

사물인터넷 (Internet of Things)

김태운

목차

- Non-IP 기반의 WPAN 기술
 - Zigbee

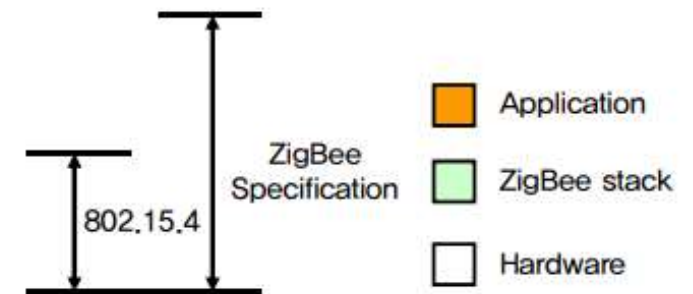
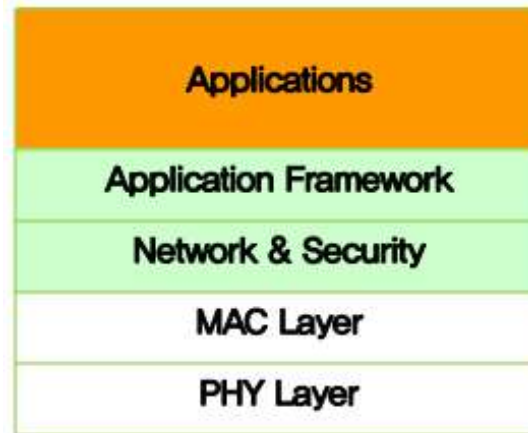
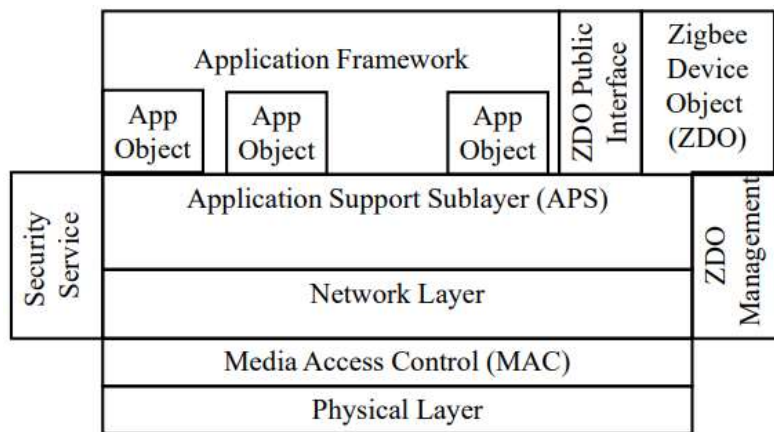
Network Layer: Non-IP 기반의 WPAN 기술

Zigbee

Zigbee

■ 소개

- Zigbee 는 IEEE 802.15.4를 기반으로 하여 설계된 Ad Hoc WPAN 프로토콜
 - IEEE 802.15.4 표준 기술에 상위 계층인 논리적 네트워크, 보안기술, 응용 계층을 덧붙여서 만들어진 표준
 - IEEE 802.15.4 표준 기술(MAC/PHY)을 준수하여 안정적, 효율적으로 동작함
 - IEEE 802.15.4 표준은 MAC/PHY 계층 기술을 정의하고 있지만 그 위 계층에 대한 명세가 없음. 또한 802.15.4는 multi-hop 통신에 대한 기능 명세가 없음. Zigbee 는 IEEE 802.15.4 표준 기술을 기반으로 상위 계층을 포괄하여 정의된 표준 기술에 해당함



■ 소개

• 표준 릴리즈 히스토리

- 2002년 Zigbee Alliance 가 설립되고 Zigbee 표준을 개발 및 관리 시작
- 2005년 : Zigbee 2004 버전 공개 (Zigbee 1.0 으로 불리며, 현재는 사용하지 않도록 권고함)
- 2006년 : Zigbee 2006 버전 공개
- 2007년 : Zigbee 2007 및 Zigbee Pro 버전 공개

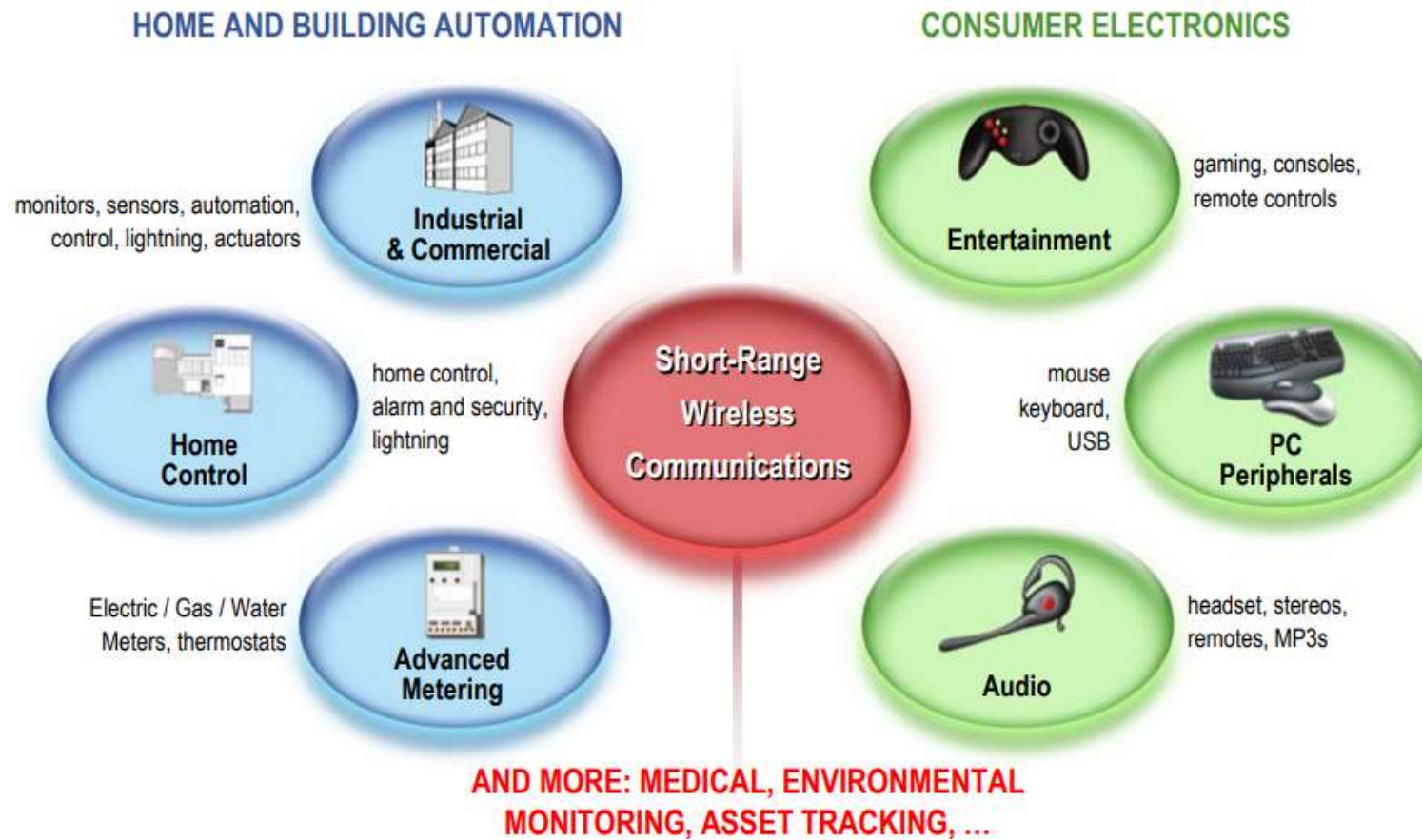
Table : ZigBee Stacks Compared

Feature	ZigBee 2006	ZigBee 2007	ZigBee Pro
Size in ROM/RAM	Smallest	Small	Bigger
Stack Profile	0x01	0x01	0x02
Maximum hops	10	10	30
Maximum nodes in network	31,101	31,101	65,540
Mesh networking	✓	✓	✓
Broadcasting	✓	✓	✓
Tree routing	✓	✓	-
Frequency Agility	-	✓	✓
Bandwidth Used By Protocol	Least	More	Most
Fragmentation	-	✓	✓
Multicasting	-	-	✓
Source routing	-	-	✓
Symmetric Links	-	-	✓
Standard Security (AES 128 bit)	✓	✓	✓
High Security (SKKE)	-	-	✓

Zigbee

■ 소개

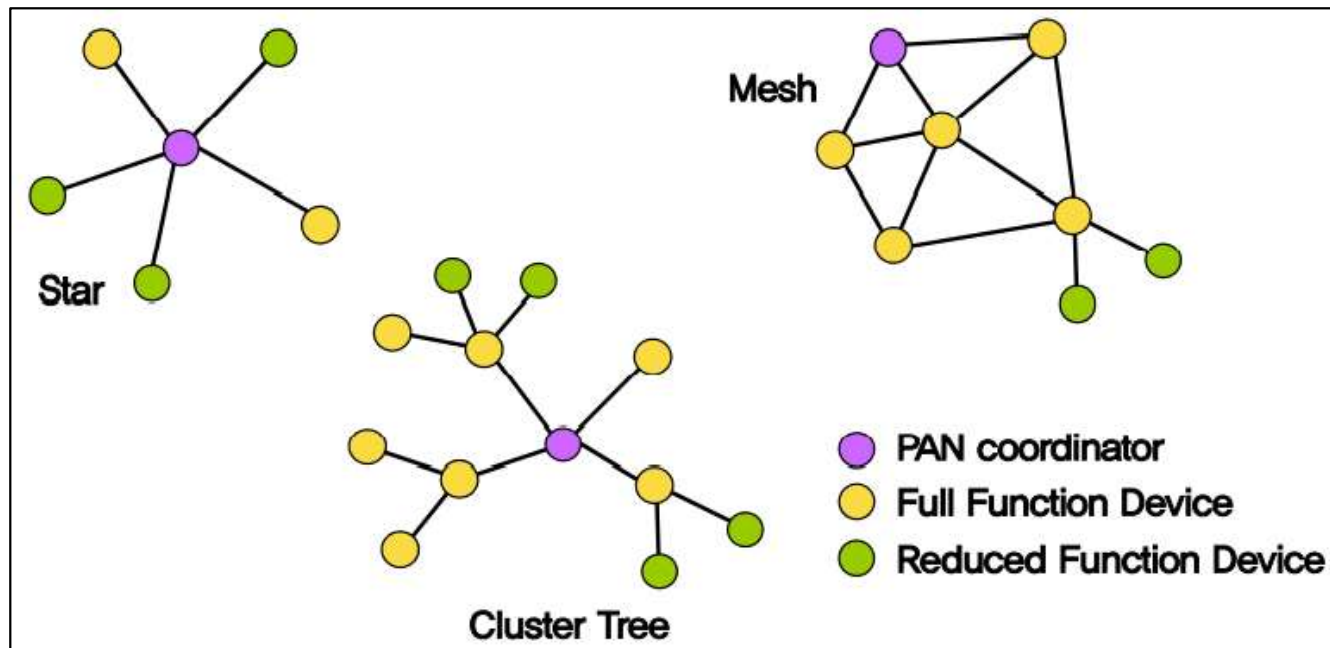
- 비용, 전력/배터리, 공간의 제약을 받는 상업 및 거주지를 위한 사물인터넷 네트워킹 기술로 개발됨



■ 소개

• 특징

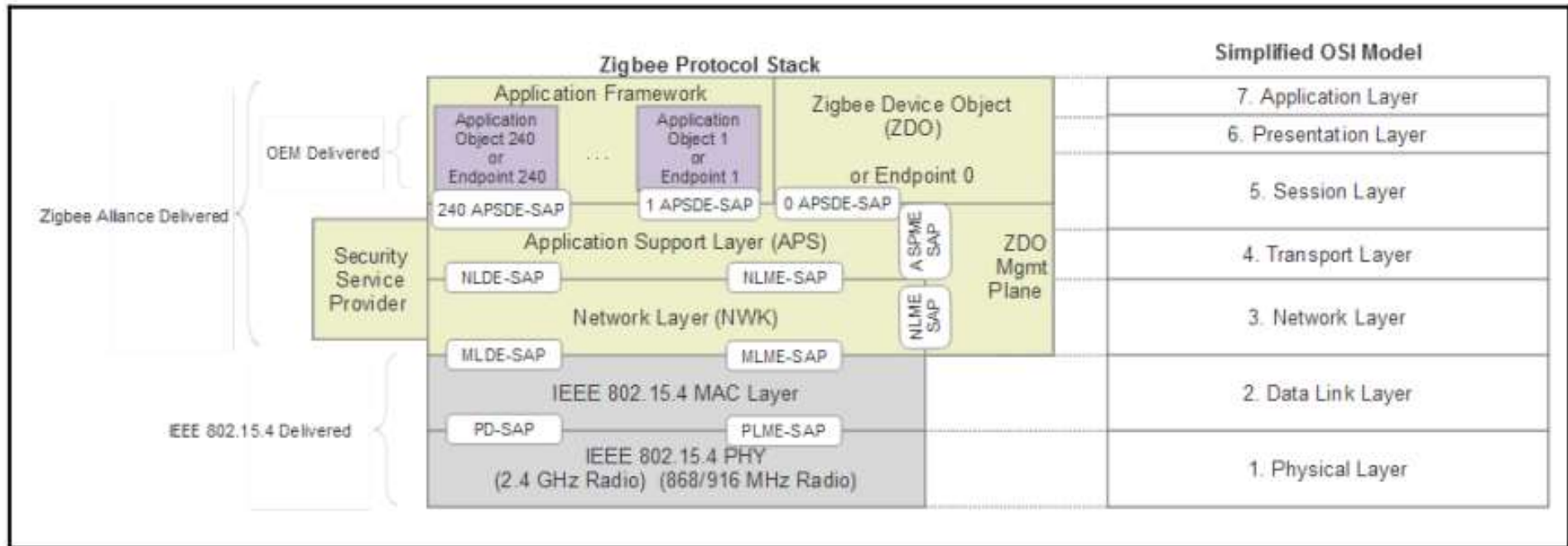
- 센서 네트워크 : 저전력, 저비용, 낮은 데이터 전송률(250 kbit/s), 다수의 노드간 연결 지원, 동작 주파수(2.4GHz ISM 밴드 및 915MHz/USA)
- 전송 범위 및 규모 : 1 ~ 100m 수준의 전송 범위, 최대 2^{16} 개 단말(약 6만 5천대)로 네트워크를 구성할 수 있음
- HW 개발의 용이성 : 프로토콜 구조가 단순하여 HW chip 개발이 용이함
- 다양한 토폴로지 지원 : star, cluster tree, mesh 토폴로지를 지원하며, multi-hop routing 을 통해 mesh network 환경에서 원거리 데이터 전송 가능



- Zigbee 네트워크 주요 구성요소: 3 principal components
 - Zigbee Coordinator (ZC) : 고성능의 Full Function Device (FFD) 는 ZC 역할 수행 가능
 - Zigbee 네트워크 설정/관리, 채널 선택, 네트워크 구성/실행 기능 수행
 - 네트워크 노드 관리(논리 네트워크 주소 할당, 단말이 mesh 에 합류하거나 떠나는 것을 제어 등)
 - 하나의 Zigbee 네트워크는 하나의 ZC를 가짐. 네트워크가 구성된 후, ZC 는 ZR 의 기능을 수행할 수 있음
 - Zigbee Router (ZR) : 고성능의 Full Function Device (FFD) 는 ZR 역할 수행 가능
 - 네트워크의 모든 구성요소와 통신하며, 패킷 중계 기능을 통해 멀티 홉 네트워킹 지원
 - ZR 역할을 수행하는 FFD는 항상 power-on/active 상태를 유지해야 하며, 이로 인해 배터리 사용량이 증가함
 - Zigbee End Device (ZED) : 제한된 성능을 가지는 저전력 Reduced Function Device (RFD) 에 해당
 - 매우 단순한 기능 만으로 구현된 단말로, Coordinator 와만 통신함
 - 데이터를 생성 또는 소비하는 단말
 - 그 외
 - Zigbee Trust Center (ZTC) : 보안/인증 관련 기능 수행
 - Zigbee Gateway : Wi-Fi 등 다른 네트워크와의 연결 수행

Zigbee

■ Zigbee 프로토콜 스택



NWK	Device management, neighbor discovery 등 수행 경로 관리, 데이터 전송, 메시지 라우팅 등 수행
APS	Network Layer 와 Application Layer 사이의 인터페이스 역할 수행
Application Objects	Remote control application 에 해당하며, End-Point (EP) 라고도 불림 각 EP 는 하나의 Application Profile 을 가짐 (다음 페이지)
End-Node	End-Device 에 해당하며, 각 EN 는 최대 250개의 Application Objects 를 가질 수 있음

Zigbee

▪ Zigbee Application Profile

Application Profile	설명
smart energy	electrical, gas, water meter reading 등
commercial building automation	smoke detectors, lights 등
home automation	remote control lighting, heating, doors 등
personal, home, hospital care (PHHC)	blood pressure, heart rate monitoring 등
telecom application	mobile phones 등
remote control for consumer electronics	가전 모니터링/제어 등
industrial process monitoring and control	temperature, pressure, position 등
등등...	



Lock
(Kwikset)



Light Bulb
(Sengled)



Hub
(Samsung)



Motion Detector
(Bosch)



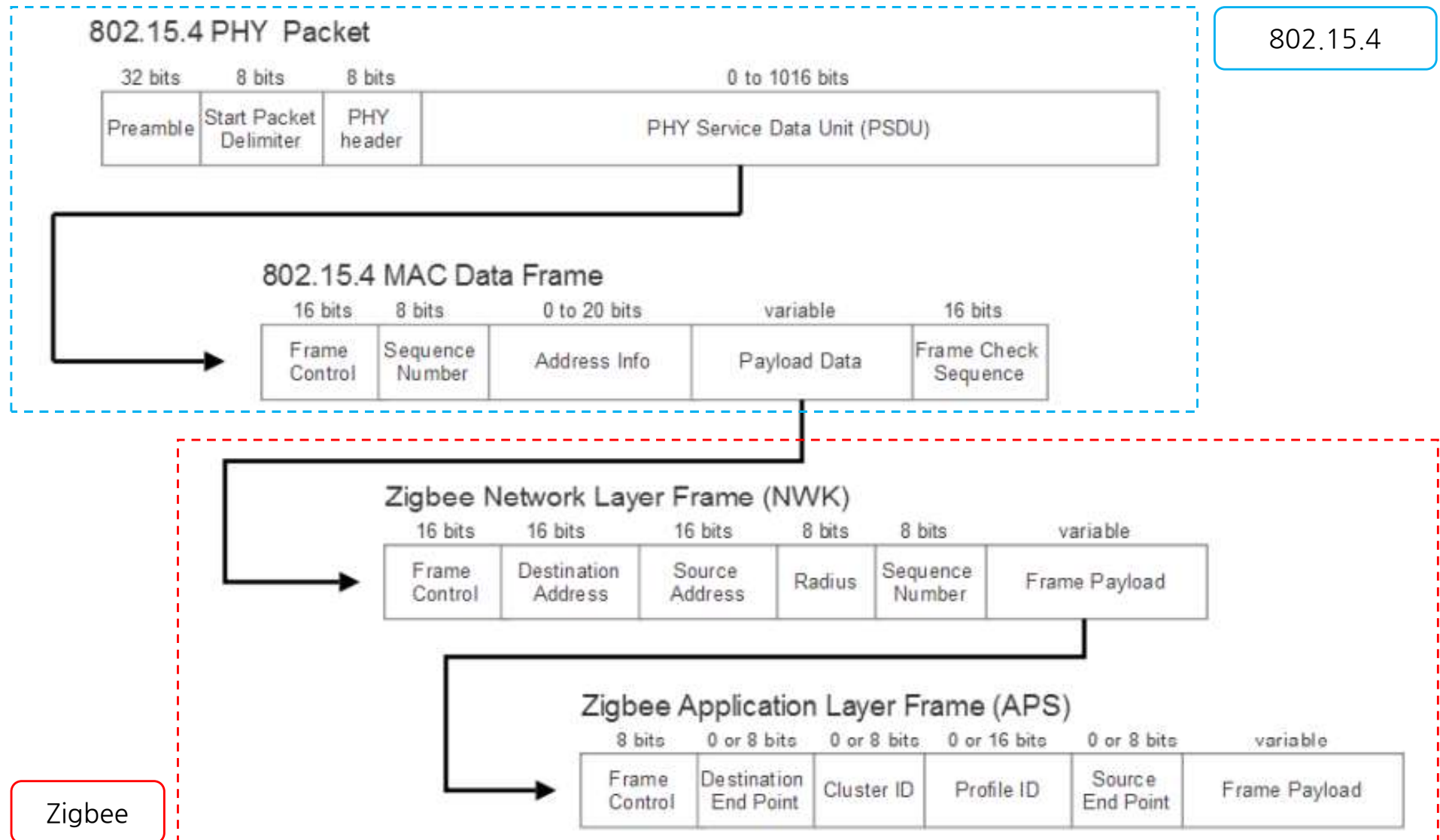
Outlet
(Samsung)



Temperature Sensor
(Visonic)

Zigbee

- Zigbee packet structure : IEEE 802.15.4 패킷 구조를 기반으로 함



▪ Device Address

- 각 단말은 64-bit 고유 주소를 필수로 가지며, PAN 합류 시 16-bit 의 short address 도 가질 수 있음
 - 두 주소 모두 IEEE 802.15.4에서 정의한 방법을 사용함
- Long address (64-bit)
 - 단말 제조사에서 할당하는 주소로, 변경 불가능
 - 상위 24-bit 는 제조사의 고유 번호 (OUI, organizational unique identifier)이고,
 - 하위 40-bit 는 제조사에서 자체 할당하는 번호
- Short address (16-bit)
 - PAN 에 합류할 때 Coordinator 에 의해서 할당하는 번호

Zigbee

- Zigbee 에서 지원하는 라우팅 기법
 - Broadcasting : 다른 모든 노드에게 패킷을 방송함
 - Mesh routing (table routing) : 경로 테이블 기반으로 라우팅 수행 (최대 30홉 거리의 목적지까지 라우팅 가능), 예: [AODV](#)
 - Source routing : 전체 전송 경로를 송신 패킷에 기록하여 전송하는 기법으로, data concentrator 가 존재하는 경우에 사용 가능 (예: DSR, Dynamic Source Routing)
- Zigbee 는 멀티 홉 전송 시 AODV 라우팅 기법을 주로 사용함

▪ AODV 소개

- Ad-hoc On-demand Distance Vector 라우팅의 약자로, distributed Bellman-Ford routing algorithm에 기반하며 Uni-cast 및 multi-cast 전송을 모두 지원함
- on-demand 및 reactive 라우팅 기법으로, 라우팅 경로를 사전에 계산하지 않음
 - 데이터 전송 요청 발생 시, 해당 목적지로 가는 라우팅 경로를 찾기 위한 Route Discovery Procedure를 수행함
 - 단, 로컬 라우팅 테이블에 해당 목적지 노드에 대한 유효한 엔트리가 존재한다면 기존의 엔트리를 사용함
 - 기존의 Distance Vector 알고리즘은 주기적으로 local distance vector를 broadcast 하는데, 이 과정이 생략되어 네트워크 대역폭 사용량 및 배터리 사용을 줄임
- 각 노드(단말)은 로컬 라우팅 테이블에 저장된 엔트리를 활용하여 통해 라우팅을 수행함
 - 라우팅 테이블은 전체 경로를 저장하지 않고, next hop 이 어디인지에 관한 정보만 저장함
 - 각 라우팅 엔트리는 **<destination addr, next hop addr, destination sequence number, life time>** 형식으로 구성됨
 - 각 라우팅 엔트리에 영향을 받는 노드를 저장한 precursor node list가 별도로 관리됨
 - 각 엔트리를 사용하거나 갱신할 때 life time 값을 업데이트 하고, life time 이 일정 시간이 경과하면 해당 경로 엔트리는 invalid(무효)로 판단하여 사용하지 않음
- 단말의 이동, 단말의 on/off 등으로 인한 라우팅 경로의 변경을 반영하기 위해 Route Maintenance Procedure를 수행함
- 이웃 노드들과의 연결 여부 확인(이웃 노드 목록 유지)을 위해 주기적으로 HELLO 메시지를 broadcast 함
- Route 경로 탐색, 관리 등을 위해 RREQ(Route Request), RREP(Route Reply), RERR(Route Error) 메시지를 사용하며, UDP로 전송함

■ AODV : 요약

• 동작 방식

1. (유효한 라우팅 엔트리가 없는 경우) Source S (송신 단말) 는 Destination D (목적지 단말) 로의 경로를 찾기 위해 RREQ (Route Request) 패킷을 broadcast 함 : Route Discover Procedure
 - RREQ 메시지는 목적지 D 에 도달하거나 또는 D 로 가는 valid route 를 알고 있는 intermediate 노드를 만날 때 까지 다른 노드에 의해 반복적으로 broadcast 됨 (반복적 broadcast = Flooding)
 - 이 때, RREQ를 수신한 노드는 reverse route 를 임시로 저장하고, 향후 RREP 메시지를 Source 로 전달할 때 사용
 2. 목적지 노드 D (또는 D 로 가는 valid route 를 알고 있는 intermediate 노드)는 RREQ 에 대한 응답으로 RREP 메시지를 회신 함
 - RREP 가 전달되는 과정에서 임시로 저장한 reverse route 를 따라서 unicast 로 전송함
 - RREP 가 회신 되는 경로에 있는 모든 노드는 (Source S, Destination D) 간의 경로를 학습함
- 이웃하는 단말과의 링크 또는 전송 경로 상의 단절이 발생한 경우, 이로 인해 영향을 받는 노드에게 이를 통지함(RERR)
 - 이를 위해, 각 라우팅 엔트리 별로, 영향을 받는 노드의 목록을 관리함
 - 인접한 노드는 HELLO 메시지를 주기적으로 교환하고, 이를 통해 링크 단절을 탐지하여 통지함
 - 또한, S 에서 D 로 데이터 전송 중에 노드 X가 다음 홉(next hop) Y 로의 전송을 실패하면 경로 단절을 탐지 & 통지함
 - 라우팅 테이블에 저장된 각 엔트리 별로 순서 번호(sequence number) 값을 사용함
 - 각 엔트리가 유효한지(유효기간이 지난 경로는 invalid route 로, 사용되지 않음), 최신의 정보인지를 판단하는데 사용
 - 또한, loop 를 탐지/방지 하는 목적으로도 사용

▪ AODV : Route Discovery Procedure

1. (유효한 라우팅 엔트리가 없는 경우) Source S (송신 단말) 는 Destination D (목적지 단말) 로 data packet 을 전달하기 위해, RREQ (Route Request) 패킷을 broadcast 함

Source address	Request ID	Destination address	Source sequence #	Destination sequence #	Hop count
----------------	------------	---------------------	-------------------	------------------------	-----------

- Source address, destination address : 송신 단말 및 목적지 단말의 IP 주소
- Request ID : 송신 단말이 내부적으로 관리하는 local counter 로, RREQ 메시지가 최초로 broadcast 될 때 마다 증가함 (intermediate 노드들이 중복해서 동일한 RREQ 메시지를 broadcast 하는 것을 방지)
- Source sequence number : RREQ 를 보낼 때의 clock counter (timestamp)
- Dest seq num : S 가 알고 있는, D 로 가는 경로에 대한 가장 최신의 sequence number (모를 경우 0으로 초기화)
- Hop count : 0 으로 초기화 되고, forwarding 될 때 마다 1씩 증가

2. RREQ 를 수신한 intermediate 노드는...

- (Req. ID) 필드 값을 기준으로, 중복 수신한 메시지라면 버림
- RREQ 내의 dest seq # 를 기준으로, 동일한 경로에 대한 최신 경로 정보를 직접 가지고 있다면 RREP 로 즉시 회신
- 그렇지 않다면 , hop count 를 증가시킨 후 다시 broadcast (이 때, reverse route 정보를 저장하고, 향후 RREP 회신 할 때 사용)

▪ AODV : Route Discovery Procedure

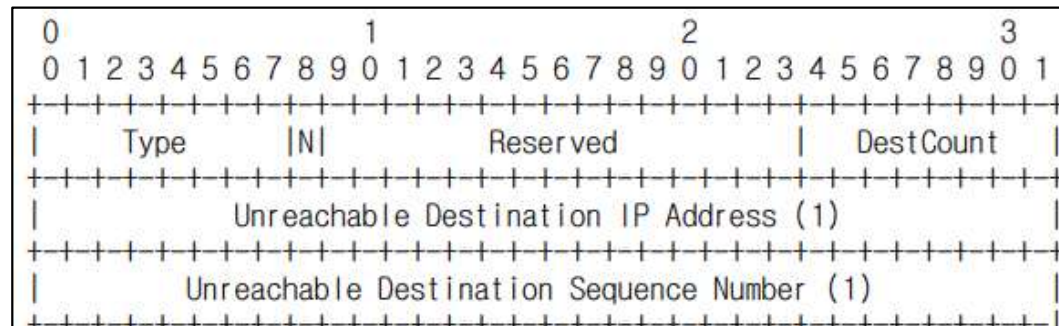
1. Source S (송신 단말) 는 RREQ (Route Request) 패킷을 broadcast
2. RREQ 를 수신한 intermediate 노드가 broadcast 함
3. 목적지 D 는 RREQ 회신 후, RREQ 를 보내준 노드로 unicast 방식으로 RREP 를 회신

Source address	Destination address	Destination sequence #	Hop count	Life time
----------------	---------------------	------------------------	-----------	-----------

- 이 때, (src addr, dst addr, hop count)는 RREP 로 부터 복사해서 사용하고, dest seq # 는 D 의 clock counter 값을 사용함
4. RREP 를 회신한 intermediate 노드는...
 - 해당 메시지를 (RREQ forwarding 할 때 저장해 둔) reverse route 로 unicast 전송
 - 또한, 해당 경로가 로컬 라우팅 테이블에 없는 경로이거나, 또는 기존 경로 정보에 비해 dest seq # 가 크거나 hop 수가 작다면 기존 경로 정보를 업데이트
 5. RREP 를 회신한 송신 단말 S 는 해당 경로를 따라 data packet 을 전송하고, 해당 경로를 사용할 때 마다 life time 값을 갱신하여 유효 기간을 늘림

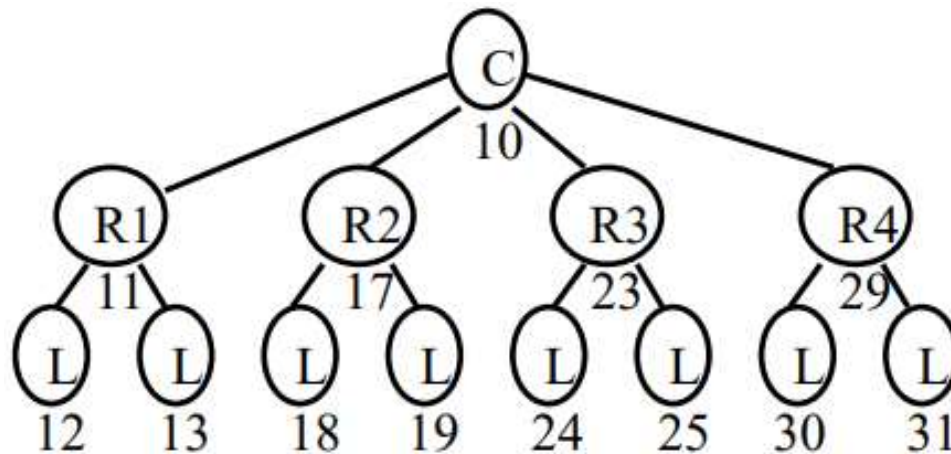
▪ AODV : Route Maintenance Procedure

- 각 라우팅 엔트리 별로, 해당 경로에 영향을 받는 노드 리스트를 별도로 보관함
- 각 노드는 주기적으로 이웃 노드에게 HELLO 메시지를 전송하고, 이에 대한 응답이 없으면 링크 단절로 간주하며 이에 영향을 받는 노드에게 PERR 패킷으로 통지함



- 또한, S 에서 D 로 패킷을 forwarding 하는 중에, 노드 X 가 next hop 인 Y 로 forwarding 실패한 경우, 이를 PERR 패킷으로 S 에게 통지함
- PERR 패킷을 수신한 S 는 다시 Rout Discovery Procedure 를 실행함

- 그 외 라우팅 기법 : Tree routing (Hierarchical Routing):
 - 노드로 구성된 트리 구조에서, 목적지 단말이 sender 노드의 하단부에 위치한다면 해당 방향으로, 그렇지 않다면 parent 방향으로 forwarding (routing 테이블을 최소한으로 사용)



- C : Coordinator
- R : Routing Node
- L : Leaf Node
- 번호 : Device number

- 예: hierarchical address 주소체계 사용 하는 상황에서 L12 ➔ L30 로 전송하려는 경우...
- L12가 parent 인 R1 으로 메시지 forwarding
- R1은 (L30이 child 가 아닌 것을 확인하고) 자신의 parent 인 C 로 forwarding
- C 는 (L30 의 주소를 기반으로 R4의 child 인 것을 확인하고) R4로 forwarding
- R4 는 L30으로 메시지를 forwarding

▪ Zigbee 최신 표준 버전 별 비교

버전	주요 내용
Zigbee Pro	<ul style="list-style-type: none"> • 기존 zigbee 스택을 발전시킨 버전으로 2007년에 발표됨 • 하위 호환성을 지원하여 zigbee 2006 버전 기기들과 완벽히 호환됨 • Stochastic addressing 기능 : random 한 방식으로 주소를 할당하고, 주소 충돌을 최소화 • Link management : 각 단말은 이웃 단말과의 link quality 를 관리함 • 동적 채널 관리 : 간섭을 경험한 단말은 channel manager 에게 이 사실을 통보하고, 다른 채널을 할당 받음 • multicast, many-to-one routing 지원
Zigbee RF4CE	<ul style="list-style-type: none"> • 2009년 Zigbee Alliance 와 RF4CE 컨소시엄이 협력하여 제정한 가전 제품 원격제어를 위한 규격 • 2.4GHz 주파수 대역을 사용하고 128bit AES 암호화 기술을 이용한 보안 기술 적용
Zigbee IP	<ul style="list-style-type: none"> • IPv6 기반의 완전한 무선 메시 네트워킹 솔루션으로 발표된 개방형 표준으로, 저전력 디바이스들을 인터넷에 직접 연결함

감사합니다.

