의 유용성을 확장하는데 사용될 수도 있다.

2) Sockets API Extensions for Stream Control Transmission Protocol (SCTP) (draft-ietf-tsvwg-sctpsocket-13.txt)

- SCTP 의 mapping 을 기술한다. 소켓 API 는 많은 OS 에 적합한 인터넷 프로토콜의 표준 mapping 을 제공한다. SCTP 는 TCP 의 많은 특성을 제공할 뿐만 아니라 SCTP 는, TCP 의 특성의 대부분을 제공할 뿐만 아니라 UDP 에 가까운 semantic 을 섞은 새로운 프로토콜이다. 이 문서는 SCTP 를 이용하기 위해 기존 소켓 API 를 사상하는 방법을 정의한다.

3) Authenticated Chunks for Stream Control Transmission Protocol (SCTP) (draft-ietf-tsvwg-sctp-auth-03.txt)

- SCTP 의 새로운 chunk type, 몇몇의 파라미터와 프로시저를 기술한다. 새로운 chunk type 은 sender 와 receiver 사이에 공유되는 key 를 사용함으로써 SCTP chunk 를 인증하기 위해 사용됩니다. 새로운 파라미터는 공유되는 key 를 확립하기 위해서 사용된다.

4) Stream Control Transmission Protocol (draft-ietf-tsvwg-2960bis-02.txt)

- SCTP 는 IP 네트워크에서 PSTN signaling 메시지를 전송하기 위해 디자인되었으나, 폭넓은 application 에서 사용할 수 있습니다. SCTP 는 IP 같은 비연결성 packet 네트워크의 위에서 운용되는 신뢰성있는 전송 프로토콜이다.

SCTP 는 중복되지 않는 전송, MTU 크기에 알맞은 data fragmentation, multiple stream 내에서 순차적 메시지 전송, 여러 user message 를 하나의 SCTP 패킷으로 bundling, multi-homing 을 지원함으로써 네트워크 레벨에서의 결함을 포용 등의 서비스를 제공한다.

5) Padding Chunk and Parameter for SCTP (draft-ietf-tsvwg-sctp-padding-00.txt)

- padding chunk 와 padding parameter 를 정의하고, reciver 측에서 요구되는 프로시저들을 기술합니다. PAD chunk 는 path MTU 발견을 위해 사용된다.

2.3 66차 IETF 회의 논의 사항

2.3.1 가. 회의 Agenda

TSVWG Agenda for IETF 65 (Montreal)
Monday July 10th, 2006
0900-1130

1) Chair's 9:00-9:15
Agenda Bashing (15 min)
NOTE WELL
Document Status and Accomplishments
New Charter
New Milestones

2) Kwok - Aggregation of Diffserv Service Classes 9:15-9:25
draft-ietf-tsvwg-diffserv-class-aggr-00 (10 min)

3) Randy and Michael - 2960bis and SCTP Padding Chunks 9:25-9:40
draft-ietf-tsvwg-2960bis-02 (15 min)
draft-ietf-tsvwg-sctp-padding-00

4) Marushin - SCTP ASCONF Chunk Transmission Ext. 9:40-9:45
draft-marushin-sctp-asconfext-01 (5 min)

5) Randy and Michael - SCTP Threats and Socket 9:45-9:55
draft-ietf-tsvwg-sctpthreat-00 (10 min)

6) Francois - RSVP Extensions for Emergency Services 9:55-10:05
draft-lefaucheur-emergency-rsvp-02 (10 min)

7) Bob - Policing and Accountability for Causing Congestion on Borders
draft-briscoe-tsvwg-re-ecn-tcp-02 10:05-10:25
draft-briscoe-tsvwg-re-ecn-border-cheat-01 (20 min)
draft-briscoe-tsvwg-re-ecn-apps-00

8) Bob and Phil - Controlled Load 10:25-10:45
draft-briscoe-tsvwg-cl-phb-02 (20 min)
draft-briscoe-tsvwg-cl-architecture-03

9) Francois - RSVP Ext for Admission Control over DS using PCN 10:45-10:55
draft-lefauchuer-rsvp-ecn-01 (10 min)

10) Georgios - Resource Unavailability PDB 10:55-11:05
draft-karagiannis-ru-pdb-02 (10 min)

2.3.2 논의된 내용 정리

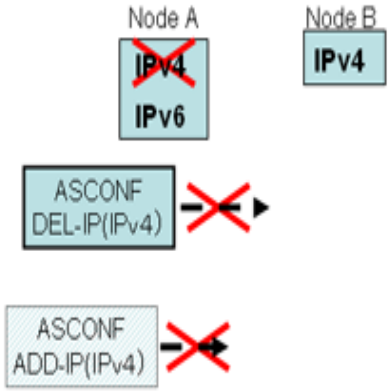
1) Randy and Michael - 2960bis
가) 변경사항
- 빠졌던 Adler-32가 CRC32c로 변경
- 빠졌던 article 또는 2~3개의 type과 문법 교정
- 나타나지 않았던 섹션이 다시 나타나게 함
- Refernece가 RFC1750에서 4086으로 업데이트
- 명료성을 위해 공백 추가
- CRC32c의 코드가 appendix 뒤에 추가

나) 향후 진행방향
- 최후 점검 및 WG으로부터의 comment가 필요
  - RFC 2960, 3309, 4460에서 빠트린 것
  - XML로의 conversion이 발생시킨 문제점

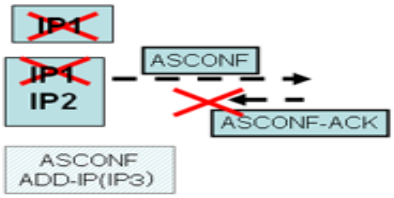
2) Randy and Michael - SCTP Padding Chunks
가) 변경사항
- 지난 회의에서 논의된 motivation이 추가되지 않음
- PMTU discovery를 위한 요구

나) 향후 진행방향
- TWGLC는 WG가 한가할 때 진행

3) Marushin - SCTP ASCONF Chunk Transmission Ext
가) 논의사항
- ASCONF transmission의 한계
  - 미해결된 ASCONF chunk가 있을 때 새로운 ASCONF chunk를 보내는 것은 금지

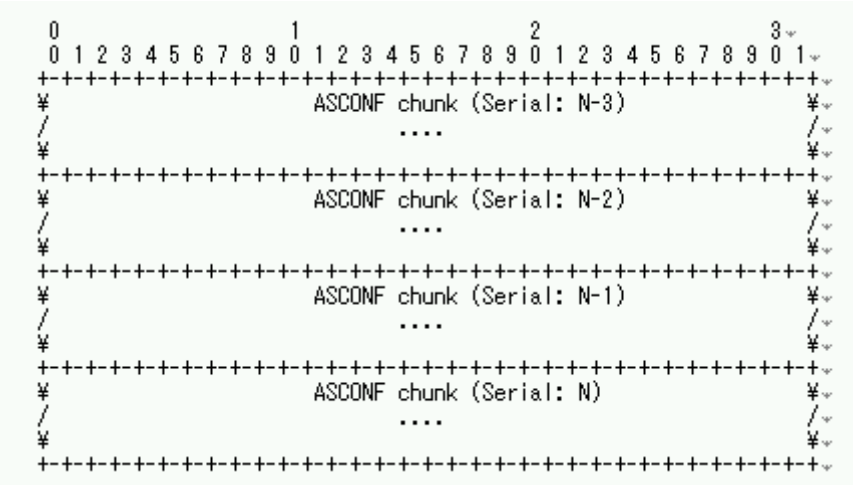


- IPv4와 IPv6를 지원하는 노드 A와 IPv4만 지원하는 노드 B가 있을 때, 노드 A가 IPv4 주소를 잃어버리면 다른 IPv4 주소를 얻어야 하지만, A는 IPv6 주소만 가지고 있으므로 ASCONF를 전송할 수 없다. 한번 이런 일이 일어나면 따라오는 ASCONF 또한 block된다.

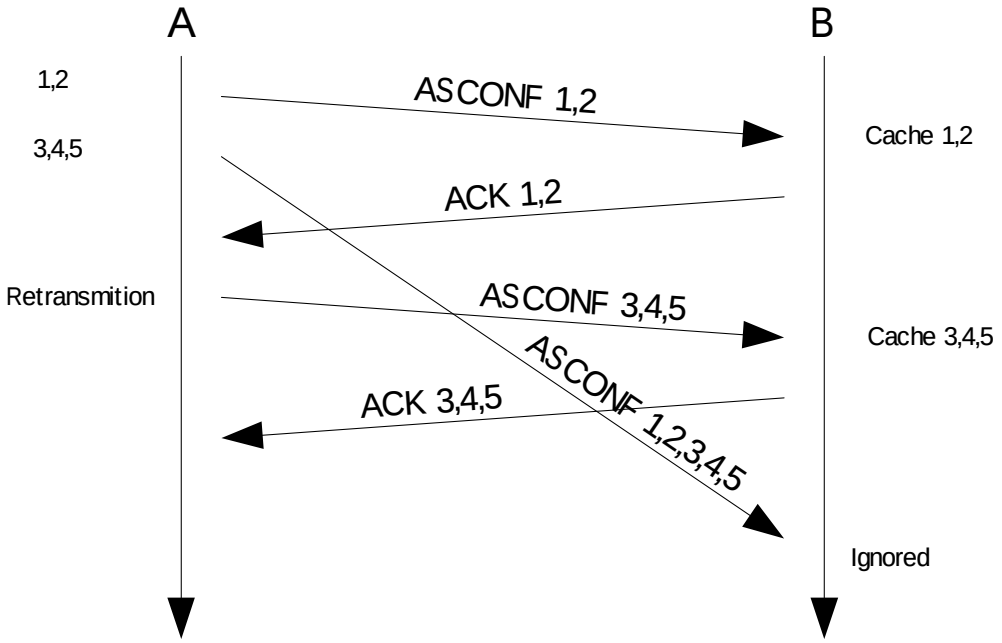


- 노드는 하나의 interface와 하나의 IP주소만을 가지고, interface가 다운되면 노드는 새로운 주소를 얻어야 하지만, ASCONF-ACK가 return되지 않아서 주소는 연결 불가능이 된다. 다른 주소를 얻어도 ASCONF는 전송할 수 없다.

- Cumulative ASCONF chunk



- ASCONF를 bundling 할 때, 모든 미해결 ASCONF는 순서대로 bundle되어야 함
- ASCONF_ACK는 bundled ASCONF의 source 주소로 return되어야 함
- Receiver는 ASCONF_ACK를 모든 ASCONF에 대하여 보내주어야 함
- ASCONF_ACK 또한 bundle되어야 함



4) Randy and Michael - SCTP Socket

가) 변경사항

- Spelling 문제 수정
- 새로 확장된 sndrcvinfo 추가
- next_flags, next_stream, next_associd, next_length, next_ppid 추가
- 4개의 새로운 소켓 옵션
- next_xx 필드가 유효하는 지를 나타내는 flag
- SCTP_GET_PEER_ADDR_INFO은 주소와 함께 사용되고 assoc-id가 사용되지 않을 때 assoc-id가 return되는 상태에 추가된 설명을 가짐.

나) 향후 진행방향

- 문서는 AUTH, ADDIP, 2960bis WGLC를 기다린 후, 얼마 후에 배포될 예정
- 이 문서는 BIS, ADD-IP, AUTH 만을 cover함
- socket API 확장을 요하는 SCTP의 추후 확장은 변경사항을 기술한 문서의 한 섹션에서 다뤄져야 함.
- 아직 보안 섹션에 일부 delivery API의 적합한 구현을 위한 작은 비트를 추가할 필요가 있음

4) Randy and Michael - SCTP threats

가) 변경사항

- WG 문서로 만들어졌으며, 문서는 거의 변경된 것이 없음
- 2960 과 ADD-IP의 알려진 모든 threats를 다룸
- 대응책이 2960Bis와 ADDIP에 AUTH와 함께 포함
- 한 공격이 아직 대비되지 못함 : 큰 INIT-ACK에 비해 작은 INIT로 행해져야 함
- padding draft가 프로시저를 가지지 않은 메커니즘을 가짐

나) 향후 진행방향

- 문서는 완성되었으며, 이 문서는 RFC4460과 진행중인 BIS 작업처럼 SCTP에서의 변경에 배경을 제공

- WGLC는 WG가 한가할 때 진행

3. shim6

3.1 Summary of the WG ‘shim6’

멀티호밍(Multihoming)이란 어떤 사이트(site)[1]나 단말이 하나 이상의 ISP(Internet Service Provider)로부터 두 개 이상의 연결성을 확보하는 것을 의미한다. 멀티호밍은 그것이 적용되는 네트워크 계층에 따라 통신 사업자 수준의 멀티호밍, 사이트 수준의 멀티호밍, 단말 수준의 멀티호밍으로 나누어 볼 수 있다. 멀티호밍은 그 적용 분야에 따라 목적이 조금씩 다르겠지만 대체로 다음과 같은 장점을 제공한다:

- ✓ 물리적인 링크의 중복성(redundancy)을 통한 오류 복구(fault tolerance)
- ✓ 네트워크 부하의 공유 및 분산 (load sharing and balancing)
- ✓ 다중 인터페이스 사용을 통한 네트워크 접속 투명성 제공
- ✓ 대역폭 증가
- ✓ 이동성 지원

이러한 장점들로 인해 멀티호밍 기법은 이미 대부분의 사이트에서 이루어지고 있다. 특히 WLAN, CDMA, WiBro 등 다양한 액세스 기술이 융합된 NGN 환경으로 다가갈수록 멀티호밍의 요구사항은 더욱 증가될 것이며, 이종 망간의 이동성까지 고려할 때 멀티호밍에 관한 요구사항은 지금과 같이 사이트 수준뿐만 아니라 단말 수준에 이를 것으로 예상된다.

현재의 IPv4 네트워크에서의 사이트 멀티호밍은 BGP(Border Gateway Protocol)에 의해 자연스럽게 제공되고 있다. BGP는 AS(Autonomous System) Number가 다른 자치 네트워크 간에 서로 라우팅 정보를 주고 받아 도메인 간 라우팅을 가능하게 하는 프로토콜이다. BGP 프로토콜을 사용하면, 멀티호밍을 구성한 사이트와 연결된 ISP는 자신이 서비스하는 것보다 더 긴 IP 주소 블록과 자신이 서비스하지 않는 IP 주소 블록을 상위로 전달하는 것 만으로, 특별히 다른 메커니즘이 필요 없이 간단히 멀티호밍을 지원할 수 있게 된다. 반면, BGP를 사용한 멀티호밍 방법은 DFZ(Default-free zone)[2]에서의 라우팅 테이블의 급증을 초래하는 심

[1] 본 보고서에서 사용되는 사이트(site)란 특정 IP 망에 대한 운영과 어드레싱(addressing) 계획 및 라우팅(routing) 정책 등을 수행하는 네트워크 Entity를 의미하며 이는 RFC 3852 “IPv6 Site-Multihoming Goals[3]”의 정의를 그대로 따른다.

[2] DFZ (Default-free zone)는 기본 경로를 사용하지 않고 “full BGP table”을 가지고 있는 코어 네트워크 또는 “full BGP table” 자체를 지칭한다.

각한 단점을 가지고 있다. IETF에서는 이 문제를 해결하기 위하여 RFC 2260 “Scalable Support for Multi-homed Multi-provider Connectivity)” 표준의 제정으로 다중 연결된 ISP 중 하나에 문제가 발생한 경우에만 라우팅 정보를 상위로 전달하는(Auto-route injection) 방법을 제시하였다.

IPv6는 프로토콜의 특성상 한 호스트가 여러 주소를 가질 수 있으며, IPv4의 CIDR[3]과 같이 ISP를 중심으로 계층적으로 구성이 되어있다. 그러나 IPv6의 주소는 128bit로 IPv4보다 4기존의 것 보다 훨씬 더 많은 Network Prefix 들로 인해 기존의 방법대로 멀티호밍을 구성하는 것은 확장성 면에서 문제가 있음을 쉽게 알 수 있다. IETF에서도 RFC 2772, “6Bone Backbone Routing Guidelines”을 표준으로 제정하여 6Bone(IPv6 Backbone Network)에서 다음과 같은 기존 IPv4 방식의 멀티호밍을 금지하고 있다:

- ✓ ISP는 다른 ISP의 IP 주소 블록을 상위로 절대 전달하지 않는다.
- ✓ 사이트는 그들이 할당 받은 IP 주소 블록보다 긴 주소 블록을 상위 ISP에게 절대 전달하지 않는다.

이 두 가지 제한으로 인해 IPv6 멀티호밍을 위해서는 다른 해법이 필요한 상황이고, IETF에서는 우선 IPv4 멀티호밍 표준인 RFC 2260을 IPv6에 맞게 수정한 RFC 3178 “IPv6 Multihoming Support at Site Exit Routers”을 제정하였다. 이것은 멀티호밍을 구성한 사이트의 출구 라우터(Exit Router)와 해당 사이트에 연결된 ISP간의 터널링 인터페이스를 사용하여 ISP의 문제 발생시 연결성을 보장하는 방법이다. 이 방법은 멀티호밍 자체는 해결할 수 있지만 터널링에 따른 성능 저하나 ISP 자체의 문제에는 대처하지 못하며, 특히 멀티호밍의 다른 장점인 부하 분산 및 공유, 이동성 지원 등 많은 부분에서 다른 해결책이 요구되고 있다.

이와 관련하여 IETF Multi6(Site Multihoming in IPv6) WG에서는 여러 가지 해결책에 관한 기고서를 제안 받았다. 대표적으로 MIP(Mobile IP)의 binding을 이용한 방법, IPv6의 Router Renumbering에 의한 방법, 멀티호밍을 지원하는 L4계층의 프로토콜인 SCTP(Stream Control Transmission Protocol)을 이용하는 방법 등이 있으나 Multi6에서는 HIP(Host Identity Protocol)의 ID/Locator의 분리 개념을 도입하고, 하나의 ID와 여러 Locator간의 매핑(mapping) 정보를 L3와 L4계층 사이에 추가하는 Layer 3 Shim (L3Shim) 해법을 제안하였다. Shim6(Site Multihoming by IPv6 Intermediation) WG는 이러한 L3Shim 해법에 관한 표준화를 진행하기 위하여 Multi6 WG 후속으로 시작이 되었다.

Shim6 WG에서는 L3Shim을 사용한 멀티호밍의 요구사항으로 크게 다음과 같은 것들을 언급하고 있다.

- ✓ IPv6만을 고려하며 IPv6 NAT 장치는 없다고 가정

[3] 기존의 IP 주소 할당은 Class 단위로 이루어 졌으나, Class C (24bit network prefix) 주소의 사용이 증가함에 따라 라우팅 테이블이 지수 배로 커지는 문제가 발생하여 현재의 IP 주소 할당은 CIDR(Classless Inter-Domain Routing) 방식을 따른다.

- ✓ 기존에 존재하는 세션과 새로 설정하는 세션의 Re-homing의 처리
- ✓ 상위 계층에서는 고정된 ULID(Upper Layer Identifier)만 볼 수 있으며 Shimm 계층 아래의 주소 변경은 볼 수 없다.
- ✓ 수많은 멀티호밍 지원 사이트들이 존재하는 경우에도 전체 라우팅 시스템이 지원할 수 있게 확장성을 고려한다.
- ✓ Shim6를 지원하는 노드가 이동성 지원을 위해 MIPv6를 사용할 수 있지만 이동성에 관련된 부분은 직접적으로 다루지 않는다.
- ✓ 정적 또는 동적인 주소를 다루는 최적화된 방법을 제안한다.

이 외에도 언급되고 있는 요구사항들은 Shim6 WG Charter를 참조한다.

3.2 Introduction to shim6 WG Documents

초기에 채택되었던 드래프트 문서들(Architecture, Functionality 등)은 현재 유효기한이 만기가 되어서 현재 유효한 Shim6 WG의 WG 문서들은 다음과 같다.

- ✓ Level 3 multihoming shim protocol
  - Shim6의 기본 프로토콜 규격문서로, 전체적인 설계의 목적과 프로토콜에 관한 개요, 세세한 메시지 형식 등을 다룬다.
- ✓ Hash Based Address (HBA)
  - 멀티호밍을 지원하는 사이트가 Prefix가 서로 다른 여러 개의 주소를 안전하게 바인딩(binding) 하기 위한 방법을 다룬다. 기본적인 아이디어는 주소 자체에 여러 Prefix정보를 포함하는 것이며, 이를 위해 사용 가능한 Prefix들과 난수(random number)를 사용하여 생성한 Hash Digest를 Interface ID라 정의하고 이 Interface ID 앞부분에 각각의 Prefix를 추가하여 생성한 여러 개의 주소를 HBA(Hash Based Address)라고 부른다.
- ✓ Failure Detection and Locator Pair Exploration Protocol for IPv6 Multihoming
  - Shim6를 사용하여 통신 중인 두 호스트간의 실패탐지(Failure Detection)와 새로운 주소 쌍으로의 전환을 위한 조사(Exploration) 규약을 정의한다.
- ✓ Default Locator-pair selection algorithm for the SHIM6 protocol
  - Shim6를 지원하는 두 Endpoint간에 기본적인 통신을 위한 Locator 쌍의 결정에 관한 문서로, 기본적인 고려사항과 실제 Locator쌍을 결정하는 알고리즘들 다룬다.
- ✓ Applicability Statement for the Level 3 Multihoming Shim Protocol
  - IPv6 네트워크에서 멀티호밍의 지원을 위한 Shim6 프로토콜의 적용 가능성을 논의하는 문서로서, 응용 시나리오 및 Shim6의 Capability, 멀티호밍 지원은 위한 다른 프로토콜과의 연동 문제 등을 다룬다.

현재까지 RFC로 승인된 것은 없고 HBA문서만이 AD(Area Director) Evaluation과정에 있다.

3.3 Discussion about shim6 at the meeting

3.3.1 Agenda

1) Administriva (5 minutes)
   - Mailing list: http://ops.ietf.org/lists/shim6/
   - Scribe?
   - Blue Sheets
   - Agenda Bashing

2) Status of "base specification" document set (15 minutes)

   A. Level 3 multihoming shim protocol
      http://www.ietf.org/internet-drafts/draft-ietf-shim6-proto-05.txt

   B. Hash Based Addresses (HBA)
      http://www.ietf.org/internet-drafts/draft-ietf-shim6-hba-01.txt

   C. Failure Detection and Locator Pair Exploration Protocol for IPv6 Multihoming
      http://www.ietf.org/internet-drafts/draft-ietf-shim6-failure-detection-05

3) SHIM6 Applicability

   A. Applicability (Marcelo Bagnulo, Joe Abley) (15 minutes)
      Applicability Statement for the Level 3 Multihoming Shim Protocol
      http://www.ietf.org/internet-drafts/draft-ietf-shim6-applicability-01.txt

4) SHIM6 Implementation Report (10 minutes)

   A. Progress report on SHIM6 Implementation, Taewan You (ETRI)

5) SHIM6 Extension Drafts

   A. Locator Pair Selection (Marcelo Bagnulo) (15 minutes)
      Default Locator-pair selection algorithm for the SHIM6 protocol
      http://www.ietf.org/internet-drafts/draft-ietf-shim6-locator-pair-selection-00.txt

   B. ESD (Erik Nordmark) (15 minutes)
      Extended Shim6 Design for ID/loc split and Traffic Engineering
      http://www.ietf.org/internet-drafts/draft-nordmark-shim6-esd-00.txt
      ** Eric wont be able to make it this time around - so the chairs
         will request WG comments on the draft

   C. Ingress Filtering (Marcelo Bagnulo) (10 minutes)
      Ingress filtering compatibility for IPv6 multihomed sites
      http://www.ietf.org/internet-drafts/draft-bagnulo-shim6-ingress-filtering-00.txt

   D. Privacy Analysis (Marcelo Bagnulo) (10 minutes)
      Privacy Analysis for the SHIM6 protocol

http://www.ietf.org/internet-drafts/draft-bagnulo-shim6-privacy-00.txt

E. Socket API (Shinta Sugimoto) (15 minutes)
Socket Application Program Interface (API) for Multihoming Shim
http://www.ietf.org/internet-drafts/draft-sugimoto-multihome-shim-api-00.txt

6) WG Direction

3.3.2 Results

1) Status of "base specification" document set

Hash Based Address draft 문서는 지난 2005년 10월에 WG Last Call을 거쳐 현재 AD(Area Director) Evaluation 중이고, Protocol Specification 문서는 2006년 초에 WG Last Call을 통과했고 Failure Detection과 Locator Pair Exploration은 아직 Last Call를 통과하지 못했다.

그러나 AD에 의해 Protocol Specification 문서는 Last Call을 통과하지 못한 나머지 두 문서와 함께 검토되어야 한다고 요청되어서 이번 회의에서는 나머지 3개의 Shim6 기본 규격 문서들(Protocol Specification, Failure Detection and Locator Pair Exploration)에 대한 WGLC(Working Group Last Call)을 위한 요청을 했지만 CGA와 HBA간의 IPR 문제, IPsec과 ULID, HBA의 보안성 검토 등의 이유로 합의를 이루지 못했다.

2) Ingress Filtering and Exit Path Selection (Marcelo Bagnulo)

이 문서는 네트워크에서의 Ingress Filtering과 이미 멀티호밍을 구성한 레거시 사이트들과의 연동에서 발생하는 문제를 다루는 방법들을 논의한 것으로, 이번 회의를 통해 WG Document로 요청이 되었다.

3) Socket API for multi-homing Shim (Shinta Sugimoto)

이 문서는 Shim6를 사용한 멀티호밍의 지원을 위한 Socket API의 규격이며, 이번 회의를 통해 WG Document로 요청이 되었다.

3.3.3 Future Work

회의의 마지막 부분에서 Shim6 WG의 방향에 관한 논의가 약간 있었는데 그것은 이미 기본 규격이 상당한 분량으로 작성되었으므로 정말로 필요한 경우 외에는 추가하지 않도록 한다는 것이다. 또한 조금 더 표준화 진행에 속도를 내어 기본 규격에만 머무르지 말고 구현 사례와 정용성에 관한 Feedback을 좀더 받자는 논의가 오고 갔다.

또한 기본 규격들이 WGLC를 거칠 수 있도록 앞서 나왔던 문제점들에 대한 해결책을 강구해야 할 것이다.

4. mipshop

4.1 MIPSHOP WG 개요

Mobile IPv6 는 IPv6를 지원하는 이동 단말이 새로운 IP 영역으로 이동하더라도 기존의 IP 영역에서 부여 받은 IPv6 주소를 지속적으로 사용할 수 있도록 하는 IP 이동성 지원 프로토콜이다. 일반적으로, 이동 단말이 이종 망 네트워크 환경에서 기존 영역에서 다른 IP 영역으로 이동할 때, Mobile IPv6 기법에 의해 IP 이동성이 지원되더라도 핸드오버 수행 기간동안 Signaling 오버헤드나 데이터 손실 및 네트워크 지연 등이 빈번히 발생하게 된다.

IETF MIPSHOP WG에서는 Mobile IPv6 동작 중에 발생하는 Signaling 오버헤드나 상대적으로 많은 양의 데이터 손실 등을 보완하기 위해 Mobile IPv6의 확장된 버전의 IPv6 기반 핸드오버 지원 프로토콜 개발에 주력하였다. 이러한 노력으로 Hierarchical Mobile IPv6 (HMIPv6, RFC 4140) 와 Fast Hierarchical Mobile IPv6 (FMIPv6, RFC 4068) 프로토콜들을 설계하고 Experimental RFC로써 표준화하였다.

HMIPv6는 Mobile Node (MN)과 Home Agent (HA), 그리고 하나 이상의 Correspondent Node (CN)간에 발생되는 핸드오버 Signaling의 양과 핸드오버 수행 시간을 줄일 수 있도록 설계되었으며, FMIPv6는 MN이 새로운 링크에 대한 연결 설정을 완료한 후, 곧바로 기존 링크에서 새로운 링크로 IP 연결성을 보장해 줌으로써 핸드오버 수행 중 데이터 손실을 줄일 수 있도록 설계되었다.

더욱이, 현재 MIPSHOP charter에서는 앞서 표준화한 FMIPv6와 HMIPv6가 IEEE 802.11 네트워크에서 어떻게 동작하는지에 대한 구체적인 시나리오에 대한 문서를 Informational RFC로 표준화하였다. 현재까지, 본 WG에서는 FMIPv6와 HMIPv6에 대한 더 많은 구현결과를 가지고 많은 성능 분석을 수행하고 있으며, IEEE 802.11네트워크 뿐만 아니라, 향후 차세대 무선 접속 기술로써 기대되고 있는 IEEE 802.16(e) 및 다른 무선 접속 기술과의 연동 시나리오에 대해 표준화를 진행시킬 것을 향후 MIPSHOP의 charter에 포함하고 있다.

뿐만 아니라, 현재 IEEE 802.21 Media Independent Handoff (MIH)서는 이기 종의 무선 접속 기술들을 지원하는 이동 단말환경에서 핸드오버를 지원하기 위해 L1 과 L2 계층 및 상위 계층에서 요구되는 핸드오버 지원 요구 사항들을 분석하고, 이들을 MI (Media Independent) Event Service (MIES), MI Command Service (MICS), and MI Information Service(MIIS)등으로 정의하고 분류하였다. MIES는 하부 계층에서 발생되는 상태 변화에 대한 정보를 이벤트 형식으로 구성하여 적절한 핸드오버나 무선 통신을 제공하도록 하고 있으며, MICS는 이동 단말이 하부 계층의 상태 변경을 요구할 때 Commend 형식으로 구성하여 제공하는 정보 교환으로써, 하부 계층에 더 많은 MIES 정보를 요구할 때 사용될 수 있다. 마지막으로, MIIS는 현재 속해 있는 서비스 네트워크의 위치 정보나 topological 정보를 제공하는 MIH의 서비스 중 하나이다.

향후, MIPSHOP에서는 IEEE 802.21 MIH WG과 연계하여 MIH에서 진행 중인 핸드오버 지원에 대한 서비스 요구 사항들을 분석하고, MIH 서비스 기반의 FMIPv6 및 HMIPv6 기반 IP 핸드오버 지원 시스템에 대한 추가적인 표준화작업을 진행할 예정이다. 이를 위해,

MIH서비스에 대한 정보를 전달하기 위해 추가적인 프로토콜을 설계할 예정이며, CN이 MIH 서비스를 지원하지 않더라도 L3 레벨에서 FMIPv6 와 HMIPv6에 의해 MIH 기반 IP 핸드오버를 지원할 수 있도록 하는 표준을 제정할 예정이다.

MIPSHOP WG의 표준화 진행을 위한 Working Items들은 다음과 같다.

1. HMIPv6의 추가적인 보완 작업 및 이를 새로운 표준에 반영
   A. MN-MAP 보안 고려사항에 추가 작업
   B. 기존의 HMIPv6에 대한 보완
2. FMIPv6의 추가적인 보완 작업 및 이를 새로운 표준에 반영
   A. AAA 프로토콜과 SeND의 보안 Key를 이용한 MN-AR (Access Router) 보안 문제에
   B. 기존의 FMIPv6 표준의 보완
3. Informational RFC 반영을 위한 서로 다른 링크 계층상에서 FMIPv6 응용 프로그램 개발
   A. IEEE 802.16e 와 3G CDMA 2K 네트워크 연동 시나리오
3. 보안이 강화된 MIPv6 Return Routability 메커니즘을 개선하기 위한 표준 문서 작성
4. IEEE 802.21과 MIPSHOP간의 상호 연계를 통한 강화된 MIPv6 기반 IP 핸드오버 표준화 작업 추진

4.2 WG 표준 문서

본 절에서는 현재까지 MIPSHOP WG에서 표준화된 문서에 대해 간략히 서술한다.

4.2.1 Fast Handover for Mobile Ipv6 (RFC 4068)

FMIPv6는 기존의 Mobile IPv6의 구현문제에서 지적되고 있는 긴 핸드오버 지연 시간을 최소화 시키기 위해 L3 핸드오버가 시작되기 전, 미리 핸드오버 수행 절차를 진행하도록 디자인된 Mobile IPv6의 확장 프로토콜이다.

일반적으로 IP 이동성에서 핸드오버 지연은 크게 MD (Movement Detection)과정과 CoA (Care of Address) 설정과정에서 발생하는 IP 연결성 지연 부분과 서비스 노드로부터 이동 노드로 직접 데이터를 받기 위한 RR (Return Routability) 과정을 포함하는 Binding Update 지연 부분으로 크게 나눌 수 있따.

FMIPv6에서는 위의 지연을 줄이기 위해 링크 계층의 정보를 이용한 L2 트리거와 L2 핸드오버 이전에 L3 핸드오버를 수행하게 된다. 여기서 L2 핸드오버는 L2에서 수행되는 하부 계층의 핸드오버로써 하드 (Hard) 핸드오버로써, IEEE 802.11 네트워크에서 AP (Access Point)가

변경되는 과정을 말하며, L3 핸드오버는 Mobile IPv6에서 CoA 주소가 생성된 절차를 말한다.

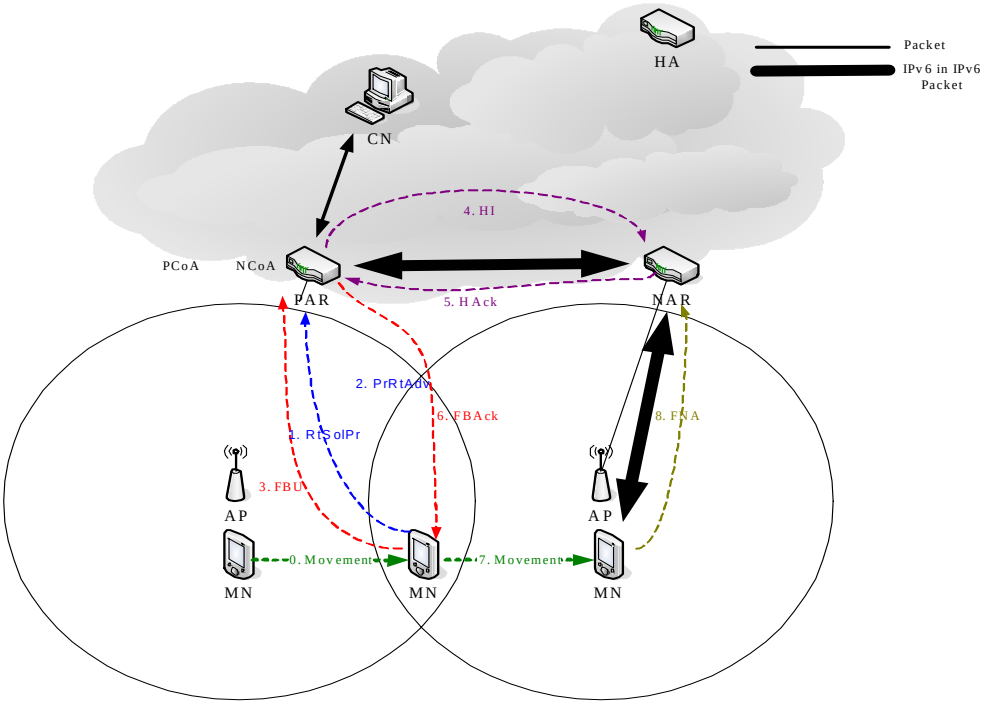


그림 1 FMIPv6의 동작 과정

FMIPv6에는 이동노드가 L2 핸드오버 이전에 L3 핸드오버를 수행하기 위한 'Predictive Mode'와 L2 핸드오버 수행 후 L3 핸드오버가 수행되는 Reactive Mode' 시나리오로 구성된다. 그림 1에서와 같이, 'Predictive Mode'의 Fast 핸드오버 동작은 최초 'AP 스캐닝'에 의해 단말이 이동해야 할 시점을 triggering 하면서 시작된다. 이동노드는 자신이 이동 가능한 AP를 관장하는 NAR에 관한 정보를 얻기 위하여 PAR (Previous Access Router)에 RTSolPr (Router Solicitation for Proxy Advertisement) 메시지를 보내고, 그 응답으로 NAR로부터 PrRtAdv (Proxy Router Advertisement)메시지를 받는다. 그리고 이 메시지에 포함된 Prefix 정보로부터 자신이 사용할 NcoA (New Care of Address)을 생성하고 그 유효성을 검증하기 위해 FBU 메시지에 NCoA를 담아서 PAR로 보낸다.

PAR은 이동노드를 대신하여 NCoA의 유효성 확인검사를 위해서 NAR(New Access Router)로 HI (Handover Initiate)메시지를 보내고, 그것에 대한 응답 메시지인 Hack (Handover Acknowledge)을 수신한다. 그리고 이 유효성 여부를 이동노드에게 통지하기 위해서 Fback (Fast Binding Acknowledgement) 메지를 보낸다. 이동노드가 계속 움직여 PAR 링크를 벗어나면, PAR은 이동노드에게 전달할 데이터를 터널링 (tunelling)을 통해서 NAR로 전달 시 킨다. 이동노드가 Fback를 수신하고 NAR 링크에 들어가게 되면, FNA (Fast Neighbor Advertisement)을 NAR에 전송하여 자신이 접속을 알리고 이동노드에게 배달된 패킷을 신속히 수신한다.

반면, ‘Reactive Mode’는 ‘Predictive Mode’와 마찬가지로 이동노드는 자신이 이동 가능한 AP를 관장하는 NAR에 관한 정보를 얻기 위하여 PAR에 RtSolPr 메시지를 보내고 NAR로부터 그 응답인 PrRtAdv 메시지를 받는다. 그러나 이동 노드는 이미 PAR영역을 벗어나 NAR 영역으로 들어가고 있는 상태이기 때문에 FBU를 PAR로 보내지 못하고 NAR 영역에서 FNA메시지에 FBU를 담아서 NAR로 전송한다.

NAR은 이동노드의 PAR로 FBU를 보내고, 그 응답인 Fback를 받는다. 그리고 NAR은 PAR로 배달된 이동노드의 데이터를 받아서 자신이 링크로 접속한 이동노드에게 그 데이터를 전달한다.

Fast MIPv6는 네트워크 계층에서 신속한 이동성을 지원한다. 그러나 보다 실현 가능한 Fast 핸드오버를 지원하기 위해서는 L2에서의 L2 핸드오버가 고려된 이동 감지가 효과적으로 지원되어져야 한다.

4.2.2 Hierarchical Mobile Ipv6 mobility management (RFC 4140)

HMIPv6는 이동 노드의 이동을 지역적으로 관리함으로써 이동 노드의 핸드오버로 인한 Signaling의 양을 줄여주는 프로토콜이다. HMIPv6는 MAP (Mobility Anchor Point)라는 새로운 구성요소를 정의하고 도메인 레벨의 CoA와 링크 레벨의 CoA를 정의하였다. 도메인 레벨의 CoA는 이동노드가 MAP 도메인의 Prefix를 기반으로 생성한 CoA로써 Regional CoA 라고 한다. 링크 레빌의 CoA는 액세스 라우터의 Prefix를 기반으로 생성한 CoA이며, on-link Care-of Address (LCoA)라고 한다. 이동 노드는 생성한 RCoA와 LCoA를 MAP에 등록하고 RcoA를 자신의 HA와 상대 노드에게 등록한다. 만약 이동 노드가 한 MAP 도메인 내의 액세스 라우터 간 이동을 하였다면, 이동 노드는 LcoA를 생성하고 MAP 도메인이 변경되지 않았으므로 새로운 RcoA는 생성하지 않는다. 그러므로 이동 노드의 MAP 도메인 내의 이동은 이동 노드와 HA, 상대 노드간의 Signaling을 줄여준다.

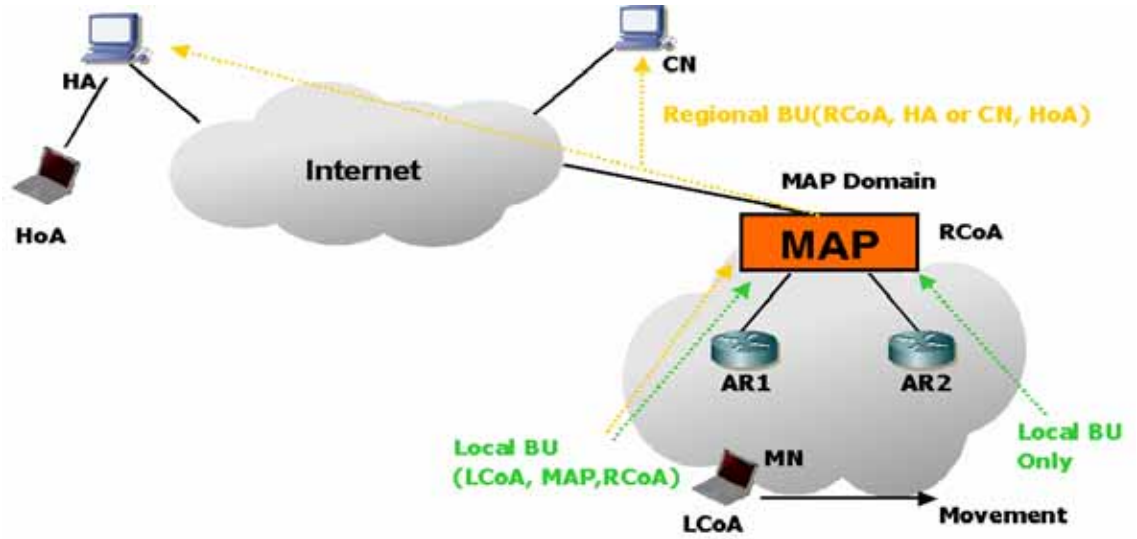


그림 2 HMIPv6의 동작 과정

HMIPv6에서는 이동 노드의 이동을 두 가지로 나눈다. 하나는 한 MAP 도메인 내에서 액세스 라우터간 이동을 했을 때를 가리키며, 이것을 Micro Mobility 핸드오버라고 말한다. 다른 하나는 이동 노드가 한 MAP 도메인에서 다른 MAP 도메인으로 이동하였을 때를 가리키며 이것은 Macro Mobility 핸드오버라고 말한다. HMIPv6는 이동 노드가 Micro Mobility 핸드오버를 수행하는 경우에 중점을 맞추고 있다. 그림 2와 같이, HMIPv6에서 이동 노드가 새로운 MAP 도메인으로 진입하였을 때, 이동 노드는 새로운 액세스 라우터로부터 RA 메시지를 수신한다. 이동 노드는 AR의 Prefix를 기반으로 LcoA를 생성하고, AR은 이동 노드의 LcoA에 대한 DAD를 수행한다. LcoA 주소는 이동 노드가 AR로 이동할 때마다 새롭게 생성된다. 그리고 이동 노드는 RA메시지의 MAP option에 포함된 MAP의 Prefix를 기반으로 새로운 RcoA를 생성한다. RcoA 주소는 이동 노드가 다른 MAP 도메인으로 이동하기 전까지 변경되지 않는다.

이동 노드는 RcoA와 LcoA를 생성한 후, 두 주소를 포함한 LBU(Local Binding Update) 메시지를 MAP에게 보낸다. MAP은 LBU메시지를 수신한 후, RcoA 주소에 대한 DAD 검사를 수행한다. MAP은 이동 노드의 RcoA주소가 도메인 내에서 유일함을 확인한 후 MAP은 자신의 Binding Cache에 이동 노드의 두 주소를 저장한다.

이 후, MAP은 MIPv6에서 이동 노드의 HA가 이동 노드의 HoA와 CoA에 대하여 Proxy를 수행하는 것처럼, Proxy Neighbor Advertisement 메시지를 이용하여 이동 노드의 RcoA로 도다달하는 패킷들을 가로채어 이동 노드의 LcoA로 터널링하여 전달한다.

MAP가 이동 노드의 RcoA와 LcoA를 Binding Cache에 저장한 후, 이동 노드는 자신의 HA에게 위치 등록을 하기 위하여 Binding Update 메시지를 보낸다. Binding Update 메시지를 전송하는데 이 때 목적지 주소는 이동 노드의 RcoA가 된다. MAP은 이동 노드의 메시지를 가로채어 이동 노드의 LcoA로 패킷들을 터널링하여 전달한다. HA와의 위치등록이 완료된 후, 이동 노드는 상대 노드들에게 위치 등록을 할 수 있게 된다.

4.2.3 Mobile IPv6 Fast Handover for 802.11 Networks (RFC 4260)

FMIPv6는 MIPv6에서 야기되는 긴 핸드오버 지연시간을 줄이기 위해 하부 계층 (e.g., 링크 계층)의 도움으로 L2나 L3핸드오버 이전에 새로운 CoA를 등록하고, 기존 AR과 새로운 AR과의 터널링을 통해 IP 연결성을 보장해 줄 수 있는 프로토콜이다. 본 RFC 4260에서는 IEEE 802.11 네트워크 기술에서 제공하고 있는 L2 핸드오버와 FMIPv6의 L3핸드오버 기술이 연동되어 어떻게 동작하는지에 관해 언급하고 있다. 특히, 본 문서에서는 IEEE 802.11 환경에서 야기될 수 있는 시나리오에 따른 FMIPv6의 동작 과정을 보여주고 있다.

먼저 IEEE 802.11에서 제안하고 있는 L2 핸드오버 기술을 자세히 알아보도록 한다.

일반적으로, 802.11 핸드오버는 하나의 AP에서 다른 AP로 기존의 연결을 변경 (so-called “re-association”)할 때 수행되며, 이 과정은 다음과 같은 단계로 구성된다.

0. STA (mobile Station)이 이동함에 따라 현재 연결 설정된 AP로부터 전파 전송 환경이 악

화될 때 STA는 핸드오버 수행의 필요성을 인지하게 된다.

1. STA는 현재 사용 가능한 AP들을 조사 (scan) 한다. STA에 의해 조사된 결과는 사용 가능한 AP들의 리스트가 될 것이고, 각 AP들의 신호 강도를 비롯한 물리계층의 정보들이 포함될 수 있다.

2. STA은 사용가능 한 AP들 중 가장 적합한 AP를 선택하고, 선택된 AP들과의 물리 계층과 MAC 계층과의 시간적 동기를 맞추기 위해 시도한다.

3. STA는 새로이 선택된 AP와 인증 과정을 시도하며, 이때 AP가 "Open System" 방식의 인증 시스템을 지원할 경우, AP와 STA는 two-way 방식의 message 교환을 수행한다.

4.STA는 새로운 AP에게 association과 re-association을 요청한다. STA가 AP와 "re-association" 과정을 수행하는 경우, AP는 STA에게 현재 서비스 중인 AP의 MAC 주소를 요청하고, 일반적인 association은 이를 요청하지 않는다.

5. L2 핸드오버 과정에서 IEEE 802.11i 표준을 지원한다면, STA는 AP사이에 Step 3에서 802.1x EAP-on-LAN 절차가 수행될 것이다.

6. 새로이 연결 설정된 AP는 STA에게 로컬 LAN 상으로 Layer 2 Update 프레임을 보내서, 연결된 Ethernet bridge의 table을 Update 시킨다.

한편, FMIPv6 핸드오버는 아래와 같은 메시지 교환 방식으로 구성된다.

a. MN는 이웃 AR들을 찾기 위해 RtSolPr 메시지를 보낸다.

b. MN는 현재 사용 가능한 이웃 AR과 AP들의 정보들 (AP-ID, AR-Info)을 포함한 PrRtAdv 메시지를 수신한다.

c. MN는 이전에 현재 연결된 AR (PAR) 에게 FBU 메시지를 보낸다.

d. PAR은 새로운 AR (NAR) 에게 HI (Handover Initiate) 메시지를 보낸다.

e. NAR은 HAck(Handover Acknowledge) 메시지를 PAR에게 보낸다.

f. PAR은 새로운 링크를 사용하여 MN에게 Fback 메시지를 보낸다.

g. MN는 새로운 NAR로 이동한 후, NAR에게 FNA 메시지를 보내어 핸드오버 절차를 종료한다.

다음은 본 문서에서 고려하고 있는 시나리오에 관하여 설명한다. 각 시나리오는 앞서 언급한 802.11의 L2 핸드오버 과정의 단계 번호와 FMIPv6 수행 과정에서 언급한 단계 번호를 참조한 번호들의 순서에 따라 시나리오가 구별된다.

A. 시나리오 1abcdef23456g

이 시나리오는 FMIPv6 표준에서 “Predictive Mode”에 해당하는 것으로써, MN이 L3 핸드오버 이전에 주기적으로 802.11의 ‘scan’ 기능을 수행하고, FBU 메시지를 전송하는 것을 의미한다. 본 시나리오에서는 FNA 메시지만이 L3 핸드오버 수행 후에 전송된다는 것에 주목한다. 본 시나리오의 동작 절차는 시나리오 이름과 같이 802.11의 L2 핸드오버에서 Step 1과 2 사이에 FMIPv6의 L3 핸드오버가 수행되고, L2 핸드오버가 끝나는 Step 6이 수행된 후, FMIPv6의 Step g인 FNA를 전송하게 된다.

B. 시나리오 ab123456cdefg

시나리오 ab123456cdefg는 FMIPv6 표준에서 “reactive mode”에 해당하는 것으로써, 802.11의 L2 핸드오버가 수행 완료된 후 FMIPv6가 동작하는 방식이다. 여기서 FMIPv6의 ab는 단지 이웃 AR과 AP들의 정보를 얻기 위해 수행되는 과정이며, 특히 MN이 새로운 서브네트웍으로 이동하였을 때 FNA (FBU를 동반)을 보내기 위해 수행된다.

C. 시나리오 123456abcdefg

시나리오 123456abcdefg는 MN이 L2 핸드오버 실행 이전에 NAR에 대해 어떠한 정보도 얻을 수 없는 상황으로써, FMIPv6 표준에서 정의하고 있는 완전한 “reactive mode”이다. 본 시나리오에서는 핸드오버 수행 이후, NAR의 RA 메시지를 통해 NAR과 해당 AP의 정보를 얻게 되며 FNA는 FBU를 동반하여 핸드오버 수행 이후, 즉각적으로 전송될 수 있다. 본 시나리오에서는 핸드오버 이전에 NAR의 정보를 얻을 수 없는 상황이거나, 시나리오 B에서 PrRtAdv 메시지 수행 후 알 수 있는 NAR들의 정보가 무수히 많아서 적절한 NAR을 선택할 수 없는 상황이 될 수 있다. 본 시나리오에서는 L2 핸드오버 수행이 끝난 후, NAR에 대한 정보를 FMIPv6의 수행 중에 알 수 있거나 다른 형태의 기술을 통해 NAR에 대한 정보를 알 수 있을 것이라는 가정 하에서 FMIPv6가 수행된다.

4.3 WG Internet Drafts

본 절에서는 현재 MIPSHOP WG에서 표준화 진행 중인 Internet Draft들에 관하여 간략히 설명한다.

4.3.1 Mobile Ipv6 Fast Handovers over IEEE 802.16e Networks

본 문서는 IEEE 802.16(e)상에서 FMIPv6의 동작 시나리오에 관한 내용을 담고 있다. 특히, IEEE 802.16(e) 표준에서 제안하고 있는 L2 hard 핸드오버 시에 전송되는 Message들과 IEEE 802.21에서 정의하고 있는 L2와 L3 레벨간의 핸드오버 지원을 위한 Triggering 메시지들을 기반으로 FMIPv6 핸드오버 수행의 구체적인 세부 절차에 관해 언급하고 있다.

다음은 본 문서에서 사용하고 있는 IEEE 802.16(e)의 L2 핸드오버 관련 메시지들의 간략한 용어 설명이다.

MOB_NBR-ADV
: IEEE 802.16e Neighbor 광고 메시지, 주변 BS의 정보를 Serving BS가 주기적으로 광고

MOB_MSHO-REQ
: MN이 BS에게 IEEE 802.16e 핸드오버 요청 메시지

MOB_BSHO-RSP
: BS가 MN에게 IEEE 802.16e 핸드오버 응답 메시지

MOB_BSHO-REQ
: BS가 MN에게 IEEE 802.16e 핸드오버 요청 메시지

MOB_HO-IND
: MN가 BS에게 IEEE 802.16e 핸드오버 실행하도록 하는 메시지

BSID
: IEEE 802.16e BS ID

다음은 IEEE 802.21에서 제안된 L2에서 L3 계층으로 전달되는 Triggering 이벤트들의 간략한 용어 설명이다.

New_BS_Found (NBF)
: New BS가 발생되었을 시 발생되는 L2 트리거

Link_Going_Down (LGD)
: 공 L2 링크가 끊길 것이라고 알려주는 L2 트리거

Link_Up (LUP)
: New BS와 L2연결을 성공했을 경우 발생하는 L2 트리거

Link_Switch (LSW)
: New BS와 링크를 교환 시 발생하는 L2트리거

IEEE 802.16e 기반의 FMIPv6 작동 과정을 설명하기 전에, IEEE 802.16e 표준에서 제안하고 있는 L2 레벨의 hard 핸드오버 과정을 앞서 언급한 IEEE 802.16e의 핸드오버 수행 메시지들을 가지고 간략히 설명한다.

IEEE 802.16e를 지원하는 MN은 자신이 속한 기지국으로부터 주기적으로 광고 되는

MOB_NBR-ADV 메시지를 수신한다. MN은 MOB_NBR-ADV 메시지를 통해 인접 기지국들의 ID의 목록을 획득하고 스캐닝을 통해 취득한 실시간 링크 정보를 바탕으로 적절한 기지국을 선택한다. MN은 Serving BS로부터 제공되는 서비스 품질과 신호 세기 등을 비교하여 핸드오버가 가능한 기지국들의 리스트를 MOB_MSHO-REQ에 실험 기지국에게 전송하고 기지국은 그 중 추천하는 기지국들의 리스트를 MOB_BSHO-RSP 메시지에 포함하여 회신 한다. MN이 MOB_BSHO-RSP를 수신하고 목적지 기지국을 결정했다면, Serving BS에게 MOB_HO-IND 메시지를 보내어 핸드오버를 최종적으로 통지하고 곧 바로 핸드오버를 실행한다. MOB_HO-IND를 전송한 시점부터 단말은 Serving BS를 통해 더 이상 데이터를 송수신 할 수 없으므로 새로운 네트워크로 이동한 후 가능한 신속하게 Re-entry 절차를 수행해야 한다.

다음 그림에서 본 문서에서 제안하는 IEEE 802.16e 기반 FMIPv6의 동작 과정을 보여주고 있다.

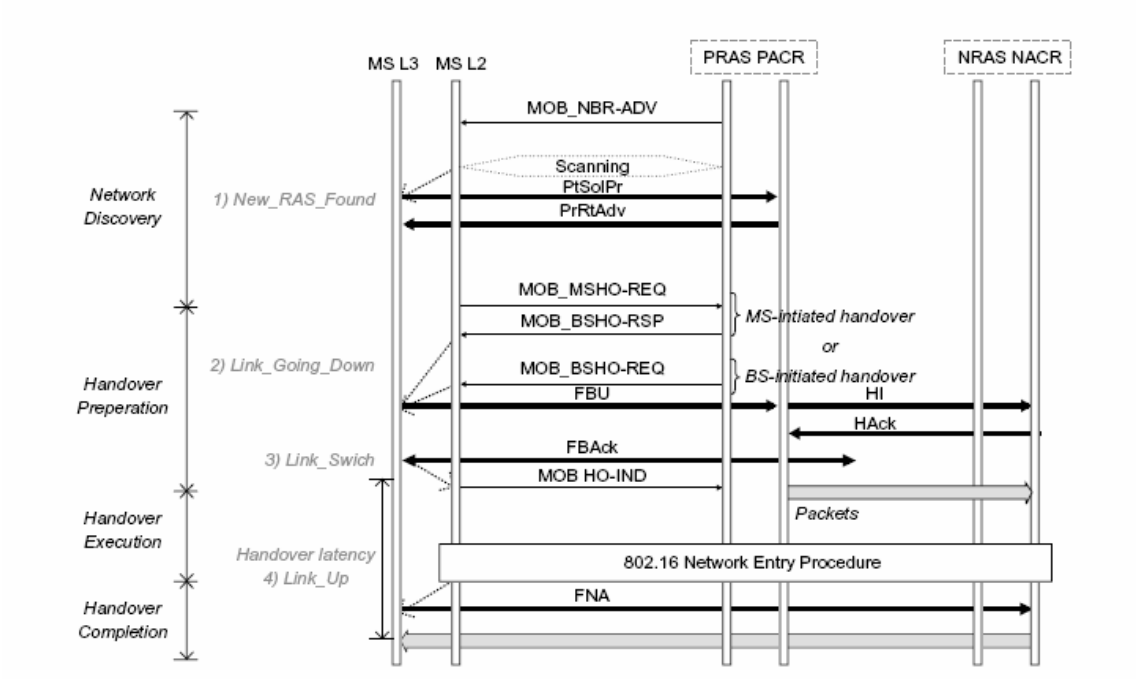


그림 3 IEE 802.16e 기반의 FMIPv6 수행 절차

위의 그림과 같이, BS는 주기적으로 MOB_NBR-ADV 메시지를 주기적으로 광고하고, MN이 이를 받아서 적절한 기지국을 선택하고 결정한다. MN은 L2의 NBS (New_BS_Found)을 L3에게 Triggering하고 RtSolPr 와 PrRtAdv 메시지를 PAR과 교환하고 AR Discovery 과정을 수행한다. 이후, MN는 MOB_MSHO-REQ와 MOB_BSHO-RSP를 교환한 후, L2 핸드오버를 시작한다. MN이 L2 핸드오버의 시작 메시지를 수신할 경우, L2는 L3에게 Ling_Going_Down Triggering 이벤트를 발생시키고, L3가 Link_Going_Down 메시지를 수신하면, MN는 PAR과 FBU, FBAck를 교환하고 PAR은 그 사이에 NAR과 HI, HACK를 이용하여 터널을 생성한다. MN은 PAR에게 MOB_HO-IND를 보내 실제 핸드오버의 수행을 알리고, MN은 대상 BS로의 핸드오버를 수행하고, 802.16e의 802.16e 네트워크 엔트리 절차를 수행한다. 802.16e 핸드오버 과정이 끝나

면, L2는 Link_UP 메시지를 Triggering 하고 MN은 FNA를 NAR에게 전송한다. 마지막으로, NAR이 MN으로부터 FNA를 수신하면 버퍼링된 데이터를 MN에게 전송한다.

4.3.2 Mobile IPv6 Fast Handovers for 3G CDMA Networks

본 문서는 3G CDMA 네트워크 환경에서 FMIPv6 수행 시나리오에 대해 설명한다. 3G CDMA 에서는 기존의 무선 접속 기술에서 제공하는 L2 핸드오버 방식과 달리, Access Network 기반의 hard 핸드오버가 수행된다. 다시 말해서, Pilot channel들을 이용하여 BS들의 신호 강도 및 Air Interface의 정보들을 수집하고, MN와의 협상을 통해 Network이 핸드오버 수행을 결정하게 된다.

일반적으로 3G 네트워크에서는 MN이 아닌 Network기반의 핸드오버가 수행되기 때문에 FMIPv6의 “Predictive Mode” 방식이 적용될 수 있다. 그러나, Network가 NAR에 대한 정보를 RtSolPr/PrRtAdv 메시지 교환에 의해 알 수 없을 경우, 3G CDMA 네트워크에서 FMIPv6는 “Reactive Mode”로 동작하게 된다. 특히, 3G CDMA 네트워크에서는 핸드오버 수행을 위한 링크 정보를 ‘Handover Assist Information’ 이라고 정의하고, 기존의 FMIPv6 표준에서 정의하고 있는 New AP Link Layer Address (LLA)을 확장하도록 권고하고 있다. 이는 3G 네트워크에서는 AP방식이 아닌, BS의 Sector별 Pilot Channel에 의해 링크 계층 핸드오버가 수행되기 때문이다.

또한, 본 문서에서는 Selective bi-casting 방식을 제안하고 있다. Selective bi-casting 방식은 MN이 하나 이상의 라디오 신호를 수신할 수 있을 때, PAR, HA 혹은 NAR이 MN가 해당 signal을 선택적으로 bi-casting 함으로써 데이터 손실 및 핸드오버 처리 시간을 줄일 수 있도록 하고있다.

4.4 IETF 66th 회의 논의 사항

4.4.1 회의 Agenda

1. Agenda review, Blue sheets and volunteers for taking notes and Jabber scribe

2. WG status and I-Ds update

3. Using Cryptographically Generated Addresses (CGA) to secure HMIPv6 Protocol (HMIPv6sec)

4. Authenticating FMIPv6 Handovers

5. Handover Keys Using AAA

6. Distributing a Symmetric FMIPv6 Handover Key using SEND

I-D: draft-kempf-mipshop-handover-key-00.txt

7. Fast Handovers for Mobile IPv6
I-D: draft-ietf-mipshop-fmipv6-rfc4068bis-00.txt

8. Hierarchical Mobile IPv6 Mobility Management (HMIPv6)
I-D: draft-soliman-mipshop-4140bis-00

9. Applying Cryptographically Generated Addresses and Credit-Based Authorization to Mobile IPv6
I-D: draft-arkko-mipshop-cga-cba-04.txt

10. Media Independent Handovers: Problem Statement
I-D: draft-hepworth-mipshop-mih-problem-statement-02.txt

11. Design Considerations for MIH Transport

12. Supporting Media Independent Handover Protocols with GIST
I-D: draft-hancock-mipshop-gist-for-mih-00.txt

13. Network initiated handovers problem statement
I-D: draft-melia-mipshop-niho-ps-00

14. Transport of Media Independent Handover Messages Over IP
I-D: draft-rahman-mipshop-mih-transport-00.txt

15. Symmetric-key Based IPv6 Addresses
I-D: draft-narayanan-pba-01.txt

16. AR information for FMIPv6 Messages Over IP
I-D: draft-zhang-mipshop-fmip-arinfo-00.txt

4.4.2 IETF 66th MIPSHOP WG 회의 내용 정리

이번 IETF 66th MIPSHOP WG에서는 13개의 Draft 내용이 발표되었다. 그 중, 두 발표가 FMIPv6와 HMIPv6 표준 문서에 대한 Updated Draft이고, 5개가 FMIPv6와 HMIPv6에서 보안 강화를 위한 Draft이고, 나머지는 대부분 IEEE 802.21 WG에서 추진하고 있는 MIH에서 MIPv6 연동 사항에 대한 발표이다. 또한, Network-Initiated 핸드오버에 대한 문제 제기에 대한 Draft 발표가 있었다. 발표된 Draft의 제목에서부터 알 수 있듯이, MIPSHOP에서도 FMIPv6와 HMIPv6의 보안 문제, 구체적으로 Handover Key에 대한 보안 강화와 관련된 내용이 주요 이슈가 되고 있다. 특히, MIPv6와 IPSEC 간의 연동 문제에서 Handover Key의 교환 문제 등이 표준화 이슈가 되고 있다.

또한, MIPSHOP WG에서는 IEEE 802.21 MIH WG에서 승인된 MN의 L2 및 L3 핸드오버 지원 프레임워크를 바탕으로 MIPv6와의 연동 문제를 집중적으로 논의하였으며, MIPSHOP에서는 IEEE 802.21 MIH 정보를 전송할 전송 계층 표준 프로토콜을 설계할 움직임이 보이고 있다. 현재 MIPSHOP에 참여하는 많은 멤버들이 802.21 WG에서 활발히 활동하고 있으며, 802.21 MIH와 FMIPv6와의 연동 관련된 Draft 문서가 많이 제출되고 있다. 이번 66차 회의에서는 새로운 Working Item으로 승인된 문서는 없으며, 대부분의 발표에 대한 논쟁이 회의장에서 끝나지 않아 Mailing List의 이슈로 대체하도록 하였다.

4.4.3 향후 진행 방향

이번 IETF 66th MIPSHOP에서는 현재까지 제출된 Draft 중 몇 개의 발표가 있었으며, 뚜렷이 결정된 사항은 없어 보인다. 본 WG의 향후 진행 방향은 아마도 MIPv6의 핸드오버 Key 분배 관련된 보안 사항과 CGA 사용에서 추가 보완사항이 MIPSHOP의 향후 지속적인 주요쟁점이 될 것으로 예상되며, 좀 더 기대되는 사항으로는 IEEE 802.21 MIH WG과의 협력 및 연동 관련 사항이 차후 많은 쟁점화가 될 것으로 예상된다. 특히, IEEE 802.21에서 사용될 전송 계층 프로토콜과 관련된 내용은 주위 깊게 살펴볼 사항으로 많은 기대를 하고 있다.

4.5 결론

본 문서에서는 IETF MIPSHOP WG에 대한 간략한 설명과 현재까지 완료된 표준 문서들과 현재 표준화 진행 중인 Internet Draft 문서들에 대한 내용을 요약해보았다. 또한, 이번 IETF 66th MIPSHOP WG의 주요 Agenda와 회의 내용을 간략히 담아보았다.

MIPv6는 IP 이동성 지원 프로토콜로써, 향후 상용화 기술로 이끌기 위해 IETF에서 활발히 표준화 작업이 이루어지고 있는 기술이다. 이에 MIPSHOP WG에서는 기존의 MIPv6 표준에서 문제시 되고 있는 핸드오버 지연 및 핸드오버 Signaling 처리, 보안 문제 등을 중점적으로 보완하고 이에 관한 사항들을 표준화를 진행하고 있다.

본 보고서를 작성하면서 IETF MIPSHOP WG에서 진행하고 있는 표준 기술들과 관련된 Item들을 분석하면서, MIPv6 기술에 대한 전반적인 지식을 습득할 수 있었고, 현재 MIPv6와 관련된 최근 동향들을 파악할 수 있었다. 특히, 이번 IETF 66th 회의에 참가하면서 표준 기술이 어떻게 만들어지는지, IETF 표준화 회의가 어떻게 이루어지는지에 대해 자세히 알 수 있는 계기가 되었다.

5. rserpool

5.1 Reliable Server Pooling

5.1.1 Server pool의 정의

클라이언트가 서버에 접속하기 위해 서버풀에 먼저 접속하는 매커니즘을 연구하는 WG로서 높은 신뢰성의 어플리케이션을 지원하여 서버-클라이언트 간의 관리와 작동에 대한 아키텍처와 프로토콜을 개발하는 것이 주된 목표이다. 이를 위해 다양한 어플리케이션, 블록, building block, 인터페이스, 여러 종류의 풀링방법, 보안, 아키텍처 등을 정의하며, 서버 접속 관리, 성능요구(failover, heterogeneous 지연) 등에 대한 연구를 진행하고 있다.

관련 연구 범위는 서버 풀링을 이용하여 서버에 접속하는 클라이언트가 어플리케이션의 이용을 원할하게 효율적으로 할 수 있도록 서버간에 균형있고 적절한 활용을 하도록 지원하는 것이다. Server pooling의 방법은 pool에 어떤 종류의 서버가 있는지를 추적하다가 클라이언트로부터 요청이 들어오면 클라이언트를 요청된 서버에 접속을 시켜주는 식이 된다.

5.1.2 Reliable Server Pooling의 목적

1) 어플리케이션 개발을 위한 시간과 비용의 절감

2) 세션계층에서의 오차 허용 매커니즘의 전개

3) 요구사항이 급할 경우, 오차 허용 요구 없이, 주기 후에 rservpool로 어플리케이션의 전개

4) rservpool은 개발자들에게 오차 허용을 위한 API를 제공

5) rservpool은 어플리케이션에 기본상태의 공유를 위한 간단한 building block을 제공

5.1.3 Working group의 활동 영역

1) Working Group 의 연구 분야

a. UDP, SCTP, TCP 등의 전송프로토콜 지원

b. 새로운 혼잡 제어 관리 방법

c. URI 분석 매커니즘 같은 현재작업에 대한 관계

1-1) 이 분야에서 다루지 않는 것

① reliable multicast protocols-optional
② 서버 pool 요소 간 데이터의 동기화/일관성
③ 서버 pool 요소 간 공유정보
④ transaction failover

2) 서버 pools에 클라이언트가 접속하는 구체적 방법

a. 지리적으로 분산된 서버가 같은 pool 안에서 존재하는 access 매커니즘
b. load balancing이나 구체적인 어플리케이션 할당을 하는 동적인 클라이언트의 할당을 지원하는 클라이언트 서버 binding 매커니즘(load balancing application specific assignment policy)
c. 서버 오류나, 권한 변경 같은 경우에 client/server의 자동환경 재설정

3) client/server 접속을 지원하는 server pool관리와 분산 서비스

a. server pool에 서버를 등록하고 추적을 위한 기술
b. node 오류를 탐지, 재설정, failover 하거나 서버 pool을 관리하는 프로토콜
c. server pool의 핵심적인 기술인 클라이언트가 server pool 정보에 기반하여 서버에 binding하도록 지원하는 분산서비스, 높은 수준의 유효성이 필요
d. 유연한 load assignment 와 balancing 정책 수단

4) 클라이언트가 서비스에 접속할 때의 상호작용을 위해 프록시를 사용해서 내부로 들어가는 방식

5.2 Working Group 표준문서

5.2.1 완료된 RFC

RFC3237 (Requirements for Reliable Server Pooling)

클라이언트가 서버로부터 서비스를 제공받기 위해 필요한 서버검색과 서버 간 이동에 대한 사항인 server pooling에 대한 표준 문서이다. 내용은 다음과 같다.

24시간 연결된 인터넷에서는 언제든지 서비스가 가능해야 한다. 이를 통해 많은 E-business가 24시간 연속된 영업을 하는데 이러한 성능을 위해 소유주와 시스템은 높은 신뢰도을 제공해야 한다. 이를 위해서는 어플리케이션의 높은 신뢰성와 유효성을 제공하기 위한 아키텍쳐와 프로토콜을 사용한 server pooling이 필요하다. 신뢰성 있는 server pooling은 이동성과 실시간 어플리케이션 등의 서비스 성능을 향상시킨다. Rservpool 매커니즘은 서버를 등록하여 네트워크의 기능에 유연성을 지원하게 된다. 그리고 load balancing을 통해 매커니즘에 scability의 조화가 되게 한다. 예를 들어 과다한 트래픽과 응답시간을 조정하는 데에는 pool status를 조절하는 방식을 사용하게 된다. Reserpool을 위한 요구사항은 견고성, 장애극복, 통신 모델, 처리용량, 전송프로토콜, 익명사용자에 대한 지원, 등록과 해제, 이름, 이름분석, 서버선택 방법, 시간요구와 크기조정, 확장성, 보안요소 등이 있다. 이 중 보안 요소에는 기존요소와의 호환, name space 서비스, 보안 상태 등이 요구된다.

5.2.2 진행 중인 Draft

1) Architecture for Reliable Server Pooling

Server pool은 같은 어플리케이션 기능을 제공하는 하나 이상의 서버의 집합을 말한다. 이 서버들은 Pool Elements(PEs)라고 불린다. PEs의 형태는 RSerPool 구조의 첫 번째 종류의 개체이다. 여러 개의 server pool에서 PE는 오차 허용이나 부하분산 없이 제공될 수 있다. 이 server pool은 독특한 인식자로 구별되는데 이러한 pool handle은 작은 도메인이 아닌 전체 인터넷에는 유효하지 않다. 더군다나 handle space는 고정되어 있을 것이라 생각된다. 그래서 다단계의 query는 pool handle을 해결하는 데는 적합하지 않다.

Rserpool의 두 번째 종류의 개체는 Endpoint hanNdlespace Redundancy Protocol(ENRP) server이다. ENRP 서버는 충분히 분산된 오차허용을 실시간으로 제공하도록 디자인되었다. ENRP 서버는 Pool User(PU)을 PE에 접속 시키는 것을 허용한 정보목록으로 pool handle을 조절할 수 있다. 이 정보는 IPv4/ IPv6 주소, 전송계층 프로토콜의 구체적 설명, SCTP, TCP, UDP 같은 전송계층 프로토콜과 관련된 포트 번호에 대한 것들이다.

각각의 작동은 적어도 ENRP 서버에서 이루어져야 한다. 모든 ERNP 서버는 작동 유효범위 안에서 정보를 가진다.

2) Aggregate Server Access Protocol(ASAP)

ENRP와 결합된 Aggregate Server Access Protocol(ASAP) 은 IP 네트워크에서 높은 이용률의데이터 전송 매커니즘을 제공한다. ASAP은 handle 기반의 IP 주소의 논리적통신 종단에서 고립된 address 모델을 사용한다. 그래서 어느한 쪽이 오류난 경우, 오류난 쪽의 통신 종단과 IP 주소사이의 binding을 효율적으로 제거한다.

게다가 ASAP은 완전히 투명한 server pooling과 부하 분산을 통해 pool로서 각각의 논리적 통신 목적지를 확실히 한다. 또한 서비스에 문제를 발생시키지 않고 언제든지 서버를 더하거나 뺄 수 있다.

ASAP은 SCTP에서 제공된 네트워크 레벨의 모든 장점을 가진다. Pool Element와 Pool User를 가지고 있는 각각의 전송프로토콜은 mapping document 를 수반한다. ASAP 메시지는 PE와 ENRP 서버를 통과할 때 SCTP를 사용해야만 한다.

고 이동성의 server pooling은 ASAP ENRP의 2가지 프로토콜의 결합으로 이루어진다. ASAP은 주소변환, 부하 분산 관리, 오류 관리 등의 사용자 인터페이스를 제공한다. ENRP는 높은 이용률의 handle 전송 서비스를 정의한다.

3) Endpoint Handlespace Redundancy Protocol (ENRP)

Rserpool의 요구와 구조의 기능을 완성하기 위해 ENRP는 ASAP과 결합되어 작동되도록 고안되었다. Rserpool 의 동작 범위 내에서 ENRP는 저장을 위한 고장방지 registry service, 부기, 정보검색, 분산 pool 작동과 회원 정보를 분산된 처리절차와 메시지 형식으로 정의한다.

4) Aggregate Server Access Protocol (ASAP) and Endpoint Handlespace, Redundancy Protocol (ENRP) Parameters

ENRP와 함께 ASAP은 IP네트워크에서 높은 이용률의 데이터를 전송 메커니즘을 제공한다.

각 프로토콜은 메시지 포멧의 파라메터의 여러 부분을 공유해서 함께 동작한다. 이 드래프트는 두 프로토콜 사이의 공통된 파라메터를 설명한다. 또한 포멧 뿐 아니라, ASAP와 ENRP 문서의 각각에 언급된 절차와 메시지도 제공한다.

5) Reliable Server Pooling: Management Information Base using SMIv2

Rserpool은 reliable server pooling을 제공하기 위한 프레임 워크이다. 이 문서에서는 rserpool구현에서 관리목적으로 접속되는 SMIv2 규격의 관리 정보를 설명한다.

6) Reliable Server Pooling Policies

이 문서는 name server와 pool user의 구현을 위한 고려 사항을 포함한 Reliable Server Pooling 중에서 다양한 서버 정책을 지원하는 ENRP, ASAP과 파라미터에 대해 설명한다. 일부 정책은 pool 구성요소의 동적인 부하 정보를 사용하기도 하는데 이것을 적응성이 있는 것으로 사용하지 않는 것을 비 적응성으로 분류한다. Pool 사용자의 선택은 두 가지 다른 개체에 의해 수행된다.

그러므로 이 문서에서는 패킷 형식뿐만 아니라 각각의 서버 정책을 구현하기 위한 name server와 pool 사용자 간 처리 절차에 대한 자세한 설명을 한다.

5.3 회의 논의 사항

5.3.1 회의 Agenda

1) Discussion of ASAP implementation
draft-ietf-rserpool-asap-13 (Randy Stewart)

2) Comments from Genart reviewers
draft-ietf-rserpool-asap-13
draft-ietf-rserpool-enrp-13
draft-ietf-rserpool-common-param-10(Randy Stewart)

3) Rserpool APIs
(Michael Tuexen)

4) Rsplib
(Michael Tuexen)

5.3.2 논의된 내용 정리

먼저 rserpool의 architecture에 대한 논의가 있었다. 여기에서 Architecture for Reliable Server Pooling(draft-ietf-rserpool-architecture-13.txt)이 개괄적이고 넓은 범위의 프로토콜에서의 설명으로 읽기 어렵다는 의견이 나왔다. 그래서 그룹에서는 혼동이 되는 문서는 제외하고 대신에 AD들은 오늘 언급되는 프로토콜의 짧은 개괄문서를 쓰기로 했다.

Rserpool의 구현과 데모 실행에 대해서는 ASAP이 이미 1년 전부터 테스트 되어 오고 있었다. SCTP interop은 7월 말 뱅쿠버에서 실시될 예정이었고 rserpool은 그 때 테스트 되었을 것이다.

Rserpool 소켓 API에 대해서는 현재 작업 중인데 코드와 문서 사이의 차이가 있어 더 많은 작업이 필요하다. 다른 부분을 일치시키고 문서를 업데이트할 필요가 있다.

AD기자들은 나온지 오래되어 이미 완료되었어야 할 많은 작업이 있는데 아직도 RFC정리 작업이 되지 않고 있어 그룹이 제대로 활동하지 못하고 있다고 했다. 현재도 TCP mapping 이후로 architecture, comparision, address 등의 작업이 있는데, 앞으로는 spec에 대해서 작업을 하고 다른 사항들에 대해서는 중지를 요구했다. 참가자들 또한 업데이트와 demo가 필요하고 미리 draft가 공개되지 않아 활동이 힘들다고 했다. 이러한 점을 강조하기 위해 선언이 개정될 필요가 있다. 그리고 그룹의 방향은 현재의 작업을 마무리하고 핵심 프로토콜 문서로 이동하는 것이었다. 문서목록에 작업을 수행하기 위한 사람들의 신분과 해야 할 작업이 신청되었다. 의장은 이러한 변화들에 기반한 새로운 이정표로 개정된 선언에 따라 작업할 것이다. 그 구조 문서로 대체될 문서의 목록은 다음과 같다.

Draft-ietf-rserpool-asap-13.txt Draft-ietf-rserpool-enrp-13.txt
Draft-ietf-rserpool-common-param-10.txt Draft-ietf-rserpool-threats-05.txt

그 외의 다른 문서들은 핵심 문서에 들어가지 않고 나중에 작업될 것이다.

5.3.3 향후 진행 방향 정리

Rserpool WG은 이번 표준화 회의에서는 많은 성과를 얻지는 못했다. 발표내용도 많지 않았던 데다가 발표자였던 Randy Stewart와 Michael Tuexen 에 대해 AD 들이 WG의 진행이 더디다고 불평을 늘어놓았고 발표자들은 자신들도 신경을 쓰고 싶으나 시간이 너무 부족해서 할 수가 없다는 변명을 늘어놓았다. 그렇지만 기존 문서를 대체할 새로운 문서 제작이 시작된다는 점에서 다음 67회 회의에서는 진전이 있을 듯하다.

6. dccp

6.1 서론

지난 7월 캐나다 몬트리올에서 개최된 IETF 66차 회의에서는 차세대 수송계층 프로토콜 표준인 DCCP(Datagram Congestion Control Protocol) 관련 표준제정 작업이 진행되었다. DCCP는 인터넷 실시간 멀티미디어 응용을 지원하기 위해 기존의 TCP/UDP 프로토콜을 개선한 신규 수송계층(Transport Layer) 프로토콜로서, IETF 중점 표준화 대상기술로 분류되고 있다. 이에 따라 DCCP 프로토콜은 차후에 개발되는 차세대 유무선 통신응용 서비스의 하부 수송계층 프로토콜로써 널리 사용될 것으로 전망된다.

6.2 DCCP 개요

DCCP 프로토콜은 UDP 프로토콜에 혼잡제어 기능을 추가한 것으로써, 혼잡제어 기능을 통해 유효 전송 율을 높이고자 개발되었다. 현재 TCP-like 방식 및 TCP-Friendly 혼잡제어 방식이 각각 CCID(Congestion Control Identifier) 번호 2,3,4으로 개발 중에 있다. 특히, DCCP는 혼잡제어를 위해 유지되는 연결상태(state) 정보를 활용하여, 수송계층에서의 이동성 지원기법 등으로 확장될 수 있다.

6.2.1 DCCP에 대하여

DCCP는 UDP와 마찬가지로 비신뢰적 전송을 하지만 UDP와는 달리 연결 설정 과정과 해제 과정이 있으며 데이터 송수신 과정에서 혼잡제어를 한다. 각 과정마다 사용되는 packet들은 상황과 용도에 따라 조금씩 다른 형태를 지니고 있으며 이 packet 형태는 9가지가 있다. 모든 형태의 packet에는 상대 쪽에게 부가정보를 전달하기 위한 옵션(option)이 실릴 수 있다. 또한 모든 DCCP의 연결에는 DCCP가 동작하는데 필요한 여러 특성 값인 feature들이 존재한다. 먼저 DCCP 연결 설정과 해제에 대해 알아본 후, DCCP의 9가지 packet 형식과, option과 feature들에 대해 알아보겠다. 그리고 마지막으로 DCCP에 쓰이는 혼잡제어 기법에 대해 다루겠다.

6.2.2 DCCP 연결 설정과 해제

1) 연결 설정 과정

DCCP의 연결은 두 개의 half-connection 단위로 이루어 진다는 점과 연결 설정 시 여러 특성 값 들에 대한 협상이 이루어 진다는 점이 가장 큰 특징이다. 협상되는 feature중 CCID는 혼잡제어 메커니즘에 대한 선택 값 이고 이 값에 따라 메시지 송수신과정에서 사용되는 혼잡제어 방식이 달라진다. 이 제어 메커니즘에 따라 메시지 송수신 과정이 달라지고 사용되는 feature들도 달라진다.

연결 설정 과정은 클라이언트의 connect()함수에서 DCCP-Request packet을 보내면서 시작되고 서버의 accept() 함수에서 DCCP-Response packet을 보내어 응답한다. 다시 connect에서는 서버의 응답 packet에 대해 DCCP-ACK packet을 만들어 보내고 연결 설정을 끝낸다. 이 과정에서 몇몇 feature들에 대한 협상이 이루어지며 세 번의 Packet 교환 과정에서 협상이 끝나지 않는다면 협상이 끝날 때까지 ACK Packet을 주고 받는다.

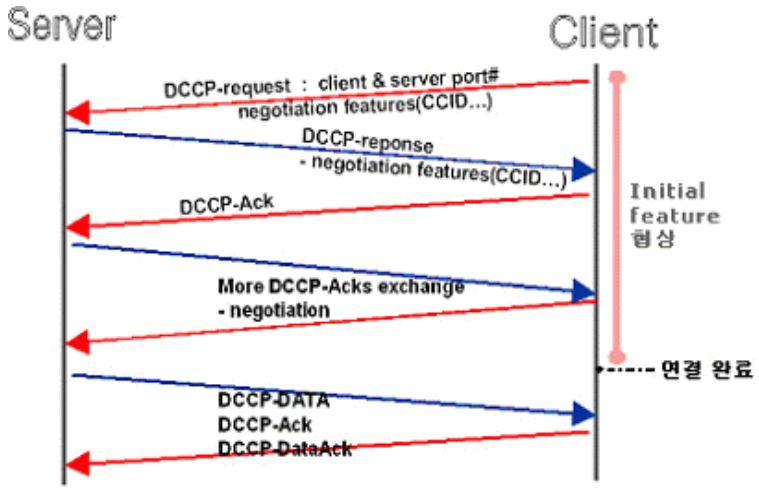
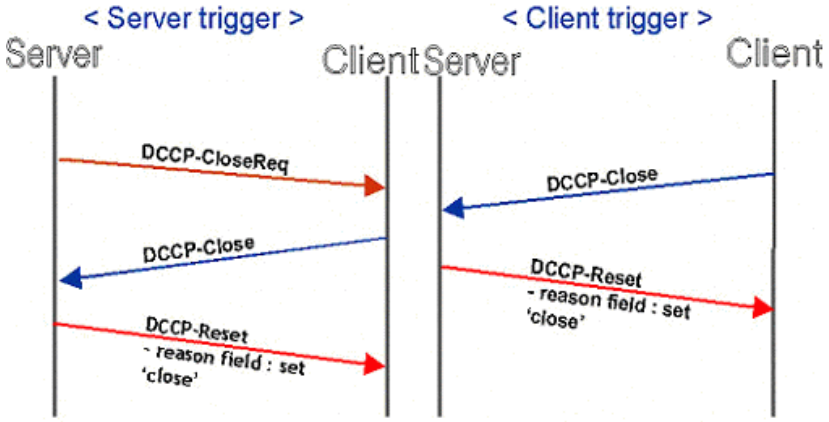


그림 1. SCTP 프로토콜 구조

2) 연결 해제 과정

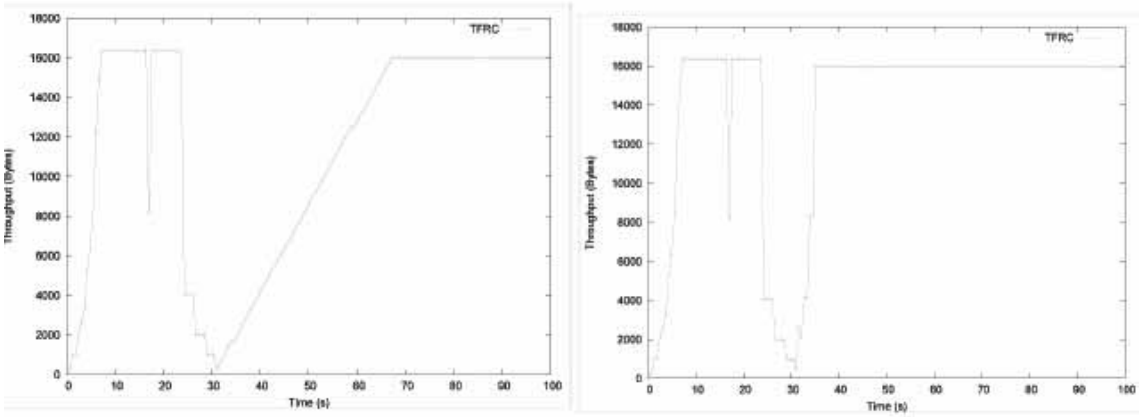
연결 해제 과정은 응용계층의 close()와 shutdown()에 의해 이루어지며 둘 중에 어느 것을 사용해도 상관없다. 해제 과정에서 사용되는 Packet은 DCCP-CloseReq, DCCP-close, DCCP-reset이며 서버와 클라이언트가 보낼 수 있는 packet 타입은 정해져 있으나 어느 쪽에서든 먼저 해제를 시작 할 수 있다. 서버가 먼저 해제를 시작하는 경우와 클라이언트가 먼저 시작하는 경우의 과정은 다음과 같다.



6.3 Session Agendas and Presentations

6.3.1 Faster Restart

현재의 ns-2(2.28) TFRC의 구현은 RFC 3448과 같이 동작하지 않는다. NS2에서와 RFC3448 사이에는 다음과 같은 차이점이 있는데 이는 다음과 같은 상황을 고려하지 않았기 때문에 발생한다. 첫 번 째는 send쪽 application이 idle한 상황에서도 보낼 back log 데이터들이 버퍼에 있다는 것이다. 그리고 sender는 이런 back log 에 기초하여 sending rate를 조절한다는 것이다. 이것을 해결 하기 위해서는 small packet을 전송하고 이것을 두 번 보낼 동안에 큰 사이즈 만 큼 전송을 하는 방안이 고려된다.



a) TFRC-SP conforming to current ns-2 implementation.

b) TFRC-SP conforming to RFC 3448.

6.3.2 TFRC Media and User Guide

DCCP User Guide – draft-ietf-dccp-user-guide-03.txt는 응용프로그램에서 어떻게 DCCP를 사용할 것인가에 대해서 이야기 하였다. IETF-62차 회의에서는 USER-GUIDE API관점과 Media issue관점으로 두 부분으로 분리 하였다. Media issue쪽은 draft-ietf-dccp-tfrc-media-01.txt draft로 새롭게 제안되었다. API쪽에서는 API 중심적으로 다시 쓰여질 필요가 있다. TFRC쪽은 구현을 기다리고 있다.

6.3.3 DCCP Implementation – Linux

Kernel 2.6.14에서는 ccid3만가지고 release되었다. 이 후에 ccid2를 포함하였다. 현재 fast restart와 VOIP와 같은 것은 포함하지 않고 있다.
현재 RFC에는 완벽하지 않고 구현상에 여러 가지 bug를 가지고 있다. Kernel-2.6.19는 개선된 ccid-2를 탑재할 것이다. 현재 구현된 DCCP가 TCP와 congestion control과 같은 상황에서 fairness 하게 동작 하는지 점검할 필요성이 있다. 현재 테스트 된 것은 다음과 같다. FREE-BSD 와 LINUX와의 동작, 브라질과 뉴질랜드 사이(18hop)에서의 테스트, 다양한 상황에서의 테스트 하기 위해 NETERM사용하였다.

6.3.4 RTP over DCCP

Implementation
TFRC는 RTP stack위에 application에서 구현하였다. 고효율의 video application 은 작은 packet interval을 가진다. 현재 TFRC를 이용했을 때 비디오 응용에서 좋은 Performance를 보이고 있다.

6.3.5 DCCP Mobility

DCCP 연결 안에서 여러 주소 바인딩과 re-binding 을 제공하기 위해서 제안되었다. 이것은 Multi-homming과 mobility를 위해 사용 되어진다. draftkohlerdccpmobility02.txt 에 의해 기술 되어져 있다. Mobility issue를 transport계층에서 사용하려는 의도는 wireless LAN은 짧은 거리에서 이용 되어지고 여러 access interface는 동시에 사용가능 하다는 것에서 착안 되었다. 그리고 transport위에 multi-homing은 다음과 같은 특징들이 있다. End host간의 multi-homing을 지원하기 위해서 ipv4과 ipv6간에 원할 한 지원, 하나의 connection 안 에서 여러 path를 제공한다. 각각의 path는 서로간에 데이터 흐름에 영향을 미치지 않는다. 대부분의 서버의 위치는 고정되어있다. 위에 같은 이유에서 DCCP에서 mobility를 제공하기 위해서 SCTP와 같은 protocol level에서의 구현, with hip, with shim6, mobile IP와의 사용과 같은 것을 고려하고 있다.

6.4 전망

현재의 DCCP가 Internet-draft문서에서 점진적인 발전을 거듭하여 전송 계층의 다른 프로토콜처럼 표준 프로토콜이 된다면 근본적인 혼잡제어를 하는 실시간 전송에 적합한 프로토콜로서 많은 응용에서 사용하게 될 것이다. DCCP(Datagram Congestion Control Protocol)는 문제점이 수정이 되고 부분적인 업데이트가 이루어지는 상황이다. 시간이 지남에 따라 SCTP 보급이 확대되면, 기존에 TCP를 통해 제공되던 응용들도 SCTP를 통해 보다 효율적으로 제공될 수 있을 것으로 전망된다.

7. 결론

지금까지 본 문서에서는 제 66회 IETF 회의의 Working Group중 5개 WG에 대해 알아보았다. 각 분야별 WG에 대한 간략한 설명과 함께 현재까지 완료된 표준 문서들과 표준화가 진행 중인 Internet Draft 문서들에 대한 내용을 정리했고 각 WG의 주요 Agenda 및 회의 내용과 앞으로의 전망까지 정리했다.

IETF Chair가 보고한 이번 IETF Meeting의 참가인수는 44개국 1,236명이었다. 국적을 보면 미국의 참가자가 절반이었고, 중국으로부터의 참가자가 증가하고 있던 것이 특징적이라고 할 수 있다. 세계 최고의 인터넷 망과 사용자 층을 가지고 있는 우리나라이지만, IETF와 같은 국제 표준화 회의에서 한국이 주도적인 목소리를 내는 것은 그 동안 힘들었다. 이번 66회 회의에서 한국인 최초로 '박수홍' 선임연구원이 16ng WG의 의장을 맡게 되었는데 이를 시작으로 한국이 국제 표준화 회의에서 좀 더 영향력을 행사할 수 있게 되기를 바란다.