

IEEE 802.16 망에서의 IPv6 ND 프로토콜 적용방안

이 주 철 Protocol Engineering Center, ETRI
장 희 진 Samsung Advanced Institute of Technology
김 형 준 Protocol Engineering Center, ETRI

● 와이브로 + IPv6 특징

와이브로 망에서 IPv6 단말의 고속 핸드오버 최적화 방안
IEEE 802.16/와이브로/Mobile-WiMAX 표준화 현황 및 전망
IEEE 802.16/와이브로 망에서의 IPv6 도입 시나리오 및 고려사항

IEEE 802.16 망에서의 IPv6 ND 프로토콜 적용방안

와이브로 네트워크를 위한 IPv6 기술 표준화
와이브로 서비스 추진 및 향후 시장 전망

● 요약

IEEE802.16은 브로드밴드 무선 액세스 망을 위한 MAC 및 PHY 계층을 정의한 새로운 프로토콜이다. 이 프로토콜은 기존에 사용되던 IEEE802.11 무선랜이나 3G와는 달리, 더 높은 대역폭 및 더 넓은 서비스 지역과 같은 장점을 가진다. IEEE802.16은 현재 TTA의 PG302 휴대인터넷 프로젝트 그룹에서 IEEE802.16e를 기반으로 국내 표준화가 마무리되어 있으며, WiBro라는 서비스 명으로 상용서비스를 준비 중에 있다. 현재 구현되어 있는 WiBro는 IPv4만을 지원하고 있기 때문에 향후 IPv6를 지원할 시에 발생할 수 있는 문제점들에 대해서는 아직 구체적으로 고려되어져 있지 않다. 특히 IEEE802.16의 MAC은 IP 프로토콜 설계시 가장 기본적으로 고려되고 있는 IEEE802.3의 그것과는 많이 다르기 때문에 이에 대한 고려없이 IPv6를 IEEE802.16 망에 적용할 경우 올바른 동작을 보장하기 어렵다. 본 논문에서는 앞서 언급한 발생 가능한 문제점 중 IPv6 ND 프로토콜에 대한 이슈를 중심으로 IEEE802.16상에서의 IPv6 적용에 관해 다루고자 한다.

1. 서론

어느덧 우리 생활의 주변을 파고든 무선랜 서비스는 xDSL, 케이블 모뎀 등을 통한 고속인터넷의 급속한 보급과 비견될 정도로 인터넷 통신방식의 혁명을 가져왔다. 이미 상업 인터넷 서비스를 위한 수많은 AP(Access Point)가 거

리 곳곳에 설치되어 장소를 구애 받지 않고 무선으로 편리하게 인터넷 서비스를 받을 수 있게 되어 있으며, 최근 생산되고 있는 노트북이나 PDA와 같은 모바일 기기에도 대부분 무선랜 인터페이스가 기본으로 탑재되고 있다. 이렇게 무선랜 사용자가 늘어남에 따라 좁은 서비스 지원영역이나, 이동중의 서비스 지원 불가 등과 같은 무선랜의 한계점들도 드러나고 있다. IEEE802.16프로토콜은 이러한 무선랜 기

술에 비하여 보다 넓은 서비스 지원영역, 이동중의 서비스 지원등과 같은 장점을 가지고 있는 새로운 브로드밴드 무선 액세스 망을 위한 프로토콜이다.

IEEE802.16프로토콜은 현재 TTA의 전파방송 기술위원회(TC3) 산하의 2.3Ghz 휴대인터넷 프로젝트 그룹에서 WiBro라는 이름으로 PHASE I 국내 표준화 작업을 완료하였으며, 현재 PHASE II 개정 작업을 진행 중이다. 현재 구현되어 있는 WiBro는 IPv4만을 지원하며, IPv6는 향후 지원할 예정으로 있다. 따라서 아직 IPv6를 도입했을 때 고려해야 할 이슈들에 대해서는 충분히 논의되지 않은 상황이다.

IPv6 코어프로토콜 중의 하나인 NDP(Neighbor Discovery Protocol) [1]는 기본적으로 멀티캐스팅 기술에 의존하고 있으며, 현재 가장 널리 쓰이고 있는 IEEE802.3의 MAC은 로컬 서브넷에서의 멀티캐스팅을 효율적으로 지원하고 있다. 또한 IEEE802.11 무선랜도 IEEE802.3의 MAC과 유사하게 멀티캐스팅을 지원하고 있기 때문에 기존의 IPv4나 IPv6의 적용시 큰 문제는 없었다. 하지만 IEEE802.16은 기본적으로 패킷망을 상정하고 만들어졌지만 앞서 언급한 두 프로토콜과 같은 멀티캐스팅 방식을 지원하지 않기 때문에, IEEE802.16망에 IPv6를 그대로 적용하면 올바른 동작을 보장하기 어렵다. 따라서 사전에 발생 가능한 문제점에 대하여 충분한 검토 및 그에 대한 솔루션이 필요하다고 보여진다.

본 논문의 구성은 다음과 같다. 2장에서는 IEEE802.16과 관련된 용어의 정리 및 IEEE802.16망에 NDP를 적용했을 경우에 고려되어야 할 이슈들을 설명하며, 3장에서는 2장에서 설명한 이슈들에 대해 가능한 해결책의 예시를 들어 보이고, 마지막 4장에서 결론을 맺는다.

2. IEEE802.16상의 NDP적용과 관련된 이슈

2.1 IEEE802.16 관련 용어

- MS: Mobile Station, 임의의 지점에서 정지해 있거나 이동하는 환경에서 가용한 모바일 서비스 환경을 이용하는 단말기. MS는 문서에서 특정한 언급이 없으면 항상 SS(Subscriber Station)의 역할을 겸한다.
- BS: Base Station, 각각의 MS에 대해서 connection을 제공, 관리 및 제어하는 장비. BS와 MS 사이의 단방향 연결 매핑은 서비스 플로우의 트래픽을 전송하는데 쓰인다.
- SS: Subscriber Station, 가입자 장치와 BS 사이의 연결을 제공하는 장비(단말기).
- 802.16 subnet : 한 BS에 접속하고 있는 모든 MS들로 구성된 서브넷(이 용어는 본 문서에서만 사용되는 용어임).
- CID: Connection Identifier, BS와 MS의 MAC들로 이루어진 연결을 식별하는 16비트 식별자. CID는 이 연결과 연관된 서비스 플로우의 QoS 파라미터를 정의하는 서비스 플로우 아이디(SFID)와도 매핑된다.
- PDU: Protocol Data Unit, peer간의 같은 프로토콜 계층 사이에 주고받는 데이터 유닛을 지칭한다. 프로토콜 계층구조에서 PDU는 하위 방향으로는(하위 계층방향) 하위 계층을 위해서 생성된 데이터 유닛을, 상위 방향으로는 하위 계층으로부터 받은 데이터 유닛을 의미한다.
- SDU: Service Data Unit, 인접한 두 프로토콜 계층 사이에서 주고받는 데이터 유닛. 하위 방향으로는 이전 상위 계층에서 받은 데이터 유닛을 의미하며, 상위 방향으로는 다음 상위 계층으로 보내진 데이터 유닛을 의미한다.

- SAP: Service Access Point, 프로토콜 스택 상에서 하위 계층이 상위계층으로 제공하는 서비스를 호출하기 위한 인터페이스.

2.2 IEEE802.16 architecture와 관련된 이슈들

A. Point-to-Multipoint connection

IEEE802.16은 기본적으로 점대다(Point-to-Multipoint) 연결의 특징을 가지고 있다. 즉, 한 BS에 접속하고 있는 모든 MS들은 BS를 거쳐서 서로 통신을 하며, 또한 BS는 특정 연결에 가입한 여러 MS들에게 동시에 데이터를 보낼 수도 있다. 따라서 설정 한 BS에 접속되어 있는 MS들이 동일한 프리픽스를 가지고 있다고 하더라도 서로 직접 통신을 할 수는 없다.

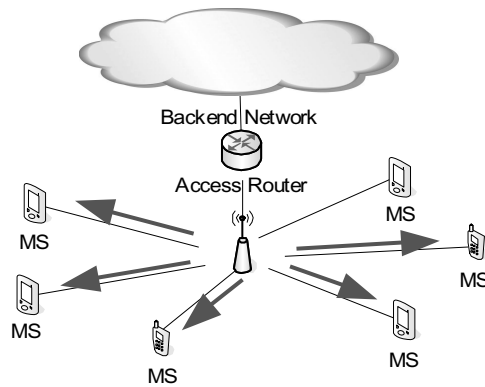


그림 1. Point-to-Multipoint

B. Convergence Sublayer

일반적으로 IEEE802.16의 MAC은 Service-Specific Convergence Sublayer(CS), MAC Common Part Sublayer(CPS), Security Sublayer와 같은 3개의 계층으로 이루어져 있다[6]. CS는 CS SAP를 통해서 받은 데이터의 MAC SDU로의 변환 및 매핑의 역할을 수행한다. 이 데이터는 MAC SAP를 통해서 MAC CPS로 전달되어진다.

또 한 가지 CS의 주된 기능은 수신한 네트워크 SDU를 관련된 파라미터를 이용해서 분류한 후, 해당되는 MAC 서비스 플로우 아이디(SFID) 및 연결 식별자(CID)를 찾아서 그것과 연관시키는 일이다.

IEEE802.16은 ATM CS 및 Packet CS와 같은 두개의 CS를 제공하는데, Packet CS는 다시 이더넷 CS와 IP CS로 나누어진다.

- 이더넷 CS: 이더넷 CS가 수신한 SDU에는 IP 헤더 및 이더넷 헤더까지 포함되어 있다. 따라서 이더넷 CS를 채용한 IPv6 MS는 이더넷 주소의 실제 쓰임새와는 별도로 address resolution을 해야한다. 또한 만약 한 BS에 접속되어 있는 MS들이 'L' 비트가 설정된 동일한 프리픽스를 할당받아 있다면, 이 MS들이 서로 통신을 하고자 할때 상대방의 이더넷 주소를 바로 얻어낼 수 있어야 한다. 하지만 이것은 앞서 언

급한 IEEE802.16의 point-to-multipoint 특성 때문에 매우 어렵다.

- IPv6 CS: IPv6 CS가 수신한 SDU에는 IP 헤더만이 포함되어 있다. 따라서 이 경우에는 address resolution이 반드시 필요하지는 않다. 하지만 IPv6 계층은 IPv6의 하위에 어떤 CS가 있는지 알 수 없기 때문에 address resolution과정을 무시할 수는 없다.

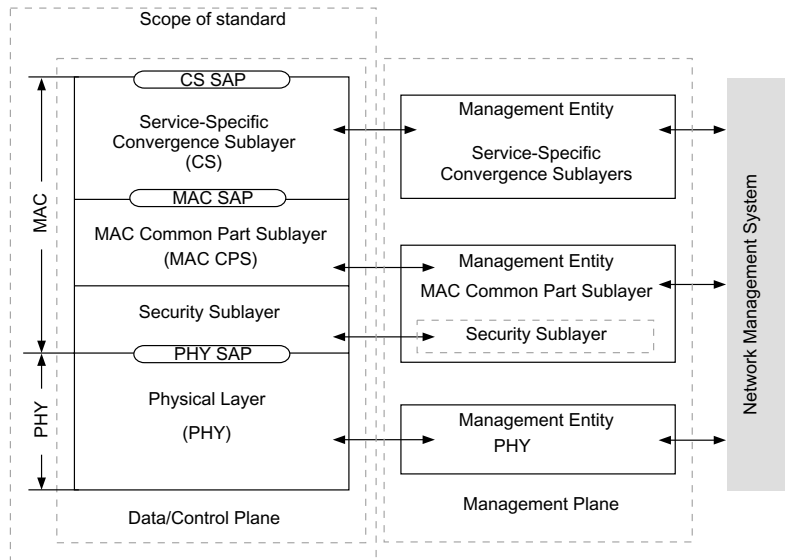


그림 2. IEEE802.16 Protocol Layering

C. Multicast Support

NDP는 그 자신의 동작을 위해서 몇몇 멀티캐스트 주소를 이용한다. 하지만 IEEE802.16은 IEEE802.3의 경우와 같은 native multicast 방식을 지원하지 않는다. IEEE802.3에서는 각 링크로컬IPv6 멀티캐스트 주소에 상응하는 MAC 주소를 만들어내며 이 주소를 인식할 수 있다 [5]. 따라서 별도의 특정한 메커니즘이 없어도 멀티캐스트 패킷을 잘 수신할 수 있다. 하지만 IEEE802.16은 MAC 계층에서 이러한 멀티캐스트 용도의 MAC 주소를 사용하지 않는다. 따라서 멀티캐스트를 지원할 별도의 다른방법을 고려하여야 한다.

D. BS Architecture & Subnet model

BS은 그 구성방법에 따라 가능한 두가지 조합이 있으며, 프리픽스는 그 할당방식에 따른 고려가능한 두가지 경우가 있다. 이 장에서는 위 각각에 대한 이슈를 살펴본다.

- 라우터가 BS와 분리된 경우: 액세스 라우터는

IEEE802.16 BS와 별도로 분리되어 있다. 이 경우 BS는 MAC과 PHY계층만을 가지고 있으며 별도의 라우터 기능은 가지고 있지 않다. 하나의 라우터와 몇몇 BS들은 IPv6 서브넷을 구성하며, BS가 IP 프로토콜 계층을 가지고 있지 않기 때문에 BS와 액세스 라우터 사이의 인터페이스에 대하여 고려하여야 한다. 따라서 SS와 액세스 라우터 사이에는 항상 IEEE802.16을 포함한 두가지 링크가 존재하게 된다.

- 라우터와 BS가 하나의 디바이스에 있는 경우: 그림 4는 라우터와 BS가 하나의 디바이스에 있는 경우를 나타낸 것이다. 이 경우 하나의 IPv6 서브넷은 하나의 라우터 및 하나의 BS로 구성된다. 이 경우에 많은 IPv6 관련 이슈들이 하부 네트워크에 상관없이 IEEE802.16 링크만을 고려하면 된다.

프리픽스 할당방식에 대한 구분

- MS당 하나의 프리픽스를 할당하는 경우: "Recommendations for IPv6 in Third Generation

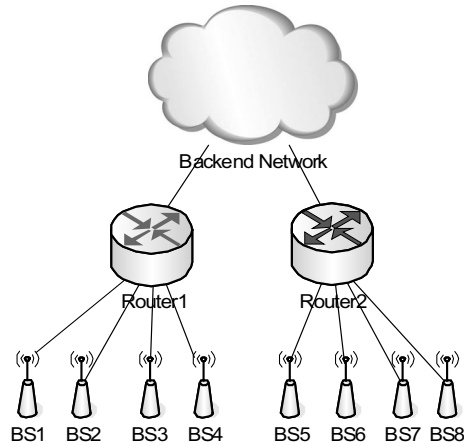


그림 3. 라우터와 BS가 분리된 경우

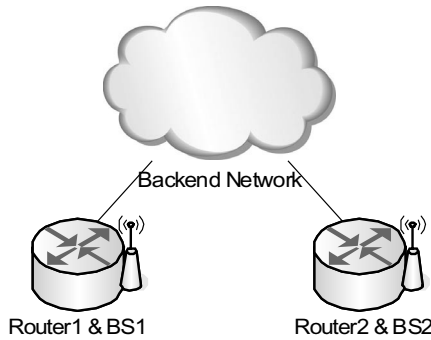


그림 4. 라우터와 BS가 하나의 디바이스에 있는 경우

Partnership Project(3GPP) Standards, “오류! 참조 원본을 찾을 수 없습니다”는 주소충돌의 가능성을 원천적으로 배제하기 위해서 하나의 PDP context당 하나의 프리픽스를 할당할 것을 권고하고 있다. 이러한 가정은 IEEE802.16에도 똑같이 적용될 수 있다. 즉 하나의 MS 당 하나의 프리픽스를 할당하여 각각의 MS와 BS로 이루어진 서브넷을 이루도록 하는 것이다. 이렇게 함으로써 주소충돌의 가능성을 원천적으로 봉쇄하여 많은 NDP동작을 간소화 시킬 수 있다.

- 서브넷 당 하나의 프리픽스를 할당하는 경우: 이 경우는 무선랜의 핫스팟영역과 비슷하게 하나의 BS에 접

속하고 있는 모든 MS들에게 동일한 프리픽스를 할당하는 경우이다. 이 경우는 주소 자동설정시의 주소 충돌검사 및 address resolution에 대해서 고려해야 한다.

E. Transport Connection

MS가 BS에 접속하면 초기화 과정으로 ranging process를 거친다. 이 과정에서 MS는 기본적으로 3개의 CID를 생성한다. 첫번째는 basic connection으로, 짧고 시간에 민감한 MAC 메시지 및 라디오 링크 메시지를 전송하는데 사용된다. 두번째는 primary management

connection으로 인증 메시지나 연결설정 메시지처럼 길지 만 시간에 크게 민감하지 않은 메시지를 전송하는데 이용된다. 마지막으로 세번째는 secondary management connection으로 DHCP와 같은 관리 메시지를 전송하는데 사용된다. 현재의 IEEE802.16 표준에서 NDP가 이러한 기본 connection들 중 하나를 이용해서 메시지를 전송하는 것이 가능한지에 대한 언급은 없다. 따라서 만약 이것이 문제가 된다면 NDP를 위한 connection을 별도로 할당해야 할 것이다.

2.3 IPv6 NDP와 관련된 이슈들

A. Address Autoconfiguration

IPv6 호스트는 링크로컬 유니캐스트 주소 및 글로벌 유니캐스트 주소를 자동설정할 수 있다[2]. 이 주소설정 과정을 완료하기 전에 IPv6 호스트는 생성된 주소의 유일성을 보장하기 위해서 주소 중복 검사(Duplicate Address Detection)를 해야 하는데, 이 DAD는 앞서 언급한 서버넷 모델과 연관이 있다.

만약 프리픽스가 각 MS별로 할당이 되어 있다면 그 MS가 속한 서버넷은 MS와 BS만으로 구성이 되어있기 때문에 사실상 주소충돌의 가능성이 없다. 따라서 실질적인 DAD의 수행이 없이도 그 결과를 예측할 수 있다. 하지만 프리픽스가 802.16 서버넷 자체에 할당이 되어 있다면, 주소중복을 확인하기 위해서 DAD 는 원래의 절차대로 수행 되어야 한다.

B. Router and Prefix discovery

MS가 802.16 서버넷에 접속했을 때 멀티캐스트 방식으로 RS(Router Solicitation) 메시지를 보내고, 그에 대한 응답을 받는 방법에 대한 고려가 필요하다.

C. Conceptual Sending Algorithm

Neighbor Discovery for IP Version 6(IPv6)[1]은 IPv6 노드가 패킷을 보낼 때 내부적으로 수행되는 알고리즘에 대해 기술해 놓았다. IPv6 노드는 패킷을 목적지로 보내기 위한 다음홉을 결정하기 위해서 destination cache, prefix list, default router list 등의 자료구조를 이용한다. 일단 다음홉이 결정되면 이 홉의 MAC 주소를 얻기 위해서 neighbor cache를 검색한다.

- Next-hop determination

다음 홉 결정은 사용하고 있는 CS와 관련이 있다. 만약 이더넷 CS가 사용되었다면 다음 홉 결정과정은 [1]에서 명시하는 과정을 통해서 결정되어야 하며, IPv6 CS가 사용되었다면 다음 홉은 항상 BS/AR이 될 것이다.

- Neighbor cache

Neighbor cache의 내용도 MS가 사용하고 있는 CS와 관련이 있다. 이더넷 CS를 사용하며 목적지 주소 프리픽스의 'L' 비트가 설정되어 있다면, neighbor cache의 내용은 목적지 MS의 MAC 주소가 될 것이다. 만약 IPv6 CS를 사용하고 있거나 프리픽스의 'L' 비트가 설정되어 있지 않다면 neighbor cache의 내용은 BS/AR의 MAC 주소가 될 것이다.

- Address resolution

Address resolution도 CS와 연관이 있다. 이더넷 CS를 사용하며 'L' 비트가 설정되어 있다면 이 과정은 [1]에 명시된 과정을 따라야 한다. 만약 'L' 비트가 설정되어 있지 않거나 IPv6 CS를 사용한다면 IPv6 MS의 다음 홉은 항상 BS/AR이 될 것이다. 또한 MS는 초기화 과정에서 BS의 MAC주소를 알 수 있기 때문에 이때의 address resolution과정은 생략될 수 있다.

- NUD(Neighbor Unreachability Detection)

유니캐스트 패킷을 전송하는 과정에서 neighbor cache 엔트리의 내용을 접근할 때마다 그 캐시의 내용의 유효성을 검사하기 위해서 NUD과정을 수행한다. 이더넷 CS를 사용하고 'L' 비트가 설정된 프리픽스를 포함하고 있다면, NUD과정은 [1]에서 명시한

과정을 따라야 하며, IPv6 CS를 사용하고 있다면 다음 홉은 항상 BS/AR이므로 이에 대해서만 NUD를 수행하면 된다.

3. 솔루션

3.1 Multicast Emulation

2.2.C에서 언급했던대로 IEEE802.16은 native multicast방식을 지원하지 않는다. 이러한 멀티캐스트를 지원하기 위해서 다음과 같은 몇가지 가능한 방법이 있다. BS는 멀티캐스트를 지원하기 위해서 멀티캐스트 그룹 및 패킷 전달을 중앙 집중적인 방법으로 관리한다. BS가 멀티캐스트 패킷을 받으면 BS는 air medium 자원의 효과적인 이용을 위해서 멀티캐스트 패킷의 종류에 따라 다음 룰 중 하나를 선택적으로 적용한다.

- 가) BS는 경우에 따라서 멀티캐스트 패킷을 필터링 시킬 수 있다. BS는 특정한 조건하에서 DAD를 위한 NS 패킷을 필터링시키고 미리 정해진 응답을 보낼 수 있다.
- 나) All-nodes multicast 패킷과 같은 멀티캐스트 패킷이 유니캐스트 방식으로 BS에 접속하고 있는 모든 MS들에게 전송되어질 수 있다. BS는 자신에게 접속되어 있는 MS의 목록을 알 수 있다. 따라서 BS는 unsolicited RA/NA 등과 같은 메시지를 MS들에게 보낼 수 있다.
- 다) Solicited-node multicast 및 all-routers multicast와 같은 멀티캐스트 패킷은 유니캐스트 방식으로 BS에 접속하고 있는 몇몇 MS 들에게만 전송되어질 수 있다. 이 경우는 BS가 멀티캐스트 그룹의 멤버들에 대한 정보를 관리할 필요가 있다.
- 라) 위와 같은 트래픽들은 공용 CID(s)를 통해서도 전송

되어 질 수 있다. 즉 위와 같이 특정 멀티캐스트 그룹에 속한 MS들에게 각각 유니캐스트로 패킷을 전송할 수도 있지만, 그 멀티캐스트 그룹을 위한 특정 connection을 정해두고 멀티캐스트 그룹 멤버들에게 이 connection으로 가입하도록 하면 한 번의 패킷 전송으로 그룹 멤버들에게 모두 전송할 수 있어 air medium자원의 낭비를 막을 수 있다.

- 마) 이 외에 특정 트래픽은 특정한 MS에게만 전달되어질 수 있다.

3.2 Transport Connection

2.2.E에서 언급한대로 MS의 초기화시 기본적으로 할당되는 3개의 connection을 NDP에 사용할 수 없다면, 이를 위한 별도의 connection을 할당해야 할 것이다.

3.3 주소 자동설정

DAD과정에 사용되는 멀티캐스트 메시지의 처리는 3.1에서 언급된 방법으로 해결될 수 있다.

3.4. Router and Prefix discovery

이 과정에서 사용되는 멀티캐스트 메시지의 처리는 3.1에서 언급된 방법으로 해결될 수 있다.

- 프리픽스 정보 옵션의 'I' 비트 설정여부
프리픽스 정보 옵션은 이 프리픽스가 on-link determination에 활용될 수 있는지에 대한 여부를 나타내는 'I' 비트 옵션을 가지고 있다. 2.2.D에서 언급한대로 프리픽스를 할당하는 방법은 두가지가 있다(각 MS당 한개씩, 802.16 subnet당 한개씩). 802.16 서브넷 당 하나의 프리픽스를 할당하는 경우

에, 실질적으로 이 서브넷을 구성하는 MS는 직접적으로 통신을 할 수는 없다 (BS를 거쳐서 통신해야 한다). 이것은 사실 802.16 서브넷을 구성하는 MS 들이 on-link이지 않다는 것을 의미하므로 불필요한 address resolution 과정을 없애기 위해서 'L' 비트가 설정되지 않아야 할 것이다.

4. 결론

IEEE802.3과는 달리 IEEE802.16은 다음과 같은 특성을 갖는다. BS와 MS사이의 링크가 point-to-multipoint의 특성을 가지며, MAC 주소가 IEEE802.16 망을 통해 전송될때 사용되지 않는다. 이러한 특성은 IEEE802.16 망에 IPv6가 즉시 도입되기 어려운 환경을 만들며, 특히 NDP와 같은 멀티캐스트에 의존적인 프로토콜의 동작을 보장하기 어렵게 만든다. 따라서 IPv6를 IEEE802.16 망에 문제없이 도입하려면 본 고에서 언급한 문제점들에 대한 고려와 이를 해결하기 위한 적절한 솔루션의 도입이 필요하다. 본 고에서 언급한 솔루션들은 이 문제점을 해결하기 위한 예시를 든 것으로 실제 구현이나 망 구성에 따른 별도의 해결책이 존재할 수 있다. 하지만 여기서 언급한 기본적인 원리와 크게 벗어나지는 않을 것이다.

참고문헌

- [1] Narten, T., Nordmark, E., and W. Simpson, "Neighbor Discovery for IP Version 6(IPv6)", RFC 2461, December 1998.
- [2] Thomson, S. and T. Narten, "IPv6 Stateless Address Autoconfiguration", RFC 2462, December 1998.
- [3] Haskin, D. and E. Allen, "IP Version 6 over PPP", RFC 2472, December 1998.
- [4] Wasserman, M., "Recommendations for IPv6 in Third Generation Partnership Project (3GPP) Standards", RFC 3314, September 2002.
- [5] Crawford, M., "Transmission of IPv6 Packets over Ethernet Networks", RFC 2464, December 1998.
- [6] "IEEE 802.16-2004, IEEE standard for Local and metropolitan area networks, Part 16:Air Interface for fixed broadband wireless access systems", October 2004.
- [7] Shin, M., "Scenarios and Considerations of IPv6 in IEEE 802.16 Networks", draft-shin-ipv6-ieee802.16-01(work in progress), October 2005. **TTA**