제63차 IETF NSIS WG

TTA 표준화본부 전략기획팀 **박 정 환**
TTA 표준화본부 전략기획팀 차장 **장 종 표**
한국외대 컴퓨터및정보통신공학부 **정 성 호**

본 고에서는 지난 7월 31일부터 8월 5일까지 프랑스 파리에서 개최된 제 63차 IETF Meeting 중 NSIS WG의 주요 회의결과를 정리한다.

1. 개요

IETF(Internet Engineering Task Force)의 NSIS(Next Steps in Signaling) WG(Working Group)에서는 QoS(Quality of Service) 지원 등을 위해 사용될 수 있는 차세대 시그널링 프로토콜의 표준화를 추진하고 있다. 기존의 시그널링 프로토콜은 상이한 도메인들이 혼재한 환경에서 사용되기 어렵고, 성능, 확장성, 보안, 이동성 등과 관련된 주요 요구사항들을 충족시키지 못하는 문제점이 있다. 이에 따라 서로 다른 망 환경을 고려하고 다양한 요구사항들을 수용할 수 있는 차세대 시그널링 프로토콜의 표준화가 필요하게 되었다. 이러한 배경하에 구성된 IETF NSIS WG은 다양한 사용환경 및 시나리오를 고려한 차세대 시그널링 요구사항 및 프레임워크를 정립하였고, 이를 토대로 NTLP (NSIS Transport Layer Protocol) 및 NSLP(NSIS Signaling Layer Protocol)와 같은 NSIS 시그널링 프로토콜의 표준화에 박차를 가하고 있다. NTLP는 시그널링 메시지 수송을 기본 기능으로 하는 공통의 수송 프로토콜이며, NSLP는 QoS, NAT/Firewall과 같은 특정 응용별 시그널링 프로토콜로서 NTLP의 상위계층에 해당된다. 본 고에서는 먼저 NSIS 시그널링 프레임워크의 구조를 간략히 살펴보고, 제 63차 IETF 회의내용을 중심으로 NTLP, QoS와 NAT/Firewall 등을 위한 NSLP, NSIS 이동성 지원 기능, QoS NSLP QSPEC Template, NSIS QoS 모델, NSIS 보안 등과 관련된 표준화 추진현황을 살펴본다.

2. NSIS 시그널링 프레임워크

IETF NSIS WG에서는 기본적으로 데이터 플로우(flow)의 수송 경로와 동일한 경로상에서(path-coupled) 시그널링 정보의 수송/교환 및 처리를 위한 시그널링 프로토콜의 표준화를 추진하고 있다(향후에는 path-decoupled 시그널링도 고려할 예정이다). 데이터 플로우의 수송경로는 시그널링과는 관계없이 네트워크 구조 및 라우팅 프로토콜에 의해 결정되기 때문에 path-coupled 시그널링 방식에서는 시그널링 정보의 수송경로를 설정하기 위한 추가적인 라우팅 절차를 수행하지 않는다. 즉, 시그널링 메시지는 데이터 플로우의 수송 경로상에 위치한 노드들을 통해 수송된다. NSIS에서는 또한 멀티캐스트(multicast)가 아닌 유니캐스트(unicast) 데이터 플로우가 전송되는 환경만을 고려하고 있다.

NSIS 시그널링은 기본적으로 RSVP의 개념을 토대로 동작하지만, RSVP와는 달리 두 가지 일반적인 특징들이 있다. 첫째, NSIS 시그널링 방식에서는 종단간 시그널링뿐만 아니라 필요 및 상황에 따라 네트워크의 다양한 영역에서 부분적으로도 NSIS 시그널링 프로토콜을 활용할 수 있다. 둘째, NSIS WG에서 표준화된 시그널링 프로토콜은 QoS 뿐만 아니라 NAT/Firewall 등 다양한 응용을 위해 사용될 수 있다. 이러한 융통성을 제공하기 위해 NSIS WG에서는 시그널링 프로토콜 스택을 NSLP들이 동작하는 상위계층과 특정 응용에 관계없이 동작하는 NTLP의 하위계층으로 구성되는 2 계층 NSIS 프레임워크를 정립하였다. 이러한 프레임워크를 토대로 현재 NTLP 프로토콜과 QoS 시그널링 및 NAT/Firewall 시그널링을 위한 NSLP 프로토콜에 대한 표준화 작업이 활발히 추진되고 있다.

NSIS 프레임워크 관련 문서는 Siemens/Roke Manor Research의 Robert Hancock 등에 의해 작성되어 왔는데, 지난 6월에 이 문서가 RFC4080으로 등록되어 그 작업이 종료되었다. 이 RFC에서는 기존에 제시된 시그널링 요구사항을 토대로 2 계층 NSIS 프레임워크의 구조를 구체적으로 제시하고 있으며, 시그널링에 참여하는 네트워크 엔티티 모델, 시그널링과 망의 상호작용에 관한 내용을 다루고 있다. 또한 시그널링과 다른 망 계층 기능(라우팅, 이동성, 주소 변환)과의 관계 및 상호작용을 명시하고 있으며, 시그널링 동작에 영향을 주는 이벤트들이 NTLP 및 NSLP 계층에서 어떻게 처리되는가에 대해서도 기술하고 있다. RFC4080 문서에서 다루고 있는 주요 항목들을 요약 정리하면 다음과 같다.

3. NSIS 트랜스포트 계층 프로토콜 (NTLP/GIST)

NTLP 관련 WG draft로는 Siemens/Roke Manor Research의 Robert Hancock과 Columbia 대학의 Henning Schulzrinne이 작성한 draft-ietf-nsis-ntlp-07 문서가 있다. 이 draft에서는 per-flow 시그널링 메시지의 라우팅 및 수송을 위한 NTLP 프로토콜의 구조와 동작을 명시하고 있다. NTLP는 공통의 메시징 계층(messaging layer) 프로토콜인 GIMPS (General Internet Messaging Protocol for Signaling)와 기존의 수송 및 보안 프로토콜로 구성된다. GIMPS는 상위계층의 다양한 시그널링 응용 프로토콜들이 사용하는 공통의 수송 프로토콜로서 상위 응용계층과 관련된 상태 정보를 유지하지 않고, 단지 데이터 플로우 수송경로를 따라 시그널링 메시지를 수송하는데 필요한 상태정보만을 유지관리하며, NSIS의 peer를 발견하기 위해 사용된다. 최근에는 NTLP 상호운용성 시험을 통해 draft-ietf-nsis-ntlp-06 문서에서 명시된 기능확인이 이루어져 일부 이슈들(on-reverse-path threat, NAT traversal, 데이터 포맷, 오류 메시지 추가 등)을 해결한 후 곧 IESG 검토 단계에 돌입할 것으로 예상된다.

지난 제 63차 회의에서는 GIMPS의 새로운 이름을 결정하기 위한 논의가 있었는데, 제안된 이름 중 많은 지지를 받고 있는 것은 GIST(General Internet Signaling Transport)로서 현재까지 별다른 반대가 없어 향후에는 이 이름으로 문서가 작성될 예정이다.

4. NSLP 시그널링 계층 프로토콜 (NSLP)

NSIS 시그널링 프레임워크는 다양한 NSLP 프로토콜들이 수용될 수 있도록 정의되어 있으나, 현재 NSIS WG에서 중점적으로 표준화를 추진하고 있는 NSLP 프로토콜에는 네트워크에서 QoS 자원예약을 수행하기 위한 QoS NSLP와 NAT(Network Address Translator) 및 Firewall 환경에서 사용될 수 있는 NAT/Firewall NSLP가 있다. 최근에는 Metering NSLP 등이 제안되었으나 아직 WG draft로 채택되지는 않았다.

QoS NSLP는 RSVP의 개념을 토대로 하고 있으나 그 기능이 많이 확장되어 설계되고 있다. QoS NSLP는 특정 QoS 모델에 제한 받지 않는 독립적인 구조를 가짐으로써 서로 다른 QoS 모델을 수용할 수 있도록 설계되고 있다. QoS NSLP에서는 RSVP의 구조 및 동작을 복잡하게 했던 멀티캐스트 플로우 지원은 고려하고 있지 않다. 지난 제 63차 IETF 회의에서는 QoS NSLP의 구조 및 동작을 기술하고 있는 최신 버전의 WG draft (draft-ietf-nsis-qos-nslp-07)가 제출되었고, Siemens/Roke Manor Research의 Andrew McDonald가 발표하였다. 향후에는 QoS 관련 이슈 뿐만 아니라, 보안과 AAA 관련된 이슈들이 구체적으로 논의될 예정이다.

NAT/Firewall NSLP는 path-coupled NAT/Firewall 시그널링을 위한 시그널링 응용 프로토콜이다. NAT와 Firewall은 오랫동안 인터넷에서 사용되어 왔는데, NAT는 IPv4 주소부족 문제를 해결하기 위해 주소 공간(address space)을 확장시켜 왔으며, Firewall은 네트워크의 보안을 강화시켜 주었다. 일반적으로, 이러한 Firewall과 NAT는 특정 응용 트래픽(예를 들면, HTTP 트래픽)만 통과시키기 때문에 많은 응용들의 장애물이 되어 왔다. 특히, IP 텔레포니와 같이 매우 동적인 특징을 갖는 응용이 Firewall과 NAT를 통과하는데 어려움을 겪고 있어 제대로 동작하지 못하고 있다. 이러한 문제점을 해결하기 위해 ALG (Application Level Gateway)들이 통합되어 Firewall과 NAT를 동적으로 configure 하는 방식이 제안되었으며, MIDCOM(Middlebox communication) 관련 표준화 작업이 진행되고 있다.

NAT/Firewall 시그널링은 데이터 플로우의 수송경로에 있는 노드를 통과한다는 점에서 QoS 시그널링과 유사하다. 즉, NAT/Firewall NSLP도 RSVP와 마찬가지로 path-coupled 시그널링 프로토콜로서 NTLP의 상위계층에서 동작하며, Firewall에서 pin-hole을 열고, 데이터 수송경로상에서 NAT 주소를 맵핑하여 뒤이어 도착하는 데이터 패킷들이 NAT/Firewall 장비를 통과할 수 있게 한다.

제63차 IETF 회의에서는 NAT/Firewall NSLP의 구조 및 동작을 기술하고 있는 최신 버전의 WG draft(draft-ietf-nsis-nslp-natfw-07)가 ENST의 Cedric Aoun에 의해 발표되었다.

5. NSIS 프로토콜의 이동성 지원

IETF NSIS WG에서 다루고 있는 최근 이슈 중 하나는 이동성 지원이다. QoS 관점에서 볼 때, 이동망 환경에서의 기본 요구사항은 MN(Mobile Node)의 망 접속점(point of attachment)이 변경되어도 기존에 제공받고 있던 서비스의 품질을 지속적으로 제공하는 것이다. 그러나, MN의 핸드오버가 발생할 때 특정 플로우에

게 보장하기로 한 QoS가 제공되지 않을 수 있다. 이러한 QoS 위반은 핸드오버로 인한 패킷 손실, 지연, 또는 서비스 거부 등으로 인해 발생할 수 있는데, 서비스 품질저하를 최소화하기 위해 핸드오버 이전에 특정 플로우에게 명시적으로 자원(resource)이 할당된 경우에는 핸드오버 후 새로운 경로에서도 동일한 자원이 신속히 제공되어야 한다. 이를 위해 효율적인 QoS 시그널링 프로토콜이 필요하다.

자원예약을 위해 이미 RSVP를 비롯한 다양한 시그널링 프로토콜들이 제안되었으나 이들 중 대부분이 이동망 환경에서 동작하기에는 적합하지 않거나 제한적으로 이동성을 지원하고 있다. 예를 들어, RSVP는 플로우의 고정된 발신지(source) 및 목적지(destination)의 IP 주소와 시그널링 세션을 식별하기 위한 포트 정보 등에 의존하고 있으며 MIP(Mobile IP) 동작환경을 충분히 고려하지 않고 있다. IETF NSIS WG에서는 현재 설계되고 있는 NTLP와 NSLP와 같은 NSIS 시그널링 프로토콜이 이동망 환경에서도 잘 동작할 수 있도록 이동성 지원 관련 사항들을 검토하고 있다. 제 63차 IETF 회의에서는 한국이 리드하고 있는 WG draft인 draft-ietf-nsis-applicability-mobility-signaling-02.txt(Applicability Statement of NSIS Protocols in Mobile Environments)가 발표되었다. 이 draft의 목적은 기존의 NTLP/GIST 및 다양한 NSLP 프로토콜이 이동성을 고려하여 설계되도록 함으로써 핸드오버 등 이동성 이벤트가 발생하는 이동망 환경에서도 NSIS 시그널링 프로토콜이 잘 동작할 수 있도록 하는 것이다. 이 draft에 대한 작업은 현재 설계중인 NTLP, NSLP와 같은 기존의 NSIS 시그널링 프로토콜의 설계를 지원하는 차원에서 진행되고 있으며, NSIS 시그널링 프로토콜의 표준화 작업을 지연시키지 않는 범위 내에서 신속히 진행되는 것을 전제로 하고 있다. 최근 들어 NTLP 및 NSLP 프로토콜의 표준화가 활발히 이루어짐에 따라 조만간 이 draft의 완성도 역시 높아질 것으로 보인다.

향후에는 특히, Mobile IP 관련 API, invalid NSIS responder problem, refresh timer value selection, IP-tunneling 상황에서의 CRN discovery/path update Localized path update, multihoming support 등의 이슈들과 make-before-break, last node problem, priority over signaling API, explicit indication of refresh, node failure/restart handling 등의 이슈들이 논의될 예정이다.

6. QoS-NSLP QSPEC Template 및 QoS 모델

IETF NSIS WG에서는 현재 설계되고 있는 QoS NSLP의 시그널링 메시지를 이용하여 QoS 파라미터들을 수송할 수 있도록 QoS-NSLP QSPEC Template를 정의하고 있다. 이 QSPEC Template는 특정 QoS 모델에 국한되지 않고 다양한 QoS 모델을 수용할 수 있도록 정의되고 있는데, 이를 통해 상이한 도메인들이 혼재하는 환경에서 종단간 QoS를 제공하는데 사용될 수 있다. 최신의 QSPEC Template 내용은 WG draft인 draft-ietf-nsis-qspec-05 문서에 기술되어 있는데, 제 63차 IETF 회의에서 Siemens의 Cornelia Kappler가 그 내용을 발표하였고, H.460/H.323 파라미터를 포함하는 것에 대한 반대의견이 제시되었다.

한편, QoS 모델과 관련된 WG draft인 draft-ietf-nsis-rmd-03(Resource management in DiffServ QoS Model: RMD-QOSM)와 draft-ietf-nsis-y1541-qosm-00(Y.1541-QOSM - Y.1541 QoS Model for Networks Using Y.1541 QoS Classes)이 Ericsson의 Attila Bader와 AT&T의 Jerry Ash에 의해 각각 발표되었다. 그 외에도 QoS 모델과 관련하여 다음 2건의 draft들이 제출, 발표되었다.

- draft-jeong-nsis-3gpp-qosm-01(3GPP QoS Model for Networks Using 3GPP QoS Classes)

- draft-kappler-nsis-qosmodel-controlledload-02(A QoS Model for Signaling IntServ Controlled-Load Service with NSIS)

상기 draft들은 현재 작업이 진행되고 있는 QoS-NSLP가 DiffServ, IntServ, 3GPP 등 다양한 QoS 제공 환경에서 적용될 수 있도록 여러 NSIS QoS 모델을 정립하고자 제출된 것이다. 특히, 상기 3GPP QoS 모델은 한국의 정성호 교수가 발표한 것으로 3GPP의 관심이 있는 경우 WG draft로 채택될 예정이다.

7. NSIS Security

NSIS Security Threats 관련 문서가 지난 6월에 RFC4081(Security Threats for Next Steps in Signaling)로 최종 등록됨에 따라 NSIS 보안관련 일반적인 사항들에 대한 논의가 완료되었다. 향후에는 각 프로토콜 관련 세부 보안 관련 사항들이 추가적으로 현재의 각 WG draft에서 기술될 예정이다.

8. 결론 및 향후 전망

본 고에서는 차세대 시그널링 프로토콜의 표준화를 수행하고 있는 IETF NSIS WG의 표준화 추진현황을 살펴보았다. 특히, 제 63차 IETF 회의내용을 중심으로, NTLP, QoS NSLP, NAT/Firewall NSLP, NSIS 이동성 지원 기능, QoS NSLP QSPEC Template, NSIS QoS 모델, NSIS 보안 등과 관련된 표준화 작업 현황을 살펴보았다.

IETF NSIS WG에서는 차세대 시그널링을 위한 요구사항 및 프레임워크를 이미 정립하였고, 핵심 시그널링 프로토콜인 NTLP와 NSLP의 설계에 박차를 가하고 있다. NTLP(GIST)는 QoS, NAT/Firewall을 비롯한 다양한 시그널링 응용을 수용할 수 있도록 설계되고 있으며, 최근에는 상호운용성 시험을 성공적으로 마쳐 일부 미해결 이슈들을 해결하여 곧 IESG 검토 단계에 돌입할 예정이다.

최근 RFC4080으로 등록된 NSIS 시그널링 프레임워크 문서는 다양한 NSLP가 수용될 수 있도록 작성되었으나, 현재까지는 QoS 지원 및 NAT/Firewall 환경에 사용될 수 있는 NSLP가 설계되고 있다. QoS NSLP는 RSVP의 개념을 토대로 그 기능이 확장되어 설계되고 있으며, 현재 sequence number handling, protocol components for authentication and authorization, receiver-initiated reservations, packet classifiers, last node issues, error handling, hop counts, formatting of objects and message header, tunnelling case 등의 이슈들이 해결되어야 한다. 최근에는 QoS NSLP가 다양한 네트워크에서도 사용될 수 있도록 NSIS QoS 모델에 관한 표준화가 추진되고 있다. 현재, RMD QoS 모델, Y.1541 QoS 모델이 이미 WG draft로 채택되어 DiffServ 및 Y.5141 기반 네트워크에서 NSIS를 적용하는 모델에 대한 논의가 이루어지고 있다. 아울러, 최근에는 3GPP QoS 모델, IntServ Controlled-Load 모델이 제시되어 NSIS의 적용범위를 확장하고 있다. 한국에서 제시된 3GPP QoS 모델은 추후 3GPP의 관심이 있을 경우 WG draft로 상정될 예정이다.

NAT/Firewall NSLP도 QoS NSLP와 같이 path-coupled 방식을 기반으로 설계되고 있으며, 현재 security, migration(traversal of NSIS unaware NATs), intra-realm signaling,

interworking with SIP 등 다양한 이슈들이 해결되어야 한다.

아울러 NSIS WG에서는 현재 설계되고 있는 NTLP 및 NSLP가 이동망 환경에서도 잘 동작할 수 있도록 이동성 지원을 위해 필요한 사항들을 검토하고 있다. 특히, 이전 경로와 새로운 경로가 만나는 CRN (crossover node)의 신속한 발견, dead peer의 발견, 새 경로에서의 신속한 상태정보 설정 및 옛 상태정보 해제, 핸드오버 후 상태정보의 갱신, MIPv4/MIPv6 등의 매크로 이동성 프로토콜과 마이크로 이동성 프로토콜들과의 상호작용, NTLP와 NSLP간의 이동성 지원기능 분배, authentication 및 authorization 모델, ping-pong 형태의 핸드오버 및 다중 플로우 지원, IP 터널링을 고려한 NSIS 이동성 지원, Multi-homing 지원 등 다양한 이슈들을 검토하고 있다. NSIS WG에서는 QoS 및 이동성 지원과 관련하여, ITU-T, 3GPP 등의 표준화 기구와 협력 방안을 모색하고 있다.

NSIS Security Threats 관련 문서가 지난 6월에 RFC4081(Security Threats for Next Steps in Signaling)로 최종 등록됨에 따라 NSIS 보안 관련 일반적인 사항들에 대한 논의가 완료되었다. 향후에는 각 프로토콜 관련 세부 보안 관련 사항들이 추가적으로 현재의 각 WG draft에서 기술될 예정이다.

현재 NSIS WG의 표준화 작업을 통해 등록된 RFC는 Requirements of a Quality of Service (QoS)Solution for Mobile IP(RFC 3583), Requirements for Signaling Protocols(RFC 3726), Analysis of Existing Quality of Service Signaling Protocols(RFC 4094), Next Steps in Signaling Framework(RFC 4080), Security Threats for Next Steps in Signaling(RFC 4081) 등이며, 조만간 RSVP Security Properties, NTLP (GIST) 등이 RFC로 등록될 전망이다. TTA