인터넷 주소자원 관련 IETF WG 연구동향*

김건웅[0*] 송병권[**] 박찬기[***] 김원[***]
목포해양대학교[*], 서경대학교[**], 한국인터넷진흥원[***]

A Survey on the Activities of IETF WGs that Related to the Internet Address Resources

Geonung Kim[0*], Byung-Kwen Song[**], Chan-Ki Park[***] Weon Kim[***]
Mokpo National Maritime University[*], Seokyeong University[**],
National Internet Development Agency of Korea[***]

요 약

인터넷 주소자원과 관련된 연구 중 활발히 진행되고 있는 분야가 이동성과 멀티홈 제공에 관련된 분야들이다. 그들 중 대표적인 것인 HIP인데, 이것은 네트워크 계층과 트랜스포트계층 사이에 새로운 계층과 프로토콜을 제안하여 제한된 형태의 신뢰성과 이동성, 멀티홈 등을 지원하고 있다. 현재 멀티홈과 이동성을 제공하고자 하는 다양한 연구가 진행 중이며, 인터넷 망 망구조의 변화가 예상된다.

1. 서론

인터넷 주소자원과 관련된 연구 중 활발히 진행되고 있는 분야가 이동성과 멀티홈 제공에 관련된 분야들이다. 이러한 이동성 제공과 멀티홈 제공을 위해 인터넷의 식별자와 주소를 분리하고자 하는 연구는 수차례에 걸쳐 제시되어 검토되었으나 결론을 내리지 못하고, 다양한 실험적 접근이 이루어지고 있다. HIP(Host Identity Protocol)[1]는 그들 중 대표적인 프로토콜로서 하부 구조나 프로토콜, NAT 등의 기존 하부구조와의 연계 방안 등이 모색된 상태이며, 공개적인 구현 결과도 발표된 바 있다.

한국인터넷진흥원에서는 이러한 인터넷 주소 자원에 대한 연구 동향을 지속적으로 분석하고 있으며, 신기술에 대한 실험, 분석 및 관련 표준안 개발을 지속적으로 추진 중이다. 본 논문은 인터넷 주소자원에 관련된 IETF의 연구들, 특히 HIP에 대해 진행 중인 연구를 분석한 결과를 담고 있다.

먼저 2장에서는 멀티홈을 제공하기 위한 여러 가지 접근 방식을 살펴보고, 특히 Shim6 WG[2]의 동향을 정리하고, 3장에서는 이동성 제공을 위한 Mobile IP[3]의 기본 개념과 MEXT(Mobility EXTentions for IPv6) WG[4], NETLMM (Network-based Localized Mobility Management) WG[5]의 동향을 정리한다. 4장에서는 HIP의 기본 개념과 랑데부 메커니즘 등을 정리하고 5장에서 결론을 맺는다.

2. 멀티홈과 식별체계

현재 고려되고 있는 멀티홈 형태는 호스트 멀티홈과 사이트 멀티홈이다. 호스트 멀티홈의 경우 호스트가 전역 IP 주소를 2개 이상 가지는 경우인데, 이러한 주소들은 하나의 ISP에 속해 있을 수도 있고, 하나의 인터페이스에 2개 이상의 주소를 부여하거나, 또는 복수개의 인터페이스에 각각의 주소가 부여될 수도 있다. 사이트 멀티홈의 경우 공중 인터넷과의 연결을 2개 이상 가지고 있는 경우를 뜻하는데, 이때 동일한 ISP에 복수개의 연결을 가질 수 도 있고, 복수개의 ISP에 연결을 가질 수도 있다.

이러한 멀티홈을 구성하게 되는 이유는 첫째, 하나의 ISP가 다운되어도 다른 ISP를 이용하여 서비스를 계속 할 수 있도록 하는 장애 극복(fault tolerance)과 예비(redundancy) 기능이 가능하며, 둘째, 2개 이상의 ISP를 통해 서비스함으로써 전체 처리율(throughput)을 높일 수 있는 부하 균형(load balancing)이 가능하며, 셋째, 서비스 가격이나 정책에 따라 해당 서비스의 비용이 제일 저렴한 ISP를 선택할 수 있도록 하기 위해서이다.

이러한 멀티홈을 지원하기 위한 여러 가지 방안들을 분류해 보면 다음과 같다[6].

- IPv4 접근 방식 : IPv4의 접근방식과 같이 사이트의 지역 프리픽스를 도메인간 라우팅 시스템에 알리는 방식이다. 이러한 프리픽스가 최상위 라우팅 시스템 DFZ(default free zone)까지 전파되어야 하는데, 이 때문에 확장성 문제가 있다.
- IPv6 라우팅 방식 : IPv6의 라우팅에 새로운 방법을 추가하여 문제를 해결하기 위한 방법들이다.
- 식별자/위치 (2 공간) 방식 : 여러 가지 방식들이 제안되고 있는데, 이들은 모두 노드를 지칭하는 식별자와 인터넷 위치주소를 구별하는 것이다.
- 이동성 방식 : 이동성을 멀티홈의 특별한 경우로 보는 방식으로 Mobile IPv6를 비롯해 여러 가지 방식이 제안되고 있다.
- 트랜스포트 방식 : 기존의 트랜스포트나 다른 상위 계층 프로토콜이 멀티홈을 지원하지 않는데 반해 새로 제안되고 있는 방식들은 주소 변화에 따른 지원이 상위 계층에 포함되어야 한다는 방식이다.
- Site Exit 라우터와 호스트 동작 : 이 부류의 방식들을 사이트 출구 라우터와 호스트들의 동작을 수정하여 멀티홈을 지원하는 것이다.

* 본 연구는 2008년 한국인터넷진흥원의 표준화 연구과제의 결과물임.

그 중에서 위치주소와 식별자를 분리하는 방식으로 제안된 것들은 다음과 같다.

- Multihoming without IP Idetifiers (NOID)
- Weak Identifier Multihoming Protocol (WIMP/WIMP-F)
- LIN6
- HIP
- Cryptographic based Identifiers
- Strong Identity Multihoming
- Hashed Based Addressing

이러한 멀티홈을 지원하는 것은 IPv4보다는 IPv6에서 훨씬 적합한데, 그것은 복수 주소에 대한 동적인 감지와 상속이 훨씬 용이하기 때문이다. IPv6 호스트가 망에 접속하는 경우 IPv6 라우터들로부터 라우터 광고 메시지를 받을 수 있고, 또한 자동설정 방법으로 각각의 망에 대해 전역적으로 유일한 주소를 할당할 수도 있다. 따라서 IPv6 호스트는 부팅이 되는 순간 멀티홈이 가능하다.

2004년 61차 IETF 회의 때 IPv6 사이트 멀티호밍의 표준을 담당하는 Multi6 워킹그룹에서 여러 가지 제안된 솔루션들 중 식별자와 위치정보를 분리하여 멀티호밍을 지원하는 기고서들을 종합하여 Shim을 제안하였고, 2004년 62차 IETF 회의에서 Multi6 WG를 종료하고, Shim6 워킹그룹에서 Shim의 표준화를 진행하도록 결정하였다[2].

Shim은 기본적인 개념은 HIP와 유사하지만 오직 IPv6 사이트 멀티호밍만을 지원하기 위한 방법으로 제안되었다. 이것은 다른 에이전트의 도움 없이 오직 호스트에 식별자와 위치 주소를 매핑하는 Shim 계층만 존재하면 멀티호밍이 가능하며 기존 단말들과의 호환성을 보장한다. 이를 위해 먼저 호스트의 식별자는 새로운 이름 공간을 사용하지 않고 기존 IP 주소를 사용한다[7].

다음 그림은 Shim6에서의 식별자와 위치정보와의 관계를 보여주는데, Shim6에서는 상위 계층의 식별자로 하위 위치정보(IP 주소)들 중 하나를 선택하여 이용하며, 통신 중인 링크의 문제로 인해 다른 링크를 사용해야 하는 경우 위치 주소가 변경되어도 처음 세션을 맺은 식별자는 유지된다.

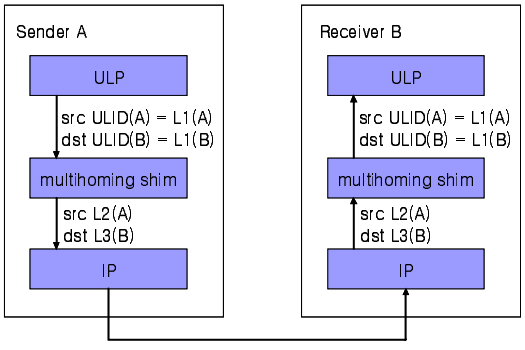

그림 1. Shim6에서 ULID와 Locator의 관계[7]

3. 이동성과 식별체계

인터넷에 있는 이동 노드들에게 이동성 제공을 위한 대표적인 연구가 Mobile IP인데, 이것에 대한 요구 사항은 다음과 같다. 먼저 이동 노드는 IP 주소를 바꾸지 않고 인터넷에 링크층의 접촉점을 바꾼 후에 다른 노드들과 통신할 수 있어야 한다. 또한 이동 노드는 이러한 이동 기능들을 하지 않는 다른 노드들과 통신할 수 있어야 한다. 새로운 구조 하에서 작동하지 않는 호스트 또는 라우터에서는 프로토콜의 향상이 요구되지 않으며, 이동 노드의 위치에 대하여, 또 다른 노드들을 갱신하는데 사용되는 메시지들은 원거리 수신 전환 발생을 막기 위해서 인증되어져야 한다[3].

이동 노드가 인터넷에 직접 접속되는 링크는 종종 무선 링크가 될 수 있는데, 이 경우 링크는 낮은 대역폭을 가질 수 있고 일반적인 유선망보다 더 높은 에러율을 가질 수 있다. 또한 이동 노드는 전력소비를 최소화하는 것이 중요하다. 그러므로 링크 상에 보내지는 관리 메시지의 수가 최소화 되어져야 하고 이들 메시지의 크기는 가능한 한 작아야 한다.

Mobile IP에서는 홈 네크워크 상에서 장기의 IP 주소가 이동 노드에 부여되는데, 이를 홈 주소(home address)라 지칭하며, 고정된 호스트에 주어진 영구 IP 주소와 같은 방식으로 관리되어진다. 이동 노드가 자신의 홈 네트워크에서 멀어졌을 때 COA(care-of address)가 이동 노드와 관계되어지고, 이것은 이동 노드의 현재 접속점을 나타낸다. 이동 노드는 모든 IP 데이터그램에 대해 소스 주소로 자신의 홈 주소를 사용한다.

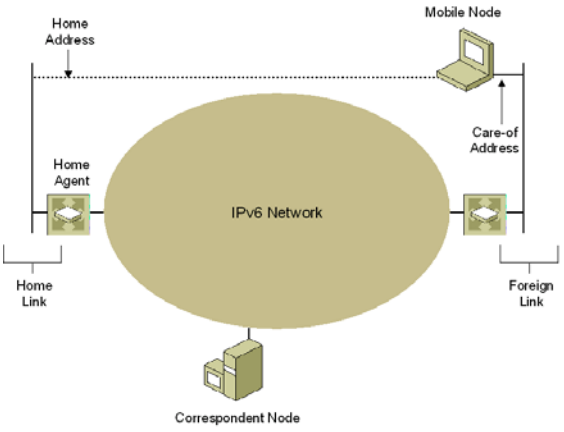

그림 2. MobileIPv6 의 요소

Mobile IPv6는 IP 상위계층에게 투명성을 지원하는데, 이를 기반으로 하는 망 이동성(NEMO: network mobility) 메커니즘은 망 전체가 이동하는 것을 관리할 수 있도록 해준다. MEXT 그룹은 RFC 3775 (Mobile IPv6), RFC 3963 (NEMO), RFC 4877 (Mobile IPv6 Operation with IKEv2)를 기반으로 하여, 기존의 MIP6, NEMO, MONAMI6 WG의 작업을 이어받아 작업을 계속 진행 중이다. MEXT WG의 중요 목표는 보다 넓은 범위에서 적용될 수 있도록 IPv6 이동성을 확장하고, 적용 시나리오를 개발하는 작업을 계속하며, 구현이나 상호운용 과정에서 나타나는 문제점들을 해결하는 것이다[4].

한편, IP 노드의 이동성 관리시 지역 이동성(localized mobility)과 글로벌 이동성(global mobility)을 분리하여 관리하는 것이 더 효율적이라는 주장이 힘을 얻고 있는데, 여기서 지역화된 이동성은 관리가 가능한, 연속적인 부분망의 집합 내에서 일어나는 이동성이고, 글로벌 이동성은 그러한 경계를 넘어

가는 이동성이라 볼 수 있다. 이러한 지역화된 이동성에 관련된 연구로 수행된 것 중 대표적인 것이 FMIPv6(Fast-Handovers for Mobile IPv6)와 HMIPv6(Hierarchical Mobile IPv6)이다. HIP와 MOBIKE(IKEv2 Mobility and Multihoming) 연구가 보다 더 다양한 이동성에 대한 요구를 인식시켰고, WLAN 인프라는 호스트 스택의 참여 없이 이동성 지원이 가능하다는 것을 보여주어 새로운 시도를 하게 되었다. 여기서는 먼저 다음 그림과 같이 지역 이동성과 글로벌 이동성의 범위를 결정하고 보다 효율적인 이동성 제공 방안을 모색하고 있다. 호스트가 아닌, 망 차원에서의 이동성 제공이라는 새로운 접근 방식은 앞으로의 많은 변화를 예고하고 있다[5][10][11].

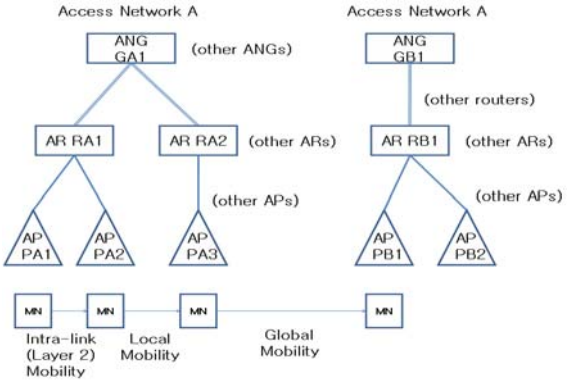

그림 13. 지역 및 글로벌 이동성 관리 영역

4. HIP(Host Identity Protocol)

현재의 인터넷은 두개의 중요한 이름 공간을 가지고 있는데, 그것들은 IP(Internet Protocol) 주소와 DNS(Domain Name Service) 이름이다. 이들은 오늘날의 인터넷이 존재할 수 있도록 하는 여러 가지 기능들을 제공하고 있다. 그러나 그것들은 두 개의 이름 공간만으로 모든 기능들을 담으려고 하는 과정에서 의미의 중복이 발생하고 과도한 기능 확장으로 이름 공간이 복잡해지는 문제점들이 발생했다[1][12].

호스트 정체성(HI: Host Identity) 이름공간은 이러한 IP와 DNS 이름 공간 사이를 채우기 위해 생겨난 것으로서, 호스트 식별자(HI: Host Identifier)들로 구성된다. 이때 하나의 HI는 암호화되어 있으며, 비대칭형 암호쌍 중 공개키로 볼 수 있다. 각 호스트는 적어도 하나의 HI를 가져야 하며, 일반적으로 하나 이상의 HI를 갖는다. 각 호스트 정체성은 하나의 호스트를 식별한다. 즉 두 호스트는 같은 HI를 가질 수 없다. 호스트 정체성과 그것에 대응하는 호스트 식별자는 공개적(DNS로 발표)일 수도 있고 미발표될 수도 있다.

이러한 호스트 식별자는 IKEv2와 같은, 많은 인증 시스템에서 이용될 수 있지만 HIP(Host Identity Protocol) 구조(architecture)에서는 HIP라고 부르는 새로운 프로토콜과 HIP 기본 교환(base exchange)라고 부르는 암호화된 교환을 제시한다. 새로운 프로토콜은 시스템들 간에 제한된 형태의 신뢰를 제공하며, 이동성, 멀티홈, 동적 IP 주소변경를 확장하며, 프로토콜 번역/변환을 지원하고 DOS(denail- of-service)와 같은 종류의 공격을 줄여준다.

이러한 특징들을 만족하는 새로운 이름공간을 호스트 정체성 이름공간이라고 하는데, 이러한 이름공간을 이용한다는 것은 망 계층과 트랜스포트 계층 사이에 새로운 프로토콜 계층 – HIP를 필요로 한다. 또한 이들 이름은 인증 서비스를 제공하기 위하여 공개키 암호화에 기반을 두고 있다.

호스트 정체성 이름공간의 하나의 이름, 즉 하나의 호스트 식별자는 IP 스택을 가지고 있는 어떤 시스템을 명명할 수 있는, 통계적으로 전세계에 걸쳐 유일한 이름을 나타낸다. 이러한 정체성은 일반적으로 하나의 IP 스택에 연관되어 있고, 하나의 시스템은 여러 개의 정체성을 가질 수 있다. 이때 그들 중 일부는 '잘 알려진' 것들이고 일부는 미발표되거나 익명으로 된 것들이다.

또한 시스템은 스스로 자기 자신의 정체성을 주장할 수도 있고, 어떤 것들은 DNSSEC, PGP, X.509와 같이 정체성을 증명하기 위해 제 3의 인증자를 이용할 수 있다. HIP에서 호스트 식별자는 처음에 DNSSEC을 통해 인증받도록 되어 있고, 따라서 구현에서는 최소한 기본적으로 DNSSEC을 지원해야 한다. HIP의 저자들은 공개키 쌍의 공개키가 가장 좋은 HI로 판단하고 있다. HIP 프로토콜 문서에서 언급된 것과 같이 공개키 기반 HI는 HIP 패킷을 인증하고, man-in-the-middle 공격을 방어할 수 있다. HIP의 denial-of-service 공격을 방어하기 위해 데이터그램의 인증이 필수적이므로 HIP의 Diffie- Hellman 교환은 인증되어야 한다. 따라서 실제로는 공개키 기반 HI와 인증된 HIP 메시지만이 지원된다.

호스트 정체성은 인터넷 프로토콜에 두가지 중요한 기능을 제공한다. 먼저 망과 트랜스포트 계층을 분리시킨다. 이러한 분리는 두 계층의 독립된 진화를 가능하게 한다. 또한 여러 망이 연결된 환경에서 종단간 서비스를 제공한다. 두 번째 기능은 호스트 인증 기능이다. HI가 하나의 공개키이므로 이 키는 IPSec과 같은 보안 프로토콜에서의 인증에서 이용될 수 있다.

실제로 인터넷 프로토콜에서는 호스트 식별자가 직접적으로 이용되지 않는다. 실제로는 대응하는 호스트 식별자가 다양한 DNS나 LDAP 디렉토리에 저장되어 있고, HIP 기본 교환에서만 전달된다. 다른 프로토콜에서는 HIT(Host Identity Tag)가 호스트의 정체성을 나타낸다. 호스트 정체성의 또 다른 표현인 LSI(Local Scope Identifier)도 프로토콜과 API들에서 이용될 수 있다.

HIT는 호스트 정체성을 128비트로 표현한 것이다. 일반적으로 이것은 호스트 식별자의 암호화 해쉬로 얻어지는데, 이러한 HIT의 사용은 고정된 길이로 인해 프로토콜 코딩이 용이하고, 작은 패킷 크기로 인해 전송 과정에서 이득을 볼 수 있다는 점과 암호화 알고리즘에 독립적으로, 일관된 형태로 식별이 가능할 수 있다. LSI 역시 호스트 정체성의 다른 표현인데 32비트의 길이를 갖는다. 이것은 현재의 프로토콜과 API들에서 호스트 정체성을 이용하고자 할 때 유용하게 쓰일 수 있으며, 약점은 작은 크기로 인해 전세계적으로 이용할 수는 없고, 지역적으로만 이용이 가능하다는 점이다.

다음은 HIP 기본 교환을 보여준다. 초기자와 응답자 사이에는 4개의 메시지가 교환되고 그 과정을 거쳐 HIP 연관(Association)을 얻게 된다.

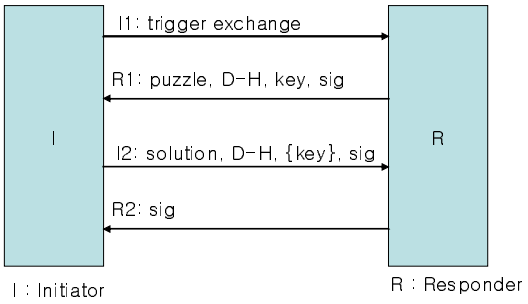

그림 4. HIP base exchange[12]

HIP에서는 이동성, 멀티홈, 동적 주소변경을 위해 랑데부 메커니즘을 제공하고 있는데, 이 경우 초기자는 응답자에게 직접 메시지를 보내는 것이 아니라 랑데부 서버에게 I1을 보내고 그것이 응답자에게 I1을 전달함으로써 HIP 연관을 얻게 된다[9][10].

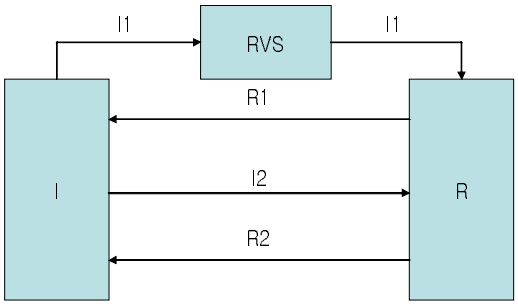

그림 5. RVS를 이용한 연관 설정 과정[15]

.현재 인터넷 상에서 공식적으로 운영되고 있는 대표적인 등록 체계가 DNS인 관계로, 공개될 필요가 있는 호스트 식별자는 DNS에 저장하는 것이 가장 현실적인 대안으로 보여진다. 다음은 HIP의 연관 설정 과정에서 DNS가 참여하는 경우들을 보여주고 있다.

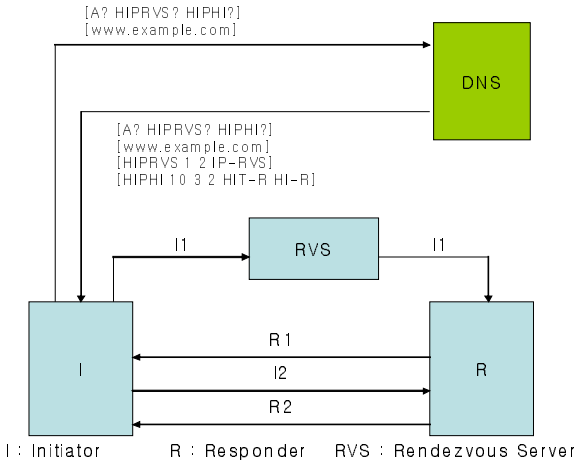

그림 6. 랑데부 서버가 있는 경우 DNS의 참여[15]

DNS에서 저장할 공개된 호스트 식별자는 새로 정의하는 새로운 RR(Resource Record) 타입 HIPHI RR로 저장된다. 이러한 RR 타입은 IPSECKEY RR과 아주 유사하다[16].

5. 결론

본 논문에서는 인터넷 주소자원과 관련된 연구 중 이동성과 멀티홈 제공에 관련된 분야들을 살펴보고 정리하였다. 아직까지는 실험적으로 진행 중인 HIP, MEXT WG의 연구가 본격적으로 진행되어, 도입이 결정되는 경우 망 구조에 대한 근본적인 변화가 올 수 있다. 한국인터넷진흥원에서는 이러한 인터넷 주소 자원에 대한 연구 동향을 지속적으로 분석하고 있으며, 앞으로도 인터넷 주소자원 관련 신기술에 대한 실험, 분석 및 관련 표준안 개발을 지속적으로 추진할 계획이다.

참고문헌

[1] http://www.ietf.org/html.charters/hip-charter.html
[2] http://www.ietf.org/html.charters/mext-charter.html
[3] http://www.ietf.org/html.charters/shim6-charter.html
[4] http://www.ietf.org/html.charters/mip4-charter.html
[5] http://www.ietf.org/html.charters/netlmn-charter.html
[6] Lear, E. and R. Droms, "What's In A Name: Thoughts from the NSRG", draft-irtf-nsrg-report-10 (work in progress), September 2003
[7] Nordmark, E., M. Bagnulo, "Shim6: Level 3 Multihoming Shim Protocol", draft-ietf-shim6-proto-10(work in progress), 2008
[8] N. Montavont, R. Wakikawa, T. Ernst, C. Ng, K. Kuladinithi, “Analysis of Multihoming in Mobile IPv6”, draft-ietf-monami6-mipv6-analysis-05(work in progress), 2008
[9] Hesham Soliman, “Mobile IPv6 Support for Dual Stack Hosts and Routers (DSMIPv6)”, draft-ietf-mext-nemo-v4traversal-03(work in progress), 2008
[10] J. Kempf, “Problem Statement for Network-Based Localized Mobility Management (NETLMM)”, RFC 4830, 2007
[11] J. Kempf, “Goals for Network-Based Localized Mobility Management (NETLMM)”, RFC 4831, 2007
[12] Moskowitz, R., P. Nikander, "Host Identity Protocol Architecture", RFC 4423, IETF, 2006
[13] Moskowitz, R., P. Nikander, P. Jokela, T. Henderson, "Host Identity Protocol", RFC 5201, 2008
[14] T. Henderson, "End-Host Mobility and Multihoming with the Host Identity Protocol", RFC 5206, 2008
[15] Laganier, J., L. Eggert, "Host Identity Protocol (HIP) Rendezvous Extension", RFC 5204, 2008
[16] P. Nikander, J. Laganier, "Host Identity Protocol (HIP) Domain Name System (DNS) Extension", RFC 5205, 2008