**IEEE 802.11 무선 네트워크 규격 요약 문서.**

**작 성 자 : 김 정 호**

**작 성 일 : 2012년 2월 14일**

**목차**

[**1. 무선 네트워크 구성도.** 4](#_Toc317066656)

[**1.1 IEEE 802.11 이란?** 4](#_Toc317066657)

[**1.2 전송 방식 표준.** 4](#_Toc317066658)

[**2. IEEE 802.11 계층 구조.** 6](#_Toc317066659)

[**2.1 Layer 구조.** 6](#_Toc317066660)

[**2.2 기본 데이터 전송 동작** 7](#_Toc317066661)

[**3. 단말기와 AP의 연동 과정.** 9](#_Toc317066662)

[**3.1 탐색 과정.** 9](#_Toc317066663)

[**3.2 Join(참여)** 11](#_Toc317066664)

[**3.3 인증 절차.** 11](#_Toc317066665)

[**3.4 결합(Association)** 11](#_Toc317066666)

[**4. 프레임 구조.** 12](#_Toc317066667)

[**4.1 802.11 프레임 구조.** 12](#_Toc317066668)

[**4.2 MAC 프레임 구조.** 13](#_Toc317066669)

**■ 서문**

무선 네트워크 디바이스 드라이버를 개발하기에 앞서 무선 네트워크에 대한 지식이 전무한 상태에서 디바이스 드라이버를 개발하려면, 무엇을 먼저 해야 하는가에 대해 고민을 하였다. 개발해야 하는 드라이버는 Windows CE용 드라이버이다. 개발 시점에 가지고 있는 자료로는 안드로이드용 디바이스 드라이버 소스와 인터넷에서 찾은 Windows용 디바이스 드라이버 소스이다. 안드로이드용 소스는 검증되었고 또한 사용되고 있는 소스이기에 문제가 없었지만 Windows 용은 인터넷에서 찾은 검증되지 않는 소스이다. 또 한 WLAN 칩 제조 밴드들로부터 Windows용 소스를 요구하였지만 줄 수 없다는 답변을 받은 상태이다. 이러한 상태에서 고심 끝에 내린 결론은 무선 네트워크 규격문서부터 보는 것이었다. 우리가 일반적으로 WIFI 라고 부르는 무선 네트워크는 IEEE 802.11 이라는 규격이다. 802.11의 규격 문서는 총 1233 페이지에 달하지만 기본적인 구조가 설명이 되어있는 부분은, 5~7장으로 우선 이 장들을 파악 하기로 하였다. 일반적으로 WIFI 기능이 지원되는 기기에서 무선 네트워크에 접속하기 위해서는 AP(Access Point)라는 기기에 접속을 해야 한다. 일단 AP에 접속이 되면 그 다음부터는 유선 네트워크와 같이 사용을 할 수 있기 때문에 무선 네트워크 디바이스 드라이버 개발자의 입장에서는 단말에서 AP에 접속하는 것까지만을 다루면 될 것이다. 무선 네트워크에서 중요시 되는 부분 중 하나가 보안 관련인데, AP에 아무 단말이나 접속할 수 있는 것이 아니라 허용된 단말만이 접속을 할 수 있기 때문에 보안 관련 부분을 보지 않을 수 없다. 그러나 우선 AP와 단말의 접속에 중점을 두고 보안 관련 부분은 차 후에 살펴볼 것이다. 보안 관련 부분이 방대할 뿐 아니라 드라이버 개발자 입장에서는 AP와의 접속이 우선이기 때문이다.

단말에서 AP에 접속하기 위해서는 우선 “Scan”을 한다. 단말의 입장에서 주변에 사용 가능한 AP가 있는지 없는지를 확인하기 위해서다. 그래서 사용가능 AP 리스트를 확보한 다음 “Probe”를 요청하여 AP와 접속한다. AP와 접속한다 해서 연결이 되는 것이 아니라 해당 AP가 단말이 네트워크를 사용할 수 있게 인증을 해줘야 한다. 누구나 사용할 수 있는 AP이면 무조건 인증을 해 주겠지만, 사용 제약이 걸려있는 AP이면 인증 번호 등을 사용하여 인증을 받아야 한다. 인증절차를 거치면 AP와 연동이 되고 그 다음부터는 AP를 통해 네트워크를 사용할 수 있다. AP와 연동이 되는 시점이 유선 네트워크로 따지면 네트워크 케이블을 단말에 연결한 상태이다.

**IEEE 802.11 무선 네트워크 규격**

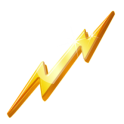
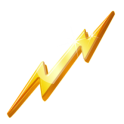
# **1. 무선 네트워크 구성도.**

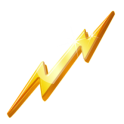
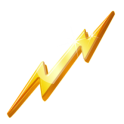
**Distribution System**

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\7DDQNROY\MC900428999[1].WMFC:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\7DDQNROY\MC900428999[1].WMF

**AP**

**AP**









**BSS**

**BSS**

그림 1

## **1.1 IEEE 802.11 이란?**

IEEE802.11은 흔히 무선랜 또는 Wi-Fi라고 부르는 좁은 지역을 위한 컴퓨터 무선 네트워크에 사용되는 기술로 IEEE의 LAN/MAN 표준 위원회 (IEEE802)의 11번째 워킹 그룹에서 개발된 표준을 의미 한다.

## **1.2 전송 방식 표준.**

**- 802.11(초기 버전)**

802.11은 2Mbps의 최고속도를 지원하는 무선 네트워크 기술로, 적외선 신호나 ISM대역인 2.4GHz 대역 전파를 사용해 데이터를 주고 받으며 여러 기기가 함께 네트워크에 참여할 수 있도록 CSMA/CA 기술을 사용한다. 하지만 규격이 엄격하게 정해지지 않아서 서로 다른 회사에서 만들어진 802.11 제품 사이에 호환성이 부족했고 속도가 느려서 널리 사용되지 않았다.

**- 802.11b**

802.11b는 802.11 규격을 기반으로 더욱 발전시킨 기술로, 최고 전송속도는 11Mbps이나 실제로는 CSMA/CA 기술의 구현 과정에서 6~7Mbps 정도의 효율을 나타내는 것으로 알려져 있다. 표준이 확정되자마자 시장에 다양한 관련 제품이 등장했고, 이전 규격에 비해 현실적인 속도를 지원해 기업이나 가정 등에 유선 네트워크를 대체하기 위한 목적으로 폭넓게 보급되었으며, 공공장소 등에서 유무상 서비스를 제공하는 업체도 생겨났다.

**- 802.11a**

세 번째로 등장한 전송방식인 802.11a는 5GHz 대역의 전파를 사용하는 규격으로, OFDM 기술을 사용해 최고 54Mbps까지의 전송 속도를 지원한다. 5GHz 대역은 2.4GHz 대역에 비해 다른 통신기기(무선전화기, 블루투스등)와의 간섭이 적고, 더 넓은 전파 대역을 사용할 수 있다는 장점이 있지만, 신호의 특성상 장애물이나 도심 건물 등 주변 환경의 영향을 받기 쉽게 받고, 2.4GHz 대역에서 54Mbps 속도를 지원하는 802.11g 규격이 등장하면서 현재는 널리 쓰이지 않고 있다.

**- 802.11g**

네 번째로 등장한 802.11g 규격은 a 규격과 전송 속도가 같지만 2.4GHz 대역 전파를 사용한다는 점만 다르다. 널리 사용되고 있는 802.11b 규격과 쉽게 호환되어 현재 널리 쓰이고 있다.

**- 802.11n**

802.11n은 상용화된 전송규격이다. 2.4GHz 대역과 5GHz 대역을 사용하며 최고 600Mbps까지의 속도를 지원하고 있다.

**1.2 802.11 구조.**

그림 1과 같이 802.11의 기본 구성 요소로서 AP, STA(단말기), BSS가 존재 한다. STA는 WLAN 이 장착된 단말기를 말하며 AP는 우리가 알고 있는 무선 AP(Access Point)이다. BSS는 AP와 이것에 접속되어 있는 STA의 구성을 뜻한다.

# **2. IEEE 802.11 계층 구조.**

## **2.1 Layer 구조.**

WLAN의 계층 구조는 Data Link Layer 와 PHY Layer로 구성 되어 있다.

**PLCP**

**MAC**

**PMD**

MAC Layer Management Entity(**MLME**)

PHY Layer Management

Entity(**PLME**)

Station

Management

**Data Link**

**PHY**

그림 2

■ **PMD(Physical Medium Dependent)** 계층: 변복조를 하는 무선 모뎀 기능을 수행한다. 즉 Air로부터 오는 무선 신호를 디지털 신호로 바꾸어 주는 역할을 하는 곳이다.

■ **PLCP(Physical Layer Convergence Protocol) 계층:** MAC 계층과 다양한 Hardware(PMD 계층)을 정합시켜 주는 역할을 하는 곳이다.

■ **MAC(Medium Access Control) 계층:** Data나 Probe, Beacon 등의 MAC Management용 프레임을 CAMA/CA 절차에 의해 전송하는 역할을 하는 곳이다. 즉 MAC 프레임 전송 및 제어를 담당하는 곳이다.

■ **MLME(MAC Layer Management Entity):** 전원관리, 탐색, Join, 인증, 결합, 리셋, 결합, 시간동기 등의 MAC 계층의 운영에 필요한 관리 기능을 하는 역할을 한다.

■ **PLME(Physical Layer Management Entity):** PMD(물리계층)에 대한 리셋, 모뎀의 동작 값 설정에 관여 한다.

■ **SM(Station Management):** 상위 계층 사용자로부터 리셋, 스캔, 연결 요청 등의 명령에 의해 MLME나 PLME블록을 제어 하는 역할을 한다.

## **2.2 기본 데이터 전송 동작**

IEEE 802.11 의 전송 방식은 CSMA/CA로 전송 방식은 우선 네트워크통신 상태를 점검한 후 네트워크가 Busy 상태가 아니면 데이터를 전송 하는 방식이다.

**1) 기본 전송 동작.**

**Busy Medium**

**Backoff-Window**

**Next Frame**

DIFS

DIFS

Defer Access

Contention Window

Slot time

Select Slot and Decrement Backoff as long as medium is idle

그림 3

송신 측은 최초로 프레임 송신 시도 시 채널이 Busy 상태이면 채널이 Idle 상태가 될 때까지 기다린다. 그리고 채널이 Idle 상태가 되면 DIFS(DCF Inter-frame spacing)동안 기다린다. 그리고 나서 추가로 슬롯타임의 시간을 지연한 후 여전히 채널이 Idle 한가를 확인 후 프레임을 전송한다. 대기 슬롯타임의 개수는 랜덤 하게 정해지는데 그 이유는 만약 송신하기를 원하는 단말이 여러 대일 경우 동일 시간 동안만 대기 후 전송을 시도하면 충돌이 일어날 확률이 높기 때문에 이러한 현상을 피하기 위해 슬롯타임의 개수를 랜덤 하게 정한다.

**AP**

Data/ACK

Busy

data

**단말**

**송신 시도**

**송신 시작**

그림 4

또 한 잡음이 예상되는 무선 채널의 특성을 고려하여, 데이터 프레임의 수신에 대한 ACK 패킷을 내보낸다.

**2) RTS/CST 동작.**

**ACK**

**RTS**

**DATA**

**CTS**

**NAV(RTS)**

**NAV(CTS)**

**DATA**

**SIFS**

**DIFS**

**Defer access**

**단말1**

**AP**

**단말2**

그림 5

각 단말이 프레임을 송신할 때, 채널 점유시간(NAV)이 포함된 RTS 프레임으로 이 시간 동안의 대역을 예약 한다. 이 채널 점유시간(NAV)은 이어서 송신될 데이터 패킷과 ACK패킷에 의한 채널 점유시간을 모두 더한 것이다. 만약 SIFS기간 이후에 AP로부터의 CTS 응답이 도착한다면, 즉시 데이터 패킷의 송신을 개시하고, AP로부터의 ACK패킷을 대기 한다. 물론, 이 CTS 프레임에도 NaV값이 수납되어 있는데, 이 값은 RTS 프레임에 수납되었던 NAV값에서 SIFS+CTS 전송시간이 감소된 것이다. 이러한 RTS/CTS 과정에서 다른 단말들은 RTS와 CTS에 기록된 NAV값 동안 자신들의 전송을 지연 시킨다.

# **3. 단말기와 AP의 연동 과정.**

단말기와 AP의 연동과정은 탐색, Join, 인증, 결합의 과정을 거친다. 탐색은 주변에 연결 가능한 AP를 찾는 것이고 Join은 연결하고자 하는 AP를 선택하는 것이다. 인증은 AP와의 인증 절차와 암호화 방식을 협상하는 과정이고 결합은 인증 절차를 거친 후 네트워크를 사용할 수 있는 상태를 말 한다.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\7DDQNROY\MC900428999[1].WMF

Beacon

Probe Request

Probe Response

IEEE 802.11 Open Authentication request

IEEE 802.11 Open Authentication response

Association Request

Association Response with client AID

그림 6

## **3.1 탐색 과정.**

탐색 과정은 수동 탐색 방법과 능동 탐색 방법 두 가지가 있다. 첫 번째 수동 탐색은 AP로부터 Beacon 메시지를 수신한다. 이 과정을 각 채널마다 수행 한다. 능동 탐색에 비해 단순히 수신만 하므로 전원을 절약 할 수 있지만 탐색 시간이 길다. 두 번째 능동 탐색은 각 채널 마다 능동적으로 Probe를 요청 메시지를 발송하고, 각 AP로부터의 Probe 응답을 수신하여 처리 한다. 또는 특정 채널이나 SSID를 지정할 수도 있기 때문에 탐색시간이 짧다.

**1) 능동 탐색 과정.**

그림 7과 같이 단말은 특정한 SSID를 설정하지 않은 Probe 메시지를 각 채널 별로 송신한다. 이 송신에 대하여, 관련된 AP는 자신의 SSID를 명시한 Probe 응답 메시지로 응답한다. 이 응답 메시지가 수신되면, capability(ESS, IBSS, CF, Privacy 등), SSDI, support rate등에 대한 정보를 BSS Description 테이블에 기록할 수 있다. 이러한 과정을 모든 채널에 대하여 수행한 다음, 완전히 작성된 정보를 BSS Description 테이블의 내용 탐색을 요청한 프로세서에 전달 하면 된다.

Probe 응답 메시지를 기다리기 위한 시간 값으로 Min Channel Time을 사용한다. 만약, 응답 메시지가 이 기간 내에 도착하지 않으면, 다음 채널을 검사한다. 반면에 응답 메시지가 이 기간 내에 수신되면, 다른 AP로부터의 응답도 기대할 수 있으므로, Probe 시간 값을 Max Channel Time 값으로 수정하여 추가의 응답을 대기한다.

Probe

resp

**AP 1**

**(CH2)**

**AP 2**

**(CH2)**

**단말**

Probe

Req(CH1)

Probe

Req(CH2)

ACK

Probe

resp

ACK

Min channel

Time

Min channel

Time

Max channel Time

그림 7 능동탐색과정

**2) 수동 탐색 과정.**

그림 8과 같이 단말은 각 채널 별로 AP가 송신하는 Beacon 메시지의 수신을 일정시간 대기한다. 만약, 이 기간 내에 Beacon 메시지가 수신되면, 이 Beacon 메시지에 명시된 capability, SSDI, supported rate 등에 대한 정보를 BSS Description 테이블에 기록한다. 이러한 과정을 모든 채널에 대하여 수행한 다음, 완전히 작성된 정보를 BSS Description 테이블의 내용 탐색을 요청한 프로세서에 전달 한다.

**AP 2**

**(CH2)**

**AP 1**

**(CH1)**

**단말**

B

B

B

B

B

B

B

B

CH1 검색

CH2 검색

Beacon interval

Target beacon transmission time(TBTT)

Scan Request(ScanType = passive)

그림 8 수동탐색과정

## **3.2 Join(참여)**

탐색 결과로 얻어진 BSS Description Set으로부터 가장 신호세기가 센 AP를 선택하거나 또 다른 규칙으로 선택한 특정 AP의 BSS description 정보를 이용하여 MAC Layer에 제시한다. 이 후 선택된 AP로부터의 Beacon 메시지가 수신되면, 이 메시지에 수록된 정보를 이용하여 동작 Parameter 와 Time Stamp 값으로부터 AP와의 시간동기를 수행한다. 이 참여과정에서 특별한 프레임이 단말로부터 송신되는 것은 아니다. 단순히, 선택한 AP로부터의 Beacon 메시지가 수신되면, 자신이 선택한 동작 Parameter가 일치하면 참여가 성공하였다고 상위 계층에 보고한다.

## **3.3 인증 절차.**

참여과정에 의해, 해당 AP에 대한 정보를 수집하였다면, 이 AP에 대한 결합을 수행해야 한다. 이 결합이 가능 하려면, 먼저 인증 절차가 수행되어야 한다. 이러한 인증과정은 전송매체에 대한 보안이 취약한 무선망에서 인증을 거치기 않은 단말은 무선 채널을 사용할 수 없도록 하기 위한 것이다.

802.11에서 사용하는 인증방식은 링크계층의 인정 절차를 수행하는 것일 뿐, 종단간 인증절차는 수행하지 않는다. 즉, 802.11의 인증은 단말이 AP까지의 무선 링크를 사용할 수 있도록 하는 수준의 인증절차만 지원한다. 참고로, Open System 인증절차의 경우 패킷의 교환 절차는 그림 9와 같다. 이 경우, AP는 인증 요청에 대해 무조건 인증한다.



C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\7DDQNROY\MC900428999[1].WMF

탐색/Join

Status = 0

Aut TransactionSeq=1

Aut Alg Num=0

Aut.Req

802.11 MAC-ACK

Aut. Response

Aut Alg Num=0

Aut TransactionSeq=2

Status=Success

802.11 MAC-ACK

결합

그림 9 인증절차

## **3.4 결합(Association)**

인증절차가 성공하면, 연결과정의 마지막인 결합과정이 수행된다. 결합이란 단말이 해당 AP에게 한 멤버로 참여하는 의미이다. 결합과정이 성공하면, 단말은 AP로부터의 결합 응답 메시지에 수납된 해당 단말에 대한 결합 ID(AID)를 할당 받게 된다. 결과적으로, 이 결합절차에 의해 해당 단말이 이 AP에 최종적으로 연결되어, 단말은 이 AP를 경유하여 다른 단말과의 통신이 가능하게 된다. Ethernet 환경의 RJ-45 컨넥트와 단말이 연결된 상태와 같은 조건이 된다.

# **4. 프레임 구조.**

## **4.1 802.11 프레임 구조.**

802.11의 프레임 구조는 아래와 같이 Preamble, PLCP Header, MAC Data, CRC로 구성이 되어 있다.

**Preamble**

**PLCP Header**

**MAC Data**

**CRC**

Synchronization(128 or56)

SFD(16)

**Preamble**

■ Preamble : 128 or 56 비트의 길이를 가지는 long Preamble 과 short Preamble 두 가지가 정의 되어 있다.

- Synchronization: 비트 동기용으로 사용되며 long 타입과 short 타입에 대하여 각각 1과 0으로 구성이 되어 있다.

- SFD(Start Frame Delimiter): 실제 프레임의 시작을 찾을 수 있도록 하는 특정 비트 열로서, long 타입과 Short 타입의 경우 각각 0xF3A0 와 그 역순의 비트로 구성이 되어 있다.

Signal(8)

Length(16)

**PLCP Header**

Service(8)

CRC(16)

■ PLCP Header: Preamble 다음에 위치한 48bit 영역으로, 물리 계층에서 사용하는 동작 값들을 지시한다.

- Signal: Payload 부분의 전송 속도를 표시한다. Ex) 0x0A(10Mbps), 0x14(20Mbps)

- Service: 16비트의 길이 영역으로는 최대 8Mbps밖에 표시할 수 없는 문제를 해결하고, 고정 클럭 및 변조 방식을 지시하는 용도로 사용된다.

- Length: Packet의 전송 바이트 개수를 나타낸다.

- CRC:

## **4.2 MAC 프레임 구조.**

802.11 MAC 프레임 구조는 아래와 같다. MAC 헤더의 길이는 Address 4 영역의 유무에 따라 30 또는 24 바이트이며, 프레임 바디의 최대 길이는 2312 바이트 이다. 또 한, WEP 암호화가 사용될 경우, 8 바이트가 추가된다.

Frme

Control

Duration/

ID

Address 1

Address 2

Address 3

Sequence

Control

Address 4

Frame

Body

CRC

**MAC Data**

2

2

6

6

6

2

6

0 - 2312

4

**1) 프레임 제어 영역.**

**Frame Control**

Protocol

Version

Type

Subtype

To

DS

From

DS

More

Frag

Retry

Pwr

Mgt

More

Data

WEP

Order

2

2

4

1

1

1

1

1

1

1

1

■ Protocol Version: 0x00

■ Type : 전송되고 있는 프레임의 타입을 알려 준다.

- (00) Management 프레임.

- (01) Control 프레임.

- (10) Data 프레임.

- (11) Reserved.

■ Subtype: 각 프레임에 대한 세부적인 프레임의 종류를 구분한다.

■ ToDS, FromDS: DS(Distribution System)의로부터의 수신 및 송신을 구분한다.

■ More Fragment: 하나의 MAC 프레임이 여러 개의 짧은 프레임으로 분할되어 전송될 때 분할된 마지막 프레임을 제외하고는 이 Bit를 1로 설정한다.

■ Retry: 재전송된 것임을 표시하고, 중복 송신된 것인지 판단할 수 있도록 한다.

■ Pwr Mgt: 이 Bit가 1일 경우 단말이 곧 전원절약 모드에 들어감을 표시하는 것이고, 0일 경우 활성 모드로 진입할 예정임을 표시한다.

■ More Data: 전원 절약모드에서, AP가 단말에 전달해야 할 프레임이 더 있음을 표시한다.

■ WEP: 해당 프레임이 WEP(Wired equivalent privacy),TKIP,CCMP 등의 무선 구간 암호 방식에 의한 암호화가 되어 있음을 표시한다.

|  |  |  |
| --- | --- | --- |
| **Type** | **Sub Type** | **Description** |
| 00 | 0000 | Association Request |
| 0001 | Association Response |
| 0010 | Re-association Request |
| 0011 | Re-association Response |
| 0100 | Probe Request |
| 0110 | Probe Response |
| 0110-0111 | Reserved |
| 1000 | Beacon |
| 1001 | ATIM |
| 1010 | Disassociation |
| 1011 | Authentication |
| 1100 | Deauthentication |
| 1101 - 1111 | Reserved |
| 01 | 0000 – 1001 | Reserved |
| 1000 | Block ACK Request |
| 1001 | Block ACK |
| 1010 | PS-Poll |
| 1011 | RTS |
| 1100 | CTS |
| 1101 | ACK |
| 1110 | CF-End |
| 1111 | CD-End + CF-ACK |
| 10 | 0000 | Data |
| 0001 | Data + CF-ACK |
| 0010 | Data + CF-Poll |
| 0011 | Data + CF-ACK + CF-Poll |
| 0100 | Null(no data) |
| 0101 | CF-ACK(no data) |
| 0110 | CF-Poll(no data) |
| 0111 | CF-ACK + CF-Poll(no data) |
| 1000 | Qos Data |
| 1001 | Qos Data + CF-ACK |
| 1010 | Qos Data + CF-Poll |
| 1011 | Qos Data + CF-ACK + CF-Poll |
| 1100 | Qos Null(no data) |
| 1101 | Reserved |
| 1110 | Qos CF-Poll(no data) |
| 1111 | Qos CF-ACK + CF-Poll(no data) |
| 11 | 0000 - 1111 | Reserved |

**2) Duration / ID**

Duration은 이 시간 동안 다른 단말들의 채널 사용이 연기되도록 무선 링크를 예약하는 시간 값인 NAV(Net Allocation Vector)값이 수납된다. 이 때, 최상위 비트의 값은 0이다. 나머지 15bit의 값은 usec 단위의 NAV 값이다.

ID는 전원절약 모드에 있는 단말이 주기적으로 깨어나면서, 그 동안 자신에게 전달되어야 할 프레임을 AP가 보관하고 있는지 질의하는 PS-Poll 메시지를 송신할 때, 자신이 결합된 AP로부터 부여 받은 결합번호(AID)를 Duration/ID 영역에 수납하여 전송한다. AP는 버퍼를 검사하여, 이 AID에 해당되는 단말에게 전달되어야 할 프레임을 선택하여, 이것을 단말에 전달한다.

**3) Address 1,2,3,4**

DA와 SA 등 2개의 주소만 사용하는 Ethernet과 달리, 무선 LAN에서는 4개의 주소가 사용된다. 하지만, 한 프레임에서 A4가 없을 수도 있다. 일반적으로 A1은 수신 측 주소이고, A2는 송신 측 주소이다. 이러한 4개의 주소 영역의 의미는 ToDS와 FromDS 비트에 의해 결정된다.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **To DS** | **From DS** | **Address 1** | **Address 2** | **Address 3** | **Address 4** |
| To AP | 1 | 0 | BSSID(AP) | SA(STA) | DA(타 단말) |  |
| From AP | 0 | 1 | DA(STA) | BSSID(AP) | SA(타 단말) |  |
| Within Wireless DS | 1 | 1 | RX(rx AP) | TA(tx AP) | DA(rx STA) | SA(tx STA) |
| Ad hoc | 0 | 0 | DA | SA | BSSID |  |

■ DA(Destination Address): 최종 목적지 주소.

■ SA(Source Address): 프레임의 최초 송신 측 주소.

■ RA(Receiver Address)와 TA(Transmitter Address): 서로 다른 AP를 경유하는 경우, 즉 DA와 SA간에 경유하는 수신 측 AP와 송신 측 AP의 Ethernet 주소.

■ BSSID: AP의 MAC 주소.

**4) Sequence Control**

매 프레임당 할당되는 순서 번호와 분할 프레임의 순서번호로 다음과 같이 구성된다. 이들은 모드 ACK의 손실에 의한 중복된 재전송 검사와 재조립할 때 사용된다.

■ 순서번호(12Bit): 순서번호는 매 프레임 전송시 마다 1씩 증가한다. 물론 재전송되는 프레임일 경우, 순서번호를 증가하지 않는다.

■ 분할번호(4Bit): 한 프레임이 여러 개의 프레임으로 분할되어 전송될 경우, 이들간의 순서를 구분할 때 사용하는 번호이다.

**5) Frame body**

제어 및 관리용 정보나 LLC와 같은 상위계층 메시지 즉, MSDU가 수납된다. 이 영역의 최대 사이즈는 2304Byte 이다. 프레임 바디 영역이 WEP(Wired Equivalent Privacy)로 암호화될 경우, 프레임 바디는 각각 4바이트 길이의 IV(Initialization Vector)와 ICV(Integrity Check Value)등이 추가된다. 분할될 경우, 최소 길이는 256Byte 이다.