
WEIGHTLESS™

Weightless-P
System specification

Version 1.03

7 November 2017

Revision History

Version	Date	Comments
0.6	26/10/2015	FEC, RRM
0.7	30/10/2015	RF parameters, regulation compliance
0.8	3/11/2015	RF parameters
0.9	6/11/2015	Frequency hopping sequences definition
1.0	14/12/15	Final version for release

List of contributors[1]

Name	Organization
Ian Blair	CSR
Andrew Fell	TTP
Zhuo Fu	Ubiik
Fabien Petitgrand	Ubiik
Amyas Phillips	ARM
Dermot Smith	Farsite
Peter Smith	Neul
Keping Wang	Bridging Science
William Webb	Weightless SIG
Steven Wenham	Neul

[1] Contributors to both Weightless-P and to those elements of Weightless-W that are also used within Weightless-P.

Table of Contents

1 ARCHITECTURAL OVERVIEW

1.1 INTRODUCTION

Weightless-P is a standard for low-power wireless communication in public or private networks with end devices with “Internet of Things” (IoT) requirements such as limited throughput and relaxed latency. Although it can operate in any frequency band, it is currently defined for operation in license-exempt sub-GHz frequency bands (e.g. 138MHz, 433MHz, 470MHz, 780MHz, 868MHz, 915MHz, 923MHz).

The defining characteristics of Weightless-P are as follows:

- 100% bidirectional, fully acknowledged communication for reliability.
- Optimized for a large number of low-complexity end devices with asynchronous uplink-dominated communication with short payload sizes (typically < 48 bytes).
- Optimized for ultra-low-power consumption (at the expense of latency and throughput compared to cellular technologies).
- Standard data rates from 0.625kbps to 100kbps.
- Typical End Device transmit power of 14dBm (up to 30dBm).
- Typical Base Station transmit power of 27dBm (up to 30dBm).

Weightless-P networks are composed of the following elements:

- **End Devices (ED)**: the leaf node in the network, low-complexity, low-cost, usually low duty cycle
- **Base Stations (BS)**: the central node in each cell, with which all EDs communicate via a star topology
- **Base Station Network (BSN)**: interconnects all Base Stations of a single network to manage the radio resource allocation and scheduling across the network, and handle authentication, roaming and scheduling

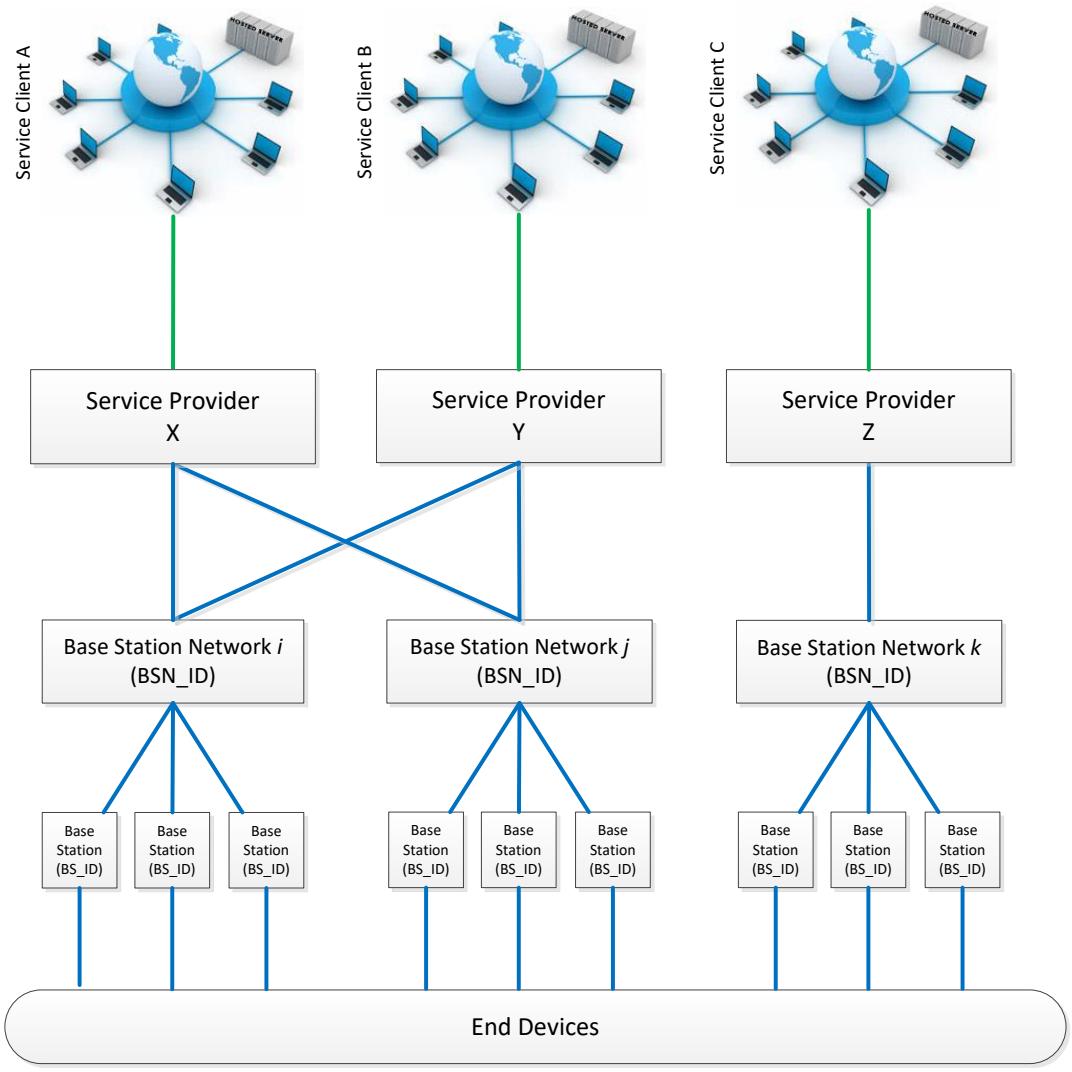

FIGURE 1-1 WEIGHTLESS-P NETWORK OVERVIEW

To achieve high network capacity (i.e. number of End Devices able to communicate in a given time period), Weightless-P combines synchronous TDMA and FDMA, offering a large number of uplink logical channels shared between independent End Devices.

The design parameters are a trade-off between energy efficiency and network capacity on the one hand (which both require high data rate and transmit power), and the achievable communication range on the other hand (which requires low data rate given the maximum transmit power restrictions).

As a reference, GSM/GPRS, which is a power-efficient cellular technology, though not designed for asynchronous short payloads, defines a fixed on-air data rate of 270.83kbps for a reference sensitivity level of -102dBm and a maximum transmit power of 33dBm. When the maximum transmit power is limited to 17dBm, this implies a data rate of around 5kbps to achieve a similar link budget.

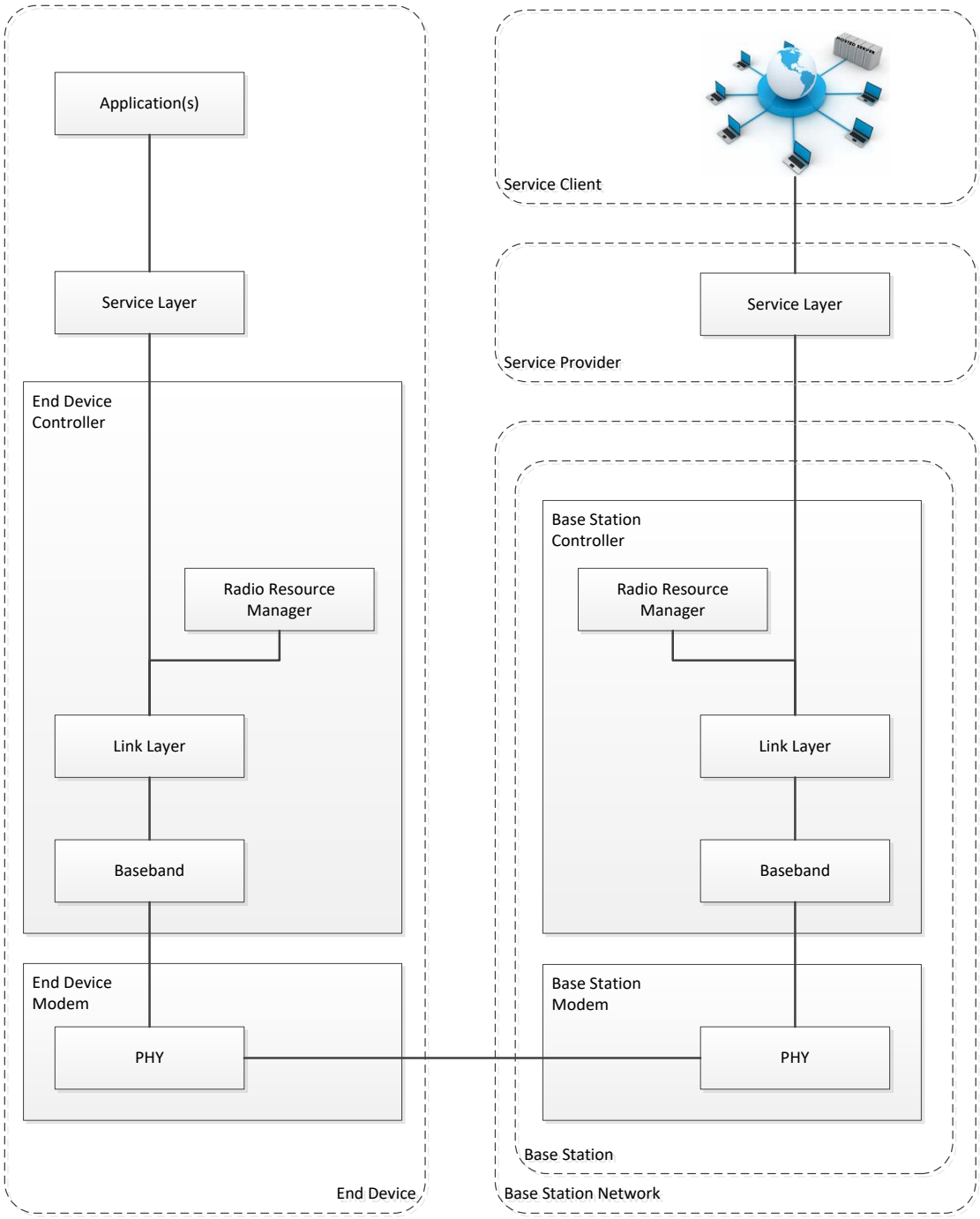

FIGURE 1-2 WEIGHTLESS-P SYSTEM OVERVIEW

1.2 SYSTEM VARIABLE TYPES

1.2.1 Universally Unique End Device Identifier (uuEID)

The uuEID is the universally unique identification of the end device. It is a 128-bit UUID as per RFC 4122.

1.2.2 End Device Identifier (EID)

The EID is a 24-bit identifier.

1.2.3 Individual End Device Identifier (iEID)

The iEID is the temporary 18-bit EID assigned to the End Device once it is registered to a Base Station. It cannot be all 0s.

1.2.4 Group End Device Identifier (gEID)

The gEID is the temporary 18-bit identifier assigned to a group of End Devices for multicast communication. It cannot be all 0s.

1.2.5 System End Device Identifier (sEID)

The sEID is a special-purpose EID. It is defined as follows:

TABLE 1-1 SYSTEM END DEVICE IDENTIFIERS

sEID name	sEID value mask (x: don't care)	Downlink use	Uplink use
EID_ALL	11 1111 1111 1111 1xxx	Broadcast	Contended access
EID_REGISTER	11 1111 1111 1111 0xxx	Registration	Contended access registration

1.2.6 Base Station Identifier (BS_ID)

The BS_ID is a 16-bit identifier of the Base Station in the Base Station Network. The value zero is not allowed.

1.2.7 Base Station Network Identifier (BSN_ID)

The BSN_ID is a 16-bit identifier of the Base Station Network. The value zero is not allowed, and the MSB indicates if the network is public (0) or private (1).

1.2.8 Service Provider Identifier (SP_ID)

The SP_ID is a 16-bit identifier of the Service Provider. The value zero is not allowed.

1.3 RADIO FRAME STRUCTURE

The Weightless-P network is a synchronous network with Base Station responsible for maintaining the timing. The radio frames from all Base Station are synchronized within +/- 1ms of each other. The radio frame structure is as follows:

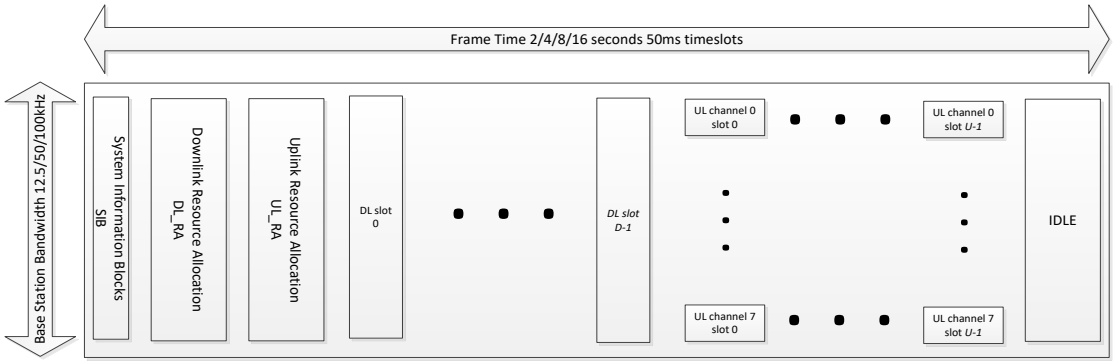

FIGURE 1-3 RADIO FRAME STRUCTURE

The radio frame has a duration of 2, 4, 8 or 16 seconds. It is composed of timeslots of 50ms each. The supported bandwidths are 12.5kHz (optional), 50kHz and 100kHz, split into respectively 1, 4 and 8 unit channels of 12.5kHz each for the uplink.

The radio frame starts with broadcast downlink information.

2 PHYSICAL LAYER

2.1 INTRODUCTION

This chapter describes the physical layer of Weightless-P, including the modulation and multiple access methods.

The major design objectives of the physical layer are listed below.

Requirement	**Design implication**
General purpose M2M solution, suitable for a diverse range of applications	Wide range of trade-offs between data throughput and available SNR. Robust to multipath delay spreads corresponding to ~15 kilometres range. Low data rate modes support communication with end devices at the periphery of cells or in poor signal propagation environments. Variable data rate provides greater throughput when SNR permits, and allows efficient scaling of system capacity with reduced cell size.
Compliant with various ISM/SRD regulatory frameworks, and capable of efficient operation in real-world unlicensed spectrum	Compliant with CCSA, FCC, ETSI, ARIB, TTA regulations. Interference mitigation through receiver diversity at base station and frequency hopping techniques.
Compatible with low power consumption End Devices	Efficient synchronisation with network, including initial acquisition and subsequent tracking. Modulation compatible with good transmit power amplifier efficiency.
Compatible with low cost End Devices	Intelligence within network concentrated at the base station (and higher network layers), such that End Device complexity is reduced. Modulation techniques selected to avoid imposing unnecessarily stringent requirements on End Device radio design.

2.1.1 Physical Channels Overview

The Physical Layer (PHY) presents three physical channels to the Baseband (BB) for processing:

- Downlink.
- Uplink.
- Uplink Contended Access.

The Downlink physical channel is used to transfer any downlink data from the Base Station to the End Device. The downlink data could be directed to an individual End Device, a group of End Devices or all End Devices within a cell.

The Uplink physical channel is a dedicated channel used to transmit data from the End Device to the Base Station.

The Uplink Contended Access physical channel is used to transmit data from the End Device to the Base Station. As the physical channel is contended, multiple End Devices are permitted to transmit on the same channel at the same time.

2.1.2 Duplex

The Weightless-P system utilizes Time Division Duplex (TDD). This allows flexible resource allocation with an adaptive switching point between downlink and uplink.

2.1.3 Resource Allocation

Each frame consists in a downlink section followed by an uplink section. The switching point between downlink and uplink sections will be dynamically adjusted based on the loading. The downlink section starts with a fixed broadcast section which carries frame synchronization, system information and resource allocation information from the Base Station to the End Devices.

2.1.4 Frequency Hopping

To provide for improved reliability with frequency diversity, reduce interference created to other systems potentially operating in the same frequency bands, and comply with the regulations, Weightless-P performs frequency hopping. The channel hop sequence is described in the System Information blocks in every frame. There is a maximum of N_{hop_ch}=64 channels. Hopping is on a per-timeslot basis.

The pseudo-random hopping sequence is defined by a length-31 Gold sequence. The output sequence $c(n)$ is defined by

$$c(n) = \left(x_1(n+1600) + x_2(n+1600)\right) \bmod 2$$
$$x_1(n+31) = \left(x_1(n+3) + x_1(n)\right) \bmod 2$$
$$x_2(n+31) = \left(x_2(n+3) + x_2(n+2) + x_2(n+1) + x_2(n)\right) \bmod 2$$

The first m-sequence shall be initialized with $x_1(0) = 1, x_1(n) = 0, n = 1,2,\ldots,30$. The initialization of the second m-sequence is denoted by $c_{\text{init}} = \sum_{i=0}^{30} x_2(i) \cdot 2^i = BSN\_ID$.

The frequency $f_{hop}(i)$ to be used for timeslot i is defined as follows:

$$f_{\text{hop}}(i) = \begin{cases} 0 & N_{\text{hop\_ch}} = 1 \\ (f_{\text{hop}}(i-1) + \sum_{k=i\cdot 10+1}^{i\cdot 10+9} c(k) \times 2^{k-(i\cdot 10+1)}) \bmod N_{\text{hop\_ch}} & N_{\text{hop\_ch}} = 2 \\ (f_{\text{hop}}(i-1) + \left(\sum_{k=i\cdot 10+1}^{i\cdot 10+9} c(k) \times 2^{k-(i\cdot 10+1)} \right) \bmod (N_{\text{hop\_ch}} - 1) + 1) \bmod N_{\text{hop\_ch}} & N_{\text{hop\_ch}} > 2 \end{cases}$$

with

$$f_{\text{hop}}(-1) = 0$$

2.1.5 Bit period

The maximum chip rate supported by Weightless-P is 100kchip/s, so the smallest time unit used across the system is Tb = 1/100k = 10µs.

2.2 DOWNLINK

2.2.1 Overview

All broadcast downlink channels (SIB, DL_RA, UL_RA) use a fixed-bandwidth 100kHz channel with a fixed chiprate of 100kchip/s.

Unicast and multicast downlink communication to End Devices supports variable data rate physical channels with the same fixed bandwidth and chip rate.

The downlink characteristics are as follows:

Multiple access method	Time-division multiple access (TDMA)
Modulation method	GMSK BT=0.3, OQPSK
Chip rate	100 / 50 kchip/s (10kchip/s optional)
Bandwidth	100 / 50 kHz (12.5kHz optional)
Datarate	3.125 / 6.25 / 12.5 / 25 / 50 / 100kbps
Spreading factor	1 for GMSK, 4 or 8 for OQPSK
FEC coding	None, rate ½ (convolutional)
Interleaving	Block-interleaving when FEC is enabled
Whitening	LFSR-based, with a seed derived from frame number and network identity

2.2.2 Spectral characteristics

GMSK and OQPSK modulation schemes are selected for their constant envelope (PAPR = 0dB), which allow optimal power efficiency at the transmitter and lower complexity at the receiver.

2.2.3 Cyclic Redundancy Code

The Header CRC will be calculated over the header, excluding the synchronization word according to the following polynomial:

$$X^8 + x^2 + x + 1$$

The Header CRC will be calculated as follows:

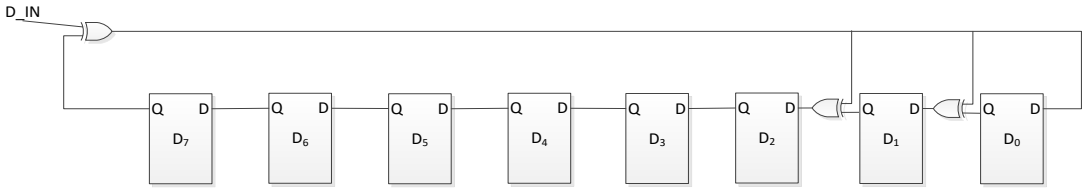

FIGURE 2-1 HEADER CRC CALCULATION

$D_{0\text{-}7}$ are seeded to 0x00 at start of CRC calculation. Header bits are applied least-significant bit first into D_IN over the payload. At the end of the CRC, the contents of the shift register are appended to the data stream such that bit D_7 is transmitted first.

The CRC will be calculated over the data payload using:

$$x^{16} + x^{12} + x^5 + 1$$

The CRC will be calculated as follows:

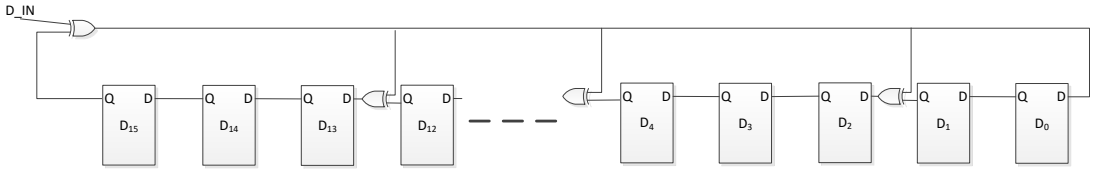

FIGURE 2-2 CRC CALCULATION

$D_{0\text{-}15}$ are seeded to 0x0000 at start of CRC calculation. Data bits are applied least-significant bit first into D_IN over the payload. At the end of the CRC, the contents of the shift register are appended to the data stream such that bit D_{15} is transmitted first.

2.2.4 Forward Error Correction

Rate ½ convolutional coding is optionally applied to provide some coding gain while being still efficient even with short packet length.

TABLE 2-1 AVAILABLE CODING RATES

Rate	FEC
1	None
½ (K=4)	Rate 1/2 non-recursive non-systematic convolutional code, using polynomials o17 and o13
½ (K=7)	Rate 1/2 non-recursive non-systematic convolutional code, using polynomials o171 and o133

The rate ½ K=4 convolutional code is terminated by appending 4 tail bits to the data bits at the input to the coder, chosen such that the final coder state will be 0.

The rate ½ K=7 convolutional code is terminated by appending 7 tail bits, all set to zero, to the data bits at the input to the coder.

Convolutional coding is applied before interleaving, and padding bits are added to fill up the interleaver matrix.

2.2.5 Interleaving

Interleaving is performed after convolutional coding to increase robustness in changing channel conditions with forward error correction, as it provides time diversity.

The interleaver is a block-interleaver with a matrix of 4 columns and 4 rows. The input bits are written into the interleaving matrix row-by-row, starting at row 0 column 0.

$$\begin{bmatrix} y_0 & y_1 & y_2 & y_3 \\ y_4 & y_5 & y_6 & y_7 \\ y_8 & y_9 & y_{10} & y_{11} \\ y_{12} & y_{13} & y_{14} & y_{15} \end{bmatrix}$$

The matrix is then read column-by-column in reverse order, starting from column 3 row 3.

$$\begin{bmatrix} y_{15} & y_{11} & y_7 & \cdots & y_8 & y_4 & y_0 \end{bmatrix}$$

2.2.6 Whitening

Whitening is employed using a seed that depends on the frame number, or, in the case of the System Information Block bursts (SIBs), the channel number. This is beneficial for the following reasons:

- It ensures that retransmitted bursts following a CRC error undergo different whitening compared with the original transmission. This provides robustness against any pathological data sequences.
- It ensures that a receiver tuned to one channel is very unlikely to decode a valid SIB from a transmitter operating on a different channel.

The whitening polynomial is PN9. The 9-bit seed is (0x100 | SFN_L), except for the SIB bursts for which the 9-bit seed is (0x1D3 ^ WARFCN).

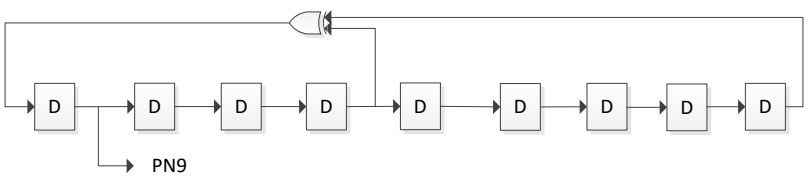

FIGURE 2-3 PN9 SEQUENCE GENERATION

Whitening is applied after interleaving and prior to modulation.

2.2.7 Packet Format

Weightless-P data packets consist in a preamble, followed by a 24-bit synchronization word, then the PHY payload:

FIGURE 2-4 PACKET FORMAT

The preamble is 0xAAAA in GMSK mode and all-zero in OQPSK (1 or 2 bytes for spreading factor 8 and 4, respectively).

The synchronization word differs whether Pilot Insertion and Forward Error Correction are applied or not. This is defined in Table 2-2.

TABLE 2-2: SYNCHRONIZATION WORD DEFINITION

Pilot Insertion	Forward Error Correction	Synchronization Word (LSB transmitted first)
ON	ON	0x21F6AF 0010 0001 1111 0110 1010 1111
	OFF	0xC9C2AF 1100 1001 1100 0010 1010 1111
OFF	ON	0xDE09AF 1101 1110 0000 1001 1010 1111
	OFF	0x363DAF 0011 0110 0011 1101 1010 1111

2.2.8 Spreading

There are two DSSS spreading factors for OQPSK mode, 4 and 8. For spreading factor 8, there are 2 sets of spreading sequences $(8,1)_0$ and $(8,1)_1$, applied to even and odd-numbered bits, respectively. The synchronization word only uses $(8,1)_0$.

TABLE 2-3: (4,1)-DSSS BIT-TO-CHIP MAPPING

Input bit	**Chip values (c_0 … c_3)**
0	1010
1	0101

TABLE 2-4: $(8,1)_K$-DSSS BIT-TO-CHIP MAPPING

k	Input bit	Chip values (c_0 … c_7)
0	0	1011 0001
	1	0100 1110
1	0	0110 0011
	1	1001 1100

2.2.9 Pilot Insertion

Pilot insertion is optional and indicated by the synchronization word.

In GMSK mode, a 4-bit pilot sequence is inserted every 64 bits. The first pilot sequence follows immediately the header.

GMSK pilot bit sequence (p_0 … p_3)
0101

In OQPSK modes, a 32-chip pilot sequence is inserted every 512 chips. The first pilot sequence follows immediately the header.

OQPSK pilot chip sequence (p_0 … p_{31})
1101 1110 1010 0010 0111 0000 0110 0101

2.2.10 Modulation

In GMSK mode, the bit sequence is modulated as Frequency Shift Keying with bit 0 corresponding to a negative frequency deviation and bit 1 corresponding to a positive frequency deviation. The modulation index is ½, and Gaussian smoothing filter is applied with BT=0.3, in accordance with §2.4, §2.5 and §2.6 of 3GPP TS 45.004.

In OQPSK mode the chip sequence is mapped to symbols (-1 for c = 0 and +1 for c = 1) and then modulated with a raised cosine pulse shape with roll-off factor of 0.8, in accordance with §18.3.2.13 of IEEE 802.15.4g-2012.

2.2.11 Typical Performance

The typical downlink performance is shown below for a 100kHz AWGN channel.

For all modulation modes, decision directed channel tracking through the payload may be performed in order to support operation with significant Doppler shift due to mobility or other factors. The performance degradation that results from any Doppler shift is dependent on the nature of the channel, the modulation mode, the spreading factor, and the channel tracking implementation.

TABLE 2-5: TYPICAL DOWNLINK PERFORMANCE

Modulation scheme	Coding rate	Spreading factor	Downlink PHY data rate (kbps)	Required SNR before FEC & spreading (dB)	FEC gain (dB)	Spreading gain (dB)	Required SNR for 10^{-4} BER (dB)	Noise figure (dB)	Required signal level at Rx input (dBm)
GMSK	1	1	**100**	12	0	0	**+12**	6	**-106**
GMSK	½	1	**50**	12	7.5	0	**+4.5**	6	**-113.5**
OQPSK	½	4	**12.5**	12	7.5	6	**-1.5**	6	**-119.5**
OQPSK	½	8	**6.25**	12	7.5	9	**-4.5**	6	**-122.5**

2.3 UPLINK

2.3.1 Overview

Contrary to the downlink where all transmission can be scheduled and synchronized across all neighbour Base Stations, the uplink needs to accommodate a large number of End Devices, which have non-synchronized traffic types. To provide for higher capacity, the uplink combines TDMA and FDMA in narrowband sub-channels (unit sub-channel is 12.5kHz).

Operation in a single 12.5kHz sub-channel allows for lower data rates and increased number of logical channels, providing better uplink capacity, especially for contented uplink channels.

For scheduled uplink transmission, the Base Station can allocate either a single 12.5kHz sub-channel, or combine the 8 sub-channels to offer a total bandwidth of 100kHz.

The uplink characteristics are as follows:

Multiple access method	Combined time-division multiple access (TDMA) and frequency-division multiple access (FDMA)
Modulation method	GMSK BT=0.3, OQPSK
Chip rate	10 / 100kchip/s
Bandwidth	12.5 / 100 kHz
Datarate	6.25 / 12.5 / 25 / 50 / 100kbps (100kHz) 0.625 / 1.25 / 2.5 / 5 / 10kbps (12.5kHz)
Spreading factor	1 for GMSK, 4 or 8 for OQPSK
FEC coding	None, rate ½ (convolutional)
Interleaving	Block-interleaving when FEC is enabled
Whitening	LFSR-based, with a seed derived from frame number and network identity
Frequency accuracy	+/- 10kHz relative to downlink for 100kHz mode +/- 1kHz relative to downlink for 12.5kHz mode

2.3.2 Cyclic Redundancy Code

Cyclic redundancy code is applied to uplink transmission in the same way as it is for downlink transmission, as per §2.2.3.

2.3.3 Forward Error Correction

Forward error correction is applied to uplink transmission in the same way as it is for downlink transmission, as per §2.2.4.

2.3.4 Interleaving

Interleaving is applied to uplink transmission in the same way as it is for downlink transmission, as per §2.2.5.

2.3.5 Whitening

Whitening is applied to uplink transmission in the same way as it is for downlink transmission, as per §2.2.6.

2.3.6 Packet Format

The uplink packet format is identical to the downlink packet format, as per §2.2.7.

2.3.7 Spreading

Spreading is applied to uplink transmission in the same way as it is for downlink transmission, as per §2.2.8.

2.3.8 Pilot Insertion

Pilot insertion is applied to uplink transmission in the same way as it is for downlink transmission, as per §2.2.9.

2.3.9 Modulation

Modulation is applied to uplink transmission in the same way as it is for downlink transmission, as per §2.2.10.

2.3.10 Power Control

Uplink power control is required to reduce interference levels in a cell and to optimize end device power consumption. It is also useful to accommodate varying densities of Base Stations, when a higher density allows smaller cells, lower transmit power, hence more frequency re-use and higher capacity.

Since uplink combines FDMA and TDMA, there is no need for adaptive low-latency closed loop power control. Open-loop power control (based on downlink RSSI) and optional slow closed-loop power control (through higher layer signaling) are sufficient.

2.3.11 Frequency Control

The End Device transmissions must be frequency-aligned to the downlink frequency as estimated by the End Device receiver, which could be a combination of frequency error and Doppler frequency shift.

The End Device is required to align its uplink transmission frequency to within +/- 500 Hz of the actual downlink transmission.

2.3.12 Typical Performance

The typical uplink performance is shown below for both 100kHz and 12.5kHz AWGN channels.

The noise floor reduction arising from the use of one 12.5kHz sub-channels is included as a 9dB processing gain. The Base Station is assumed to utilise two receive antennas for maximum ratio combining, which is included as a further 3 dB processing gain.

For all modulation modes, decision directed channel tracking through the payload may be performed in order to support operation with significant Doppler shift due to mobility or other factors. The performance degradation that results from Doppler shift is dependent on the nature of the channel, the modulation mode, the spreading factor, and the channel tracking implementation.

TABLE 2-6: TYPICAL UPLINK PERFORMANCE (100KHZ)

Modulation scheme	Coding rate	Spreading factor	Uplink PHY data rate (kbps)	Required SNR before coding & spreading (dB)	FEC gain (dB)	Processing gain (dB)	Required SNR for 10^{-4} BER (dB)	Noise figure (dB)	Required signal level at Rx input (dBm)
GMSK	1	1	**100**	12	0	3	**+9**	6	**-109**
GMSK	½	1	**50**	12	7.5	3	**+1.5**	6	**-116.5**
OQPSK	½	4	**12.5**	12	7.5	9	**-4.5**	6	**-122.5**
OQPSK	½	8	**6.25**	12	7.5	12	**-7.5**	6	**-125.5**

TABLE 2-7: TYPICAL UPLINK PERFORMANCE (12.5KHZ)

Modulation scheme	Coding rate	Spreading factor	Uplink PHY data rate (kbps)	Required SNR before coding & spreading (dB)	FEC gain (dB)	Processing gain (dB)	Required SNR for 10^{-4} BER (dB)	Noise figure (dB)	Required signal level at Rx input (dBm)
GMSK	1	1	**10**	12	0	13	**-1**	6	**-119**
GMSK	½	1	**5**	12	7.5	13	**-8.5**	6	**-126.5**
OQPSK	½	4	**1.25**	12	7.5	19	**-14.5**	6	**-132.5**
OQPSK	½	8	**0.625**	12	7.5	22	**-17.5**	6	**-135.5**

2.4 MODULATION AND CODING SCHEMES

Table 2-8 and Table 2-9 enumerate the modulation and coding schemes (MCS) for the uplink and downlink, respectively. The coding scheme information (FEC enabled or disabled) is carried in the Synchronization Word.

TABLE 2-8: UPLINK MODULATION AND CODING SCHEMES

MCS	Mode	Modulation	Spreading factor
0	100kHz	GMSK	1
1	100kHz	OQPSK	4
2	100kHz	OQPSK	8
3	12.5kHz	GMSK	1
4	12.5kHz	OQPSK	4
5	12.5kHz	OQPSK	8
6…15	RFU	RFU	RFU

TABLE 2-9: DOWNLINK MODULATION AND CODING SCHEMES

MCS	Modulation	Spreading factor
0	GMSK	1
1	OQPSK	4
2	OQPSK	8
3…7	RFU	RFU

2.5 END DEVICE RF PARAMETERS

2.5.1 Introduction

The RF specification defines the requirements on an End Device in order for it to operate satisfactorily within a Weightless-P network.

Within a Weightless-P network there are potentially large numbers of End Devices connected to a single Base Station. There will be a need to minimise the cost of the End Devices which may result in some compromise in the RF performance. However, the capacity of the network depends on the End Devices attaining some minimum level of RF

performance. This specification defines what that minimum level must be to ensure that the capacity of the network is not degraded.

2.5.2 Frequency bands

Definition: the frequency band of operation defines the potential range of frequencies which a single Base Station carrier could occupy.

A Weightless-P system will operate within a given frequency band. The frequency bands are listed in Table 2-10.

TABLE 2-10: FREQUENCY BANDS

Frequency band	Lower edge (MHz)	Upper edge (MHz)	Commonly referred to as
I	138.200	138.450	138MHz
I bis	169.400	169.600	169MHz
II	314.000	316.000	314MHz
III	430.000	432.000	430MHz
III bis	433.050	434.790	433MHz
III ter	470.000	510.000	470MHz
IV	779.000	787.000	780MHz
V	863.000	870.000	868MHz
V bis	870.000	876.000	873MHz
VI	902.000	928.000	915MHz
VI bis	915.900	916.900	915MHz
VI ter	920.500	929.700	923MHz

A Weightless-P system operates entirely within one of the bands defined above. Frequency hopping between bands or the use of different bands for uplink and downlink are not supported.

2.5.3 Channel Number

Definition: a channel number defines the carrier frequency for a specified frequency band group.

A Weightless-P Absolute Radio Frequency Channel Number (WARFCN) defines the center frequency of the channel by the relation:

$f_{MHz} = WARFCN * 0.1$

2.5.4 Frequency tolerance

Definition: the permissible ppm error in the carrier frequency of End Device transmission relative to the received Base Station carrier frequency.

The Base Station will maintain a frequency tolerance of ±1ppm.

When transmitting to the Base Station, an ED must achieve a frequency error of less than ±1ppm relative to the downlink portion of the same frame. This requirement is necessary to prevent leakage between the simultaneous uplink transmissions.

2.5.5 Symbol timing

Definition: the permissible ppm error in the symbol timing.

The fractional error in the symbol timing should be within ±100ppm of the fractional error in the carrier frequency. This requirement permits the symbol timing to be corrected once the actual carrier frequency has been determined.

2.5.6 Transmit power

Definition: the EIRP from the transmitter averaged over the synchronisation sequence and a sequence of representative symbols.

A minimum transmit EIRP is specified for the ED by the Weightless-P standard to ensure the capacity of the network is not degraded.

However, it is inappropriate to prescribe a single minimum transmit power for all devices in the network. For example, a device which only sends a few bytes per day could have a relaxed minimum transmit EIRP compared to a device which has a permanent data stream.

Therefore a minimum transmit EIRP is prescribed for different classes of device. It is essential that an appropriate class of device is adopted for each application.

Device Class	Minimum transmit EIRP
A	0dBm
B	10dBm
C	17dBm
D	27dBm
E	30dBm

2.5.7 Transmit Power control

Definition: the accuracy with which the transmit power must be set based on commands from the Link Layer.

The transmit EIRP for a given frame must not exceed the value and must be no more than 3 dB below the specified value.

2.5.8 Transmit spectral mask

Definition: the transmit spectral mask defines the maximum spurious energy which can be radiated in adjacent channels.

The transmit spectral mask at channel offset *n* is a defined as

$$P_{Mask}(n) = \begin{cases} 0dBm/1kHz, n = \pm 1 \\ -30dBm/1kHz, n = \pm 2 \\ -36dBm/1kHz, n = \pm 3 \\ -36dBm/100kHz, n \geq \pm 4 \end{cases}$$

If the ED is to be deployed in a geographic region where the regulator imposes a harsher adjacent channel emissions mask, then the ED must comply with that mask.

2.5.9 Out-of-band emissions

Definition: permissible level of unintended emissions from the End Device whose frequency lies outside the frequency band in use.

Weightless-P specifies the maximum out-of-band emission limit as -36dBm/100kHz.

However, these emissions must comply with local regulatory requirements. The local regulatory requirements may apply to idle and receive modes as well as during transmission.

2.5.10 Transmit modulation accuracy

Definition: The error vector magnitude (EVM) of the payload of the packet transmitted by the End Device.

A constraint is placed on the EVM of the payload of the packet transmitted by the End Device to ensure that the uplink link budget is maintained. The EVM is measured in a manner that is representative of a typical receiver implementation. This ensures that only transmitter degradations which would significantly impact link budget in a real system are reflected in the measurement.

Prior to measuring the payload EVM, the synchronisation word is used to estimate burst timing, frequency error and symbol timing error. Therefore, the accuracy of the synchronisation sequence is verified as a consequence of this test since inaccuracies in the synchronisation word will result in a degradation of the measured payload EVM, as for a real receiver.

For each payload block, a phase rotation is applied that minimises the measured EVM for that block. A limit is applied to the maximum allowed phase rotation as a function of the time between the end of the synchronisation sequence and the mid-point of the block being decoded. The limit is +/-0.2 rad/ms; phase rotations that exceed this limit are capped at the limit, resulting in an increase in the measured EVM for that block.

The average EVM over the symbols in the payload must not exceed -24 dB, and is calculated as follows:

$$EVM = 10\ log_{10}\{mean[(I - I_0)^2 + (Q - Q_0)^2]/P\}$$

where *I* and *Q* are the symbol's in-phase and quadrature components, I_0 and Q_0 are the closest ideal constellation point, and *P* is the power of the constellation.

2.5.11 Receiver sensitivity

Definition: the minimum received signal strength at which a specified packet error rate can be maintained.

The receiver sensitivity requirements for each modulation scheme in AWGN case are listed below. It is specified for a Bit Error Rate of 0.1%.

TABLE 2-11: RECEIVER SENSITIVITY REQUIREMENTS

Modulation scheme	Coding rate	Spreading factor	Required signal level at Rx input (dBm)
GMSK	1	1	**-105**
GMSK	½	1	**-112**
OQPSK	½	4	**-119**
OQPSK	½	8	**-122**

2.5.12 Receiver maximum input signal

Definition: the maximum level of the downlink signal at the ED which can be received error free.

The receiver maximum input signal determines how close an End Device may approach a Base Station whilst still receiving error free data. Weightless-P requires a maximum input signal level capability of at least 0dBm.

These maximum input signal levels apply to all modulation schemes.

2.5.13 Receiver adjacent channel rejection

Definition: the relative level of a Weightless-P signal in either the upper or lower adjacent channels that the End Device can tolerate for a 3dB degradation in sensitivity.

TABLE 2-12 ADJACENT CHANNEL REJECTION REQUIREMENTS

N	±1 (adjacent)	±2 (alternate)
Relative Level	40dB	40dB

2.5.14 Receiver blocking performance

Definition: the level of a blocking C.W. signal that the End Device can tolerate for a 3dB degradation in sensitivity.

TABLE 2-13 BLOCKING REQUIREMENTS

Blocking frequency offset	±2MHz	±10MHz
Level	60dB	60dB

3 BASEBAND

3.1 OVERVIEW

The Baseband (BB) is responsible for:

- Presenting a set of transport channels that the Link Layer (LL) can pass data to for transmission or receive data from.
- Connecting the physical channels to the transport channels provided by the Physical Layer (PHY).
- Structuring frames and identifying allocations within a frame.
- Transmitting frames on a Base Station and receiving frames on an End Device.
- Transmitting downlink data within a frame using the downlink physical channel on Base Station and receiving the downlink data on an End Device.
- Transmitting uplink data within a frame using the uplink physical channel on the End Device and receiving the uplink data on a Base Station.
- The Contended Access (CA) procedure using the Uplink Contended Access physical channel

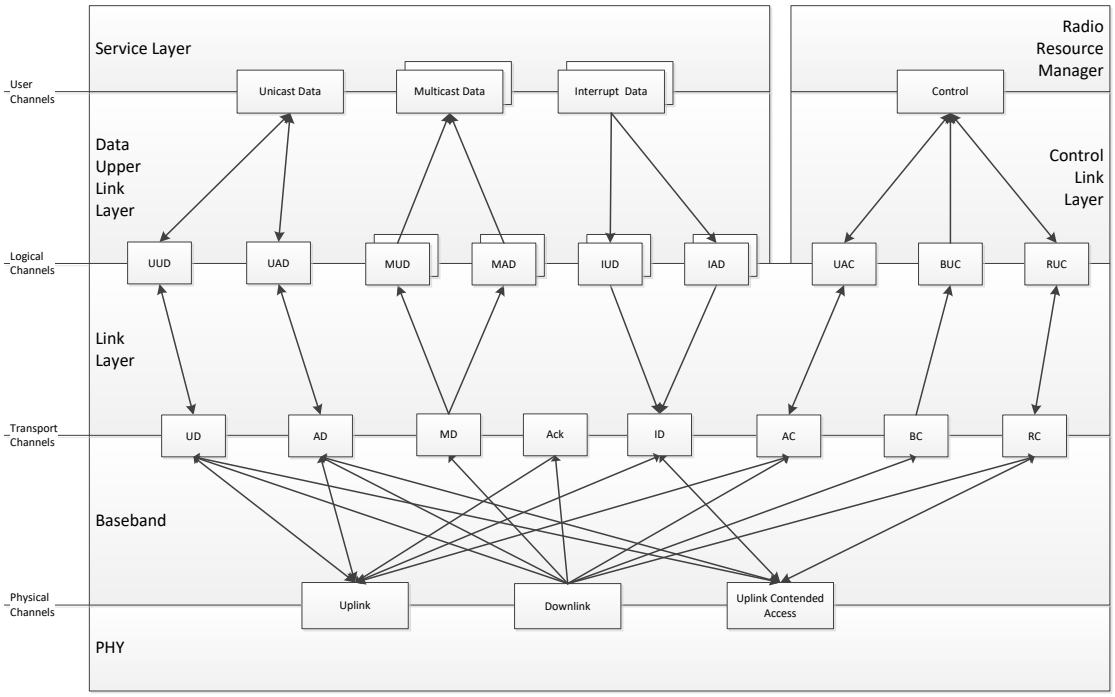

FIGURE 3-1 MAPPING OF CHANNELS

3.2 TRANSPORT CHANNELS

The BB interfaces to the Link Layer (LL) through a set of transport channels. The BB multiplexes/de-multiplexes the data from/to the physical channels into transport channels, presented to the layer above, according to channel type information and the type of addressing that was used.

The following transport channels are provided:

- Acknowledged Data (AD)
- Unacknowledged Data (UD)
- Acknowledged Control (AC)
- Multicast Data (MD)
- Interrupt Data (ID)
- Broadcast Control (BC)
- Register Control (RC)
- Acknowledgement Channel (ACK)

An ED shall have a maximum of one instance of each of the transport channels.

A BS shall have a maximum of one instance of the AD, UD, AC, MD, ID and ACK transport channels per ED and they shall be maintained separately for each ED.

There shall be one instance of the BC and RC transport channel per Base Station that is shared between all EDs.

The iEIDs used by the transport channels are assigned when an End Device registers to a Base Station. The iEIDs may be updated while the End Device is connected to a Base Station.

Not all the transport channels are permitted to use all the physical channels. The permitted physical channels for each transport channel are shown in Table 3-1

TABLE 3-1 PERMITTED TRANSPORT TO PHYSICAL CHANNEL MAPPING

Physical Channel Transport Channel	Uplink	Downlink	Uplink Contended Access
Acknowledged Data (AD)	✓	✓	✓
Unacknowledged Data (UD)	✓	✓	✓
Acknowledged Control (AC)	✓	✓	✓
Multicast Data (MD)		✓	
Interrupt Data (ID)	✓		✓
Broadcast Control (BC)		✓	
Register Control (RC)	✓	✓	✓
Acknowledgement Channel (ACK)	✓	✓	

.

TABLE 3-2 PERMITTED TRANSPORT CHANNEL BY EID

Transport Channel	Assigned iEID	Assigned gEID	sEID
Acknowledged Data (AD)	✓		✓ (EID_ALL for Contended Access only)
Unacknowledged Data (UD)	✓		✓ (EID_ALL for Contended Access only)
Acknowledged Control (AC)	✓		✓ (EID_ALL for Contended Access only)
Multicast Data (MD)	✓	✓	
Interrupt Data (ID)	✓	✓	✓ (EID_ALL for Contended Access only)
Broadcast Control (BC)			✓ (EID_ALL only)
Register Control (RC)	✓		✓ (EID_REGISTER only)
Acknowledgement Channel (ACK)	✓		

3.2.1 Acknowledged Data (AD)

The Acknowledged Data (AD) transport channel is a bidirectional channel used to transfer acknowledged user data.

The AD transport channel shall use an iEID for uplink and downlink. AD messages may also be sent from the End Device to the network using contended access with EID_ALL sEID.

3.2.2 Unacknowledged Data (UD)

The Unacknowledged Data (UD) transport channel is a bidirectional channel used to transfer unacknowledged user data.

The UD transport channel shall use an iEID for uplink and downlink. UD messages may also be sent from the End Device to the network using contended access with EID_ALL sEID.

3.2.3 Acknowledged Control (AC)

The Acknowledged Control (AC) transport channel is a bidirectional channel used to transfer reliable radio resource management messages.

The AC transport channel shall use an iEID for uplink and downlink. AC messages may also be sent from the End Device to the network using contended access with EID_ALL sEID.

3.2.4 Multicast Data (MD)

The Multicast Data (MD) transport channel is a downlink only channel that is used to transfer data from the network to the ED.

The MD transport channel does not differentiate between multicast data messages that require acknowledgement and those that do not. Retransmission is handled by the LL for each MD transport channel instance.

The MD transport channel shall use an iEID or a gEID for downlink.

3.2.5 Interrupt Data (ID)

The Interrupt Data (ID) transport channel is an uplink only channel that is used to transfer interrupt data from the End Device to the network.

The ID transport channel does not differentiate between interrupt data messages that require acknowledgement or those that do not. Retransmission is handled by the Link Layer for each ID transport channel instance.

The ID transport channel shall use an iEID or a gEID for uplink, or use contended access with EID_ALL sEID or a gEID.

3.2.6 Broadcast Control (BC)

The Broadcast Control (BC) transport channel is used to transfer unacknowledged control information from the Base Station to all End Devices within a cell.

The BC transport channel shall use EID_ALL sEID for downlink.

3.2.7 Register Control (RC)

The Register Control (RC) transport channel is a bidirectional channel used to transfer unacknowledged control messages within a cell for End Devices registering on a Base Station.

The RC transport channel shall use an iEID for uplink and downlink, EID_REGISTER sEID for contended access uplink traffic, and EID_REGISTER sEID for downlink traffic.

3.2.8 Acknowledgement Channel (ACK)

The Acknowledgement Channel (ACK) transport channel is a bidirectional channel used to transfer acknowledgement messages for data transferred over the Acknowledged Data (AD), Acknowledged Control (AC), Multicast Data (MD) and Interrupt Data (ID) transport channels.

The BB does not separate the retransmission scheme messages for each of the transport channels. The messages sent in the uplink direction are acknowledgement scheme messages for downlink transport channel messages.

The messages sent in the downlink direction are acknowledgement scheme messages for uplink transport channel messages.

The ACK transport channel shall use an iEID for uplink and downlink.

3.3 FRAME STRUCTURE

A frame consists of 6 sections, see below Figure 3-2:

- SIB: System Information Blocks, used for frame synchronization and to broadcast semi-static parameters of the Base Station and Base Station Network.
- DL_RA: Downlink Resource Allocation, composed of multiple bursts describing the allocated downlink transmission slots.
- UL_RA: Uplink Resource Allocation composed of multiple bursts describing the allocated uplink transmission slots.
- DL_ALLOC: the section for allocated downlink transmissions.
- UL_ALLOC: the section for allocated and contended uplink transmissions.
- IDLE: an idle slot in which no End Device is allowed to transmit. Reserved for measurements and future use.

FIGURE 3-2 FRAME STRUCTURE

3.3.1 System Information Blocks (SIBs)

The System Information Blocks contain semi-static parameters that End Devices only need to process when initially joining a Base Station, or when DL_RA or UL_RA indicate a SIB change by toggling SIB_FLAG.

The SIB timeslot is split into NS (1, 2, 4 or 8) slices of 50ms each for a total duration of 50ms to 400ms:

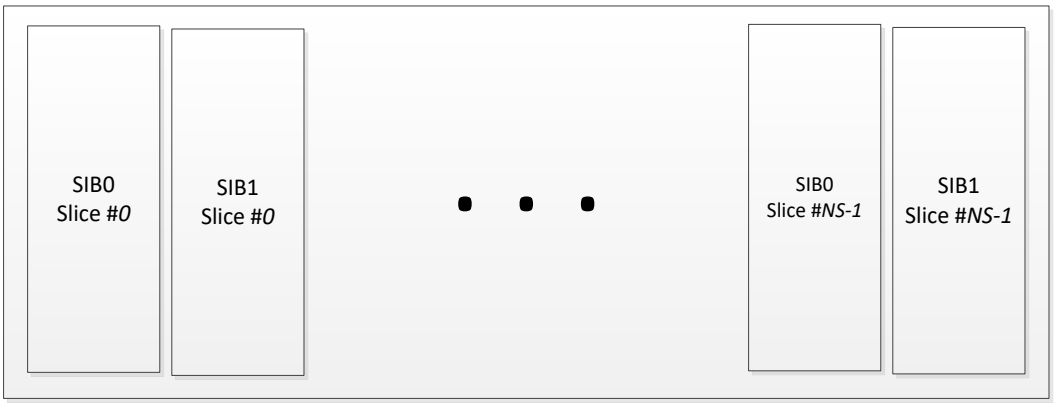

FIGURE 3-3 SYSTEM INFORMATION BLOCKS

A Base Station is required to transmit its SIB0 and SIB1 bursts in the slice it is assigned to, which is derived from the 3 least significant bits of its BS_ID:

BS_ID	Slice #
xxxx xxxx xxxx x000	0
xxxx xxxx xxxx x001	1 modulo NS
xxxx xxxx xxxx x010	2 modulo NS
xxxx xxxx xxxx x011	3 modulo NS
xxxx xxxx xxxx x100	4 modulo NS
xxxx xxxx xxxx x101	5 modulo NS
xxxx xxxx xxxx x110	6 modulo NS
xxxx xxxx xxxx x111	7 modulo NS

3.3.1.1 System Information Block 0 (SIB0)

System Information Block 0 is a mandatory information block. Its payload is as follows:

Offset (Bytes)	Length (bytes)	Name	Description
0	2	BS_ID	Base Station Identifier
2	2	BSN_ID	Base Station Network Identifier
4	2	SFN	System Frame Number
6	2	FRAME_FLAGS	Frame configuration flags (see below)
8	2	CRC	16-bit CRC of bytes 0 to 7 of SIB0 burst

3.3.1.2 SIB0 Frame Configuration flags

Position (bits)	Length (bits)	Name	Description
0…1	2	FRAME_DURATION	**00**: 2 seconds **01**: 4 seconds **10**: 8 seconds **11**: 16 seconds
2	1	VERSION	**0**: Weightless-P v1.0 **1**: RFU
3	1	SIB1_PRESENT	**0**: SIB1 is not transmitted **1**: SIB1 is transmitted
4	1	SIB_FLAG	Toggled when SIB information other than SFN is changed
5…6	2	NS	**00**: 1 slice **01**: 2 slices **10**: 4 slices **11**: 8 slices
7	1	SLICE_DURATION	**0**: 75ms DL / 150ms UL **1**: 150ms DL / 300ms UL
8…11	4	EVEN_RA_MCS	MCS used for even-numbered DL_RA and UL_RA bursts
12…15	4	ODD_RA_MCS	MCS used for odd-numbered DL_RA and UL_RA bursts

3.3.1.3 System Information Block 1 (SIB1)

System Information Block 1 is optional. It is required to be transmitted if frequency hopping is enabled, as it contains the hopping sequence information.

Offset (bytes)	Length (bytes)	Name	Description
0	1	HOP_FIRST_CH	First channel number in hop sequence
1	1	HOP_LAST_CH	Last channel in hop sequence
2	1	HOP_FLAGS	Frame configuration flags (see below)
3	1	EXTRA_FLAGS	See below
3	0…6 (NB_NCELL_CH)	NCELL_ CHx	Inter-frequency neighbor-cell channel numbers
9 + NB_NCELL_CH	0…15 (NB_BL_HOP_CH)	BL_HOP_CGHx	Blacklisted hopping channels
17 + NB_NCELL_CH + NB_BL_HOP_CH	2	CRC	16-bit CRC

If HOP_FIRST_CH equals HOP_LAST_CH, then frequency hopping is disabled. Otherwise they define the lowest and highest channel numbers (inclusive) in the hopping sequence.

3.3.1.4 SIB1 hopping flags (HOP_FLAGS)

Position (bits)	Length (bits)	Name	Description
0…5	6	HOP_CH_NB	Number of hopping channel between HOP_FIRST_CH and HOP_LAST_CH (inclusive) minus 1
6…7	2	HOP_PATTERN	RFU

HOP_CH_NB specify the number of channels in the hopping sequence. A value of 0 indicates 1 channel, a value of 63 indicates 64 channels.

3.3.1.5 SIB1 extra flags (EXTRA_FLAGS)

Position (bits)	Length (bits)	Name	Description
0…3	4	NB_BL_HOP_CH	Number of blacklisted hopping channels
4…6	3	NB_NCELL_CH	Number of inter-frequency neighbor-cell channels
7	1	RFU	RFU

3.3.1.6 SIB1 neighbor cell Base Station channels (NCELL_BS_CHx)

The End Device can autonomously discover intra-frequency neighboring Base Station by receiving the complete SIB timeslot to acquire up to 8 Base Stations.

Optionally, a Base Station can broadcast information on inter-frequency neighbor-cells by specifying the channel numbers of up to 7 inter-frequency neighbor cells in NCELL_CH0 to NCELL_CH6. These are 8-bit signed relative channel numbers in 100kHz steps. A value of 0 indicates no valid information.

3.3.1.7 SIB1 blacklisted hopping channels (BL_HOP_CHx)

The Base Station can blacklist up to 15 channels from the hopping sequence. The blacklisted channels are specified as 6 bits indexes in the hopping range. The 2 most significant bits are reserved and must be 0.

3.3.2 DL_RA

The Downlink Resource Allocation bursts are the only bursts typically processed every frame by End Devices and it is therefore critical to keep the payload small. DL_RA duration is NB_SLICES * 75ms or NB_SLICES * 150ms if SLICE_DURATION is 0 or 1, respectively:

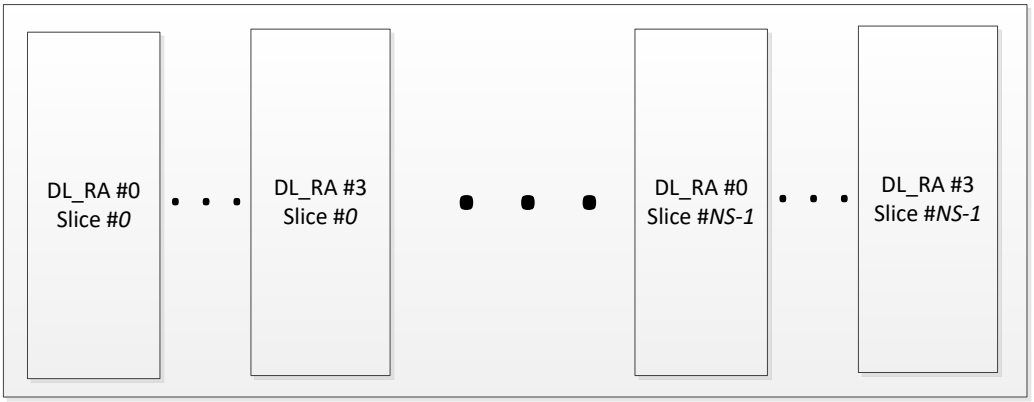

FIGURE 3-4 DL_RA STRUCTURE

Each Base Station transmits 4 DL_RA bursts DL_RA0 to DL_RA3. Base Stations are allocated slices similarly to SIB timeslot. An End Device only needs to process the DL_RA burst whose index corresponds to the 2 least significant bits of its iEID and gEID, if multicast is supported.

Each DL_RA burst is as follows:

Offset (bytes)	Length (bytes)	Name	Description
0	1	SFN_L	System Frame Number
1	1	DL_RA_FLAGS	See below
2	1	DL_START_TS_H	Index of first timeslot in allocation (8 MSB)
3	1	DL_RA_NUM	Number of downlink allocations
4	5 * DL_RA_NUM	DL_RA_INFOx	Array of downlink allocations (see below)
4 + 5 * DL_RA_NUM	DL_RA_NUM	DL_RA_MCSx	Array of downlink allocations MCSs (see below)

3.3.2.1 System Frame Number (SFN_L)

The 16-bit System Frame Number of the Base Station Network is incremented by 1 at every frame. Only its 8 least significant bits are transmitted in each DL_RA burst.

3.3.2.2 Downlink resource allocation flags (DL_RA_FLAGS)

Position (bits)	Length (bits)	Name	Description
0…1	2	DL_START_TS_L	Index of first timeslot in allocation (2 LSB)
2…6	5	RFU	RFU
7	1	SIB_FLAG	Mirror SIB_FLAG in SIB block. Toggled when there is a SIB change which requires End Device to re-acquire SIBs

3.3.2.3 Downlink resource allocation information (DL_RA_INFOx)

Each of the DL_RA_NUM downlink allocations are described with 5 bytes and combine 2 allocations as follows:

Offset (bytes)	Length (bytes)	Name	Description
0	1	DL_RA_DESC	Downlink allocation descriptor, see below
1	2	DL_RA_DST_EID0_H	First destination EID
3	2	DL_RA_DST_EID1_H	Second destination EID

DL_RA_DST_EIDx_H contains the 16 most significant bits of the destination iEID, gEID or sEID. The 2 LSB are derived from the burst index, as previously described. This forms the 18-bit iEID, gEID or sEID.

3.3.2.4 Downlink resource allocation descriptor (DL_RA_DESC)

Position (bits)	Length (bits)	Name	Description
0…3	4	DL_RA_NUM_SLOTS_0	Number of slots allocated to the first destination
4…7	4	DL_RA_NUM_SLOTS_1	Number of slots allocated to the second destination

3.3.2.5 Downlink resource allocation MCS descriptor (DL_RA_MCSx)

The MCS used for each of the DL_RA_NUM downlink allocations are described as follows:

Position (bits)	Length (bits)	Name	Description
0…3	4	DL_RA_MCS_0	MCS used for first allocation
4…7	4	DL_RA_MCS_1	MCS used for second allocation

3.3.3 UL_RA

The Uplink Resource Allocation bursts carry the uplink allocations. UL_RA duration is NB_SLICES * 150ms or NB_SLICES * 300ms if SLICE_DURATION is 0 or 1, respectively:

FIGURE 3-5 UL_RA STRUCTURE

Each Base Station transmits 8 UL_RA bursts UL_RA0 to UL_RA7. Base Stations are allocated slices similarly to SIB timeslot. An End Device only needs to process the UL_RA burst whose index corresponds to the 3 least significant bits of its iEID and gEID, if multicast is supported.

Each UL_RA burst is as follows:

Offset (bytes)	Length (bytes)	Name	Description
0	1	SFN_L	System Frame Number
2	1	UL_RA_FLAGS	See below
3	1	UL_START_TS_H	Index of first timeslot in allocation (8 MSB)
4	1	UL_RA_NUM	Number of uplink allocations
5	3 * UL_RA_NUM	UL_RA_INFOx	Array of 3-byte uplink allocations (see below)

3.3.3.1 System Frame Number (SFN)

The System Frame Number of the Base Station Network, incremented by 1 at every frame.

3.3.3.2 Uplink resource allocation flags (UL_RA_FLAGS)

Position (bits)	Length (bits)	Name	Description
0…1	2	UL_START_TS_L	Index of first timeslot in allocation (2 LSB)
2…6	5	RFU	RFU
7	1	SIB_FLAG	Mirror SIB_FLAG in SIB block. Toggled when there is a SIB change which requires End Device to re-acquire SIBs

3.3.3.3 Uplink resource allocation information (UL_RA_INFOx)

Each of the UL_RA_NUM uplink allocations are described with 3 bytes as follows:

Offset (bytes)	Length (bytes)	Name	Description
0	1	UL_RA_DESC	Uplink allocation descriptor, see below
1	2	UL_RA_DST_EID_H	Part of destination EID

UL_RA_DST_EID_H contains the 15 most significant bits of the destination iEID, gEID or sEID. The most significant bit of UL_RA_DST_EID_H is RFU and must be set to 0. The 3 LSB are derived from the burst index. This forms the 18-bit iEID, gEID or sEID.

3.3.3.4 Uplink resource allocation descriptor (UL_RA_DESC)

Position (bits)	Length (bits)	Name	Description
0…3	4	UL_RA_NUM_SLOTS	Number of slots allocated
4…7	4	UL_RA_MCS	MCS used for uplink allocation

3.3.4 DL_ALLOC

The downlink section is composed of 25ms slots. When a downlink allocation spreads over multiple slots, it is allowed for a transmission to cross one or multiple slot boundaries. If frequency hopping is applied, it is not allowed to hop during a transmission. If a transmission has spread over multiple consecutive slots, the associated hopping channels are skipped, so that the relation between a timeslot index and the hopping channel index is kept deterministic.

3.3.5 UL_ALLOC

The uplink section is composed of 25ms slots. Similar to downlink, when an uplink allocation spreads over multiple slots, it is allowed for a transmission to cross one or multiple slot boundaries. If frequency hopping is applied, it is not allowed to hop during a transmission. If a transmission has spread over multiple consecutive slots, the associated hopping channels are skipped, so that the relation between a timeslot index and the hopping channel index is kept deterministic.

3.4 BURST PAYLOAD DATA (BPD) STRUCTURE

The data payload to and from the PHY is transferred as one or more BPDs.

A DL_ALLOC or UL_ALLOC can contain 1 or more BPDs. The format of the BPD is different depending upon:

- whether it is being sent in a contended access uplink allocation,
- whether it is being sent to an individual End Device using an iEID,
- whether it is being sent to a group of End Devices using a gEID,
- the type of transport channel used.

A BPD can contain a higher layer message, part of a higher layer message or retransmission scheme message(s).

The higher layer message within the BPD may be split into 1 or more segments. Each segment has a maximum length of 256 bytes in total including segment header information which can be five or more bytes as described in the following section. It also has a 16-bit CRC.

Some BPDs transparently carry LLa and LLb fields, which are for Link Layer use, and whose meaning depends on the type of Transport Channel.

There are 5 BPD formats, 4 for the combination of complete or partial message and whether the BPD contains segments or not and a contended access BPD:

- Complete Message without Segments BPD defined in §3.4.1
- Partial Message without Segments BPD defined in §3.4.2
- Complete Message with Segments BPD defined in §3.4.3
- Partial Message with Segments BPD defined in §3.4.4
- Contended Access BPD defined in §3.4.5

3.4.1 Complete Message without Segments BPD

The Complete Message without Segments structure contains a complete higher layer message that is not split into segments. The format of the Complete Message without Segments BPD is shown in Figure 3-6.

Length (8-bit)	Flags (8-bit)	LLa (8-bit)	LLb (8-bit)	Header CRC (8-bit)	Complete Message (Length bytes)	CRC (16-bits)

FIGURE 3-6 COMPLETE MESSAGE WITHOUT SEGMENTS BPD

3.4.2 Partial Message without Segments BPD

The Partial Message without Segments BPD contains part of a higher layer message that is not split into segments. The format of the Partial Message without Segments BPD is shown in Figure 3-7.

Length (8-bit)	Flags (8-bit)	LLa (8-bit)	LLb (8-bit)	Header CRC (8-bit)	Offset (16-bit)	Message Fragment (Length bytes)	CRC (16-bits)

FIGURE 3-7 PARTIAL MESSAGE WITHOUT SEGMENTS BPD

3.4.3 Complete Message with Segments BPD

The Complete Message with Segments structure contains a complete higher layer message that is split into one or more segments. The format of the Complete Message with Segments BPD is shown in Figure 3-8.

Length (8-bit)	Flags (8-bit)	LLa (8-bit)	LLb (8-bit)	SegLen (8-bit)	Header CRC (8-bit)	Segment *0* (SegLen bytes)	Segment *0* CRC (16-bits)	...	Segment *n-1* (≤SegLen bytes)	Segment *n-1* CRC (16-bits)

FIGURE 3-8 COMPLETE MESSAGE WITH SEGMENTS BPD

3.4.4 Partial Message with Segments BPD

The Partial Message without Segments BPD contains part of a higher layer message that is split into one or more segments. The format of the Partial Message with Segments BPD is shown in Figure 3-8.

Length (8-bit)	Flags (8-bit)	LLa (8-bit)	LLb (8-bit)	SegLen (8-bit)	Offset (16-bit)	Header CRC (8-bit)	Fragment Segment *0* (SegLen bytes)	Fragment Segment *0* CRC (16-bits)	...	Fragment Segment *n-1* (≤SegLen bytes)	Fragment Segment *n-1* CRC (16-bit)

FIGURE 3-9 PARTIAL MESSAGE WITH SEGMENTS BPD

3.4.5 Contented Access BPD

The Contended Access BPD is transmitted by an End Device in an uplink contended access allocation. The format of the Contended Access BPD is shown in Figure 3-10.

The payload of the BPD contains a complete message.

Length (8-bit)	Flags (8-bit)	Payload (Length bytes)	CRC (16-bits)

FIGURE 3-10 CONTENDED ACCESS BPD

3.5 BPD FLAGS

3.5.1 Complete and Partial BPD Flags

TABLE 3-3 COMPLETE AND PARTIAL BPD FLAGS

Position (bits)	Length (bits)	Name	Description
0…1	2	MSG_TRCH	Describe which transport channel the BPD contains data from. **00**: AD Transport Channel **01**: UD Transport Channel **10**: AC Transport Channel **11**: Tunneled Transport Channel
2	1	SEG_FORMAT	**0**: BPD does not contain segments **1**: BPD contains segments
3…4	2	BB_FORMAT	**00**: BPD contains part of a message, not the start **01**: BPD contains part of a message at the start

			10: BPD contains a complete message **11**: BPD contains ACK Transport Channel message(s)
5	1	RFU	Must be set to 0
6	1	TS_INDEX	Least significant bit of the timeslot index where the BPD transmission was initiated
7	1	LAST_BPD	**0**: more BPD(s) follow **1**: last BPD in allocation

3.5.2 Contended Access BPD Flags

TABLE 3-4 CONTENDED ACCESS BPD FLAGS

Position (bits)	Length (bits)	Name	Description
0…1	2	CA_TYPE	**00**: Registration Request **01**: Transport Channel **10**: Uplink Resource Request **11**: RFU
2…3	2	CA_FLAGS	See below
4…6	3	RFU	
7	1	LAST_BPD	**0**: more BPD(s) follow **1**: last BPD in allocation

TABLE 3-5 CA_FLAGS DEFINITION

CA_TYPE CA_FLAGS	00 (Registration Request)	01 (Transport Channel)	10 (Uplink Resource Request)
00	Registration Message Identifier from LL	BPD contains AD Transport Channel	Uplink Resource Request
01		BPD contains UD Transport	RFU

		Channel	
10		BPD contains AC Transport Channel	RFU
11		BPD contains ID Transport Channel	RFU

3.6 BPD TO TRANSPORT CHANNEL MAPPING

3.6.1 AD Transport Channel Mapping

Table 3-6 defines the EID, direction, BPD structure and BPD flags values that are used to route to and from the AD transport channel.

TABLE 3-6 ROUTING PARAMETERS FOR AD TRANSPORT CHANNEL

EID	Direction	BPD Format	Flags
iEID	Both	Complete Message without Segments	xxx1 0000
		Complete Message with Segments	xxx1 0100
		First Partial Message without Segments	xxx0 1000
		First Partial Message with Segments	xxx0 1100
		Continued Partial Message without Segments	xxx0 0000
		Continued Partial Message with Segments	xxx0 0100
EID_ALL	Uplink	Contended Access BPD	xxxx 0001

3.6.2 UD Transport Channel Mapping

Table 3-7 defines the EID, uplink, BPD structure and BPD flags values that are used route to and from the UD transport channel.

TABLE 3-7 ROUTING PARAMETERS FOR UD TRANSPORT CHANNEL

EID	Direction	BPD Format	Flags
iEID	Both	Complete Message without Segments	xxx1 0001
		Complete Message with Segments	xxx1 0101
		First Partial Message without Segments	xxx0 1001
		First Partial Message with Segments	xxx0 1101
		Continued Partial Message without Segments	xxx0 0001
		Continued Partial Message with Segments	xxx0 0101
EID_ALL	Uplink	Contended Access BPD	xxxx 0101

3.6.3 AC Transport Channel Mapping

Table 3-8 defines the EID, direction, BPD structure and BPD flags values that are used route to and from the AC transport channel.

TABLE 3-8 ROUTING PARAMETERS FOR AC TRANSPORT CHANNEL

EID	Direction	BPD Format	Flags
iEID	Both	Complete Message without Segments	xxx1 0010
		Complete Message with Segments	xxx1 0110
		First Partial Message without Segments	xxx0 1010
		First Partial Message with Segments	xxx0 1110
		Continued Partial Message without Segments	xxx0 0010
		Continued Partial Message with Segments	xxx0 0110
EID_ALL	Uplink	Contended Access BPD	xxxx 1001

3.6.4 MD Transport Channel Mapping

Table 3-9 defines the EID, direction, BPD structure and BPD flags values that are used route to and from the MD transport channels.

TABLE 3-9 ROUTING PARAMETERS FOR MD TRANSPORT CHANNELS

EID	Direction	BPD Format	Flags
gEID	Downlink	Complete Message without Segments	xxx1 00xx
		Complete Message with Segments	xxx1 01xx
		First Partial Message without Segments	xxx0 10xx
		First Partial Message with Segments	xxx0 11xx
		Continued Partial Message without Segments	xxx0 00xx
		Continued Partial Message with Segments	xxx0 01xx
iEID	Downlink	Complete Message without Segments	xxx1 0011
		Complete Message with Segments	xxx1 0111
		First Partial Message without Segments	xxx0 1011
		First Partial Message with Segments	xxx0 1111
		Continued Partial Message without Segments	xxx0 0011
		Continued Partial Message with Segments	xxx0 0111

3.6.5 ID Transport Channel Mapping

Table 3-10 defines the EID, direction, BPD structure and BPD flags values that are used route to and from the ID transport channel.

TABLE 3-10 ROUTING PARAMETERS FOR ID TRANSPORT CHANNELS

EID	Direction	BPD Format	Flags
gEID	Uplink	Contended Access BPD	xxxx 1101
iEID	Uplink	Complete Message without Segments	xxx1 0011
		Complete Message with Segments	xxx1 0111
		First Partial Message without Segments	xxx0 1011
		First Partial Message with Segments	xxx0 1111
		Continued Partial Message without Segments	xxx0 0011
		Continued Partial Message with Segments	xxx0 0111
EID_ALL	Uplink	Contended Access BPD	xxxx 1101

3.6.6 BC Transport Channel Mapping

Table 3-11 defines the EID, direction, BPD structure and BPD flags values that are used route to and from the BC transport channel.

TABLE 3-11 ROUTING PARAMETERS FOR BC TRANSPORT CHANNEL

EID	Direction	BPD Format	Flags
EID_ALL	Downlink	Complete Message without Segments	xxx1 00xx
		Complete Message with Segments	xxx1 01xx
		First Partial Message without Segments	xxx0 10xx
		First Partial Message with Segments	xxx0 11xx
		Continued Partial Message without Segments	xxx0 00xx
		Continued Partial Message with Segments	xxx0 01xx

3.6.7 RC Transport Channel Mapping

Table 3-12 defines the EID, direction, BPD structure and BPD flags values that are used route to and from the RC transport channel.

TABLE 3-12 ROUTING PARAMETERS FOR RC TRANSPORT CHANNEL

EID	Direction	BPD Format	Flags
EID_REGISTER iEID	Downlink	Complete Message without Segments	xxx1 00xx
		Complete Message with Segments	xxx1 01xx
		First Partial Message without Segments	xxx0 10xx
		First Partial Message with Segments	xxx0 11xx
		Continued Partial Message without Segments	xxx0 00xx
		Continued Partial Message with Segments	xxx0 01xx
EID_REGISTER	Uplink	Contended Access BPD	xxxx xx00
iEID	Uplink	Complete Message without Segments	xxx1 00xx
		Complete Message with Segments	xxx1 01xx
		First Partial Message without Segments	xxx0 10xx
		First Partial Message with Segments	xxx0 11xx

		Continued Partial Message without Segments	xxx0 00xx
		Continued Partial Message with Segments	xxx0 01xx

3.6.8 ACK Transport Channel Mapping

Table 3-13 defines the EID, direction, BPD structure and BPD flags values that are used route to and from the ACK transport channel.

TABLE 3-13 ROUTING PARAMETERS FOR ACK TRANSPORT CHANNEL

EID	Direction	BPD Format	Flags
iEID	Downlink	Complete Message without Segments	xxx1 10xx
		Complete Message with Segments	xxx1 11xx
	Uplink	Complete Message without Segments	xxx1 10xx
		Complete Message with Segments	xxx1 11xx

3.7 ED UPLINK PROCEDURE

When an End Device is determining what to transmit within an uplink allocation, if there is data available on more than one transport channel it performs prioritization. The End Device shall always transmit in an uplink allocation. The End Device shall always fill an uplink allocation with BPDs while there is data available from transport channels. If no transport channels provide data to transmit then the BB shall transmit an ACK transport channel message with no payload. If there is a message available on the ACK transport channel with a payload it shall be sent first.

3.8 ED CONTENDED ACCESS UPLINK PROCEDURE

The End Device can transmit data in contended uplink allocations assigned to EID_ALL, EID_REGISTER or gEIDs assigned to the End Device. Data from the UD or AD transport channels can only be transmitted in allocations assigned to EID_ALL. Data from the ID transport channel can only be transmitted in allocations assigned to EID_ALL or gEIDs assigned to the End Device. Data from the RC transport channel can only be transmitted in allocations assigned to EID_REGISTER.

If an End Device determines that it should transmit in a contended access allocation it is recommended to perform a back off procedure to select which frame to transmit within. The back off procedure is to prevent multiple End Devices being triggered by the same external event from attempting contended access in the same frame with the resulting high probability of collision.

If the End Device has opportunity to transmit the message using scheduled uplink during or at the expiry of the back off period, it should be transmitted using the scheduled uplink rather than contended access.

A frame may have multiple contended uplink allocations that the End Device could transmit in. Each of the contended uplink allocations may be for the same or different EIDs and have different MCSs. The End Device shall select which uplink contended allocation to transmit in. An End Device may transmit in multiple uplink contended allocations within a frame. An End Device shall not transmit the same message more than once in the uplink contended allocations within a frame. The End Device should choose the contended access uplink allocation that it believes has the lowest MCS that will allow it to send its message successfully.

When an End Device has selected a contended uplink allocation within the frame, it shall select which slot within the allocation to start transmitting, as per slotted ALOHA. The End Device shall calculate the number of slots that are required for the data to be transmitted using the MCS for the allocation. The End Device selects a random slot between the first slot and the number of slots in the allocation minus the number of slots required for the data. The End Device shall start transmission of the message at the start of the randomly selected slot.

When mandated by the local regulation of the region of deployment, provision has to be made for additional slotted CSMA/CA procedure.

The ED can then transmit either a complete AD, UD, AC or ID transport channel message, a RC transport channel message, or an Uplink Resource Request.

3.8.1 AD, UD, AC and ID Transport Channel CA Uplink

When the ED transmits a complete AD, UD, AC or ID transport channel message in the CA uplink, it will use the following payload format for the CA BPD:

TABLE 3-14 CA BPD PAYLOAD FOR AD, UD, AC OR ID TRANSPORT CHANNEL MESSAGE

Offset (bytes)	Length (bytes)	Name	Description
0	3	iEID	The iEID of the ED
3	1	SN	Sequence Number of the message
4	1…251	PDU	Content of the message

Note: for IAD, the first byte of PDU is the IAD instance identifier

3.8.2 Uplink Resource Request CA Uplink

If an uplink contended allocation cannot contain a complete message, or the complete message cannot fit in a CA BPD, or if higher layers specifically request a dedicated uplink resource, the ED can transmit an Uplink Resource Request in a EID_ALL allocation.

The CA BPD payload will be as follows:

TABLE 3-15 CA BPD PAYLOAD FOR UPLINK RESOURCE REQUEST

Offset (bytes)	Length (bytes)	Name	Description
0	3	iEID	The iEID of the ED
3	1	RFU	

4 LINK LAYER

4.1 OVERVIEW

The Link Layer (LL) is responsible for

- Connecting the Logical Channels to the Transport Channels provided by the Baseband
- Retransmission and reliability for the Logical Channels
- Fragmentation and reassembly of data

The processing can be either Acknowledged or Unacknowledged.

4.2 LOGICAL CHANNELS

Data is taken from the baseband as a set of transport channels into the Link Layer (LL). The Link Layer multiplexes/de-multiplexes the transport channels into logical channels according to functionality (control or user data).

Logical channels are provided to send and receive user data or control traffic between an individual End Device and a Base Station or a group of End Devices and a Base Station. The logical channels can provide a reliable, acknowledged packet stream or an unacknowledged unreliable packet stream.

The following logical channels are provided:

- Unicast Acknowledged Data (UAD)
- Unicast Unacknowledged Data (UUD)
- Unicast Acknowledged Control (UAC)
- Multicast Acknowledged Data (MAD)
- Multicast Unacknowledged Data (MUD)
- Interrupt Acknowledged Data (IAD)
- Interrupt Unacknowledged Data (IUD)
- Broadcast Unacknowledged Control (BUC)
- Register Unacknowledged Control (RUC)

4.2.1 Unicast Acknowledged Data (UAD)

The Unicast Acknowledged Data (UAD) logical channel is a bidirectional channel that transfers uplink user data from the End Device to the network and downlink user data from the network to the End Device.

The user data is transferred over the AD Transport Channel. The acknowledgements are transferred over the ACK Transport Channel. The AD and ACK transport channels combine to provide a reliable, ordered packet based UAD logical channel.

LLa will be set to the Sequence Number (SN) of the message or fragment. LLb will be set to the Next Expected Sequence Number (NESN) of the UAD instance.

4.2.2 Unicast Unacknowledged Data (UUD)

The Unicast Unacknowledged Data (UUD) logical channel is a bidirectional channel that transfers uplink user data from the End Device to the network and downlink user data from the network to the End Device.

The user data is transferred over the UD transport channel. There is no additional signaling to support the UAD logical channel.

LLa will be set to the Sequence Number (SN) of the message or fragment. LLb will be set to the Next Expected Sequence Number (NESN) of the UAD instance.

4.2.3 Unicast Acknowledged Control (UAC)

The Unicast Acknowledged Control (UAC) logical channel is a bidirectional channel that transfers uplink control messages from the End Device to the network and downlink control messages from the network to the End Device.

The control messages are transferred over the AC Transport Channel. The acknowledgements are transferred over the ACK Transport Channel. The AC and ACK transport channels combine to provide a reliable, ordered packet based UAC logical channel.

LLa will be set to the Sequence Number (SN) of the message or fragment. LLb will be set to the Next Expected Sequence Number (NESN) of the UAC instance.

4.2.4 Multicast Acknowledged Data (MAD)

The Multicast Acknowledged Data (MAD) logical channel is a downlink only channel that transfers user data from the network to the End Device.

The user data is transferred over the MD transport channel. The ACK transport channel provides a transport channel for uplink acknowledgements from the End Device to the network. The MD and ACK transport channels combine to provide a reliable, ordered packet based MAD logical channel.

There may be multiple instances of the MAD logical channel, one for each of the Multicast User Channels that require acknowledged transfer.

LLa will be set to the Sequence Number (SN) of the message or fragment. LLb will be set to the instance identifier.

4.2.5 Multicast Unacknowledged Data (MUD)

The Multicast Unacknowledged Data (MUD) logical channel is a downlink only channel that transfers user data from the network to the End Device.

The user data is transferred over the MD transport channel.

There may be multiple instances of the MUD logical channel, one for each of the Multicast User Channels that does not require acknowledged transfer.

LLa will be set to the Sequence Number (SN) of the message or fragment. LLb will be set to the instance identifier.

4.2.6 Interrupt Acknowledged Data (IAD)

The Interrupt Acknowledged Data (IAD) logical channel is an uplink only channel that transfers user data from the End Device to the network.

The interrupt user data is transferred over the ID transport channel. The ACK transport channel provides a transport channel for downlink acknowledgements from the network to the End Device. The ID and ACK transport channels combine to provide a reliable, ordered packet based IAD logical channel.

There may be multiple instances of the IAD logical channel, one for each of the Interrupt User Channels that require acknowledged transfer.

LLa will be set to the Sequence Number (SN) of the message or fragment. LLb will be set to the Next Expected Sequence Number (NESN) of the IAD instance.

4.2.7 Interrupt Unacknowledged Data (IUD)

The Interrupt Unacknowledged Data (IUD) logical channel is an uplink only channel that transfers user data from the End Device to the network.

The interrupt user data is transferred over the ID transport channel.

There may be multiple instances of the IUD logical channel, one for each of the Interrupt User Channels that does not require acknowledged transfer.

LLa will be set to the Sequence Number (SN) of the message or fragment. LLb will be set to the instance identifier.

LLa will be set to the Sequence Number (SN) of the message or fragment. LLb will be set to the Next Expected Sequence Number (NESN) of the IAD instance.

4.2.8 Broadcast Unacknowledged Control (BUC)

The Broadcast Unacknowledged Control (BUC) logical channel is a downlink only channel that transfers control messages from the network to the End Device.

The control messages are transferred over the BC transport channel.

LLa will be set to the Sequence Number (SN) of the message. LLb will be set to 0.

4.2.9 Register Unacknowledged Control (RUC)

The Register Unacknowledged Control (RUC) logical channel is a bidirectional channel that transfers uplink connection control messages from the End Device to the network and downlink connection control messages from the network to the End Device.

The control messages are transferred over the RC transport channel.

4.3 USER AND CONTROL CHANNELS

4.3.1 Control Channel

The Control Channel is provided to send and receive control traffic between an individual End Device and a Base Station, specifically to / from the Radio Resource Manager. The Link Layer provides the appropriate security procedures to each control channel.

The Control Channel is used by the Radio Resource Manager to transfer messages from the End Device to the network for connection control or maintenance of the link between the End Device and Base Station.

The Control Channel also provides a stream of downlink only control messages from the network that are used to maintain the link between the End Device and the Base Station.

Depending upon the type (unicast or connection) of message being sent by the Radio Resource Manager and the connection state, the uplink messages are sent using either the UAC logical channel or the RUC logical channel.

Downlink messages are routed from the UAC, BUC or RUC logical channels to the Control Channel, along with the type of the message received (unicast, broadcast or register).

4.3.2 User Channels

The Link Layer multiplexes/de-multiplexes the logical channels into User Channels according to functionality (unicast, multicast, interrupt and acknowledgement) and also provides the appropriate security procedures to each user channel.

User channels are provided to send and receive user data between an individual End Device and a Base Station, from the network to multiple End Devices or uplink between an End Device and network. The following User Channels are provided:

- Unicast Data
- Multicast Data
- Interrupt Data

Each of the User Channels may carry either acknowledged or unacknowledged user data.

Unicast Data is a bidirectional channel between the End Device and the network that is either acknowledged or unacknowledged. The Unicast Data channel shall use the UAD logical channel for acknowledged Unicast Data or the UUD logical channel for unacknowledged Unicast Data.

Multicast Data is a downlink only channel between the network and the End Device that is either acknowledged or unacknowledged. The Multicast Data channel shall use the MAD logical channel for acknowledged Multicast Data or the MUD logical channel for unacknowledged Multicast Data.

Interrupt Data is an uplink only channel between the End Device and the network and is either acknowledged or unacknowledged. The Interrupt Data channel shall use the IAD logical channel for acknowledged Interrupt Data or the IUD logical channel for unacknowledged Interrupt Data.

4.4 FRAGMENTATION AND REASSEMBLY

On transmission, the LL is responsible for fragmenting a message so the BB can transmit BPDs that fit within DL_ALLOC or UL_ALLOC allocations.

The BB may transmit multiple BPDs within a single allocation from multiple Transport Channels, therefore there may not be a direct mapping between the size of DL_ALLOC and UL_ALLOC allocations and the amount of data transmitted from a single Transport Channel.

If the complete message from the Logical Channel does not fit within a BPD in the BB then then it must be fragmented. The LL performs this fragmentation. A message may be transmitted as fragments or as a complete message.

To fragment a message for transmission the LL first splits the message into 2 parts. The first part contains the message to be transmitted by the BB. The first part shall be sized to fit within the BPD allocation. The second part contains data that shall be transmitted at a later time.

The first part is passed to the BB for transmission. Information about the fragment is passed to the BB to allow it to set the BPD header fields.

The 2-way split can be repeated as many times as needed to split the message into multiple BPDs.

As fragmentation and reassembly does not support retransmissions, the higher layers cannot be sure that the message has been successfully received; only that it was transmitted.

The receiving LL reassembles a message by taking information received by the BB in each BPD, then reconstructing the message. For each received fragment, the message it is from is identified by the sequence number. The BPD containing the first fragment of a message indicates the total length of the message. The first message fragment shall be placed at offset 0. Each continuation message fragment is positioned at the offset specified in the received BPD. Once the complete message has been received it is passed to the relevant Logical Channel.

4.5 ACKNOWLEDGMENT AND SEQUENCE NUMBERS

The acknowledgment scheme enables error free transfer of data between a base station and End Device. It is not designed to provide any cryptographic security, or to provide confirmation that the data has been accepted by higher layers.

Each message is assigned a sequence number (SN) by the LL which is used to identify a message within the retransmission scheme, and to perform encryption/decryption.

The SN of the first message transmitted after an UAD, UAC or IAD Logical Channel has been created shall be set to 0. The SN of the first message transmitted after an MAD Logical Channel has been created shall be provided by higher layers.

The message along with its sequence number is transmitted to the receiver. The message is fragmented and reassembled as described in §4.4.

The receiver maintains and transfers to the sender the sequence number of the next message it is expecting from the transmitter; this is called the next expected sequence number (NESN). The NESN shall be set to the lowest sequence number that has not successfully been received.

When a UAD, UAC or IAD Logical Channel is created, NESN shall be set to 0. When an MAD Logical Channel is created, NESN shall be set to the SN of the first message provided by higher layers.

The size of SN and NESN are 7 bits.

The transmitter is allowed to send sequence numbers up to 63 messages beyond the last successfully received NESN, providing a window of 63 messages which have been transmitted but not successfully acknowledged.

Therefore, a message that is received that has an SN that is not in the range of NESN to NESN + 63, modulo 128, shall be considered to be a retransmission of a previously acknowledged message.

If the received message is not a retransmission of an acknowledged message then it shall be considered a new message that requires acknowledgement.

Depending upon the Transport Channel, when the receiver has successfully received a message it may increment NESN or transmit an acknowledgement to inform the transmitter that the message has been successfully received. If there is a failure during the reception of a message or a message is missing then the receiver can request that all, or a fragment, of the message is retransmitted.

If the sender does not receive a retransmission request, or NESN is not incremented to indicate that a message has successfully been received, it may optionally speculatively retransmit the message.

A message may be fragmented into two or more BPD structures. Each fragment does not have to be the same length and retransmissions may be different in size to previous transmissions.

The receiver reassembles a message identified by its sequence number. If the message has been successfully received then the message can be acknowledged. If fragments of the message have not been successfully received then the receiver may request retransmission of the missing fragments.

If a retransmission request refers to an already acknowledged sequence, the request shall be ignored. When a retransmission request is received, the sender may choose to retransmit the complete message, or only retransmit the fragment of the message indicated by the retransmission request.

The Transport Channels used to send retransmission requests or acknowledgements are unreliable, therefore requests and acknowledgements may not be successfully received. The receiver may retransmit any retransmission requests or acknowledgements.

4.6 ENCRYPTION AND DECRYPTION

Encryption and decryption are performed as described in the Security section.

5 RADIO RESOURCE MANAGER

5.1 OVERVIEW

The Radio Resource Manager (RRM) manages the radio resources that are used by Weightless-P devices.

The RRM performs the following functions:

- Information transfer for Higher Layers, in particular for Security procedures.
- Provide services to access information that is signaled through Control messages.
- Cell Selection and Reselection. The RRM will search for, select and maintain service from a Base Station.
- Establishment and maintenance of a connection with the Base Station, and registration of the ED with the Base Station.

5.2 RRM PROCEDURES

5.2.1 Network Connection

Connection to the network follows the below process:

1. ***Selection*** of Base Station and Base Station network
2. ***Registration*** to the Base Station network
3. ***Association*** to service provider (if required)
4. ***Establish*** link

5.2.2 Base Station Selection/Reselection Procedures

5.2.2.1 Overview

Weightless-P End Devices may be mobile and Weightless-P networks need to accommodate this mobility.

Also, even in static cases, Base Stations may become unavailable for service or coverage reasons. Weightless Networks need to be able to adapt.

End Devices are expected to manage their own mobility by connecting to new Base Stations as they move, or as coverage changes. Sometimes this will also require them to change networks.

Therefore, the End Device shall perform a Base Station Selection or Reselection procedure whenever:

1. An End Device is powered up.
2. Radio coverage is lost.
3. An End Device is requested by the network to find a new Base Station.
4. The network that the End Device is currently using is no longer preferred.

If the End Device has no current Network, it shall periodically perform a Base Station selection or reselection procedure, to attempt to recover service.

5.2.2.2 Base Station Selection/Reselection Procedure

An End Device should assess the detected Base Stations as candidate cells for selection/reselection.

A Base Station shall be assessed using the following information:

1. Whether the Base Station is available or not.
2. Received Signal Strength and Quality of the Base Station SIB0.

Provided the current Network remains suitable, an End Device should select the best available Base Station on the current Network.

If the End Device can no longer find available Base Stations, and the situation has persisted for 60 seconds it should look for cells on new networks.

5.2.2.3 Forced Base Station Reselection Procedure

When the End Device has found a Base Station it shall attempt to register to it by performing a Base Station Registration Procedure.

When an End Device is forced to look for a new Base Station, or if it chooses to select a new Base Station and return is allowed, the original Base Station shall be immediately treated as available if it has been determined that there are no other available Base Stations.

If return is not allowed, the original Base Station will be ignored for the purposes of reselection until an implementation-specific timer has elapsed. It is recommended for this timer to extend its duration for each consecutive connection rejection with cause “Network Declined” on that BSN.

5.2.3 Base Station Registration Procedures

5.2.3.1 Overview

Once the End Device has selected a Base Station it shall register with it.

If the End Device has an iEID, then it may use the Registration by iEID Procedure, see §5.2.3.2, else if there is sufficient space in an uplink CA transmission allocation for a uuEID it shall use the Registration by uuEID Procedure, see §5.2.3.3, else it shall use the Registration by Network Access Indicator (NAI) Procedure, see §5.2.3.4.

5.2.3.2 Registration by iEID Procedure

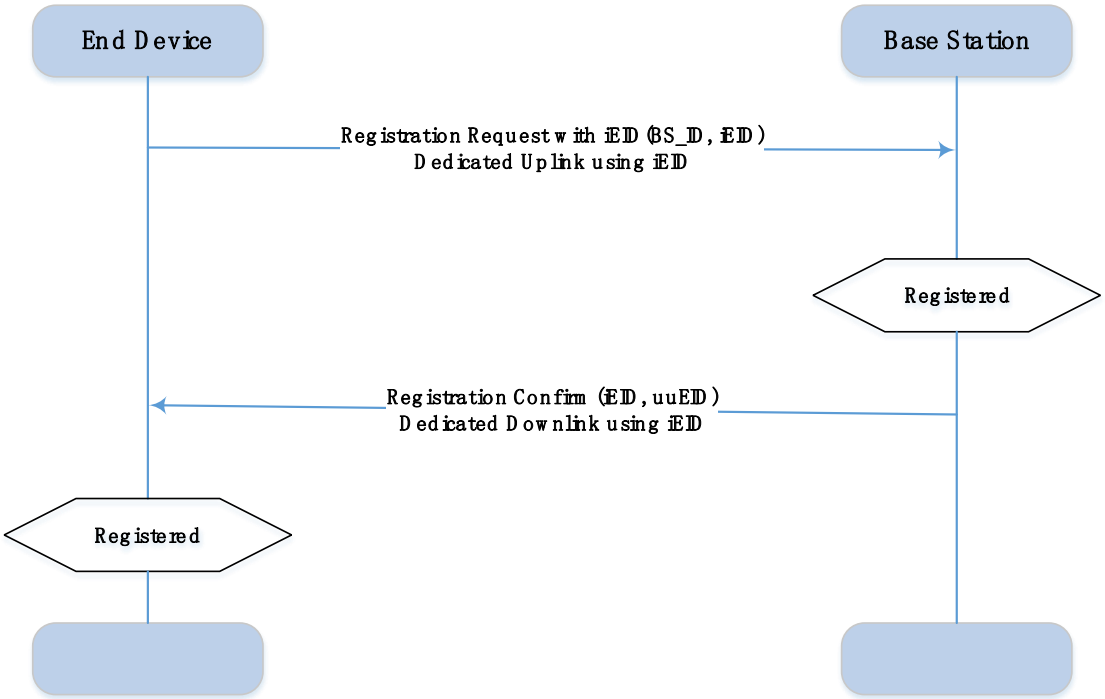

Figure 5.1: Registration by iEID Procedure (Successful Case)

This procedure starts when the End Device sends a Registration Request with iEID message through the RUC channel. This request shall contain its current iEID and the BS_ID of the Base Station that assigned this iEID.

When the Base Station receives a Registration Request with iEID message, if the target Base Station can identify the End Device using the supplied information and will accept the End Device, it shall reply with a Registration Confirm message, otherwise it shall reply with a Registration Reject with iEID message. On the Base Station, this completes this procedure.

When the End Device receives the Registration Confirm message with its uuEID, it shall consider the iEID from this message as valid and use it for subsequent communications, and this completes the procedure successfully.

If the End Device receives the Registration Reject with iEID message with its iEID, the registration has been rejected and the iEID is no longer considered valid, and this completes the procedure as unsuccessful.

If the End Device does not receive a valid response to the Registration Request with iEID message within RT5, then this completes the procedure as unsuccessful.

5.2.3.3 Registration by uuEID Procedure

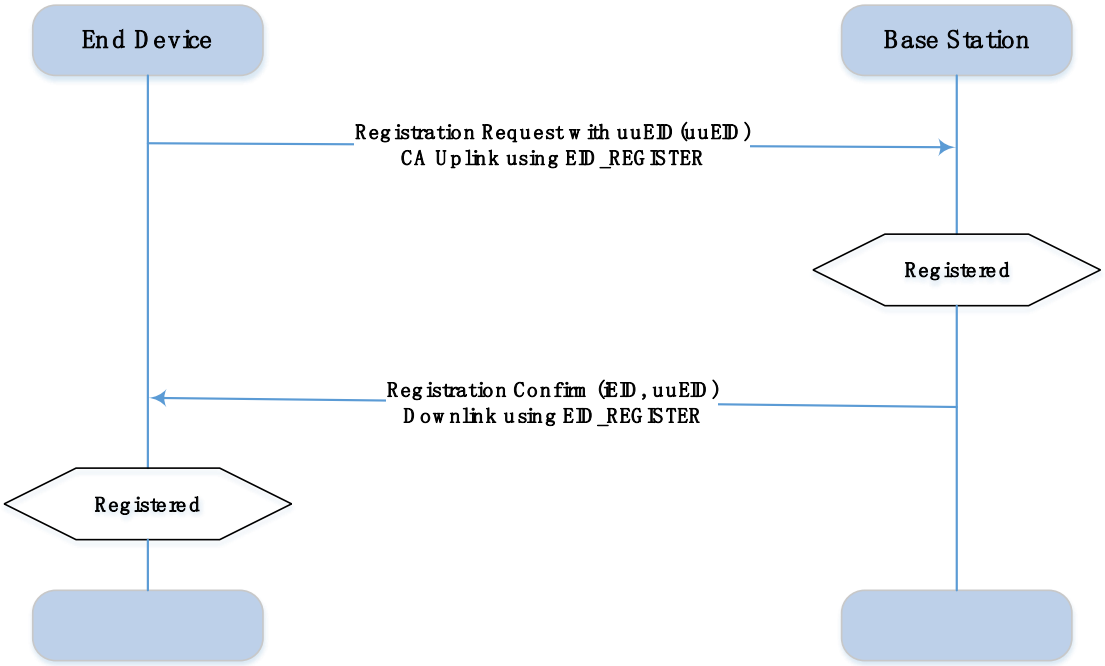

Figure 5.2: Registration by uuEID Procedure (Successful Case)

This procedure starts when the End Device sends a Registration Request with uuEID message through the RUC channel. This request shall contain its uuEID.

When the Base Station receives a Registration Request with uuEID message, if it will accept the End Device, it shall reply with a Registration Confirm message, otherwise it shall reply with a Registration Reject with uuEID message. On the Base Station, this completes this procedure.

When the End Device receives the Registration Confirm message with its uuEID, it shall consider the iEID from this message as valid and use it for subsequent communications, and this completes the procedure successfully.

If the End Device receives the Registration Reject with uuEID message with its uuEID, the registration has been rejected and this completes the procedure unsuccessfully.

If the End Device does not receive a valid response to the Registration Request with uuEID message within RT5, then this completes the procedure unsuccessfully.

5.2.3.4 Registration by NAI Procedure

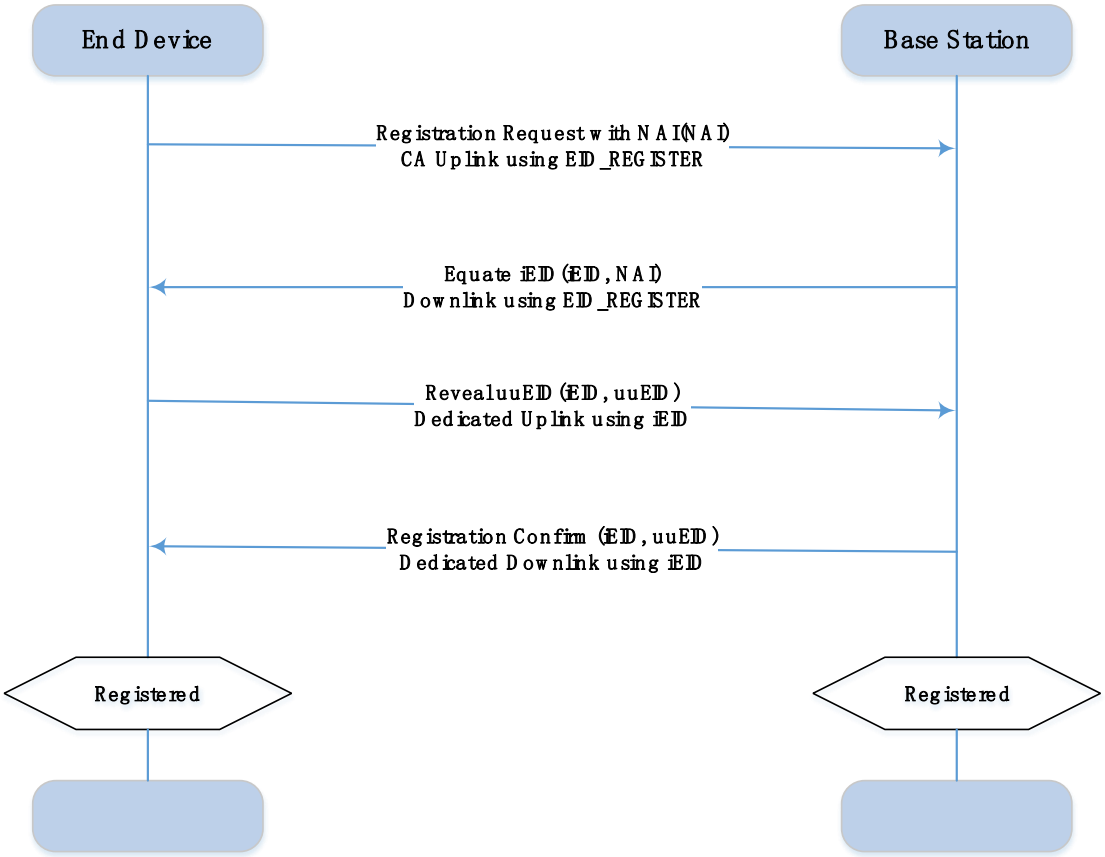

Figure 5.3: Registration by NAI Procedure (Successful Case)

This procedure starts when the End Device sends a Registration Request with NAI message through the RUC channel. This request shall contain a random NAI.

When the Base Station receives a Registration Request with NAI message, if it will accept the End Device, it shall reply with a Equate iEID message, otherwise it shall reply with a Registration Reject with NAI message.

When the End Device receives the Equate iEID message with the correct NAI, it shall respond with a Reveal uuEID message in dedicated uplink with the iEID from the CA Equate iEID message and its uuEID.

If the End Device receives the Registration Reject with NAI message with the correct NAI, the registration has been rejected and this completes the procedure unsuccessfully.

When the Base Station receives a Reveal uuEID message, if it will still accept the End Device, it shall reply with a Registration Confirm message, otherwise it shall reply with a Registration Reject with uuEID message with the uuEID from the Reveal uuEID message. On the Base Station, this completes this procedure.

When the End Device receives the Registration Confirm message with its uuEID, it shall consider the iEID from this message as valid and use it for subsequent communications, and this completes the procedure successfully.

When the End Device receives the Registration Confirm message with the iEID sent in the Reveal uuEID message but not its uuEID, then this completes the procedure unsuccessfully.

If the End Device does not receive a valid response to the Registration Request with NAI or Reveal uuEID messages within RT5, then this completes the procedure unsuccessfully.

5.2.4 Security Procedures

5.2.4.1 Overview

On registration the base station network will look up the End Device. The Service Provider may initiate association, see §5.2.4.2, or the End Device may initiate association if it is unable to perform link establishment, see §5.2.4.3. If the End Device does not have a Service Provider, or the base station network cannot provide service to the End Device the base station rejects registration.

5.2.4.2 Network-initiated Security Association Procedure

The Service Provider may initiate an Association procedure if, on entry to the Security Procedure, the Service Provider is creating a relationship with the End Device for the first time or the Service Provider requires the keys to be refreshed. On entry to the Association Procedure:

- The Network provides an Association Network Nonce to the End Device, in a WSS Network Nonce message, along with supported Cipher Suites and the SP_ID.
- The End Device generates its nonce and derives its keys from K_{master} as described in §6.4.3.1.
- The End Device responds by returning its own nonce in a WSS End Device Nonce message and a signature over all the transmitted parameters.
- The Network derives its keys from K_{master} as described in §6.4.3.1 and verifies the signature from the End Device.
- The End Device and WSS authenticate each other and confirm the keys by exchanging signatures.
- The derived keys, Network Nonce and End Device Nonce are passed to the Service Provider and used for encryption and decryption of subsequent messages of user data.

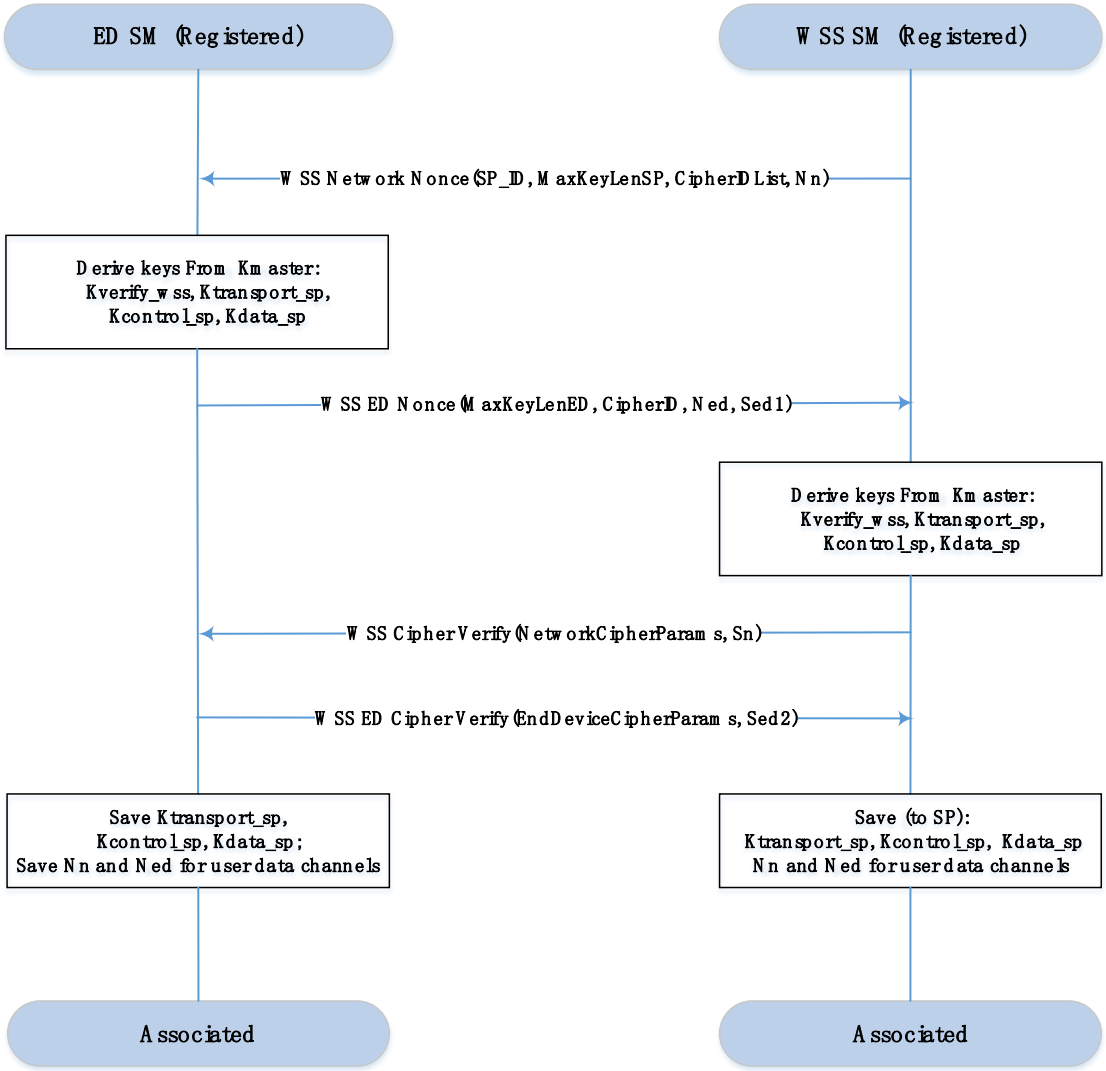

Figure 5.4: Network-initiated Security Association Procedure (Successful Case)

5.2.4.3 End Device-initiated Security Association Procedure

On entry to the security procedure the Service Provider will respond with a Service Provider Network Nonce.

If the End Device has determined that its keys are no longer valid, or are shortly becoming invalid then the End Device shall return an Association Required response.

The Association Required response causes the WSS to perform association, see §5.2.4.2.

5.2.4.4 Link Establishment Procedure

The link establishment procedure is:

- The End Device and Service Provider exchange Nonce
- Both the End Device and Service Provider derive the keys K_{verify_sp} and $K_{control\_bs}$ using the Nonces, see §6.4.3.2.

- If the key verification procedure is successful, $K_{control\_bs}$, SP Nonce and ED Nonce will be passed to the LL and used for encryption and decryption of subsequent control messages. Security is considered to be established.
- Otherwise, security is considered to have failed.

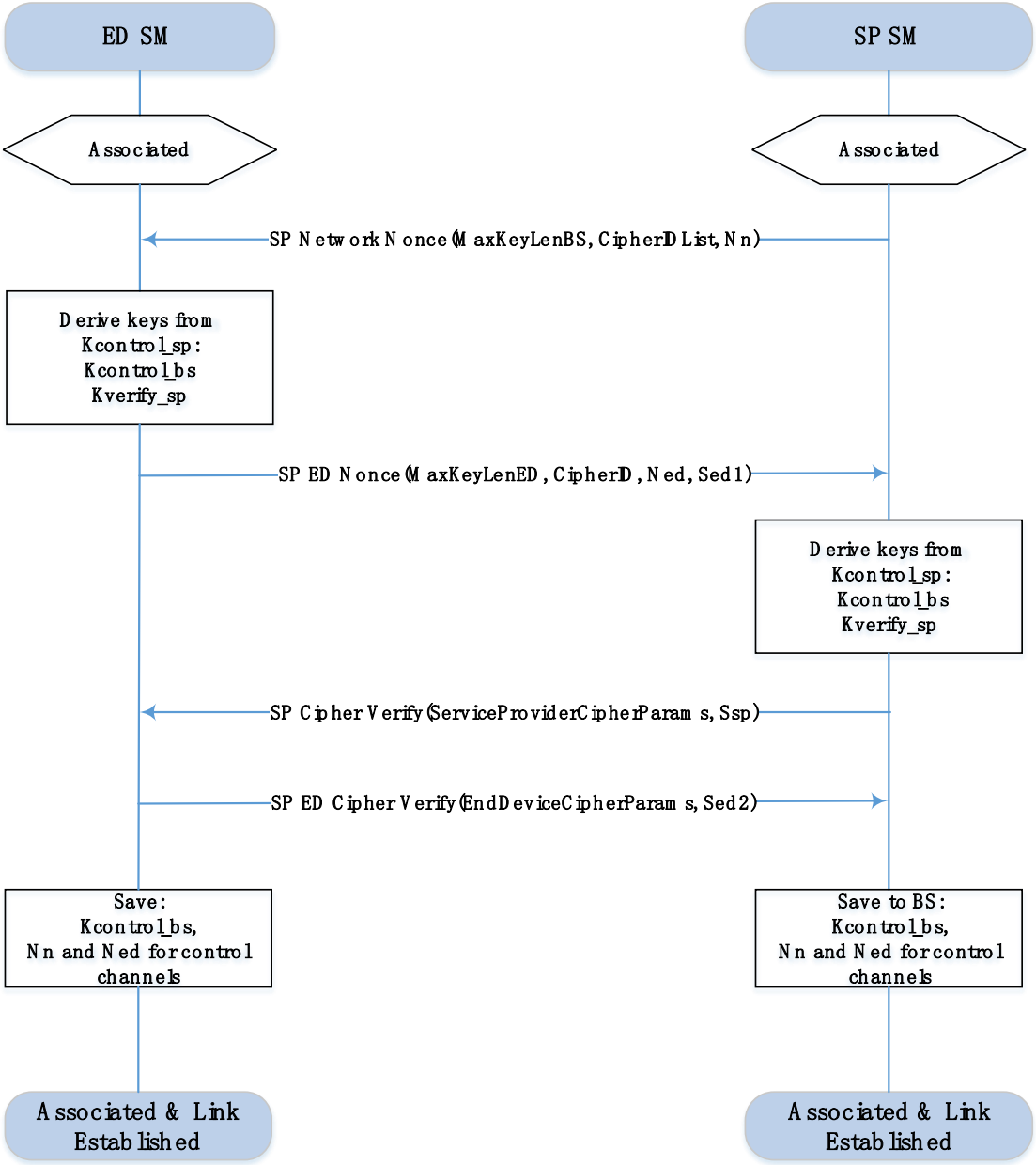

Figure 5.5: Link Establishment Procedure

5.2.5 End Device Deregistration Procedure

An End Device may choose to deregister from a Base Station without going to a different one. In this case, the End Device shall send an ED Deregister Request message to the Base Station.

When the Base Station receives an ED Deregister Request message, it shall delete the registration context after acknowledging the message. On the Base Station, this completes the procedure.

The End Device shall wait for the ED Deregister Request message to be acknowledged (for a maximum timeout period RT6), and following acknowledgement or timeout it will delete the registration context. On the End Device, this completes the procedure.

5.2.6 Base Station Deregistration Procedure

A Base Station may choose to deregister an End Device from a Base Station. In this case the Base Station will send a BS Deregister Request message to the End Device.

When the End Device receives the BS Deregister Request message, it will delete the Registration context after acknowledging the message. On the End Device, this completes the procedure.

The Base Station will wait for the Base Station Deregister Request message to be acknowledged, and following acknowledgement or expiry of an implementation-specific timeout it will delete the Registration context. On the Base Station, this completes the procedure.

5.2.7 iEID Reassignment Procedure

Once a secure link has been established, the Base Station may choose to update the End Device with a new iEID. This is sent in an iEID Reassignment Request message.

All following new messages from the Base Station that use an iEID for addressing will use the new iEID. No further messages for the End Device should be included in the remainder of the frame.

The End Device shall return an iEID Reassignment Confirm message using the old iEID, and thereafter switch to the new iEID. No further new messages from the End Device shall be included in the remainder of the frame.

Acknowledgements and retransmissions from both the End Device and Base Station will use the iEIDs that were associated with the message that they are acknowledging or repeating, hence transmission and reception opportunities for both iEIDs will be made available by the Base Station until all outstanding messages for the former iEID have been acknowledged, and retransmissions of messages with the old iEID are no longer possible.

5.2.8 Scheduled Transfer Procedure

The Base Station controls the scheduled downlink and uplink transfers in an End Device using a Scheduled Transfer message. The message can inform the End Device to:

- Add a repetitive or single Scheduled Downlink or Uplink Unicast Transfer
- Cancel a repetitive or single Scheduled Downlink or Uplink Unicast Transfer
- Add a repetitive or single Scheduled Downlink Transfer for a Multicast instance
- Cancel a repetitive or single Scheduled Downlink Transfer for a Multicast instance

Scheduled Transfers allow the End Device to only monitor the DL_RA and/or UL_RA at given points in the frame numbering sequence.

5.2.9 Join Multicast Group Procedure

For any configured instance, the End Device may receive a Join Multicast Group message. It will configure the LL for the contained instance, with a gEID and starting SN.

Following this, the multicast channel identified by the instance should be receivable from the group addressed channel, identified by the given gEID. The Base Station will configure at most one gEID per instance at a time. The End Device shall ignore Join Multicast Group requests for instances that are already in the joined state when the message is received.

Note: gEID assignments for multicast channels are only valid whilst the End Device remains registered to the same Base Station.

5.2.10 Leave Multicast Group Procedure

When the End Device receives a Leave Multicast Group message, it shall release the LL multicast channel resources associated with the instance; this will occur at the sequence number specified in the message.

5.2.11 Join Interrupt Group Procedure

For any configured instance, the End Device may receive a Join Interrupt Group message. It shall configure the LL for the contained instance with a gEID.

Following this, this instance of interrupt channel should be able to transmit using the group addressed channel, identified by the given gEID. The Base Station will configure at most one gEID per instance at a time. The End Device shall ignore Join Interrupt Group requests for instances that are already in the joined state when the message is received.

Note, gEID assignments for interrupt channels are only valid whilst the End Device remains registered to the same Base Station.

5.2.12 Leave Interrupt Group Procedure

When the End Device receives a Leave Interrupt Group message, it shall release the LL interrupt channel resources associated with the instance; this will occur immediately.

5.2.13 Power Control Procedure

A Power Control Procedure is used by the Base Station to instruct an End Device to limit its maximum transmit power.

When the End Device receives a Power Control Request message, it configures the physical layer with the power control data.

5.2.14 Measurement Procedure

When the End Device receives a Measurement Request message it should initiate the specified measurement(s) and report the measurement results in a Measurement Response message.

5.3 RRM MESSAGES

5.3.1 RRM Messages

TABLE 5-1 RRM SIGNALING MESSAGES

Message Name	Direction	Opcode	Logical Channel	Definition
Registration Request (with NAI)	Uplink	0x01	RUC	§5.3.2
Registration Request (with iEID)	Uplink	0x02	RUC	§5.3.3
Registration Request (with uuEID)	Uplink	0x03	RUC	§5.3.4
Equate iEID	Downlink	0x04	RUC	§5.3.5
Reveal uuEID	Uplink	0x05	RUC	§5.3.6
Registration Confirm	Downlink	0x06	RUC	§5.3.7
Registration Reject (with NAI)	Downlink	0x07	RUC	§5.3.8
Registration Reject (with iEID)	Downlink	0x08	RUC	§5.3.9
Registration Reject (with uuEID)	Downlink	0x09	RUC	§5.3.10
ED Deregister Request	Uplink	0x0A	UAC	§5.3.11
BS Deregister Request	Downlink	0x0B	UAC	§5.3.12
iEID Reassignment Request	Downlink	0x0C	UAC	§5.3.13
iEID Reassignment Response	Uplink	0x0D	UAC	§5.3.14
Scheduled Transfer Assignment	Downlink	0x0E	UAC	§5.3.15
Join Multicast Group	Downlink	0x0F	UAC	§5.3.16
Leave Multicast Group	Downlink	0x10	UAC	§5.3.17

Join Interrupt Group	Downlink	0x11	UAC	§5.3.18
Leave Interrupt Group	Downlink	0x12	UAC	§5.3.19
Power Control Request	Downlink	0x13	UAC	§5.3.20
Measurement Request	Downlink	0x14	UAC	§5.3.21
Measurement Response	Uplink	0x15	UAC	§5.3.22
WSS Network Nonce	Downlink	0x16	UAC (no security)	§5.3.23
WSS ED Nonce	Uplink	0x17	UAC (no security)	§5.3.24
WSS Cipher Verify	Downlink	0x18	UAC (no security)	§5.3.25
WSS ED Cipher Verify	Uplink	0x19	UAC (no security)	§5.3.26
SP Network Nonce	Downlink	0x1A	UAC (no security)	§5.3.27
SP ED Nonce	Uplink	0x1B	UAC (no security)	§5.3.28
SP Cipher Verify	Downlink	0x1C	UAC (no security)	§5.3.29
SP ED Cipher Verify	Uplink	0x1D	UAC (no security)	§5.3.30
Association Request	Uplink	0x1E	UAC (no security)	§5.3.31

5.3.2 Registration (with NAI)

TABLE 5-2 CA REGISTRATION (WITH NAI) MESSAGE FORMAT

Offset (bytes)	Length (bytes)	Name	Description
0	1	Opcode	Message opcode, see Table 5-1
1	1	NAI	Network Access Indicator random number

5.3.3 Registration Request (with iEID)

TABLE 5-3 CA REGISTRATION REQUEST (WITH IEID) MESSAGE FORMAT

Offset (bytes)	Length (bytes)	Name	Description
0	1	Opcode	Message opcode, see Table 5-1

1	2	BS_ID	Previously registered BS_ID
3	3	iEID	Current iEID on previous BS_ID

5.3.4 Registration Request (with uuEID)

TABLE 5-4 CA REGISTRATION REQUEST (WITH UUEID) MESSAGE FORMAT

Offset (bytes)	Length (bytes)	Name	Description
0	1	Opcode	Message opcode, see Table 5-1
1	16	uuEID	uuEID of End Device

5.3.5 Equate iEID

TABLE 5-5 CA EQUATE IEID MESSAGE FORMAT

Offset (bytes)	Length (bytes)	Name	Description
0	1	Opcode	Message opcode, see Table 5-1
1	3	iEID	Current iEID
4	1	NAI	Network Access Indicator

5.3.6 Reveal uuEID

TABLE 5-6 CA REVEAL UUEID MESSAGE FORMAT

Offset (bytes)	Length (bytes)	Name	Description
0	1	Opcode	Message opcode, see Table 5-1
1	3	iEID	iEID from the CA Equate iEID
4	16	uuEID	uuEID of the End Device

5.3.7 Registration Confirm

TABLE 5-7 CA REGISTRATION CONFIRM MESSAGE FORMAT

Offset (bytes)	Length (bytes)	Name	Description
0	1	Opcode	Message opcode, see Table 5-1
1	3	iEID	Current iEID
4	16	uuEID	uuEID of the End Device

5.3.8 Registration Reject (with NAI)

TABLE 5-8 CA REGISTRATION REJECT (WITH NAI) MESSAGE FORMAT

Offset (bytes)	Length (bytes)	Name	Description
0	1	Opcode	Message opcode, see Table 5-1
1	1	Cause	Reason for rejection
2	1	NAI	Network Access Indicator

5.3.9 Registration Reject (with iEID)

TABLE 5-9 CA REGISTRATION REJECT (WITH IEID) MESSAGE FORMAT

Offset (bytes)	Length (bytes)	Name	Description
0	1	Opcode	Message opcode, see Table 5-1
1	1	Cause	Reason for rejection
2	2	BS_ID	Previous BS_ID
4	3	iEID	Current iEID

5.3.10 Registration Reject (with uuEID)

TABLE 5-10 CA REGISTRATION REJECT (WITH UUEID) MESSAGE FORMAT

Offset (bytes)	Length (bytes)	Name	Description
0	1	Opcode	Message opcode, see Table 5-1
1	1	Cause	Reason for rejection
2	16	uuEID	uuEID of End Device

5.3.11 ED Deregister Request

TABLE 5-11 ED DEREGISTER REQUEST MESSAGE FORMAT

Offset (bytes)	Length (bytes)	Name	Description
0	1	Opcode	Message opcode, see Table 5-1
1	1	Reason	Deregister reason

5.3.12 BS Deregister Request

TABLE 5-12 BS DEREGISTER REQUEST MESSAGE FORMAT

Offset (bytes)	Length (bytes)	Name	Description
0	1	Opcode	Message opcode, see Table 5-1
1	1	Reason	Deregister reason

5.3.13 iEID Reassignment Request

TABLE 5-13 IEID REASSIGNMENT REQUEST MESSAGE FORMAT

Offset (bytes)	Length (bytes)	Name	Description
0	1	Opcode	Message opcode, see Table 5-1
1	3	iEID	New iEID

5.3.14 iEID Reassignment Response

TABLE 5-14 IEID REASSIGNMENT RESPONSE MESSAGE FORMAT

Offset (bytes)	Length (bytes)	Name	Description
0	1	Opcode	Message opcode, see Table 5-1

5.3.15 Scheduled Transfer Assignment

TABLE 5-15 SCHEDULED TRANSFER ASSIGNMENT MESSAGE FORMAT

Offset (bytes)	Length (bytes)	Name	Description
0	1	Opcode	Message opcode, see Table 5-1
1	1	STFlags	Scheduled Transfer flags, see Table below
2	2	StartSFN	Frame Number of the first Scheduled Transfer
4	2	Interval	Interval between Scheduled Transfers
6	2	Window	Number of frames per Scheduled Transfer

5.3.16 Join Multicast Group

TABLE 5-16 JOIN MULTICAST GROUP MESSAGE FORMAT

Offset (bytes)	Length (bytes)	Name	Description
0	1	Opcode	Message opcode, see Table 5-1
1	1	mInstance	Multicast Group instance
2	2	gEID	gEID to assign to this Multicast Group instance
4	1	StartSN	First Sequence Number to receive from this gEID

5.3.17 Leave Multicast Group

TABLE 5-17 LEAVE MULTICAST GROUP MESSAGE FORMAT

Offset (bytes)	Length (bytes)	Name	Description
0	1	Opcode	Message opcode, see Table 5-1
1	1	mInstance	Multicast Group instancee
2	2	gEID	gEID to discard
4	1	LastSN	Last Sequence Number to receive from this gEID

5.3.18 Join Interrupt Group

TABLE 5-18 JOIN INTERRUPT GROUP MESSAGE FORMAT

Offset (bytes)	Length (bytes)	Name	Description
0	1	Opcode	Message opcode, see Table 5-1
1	1	iInstance	Interrupt Group instance
2	2	gEID	gEID to assign to this Interrupt Group instance

5.3.19 Leave Interrupt Group

TABLE 5-19 LEAVE INTERRUPT GROUP MESSAGE FORMAT

Offset (bytes)	Length (bytes)	Name	Description
0	1	Opcode	Message opcode, see Table 5-1
1	1	iInstance	Interrupt Group instance
2	2	gEID	gEID to discard

5.3.20 Power Control Request

TABLE 5-20 POWER CONTROL REQUEST MESSAGE FORMAT

Offset (bytes)	Length (bytes)	Name	Description
0	1	Opcode	Message opcode, see Table 5-1
1	1	MaxTxPower	Maximum transmit power as 8-bit signed integer in dBm

5.3.21 Measurement Request

TABLE 5-21 MEASUREMENT REQUEST MESSAGE FORMAT

Offset (bytes)	Length (bytes)	Name	Description
0	1	Opcode	Message opcode, see Table 5-1
1	1	MeasFlags	**0**: SIB0 RSSI **1…255**: RFU

5.3.22 Measurement Response

TABLE 5-22 MEASUREMENT RESPONSE MESSAGE FORMAT

Offset (bytes)	Length (bytes)	Name	Description
0	1	Opcode	Message opcode, see Table 5-1
1	1	MeasFlags	**0**: SIB0 RSSI **1…255**: RFU
2	Variable	MeasResults	System Information Block RSSI in dB relative to -174dBm (unsigned 8 bits)

5.3.23 WSS Network Nonce

TABLE 5-23 WSS NETWORK NONCE MESSAGE FORMAT

Offset (bytes)	Length (bytes)	Name	Description
0	1	Opcode	Message opcode, see Table 5-1
1	2	SP_ID	Service Provider ID
3	1	keySizeN	Maximum key length supported by SP (in bytes) Should be at least 16
4	1	CipherListLen	Number of Cipher in CipherList
5	CipherListLen	CipherList	List of 1-byte Cipher identifiers
5 + CipherListLen	Variable	Nn	Network Nonce (a fresh random number)

5.3.24 WSS ED Nonce

TABLE 5-24 WSS ED NONCE MESSAGE FORMAT

Offset (bytes)	Length (bytes)	Name	Description
0	1	Opcode	Message opcode, see Table 5-1
1	1	keySizeE	Maximum key length supported by ED (in bytes) Should be at least 16
2	1	CipherID	Selected Cipher identifier
3	Variable	Ned	End Device Nonce (a fresh random number)
3 + Ned length	Variable	Sed1	Signature

5.3.25 WSS Cipher Verify

TABLE 5-25 WSS CIPHER VERIFY MESSAGE FORMAT

Offset (bytes)	Length (bytes)	Name	Description
0	1	Opcode	Message opcode, see Table 5-1
1	Variable	NCP	Network Cipher Parameters
1 + NCP length	Variable	Sn	Signature

5.3.26 WSS ED Cipher Verify

TABLE 5-26 WSS ED CIPHER VERIFY MESSAGE FORMAT

Offset (bytes)	Length (bytes)	Name	Description
0	1	Opcode	Message opcode, see Table 5-1
1	Variable	EDCP	End Device Cipher Parameters
1 + EDCP length	Variable	Sed2	Signature

5.3.27 SP Network Nonce

TABLE 5-27 SP NETWORK NONCE MESSAGE FORMAT

Offset (bytes)	Length (bytes)	Name	Description
0	1	Opcode	Message opcode, see Table 5-1
1	1	keySizeN	Maximum key length supported by BS (in bytes) Should be at least 16
2	1	CipherListLen	Number of Cipher in CipherList
3	CipherListLen	CipherList	List of 1-byte Cipher identifiers
3 + CipherListLen	Variable	Nn	SP Nonce (a fresh random number)

5.3.28 SP ED Nonce

TABLE 5-28 SP ED NONCE MESSAGE FORMAT

Offset (bytes)	Length (bytes)	Name	Description
0	1	Opcode	Message opcode, see Table 5-1
1	1	keySizeE	Maximum key length supported by ED (in bytes) Should be at least 16
2	1	CipherID	Selected Cipher identifier
3	Variable	Ned	End Device Nonce (a fresh random number)
3 + Ned length	Variable	Sed1	Signature

5.3.29 SP Cipher Verify

TABLE 5-29 SP CIPHER VERIFY MESSAGE FORMAT

Offset (bytes)	Length (bytes)	Name	Description
0	1	Opcode	Message opcode, see Table 5-1
1	Variable	SPCP	Service Provider Cipher Parameters

1 + SPCP length	Variable	Ssp	Signature

5.3.30 SP ED Cipher Verify

TABLE 5-30 SP ED CIPHER VERIFY MESSAGE FORMAT

Offset (bytes)	Length (bytes)	Name	Description
0	1	Opcode	Message opcode, see Table 5-1
1	Variable	EDCP	End Device Cipher Parameters
1 + EDCP length	Variable	Sed2	Signature

5.3.31 Association Request

TABLE 5-31 ASSOCIATION REQUEST MESSAGE FORMAT

Offset (bytes)	Length (bytes)	Name	Description
0	1	Opcode	Message opcode, see Table 5-1

6 AUTHENTICATION AND SECURITY MANAGEMENT

6.1 INTRODUCTION

The Weightless-P standard is intended to accommodate a wide variety of End Devices, business models and traffic types. It is able to provide "provision once, deploy anywhere" capabilities for low-cost, occasionally mobile devices with highly constrained energy, bandwidth and compute resources.

Weightless security aims to provide adequate protection within these constraints for a majority of use cases, including those involving billing data or confidential information. In particular, it aims to guarantee the authenticity, integrity and confidentiality of user and control data.

6.2 OPERATIONAL OVERVIEW

6.2.1 Network Functions

Weightless End Devices can be provisioned once for deployment anywhere in the world. To facilitate this, the Weightless SIG provides two central services: the Service Provider Database (SPDB), and the Weightless Security Server (WSS).

The SPDB provides a mechanism by which BSNs can determine to which Service Provider (SP) any given End Device belongs. This allows BSNs to provide service according to such agreements as they have in place with that SP. An End Device may be registered with one SP at a time, or none, in which case an appropriate SP must be assigned before service can be provided.

The WSS holds master keys, generating blocks of uuEID/K_{master} pairs and issuing them to operators, who provision them on to new EDs out of band before first connection. On first connection, End Devices authenticate with the WSS and then derive with it keys for use by the SP, which itself then derives keys with the End Device for use by the BSN/BS. The WSS also mediates the transfer of EDs from one SP to another. Master keys can also be held by the SP if required.

Private Weightless-P networks may combine the roles of BSN, SP and operator, in which case the functionality of the SPDB and WSS needs to be replicated.

6.2.2 Security Features

Weightless-P provides certainty that a message has come from the End Device identity claimed (authenticity), that the message has not been tampered with on route (integrity), and that no eavesdropper can view the message contents (confidentiality). It also guarantees message freshness by rejecting replayed messages

EDs themselves are assumed to operate as a single security domain. Although multiple applications may run on a single ED, Weightless-P does not itself guarantee any kind of security between them.

Forward security – the property that a compromise cannot affect the confidentiality of previous messages – is not provided by Weightless-P. This is because Weightless-P depends on a permanent shared secret, from which working secrets are mutually derived. Forward security requires use of a key agreement function to establish session keys.

6.2.3 Use of alternative security suites

The four components of any given cipher suite are key exchange, authentication, encryption, and digest hash. In this version of the Weightless-P specification, the corresponding functions are PSK for key exchange, complemented by NIST Special Publication 800-108's *KDF in Counter Mode* function for key derivation, with IETF RFC 5433 Extensible Authentication Protocol - Generalized Pre-Shared Key (EAP-GPSK) Method for mutual authentication, AES-CCM for message encryption and authentication, AES-KW for the special case of encryption that is key wrapping, and CMAC for message digest hash. These functions' exclusive use of symmetric keys has some drawbacks but makes them very efficient in resource-constrained embedded devices.

EDs indicate their desired suite of security functions when joining an SP. To allow the ready substitution of security functions the Weightless-P specification keeps separate their operations. By supporting multiple security suites, SPs and BSNs can maintain compatibility with older End Devices.

6.3 ISSUES FOR IMPLEMENTORS

6.3.1 Key Security

Weightless security rests entirely on the cryptographic strength of its security functions and the difficulty faced by an attacker seeking to gain access to its secret keys.

Weightless-P requires End Devices conform to at least certain minimum standards of secure key storage on End Devices. It is intended that keys held in conformant End Devices not be trivially accessible to attackers of sophistication sufficient to be able to exploit them, while adding negligible costs in design and build. Using hardened UICC-style cryptographic coprocessors is nonetheless not excluded.

Specifically, the requirements are:

1. Once programmed, keys never travel unsecured across buses that can be accessed without modification of the End Device.
2. Keys cannot be accessed on deployed devices via debug or programming interfaces.
3. It should not be possible for an attacker to modify or replace the End Device's software.
4. Any printed circuit board track carrying Weightless-P commands or messages not protected by Weightless' own security must have its own (preferably cryptographic) protection.

6.4 SPECIFICATION

6.4.1 Identity & Keys

The End Device is known to the network by its unique 128-bit identifier uuEID. The End Device and the network securely hold a shared secret symmetric key K_{master}.

Table 6-1 defines the keys that are used within Weightless-P to secure communications between an End Device and a network. All keys are 128 bits long.

TABLE 6-1 KEYS

Key Name	Description	Known To
K_{master}	Pre-shared key used to derive other keys.	ED, WSS
K_{verify_wss}	Derived by WSS and End Device then used to authenticate one another and confirm the keys have been derived correctly.	ED, WSS
$K_{transport\_sp}$	Derived by WSS and passed to the SP. Used to encrypt keys being distributed by the SP.	ED, WSS, SP
$K_{control\_sp}$	Derived by WSS and passed to the SP. Used to derive additional keys so that Base Stations can encrypt and protect RRM traffic.	ED, WSS, SP
K_{data_sp}	Derived by WSS and passed to the SP. Used to encrypt and authenticate unicast traffic between SP and ED.	ED, WSS, SP
$K_{interrupt\_sp}$	Distributed by the SP to an ED. Used to encrypt and authenticate interrupt data between the ED and SP.	ED, SP
$K_{multicast\_sp}$	Distributed by the SP to an ED. Used to encrypt and authenticate multicast data between a set of EDs and SP.	ED, SP
K_{verify_sp}	Derived by the SP and ED then used to authenticate one another and confirm the keys have been derived correctly.	ED, SP

The key hierarchy has been designed so that K_{master} does not need to be transferred from the WSS. Once $K_{transport\_sp}$, $K_{control\_sp}$ and K_{data_sp} have been created and transferred to the SP they do not need to be transferred again even when the End Device reconnects using different BSs and BSNs. Once they have been provided to the SP the WSS no longer requires them and should securely delete them.

$K_{control\_bs}$ is distributed to the BS via the BSN from the SP to allow it to manage the connection. Once $K_{control\_bs}$ has been provided to the BSN the SP no longer requires it and should securely delete it. $K_{control\_sp}$ is used to derive keys that a BS uses to encrypt and authenticate RRM message between the End Device and BS. K_{data_sp} is used to encrypt and authenticate user data between the End Device and its SP.

K_{verify_wss}, $K_{transport\_sp}$, $K_{control\_sp}$ and K_{data_sp} are derived from K_{master} when an End Device associates with a SP. K_{verify_wss} is used by the End Device and WSS to authenticate one another and verify the success of key derivation procedures and is then discarded. The WSS then passes $K_{transport\_sp}$, $K_{control\_sp}$ and K_{data_sp} to the SP.

Key derivation in Weightless-P can occur at two different times during the connection procedure:

- When an End Device associates with a SP.
- When an End Device performs link establishment with a BS.

The procedure used is the same in either case, see §6.3, but uses different input and output parameters depending on whether association or link establishment is being performed. During SP association the following keys are derived from the pre-shared key K_{master}:

- K_{verify_wss}
- $K_{transport\_sp}$
- $K_{control\_sp}$
- K_{data_sp}

Association takes place relatively infrequently, whenever an End Device associates with a SP. The association process is the same whether it takes place with an End Device's existing SP or a new SP.

During link establishment the following keys are derived from $K_{control\_sp}$:

- $K_{control\_bs}$
- K_{verify_sp}

Link establishment is performed whenever an End Device connects to a BS and may be a frequent occurrence for mobile End Devices. The procedure is the same regardless of whether it takes place with the same BS after disconnecting, with a different BS within the same BSN, or with a BS on a different BSN.

6.4.2 Key Derivation Function (kd)

The key derivation function (kd) is used to derive additional keys from a key for separate cryptographic purposes.

The key derivation function (kd) takes the following inputs, provided by the caller:

- K_I: An input key that is only used for key derivation.
- Label: variable length string set by the caller.
- Nonce Network: a nonce value set by the network
- Nonce ED: a nonce value set by the End Device
- L: Output Length

It returns the following values:

- Derived key bit stream K_o

The function performs the following operation:

$$Context = (Nonce\ Network\ ||\ Nonce\ ED\ ||\ SP\_ID\ ||\ BSN\_ID\ ||\ BS\_ID\ ||\ uuEID)$$

$$K_o = kd(K_i, Label, Context, L)$$

The input parameters Nonce Network and Nonce ED are concatenated with the SP_ID, BSN_ID, BS_ID and the uuEID to generate the value Context.

The input parameters K_I, Label, L and the calculated Context are then passed to the KDF in Counter Mode function as defined in NIST Special Publication 800-108.

The parameters K_I, Label, Context and L, and the output K_o shall have the same meaning and use as defined in NIST Special Publication 800-108.

The result of the NIST Special Publication 800-108 KDF in Counter Mode function using CMAC as the PRF function is then returned as the key stream from this function.

The resulting key stream maybe used for multiple keys, however each key shall not use part of the output used in another key generated from this invocation of the key derivation function (kd).

6.4.3 Association and Link Establishment Procedure

During a connection process End Devices must agree a cipher suite, derive keys and mutually authenticate with both SP and BSN. A combined key derivation, mutual authentication and cipher suite negotiation procedure based on IETF RFC 5433 Extensible Authentication Protocol - Generalized Pre-Shared Key (EAP-GPSK) Method.

The procedure always begins with a message from the network containing

- The network identity, if not already known to the End Device
- A fresh random Nonce

On receipt of this message the End Device generates a fresh random Nonce and uses it with the network Nonce to derive keys. One of the derived keys is used to sign subsequent messages in the procedure, in which it provides validation of the derived keys and therefore mutual authentication.

Generation of the nonces can use any random function. For example, possible methods are described in NIST SP 800-22.

The End Device generates a signature over:

- Network and End Device identities
- Network and End Device Nonces

The End Device then sends to the network a message containing:

- End Device Nonce
- The calculated signature

When the network receives this message it performs a key derivation using the same parameters as the End Device and verifies the signature from the End Device. On successful verification it considers the End Device authenticated.

The network creates a signature over these cipher suite parameters and the parameters over which the initial End Device signature is generated, and sends the network cipher suite parameters and the signature to the End Device.

The End Device verifies the signature and on successful verification considers the network authenticated and commits the derived keys. The End Device then generates parameters needed for subsequent operation of the selected cipher suite, signs them and sends the End Device cipher suite parameters and the signature to the network.

The network verifies the signature and on successful verification considers the process complete and commits the derived keys.

6.4.3.1 Association Procedure

When an ED associates with a SP it must derive all other keys from K_{master}, which it has been commissioned with and is known to the Weightless Security Server.

The End Device and the Weightless Security Server generate K_{verify_wss}, $K_{transport\_sp}$, $K_{control\_sp}$ and K_{data_sp} from K_{master} using the following algorithm:

$$K_{bitstream} = kd(K_{master}, \text{"}verify\_wss,\ transport\_sp,\ control\_sp,\ data\_sp\text{"}, Context, 512)$$

$$\{ K_{verify\_wss} \,||\, K_{transport\_sp} \,||\, K_{control\_sp} \,||\, K_{data\_sp} \} = K_{bitstream}$$

A key stream of 512 bits, $K_{bitstream}$, is generated by calling the key derivation function *kd* with its input parameter K_I set to K_{master}. Label is set to the string "*verify_wss, transport_sp, control_sp, data_sp*". Context is set as described in Section 6.4.2.

6.4.3.2 Link Establishment Procedure

If an End Device changes BS within a BSN, or reconnects to the same BS after being disconnected, or connects via a different BSN then only $K_{control\_bs}$ and K_{verify_sp} needs to be generated from $K_{control\_sp}$.

The End Device and the Service Provider generate $K_{control\_bs}$ and K_{verify_sp} from $K_{control\_so}$ using the following algorithm:

$$\{ K_{verify\_sp} \,||\, K_{control\_bs} \} = kd(K_{control\_sp}, \text{"}verify\_bs,\ control\_bs\text{"}, Context, 256)$$

The 128 bit keys K_{verify_sp} and $K_{control\_bs}$, are generated by calling the key derivation function *kd*, with its input parameter K_I set to $K_{control\_sp}$. Label is set to the string "*verify_bs, control_bs*". Context is set as described in Section 6.4.2.

6.4.4 Key Transport

When a MAD, MUD, IAD or IUD logical channel is opened, a key is transported to the ED for the instance of the logical channel being opened.

Section 6.4.4.1 defines the key wrap function that use used to wrap the key material by the sender ready for transport to the recipient. Section 6.4.4.2 defines the key unwrap function that is used by the recipient to recover the transported key material.

Key wrapping in Weightless-P uses NIST “AES Key Wrap Specification”, 16th November 2001 published on NIST’s Computer Security Resource Center web site, using an AES codebook key size of 128 bits.

This specification is essentially equivalent to IETF RFC 3394 Advanced Encryption Standard (AES) Key Wrap Algorithm, using 128 bits as the AES codebook key size. It is also essentially equivalent to NIST Special Publication 800-38F Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping using the KW mode of operation using FIPS 197 Advanced Encryption Standard (AES) with a cipher key length of 128bits (AES-128).

6.4.4.1 Key Wrap Function (kw)

The key wrap function (kw) is used to wrap key material for transport to a recipient.

The key wrap function (kw) takes the following inputs, provided by the caller:

- KEK: An input key transport key that is only used for key wrapping.
- KT: 128bit key that is being transported

It returns the following values:

- Ciphertext containing the wrapped key, C.

The function performs the following operation:

C = kw(KEK, KT)

The KEK parameter and KT parameter are passed to the NIST defined or RFC3394 defined key wrap process. The output from the key wrap process is then returned to the caller.

6.4.4.2 Key Unwrap Function (ku)

The key unwrap function (ku) is used to unwrap key material transported to a recipient so they can received the transported key.

The key unwrap function (ku) takes the following inputs, provided by the caller:

- KEK: An input key transport key that is only used for key wrapping.
- C: Ciphertext to verify and extract transported key from

It returns the following values:

- Transported Key KT, or ERROR.

The function performs the following operation:

KT = ku(KEK, C)

The KEK parameter and C parameter are passed to the NIST defined or RFC3394 defined key unwrap process. The output from the key wrap process is then returned to the caller. The result of the unwrap process can be either the transported key, or ERROR.

6.4.5 Encryption and Integrity

Encryption and authentication of logical channel data is provided by CCM. CCM is defined in NIST Special Publication 800-38C Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality. It is also defined in RFC 3610: Counter with CBC-MAC (CCM).

The MAC provides the following logical channels than can be encrypted and authenticated:

- Unicast Acknowledged Data (UAD)
- Unicast Unacknowledged Data (UUD)
- Unicast Acknowledged Control (UAC)
- Multicast Acknowledged Data (MAD)
- Multicast Unacknowledged Data (MUD)
- Interrupt Acknowledged Data (IAD)
- Interrupt Unacknowledged Data (IUD)

Table 6-2 defines which key is used to encrypt and authenticate each logical channel.

TABLE 6-2 LOGICAL CHANNEL KEYS

Logical Channel	Key
UAD/UUD	K_{data_sp}
UAC	$K_{control\_bs}$
MAD/MUD	$K_{multicast\_sp}$ for the logical channel instance
IAD/IUD	$K_{interrupt\_sp}$ for the logical channel instance

CCM defines two primary operations: generation-encryption and decryption-verification. Generation-encryption takes a payload, associated data and a nonce to produce a Message Integrity Code (MIC), which is appended to the encrypted payload and returned as the cipher text. The decryption-verification function takes the cipher text and transforms it into plain text payload and MIC. It then verifies the MIC using the recovered plain text, associated data and nonce.

CCM requires several parameters to be defined that control how CCM operates. These include the block cipher algorithm, counter generation function, formatting function and MIC length.

FIPS 197 Advanced Encryption Standard (AES) with a cipher key length of 128 bits (AES-128) shall be used as the block cipher algorithm in CCM.

The length of the MIC generated by the CCM function shall be 4 bytes (32 bits). Following the calculations in NIST Special Publication 800-38C Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, a 32 bit MIC length means an attacker has a less than one-in-one-billion chance of guessing the correct MIC for their fake message, provided no more than four authentication failures are permitted before retiring the key in use.

NIST Special Publication 800-38C Appendix A: Example of a Formatting and Counter Generation Function shall be used as the counter generation function and formatting function.

The formatting function defines how the payload, associated data and nonce are constructed into the B blocks for use in the CCM function. B_0 contains the nonce and control information and $B_1..B_x$ contain the associated data and payload.

The CCM B_0 block format shall be as defined in Table 6-3. There is no Associated Data in Weightless-P.

TABLE 6-3 FORMAT OF CCM B0 BLOCK

Position	Field	Description
0	Flags	The flags field as specified by CCM. Shall be 0x09.
1..13	Nonce	CCM Nonce
14	LengthH	Most significant byte of the length of the payload
15	LengthL	Least significant byte of the length of the payload

The counter generation function generates 128-bit Ctr_i blocks that are used to encrypt the payload data. The format of the Ctr_i blocks shall be as defined in Table 6-4.

TABLE 6-4 FORMAT OF CTR_i BLOCKS

Position	Field	Description
0	Flags	The flags field as specified by CCM. It shall be 0x01
1..13	Nonce	CCM Nonce
14	iH	Most significant bytre of counter block number i.
15	iL	Least significant byte of counter block number i.

The 13-byte CCM nonce format is the same for all logical channels and direction. The format of the CCM Nonce shall be as defined in Table 6-5.

TABLE 6-5 FORMAT OF CCM NONCE

Position	Field	Description
0..3	Counter	The counter value associated with uplink or downlink user data or control. Where 16 bit counters are used they form the LSBs of the counter and the MSBs are set to 0.
4	CCMNonceFlags	The flags value is unique for direction and logical channel.

5..8	ED Random	Random contribution to the CCM Nonce from ED.
9…12	Network Random	Random contribution to the CCM Nonce from BS when transferring control messages in UAC channel, or from SP when transferring user data in UAD, UUD, MAD, MUD, IAD, IUD channels.

When transferring control messages between ED and BS, ED Random and Network Random use those random numbers which are generated during Link Establishment Procedure; When transferring user data between ED and SP, ED Random and Network Random use those random numbers which are generated during Security Association Procedure.

The CCMNonceFlags field encodes whether the CCMNonce is being used for uplink and which logical channel. The flags field has the format defined in Table 6-6.

TABLE 6-6 FORMAT OF CCMNONCEFLAGS FIELD

Bit Position	Field	Description
0	UplinkDownlink	**0**: uplink **1**: downlink
1	UserControl	**0**: UAD, UUD, MAD, MUD, IAD, IUD **1**: UAC
2	Acknowledged	0: UUD, MUD, IUD 1: UAD, MAD, IAD, UAC
3	ZeroPayload	**0**: payload not empty **1**: payload empty
4..7	RFU	

The generation encryption function (e), see Section 6.4.6, and the decryption verification function (v), see Section 6.4.7, are cryptographic functions that are used for format input parameters and execute CCM when encrypting and decryption traffic on a logical channel, see Section 6.4.9.

Depending upon the type of logical channel different counter values maybe required, see Section 6.4.8 for details of counters used with data transfers.

6.4.6 Generation Encryption Function (e)

The generation encryption function (e) implements the encryption generation process defined in CCM.

The generation encryption function (e) has the following inputs, provided by the caller:

- Key K
- Counter Blocks Ctr
- Data Transfer Counter C
- UplinkDownlink UD
- LogicalChannel LC
- Random R (ED Random and Network Random)
- Payload P of length Plen bits

It returns the following outputs:

- ciphertext CT

The function performs the following operation:

$$CT = e(K, Ctr, C, UD, LC, R, P, Plen)$$

The generation encryption function formats counter C, UplinkDownlink (UD), LogicalChannel(LC)and random (R) parameters into the CCM nonce N that is passed to the CCM encryption generation function.

It performs the CCM encryption generation using AES-128, producing a 4-byte MIC. The resulting ciphertext CT, which includes the encrypted payload and MIC, is then returned to the caller.

6.4.7 Decryption Verification Function (v)

The decryption verification function (v) implements the decryption verification process defined in CCM.

The decryption verification function (v) has the following inputs, provided by the caller:

- Key K
- Counter Blocks Ctr
- Data Transfer Counter C
- UplinkDownlink UD
- LogicalChannel LC
- Random R (ED Random and Network Random)
- ciphertext CT of length Clen bits

It returns the following outputs:

- payload P or ERROR

The function performs the following operation:

$$P = v(K, Ctr, C, UD, LC, R, CT, Clen)$$

The decryption verification function formats counter (C), UplinkDownlink (UD), LogicalChannel (LC) and random (R) parameters into the CCM nonce N that is passed to the CCM decryption verification function.

It performs the CCM decryption verification process using AES-128, verifying the 4-byte MIC contained within the ciphertext. If the result is successful then the decrypted payload is returned, otherwise an ERROR is returned.

In Weightless no more than four ERROR results shall be accumulated on any given key before retiring it. Because K_{data_sp} is used bidirectionally, to guarantee that no more than four ERROR results can accumulate in total, no more than two ERROR results shall be allowed to accumulate at either End Device or service provider. $K_{interrupt\_sp}$ and $K_{multicast\_sp}$ are used unidirectionally, so the receiver may allow up to four errors to accumulate before considering a key compromised.

6.4.8 Data Transfer Counters

The Acknowledged data transfer counters shall be used when transferring data on the following logical channels:

- Unicast Acknowledged Data (UAD) using K_{data_sp}
- Unicast Acknowledged Control (UAC) using $K_{control\_bs}$
- Multicast Acknowledged Data (MAD) using a distributed $K_{multicast}$
- Interrupt Acknowledged Data (IAD) using a distributed $K_{interrupt}$

The Unacknowledged data transfer counters shall be used when transferring data on the following logical channels:

- Unicast Unacknowledged Data (UUD) using K_{data_sp}
- Multicast Unacknowledged Data (MUD) using a distributed key
- Interrupt Unacknowledged Data (IUD) using a distributed key

When a block of data is to be transferred it is given a counter value. The counters are 32-bit and 16-bit numbers for Acknowledged and Unacknowledged data transfer, respectively. They are initialized to 0 when the key is derived or distributed and incremented after each use of the key. Uplink and downlink have independent counters.

The counters shall not wrap. When then counter reaches its maximum value the associated key shall be reestablished using the security association and link establishment process, with new random nonces used for control messages and for user data encryption and authentication.

6.4.9 Encryption Processing

The Link Layer applies the generation encryption function (e) to the message to be transferred.

If the message is being transferred on an acknowledged logical channel then the result of the generation encryption function (e) is processed for transmission. If the message is being transferred on an unacknowledged logical channel then the counter value and the output of the generation encryption function are concatenated before transmission.

The receiving device reassembles the complete message and performs the decryption verification function (v). If the result of the decryption verification function is a valid plaintext message it is forwarded to higher layers.

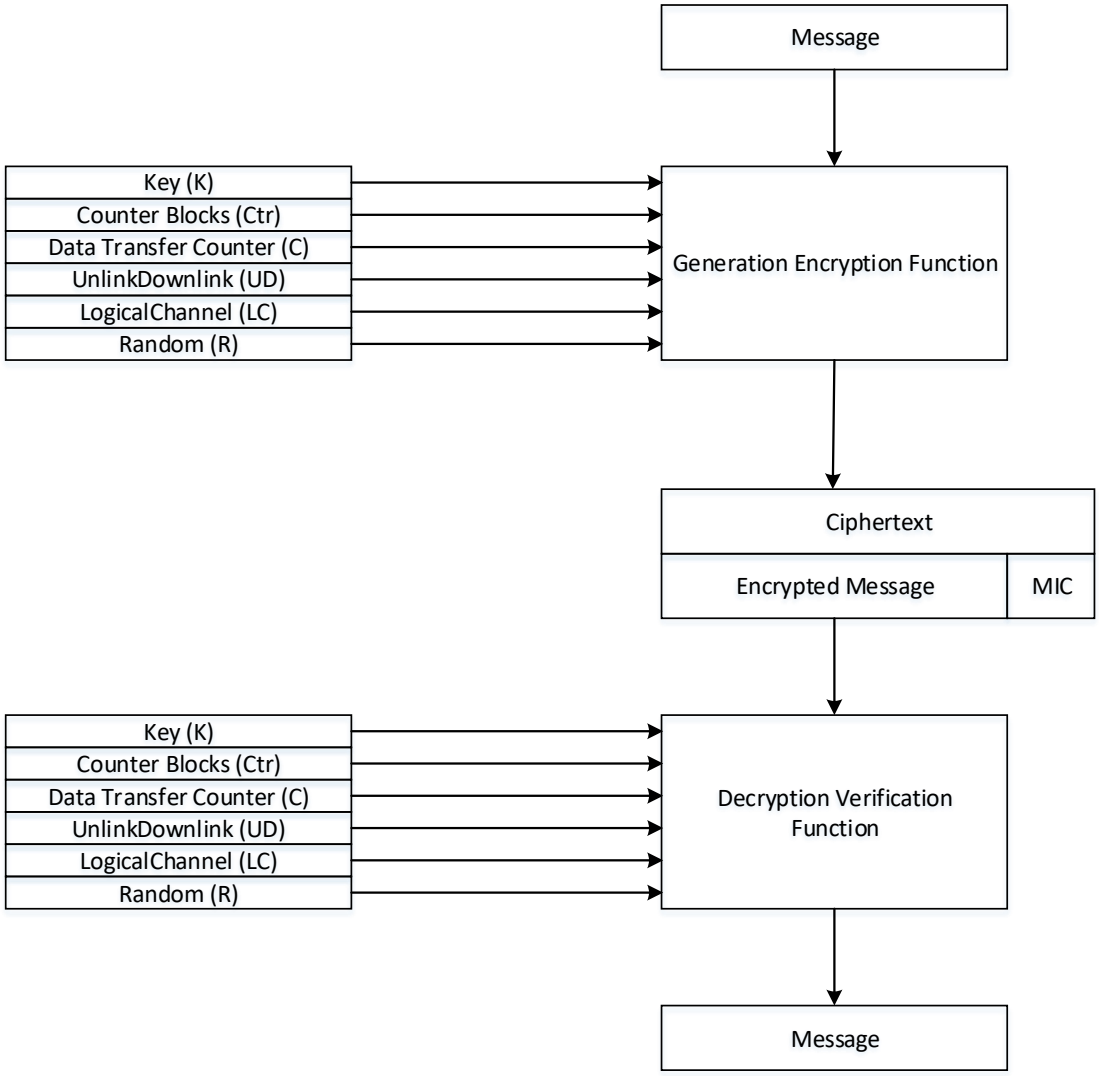

FIGURE 6-1 ACKNOWLEDGED CHANNELS ENCRYPTION/DECRYPTION

Figure 6-1 provides an overview of the inputs and outputs of the generation encryption function (e) and decryption verification function (v) when used with an acknowledged logical channel. Only the ciphertext is transmitted to the receiver, and the receiver uses a data transfer counter value C that it has determined is applicable to the message. The acknowledgment message is used to synchronize the counter C value between ED and Network.

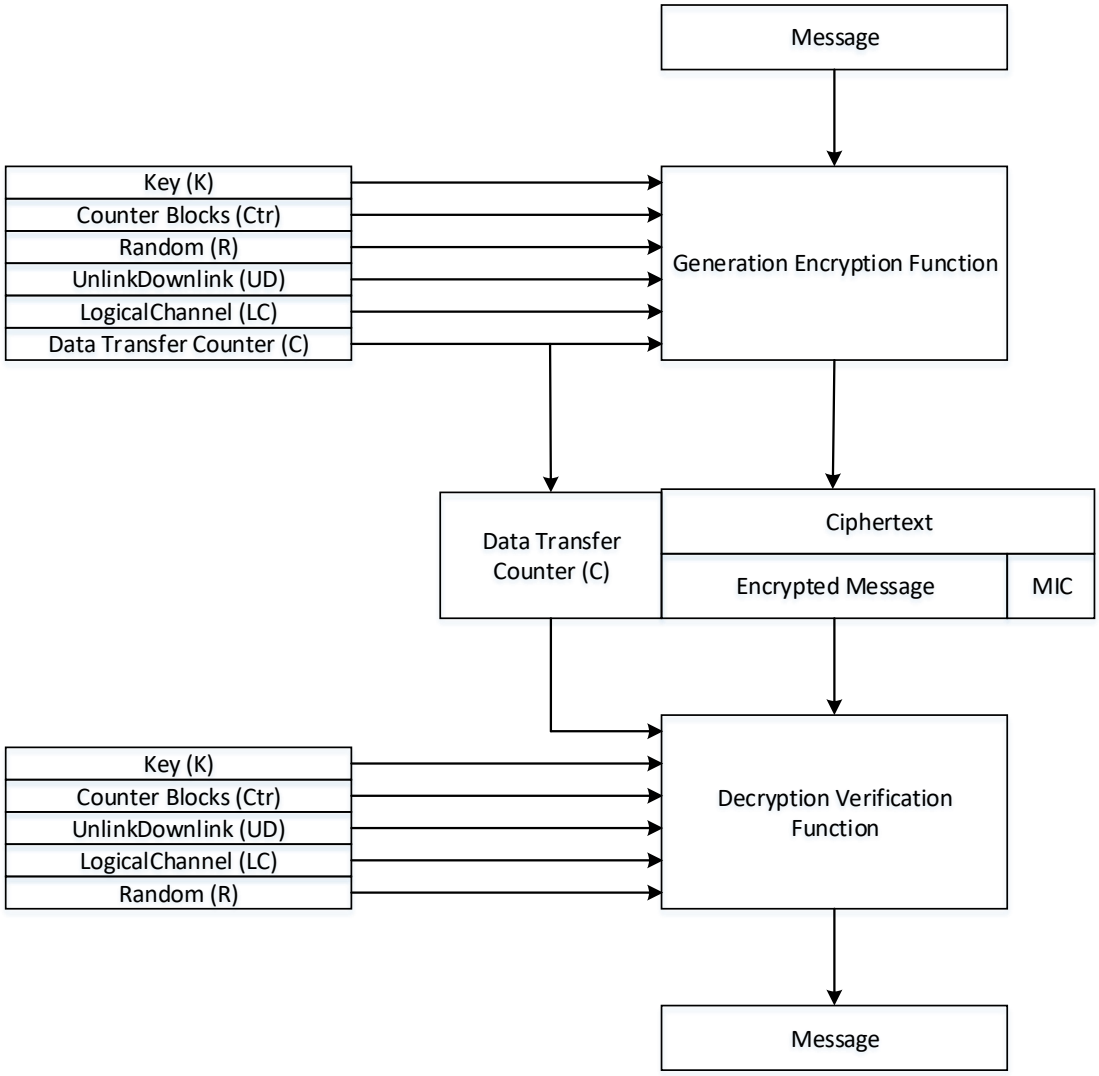

FIGURE 6-2 UNACKNOWLEDGED CHANNELS ENCRYPTION/DECRYPTION

Figure 6-2 provides an overview of the inputs and outputs of the generation encryption function (e) and decryption verification function (v) when used with an unacknowledged logical channel. The ciphertext is appended the data transfer counter C, and the both are transmitted to the receiver. The receiver uses the counter value received and the ciphertext to decrypted and verify the message.

6.4.10 Signatures

Some operations in Weightless require authorization from an entity that does not have a security session running with a device, therefore a method to provide assurance of authenticity of the requests is required. To support this a signature method is provided to allow the entity to authenticate those requests.

CMAC is used as the signature algorithm. CMAC is defined in NIST Special Publication 800-38B Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication. CMAC is also defined in IEFT RFC 4493.

FIPS 197 Advanced Encryption Standard (AES) with a cipher key length of 128 bits (AES-128) shall be used as the block cipher algorithm in CMAC.

The CMAC algorithm provides 2 functions MAC Generation and MAC Verification that are used by the Signature Generation Function (sg), see section 6.4.10.1, and Signature Verification Function (sv), see section 6.4.10.2. The suggested notation in NIST SP800-38B is used within the definitions of Signature Generation Function (sg) and Signature Verification Function (sv).

The CMAC functions require a signature length parameter, Tlen. For the use of CMAC within the Signature Generation Function (sg) and Signature Verification Function (sv) the signature length Tlen shall be set to 64 bits.

64 bits is the minimum recommended length of signature in NIST SP 800-38B.

The input Key is K_{verify_wss} during Association and K_{verify_sp} during Link Establishment.

6.4.10.1 Signature Generation Function (sg)

The Signature Generation Function (sg) takes a message to be signed and a key to perform the signature with and return a 64 bit signature calculated using the MAC Generation function defined in NIST SP 800-38B.

The signature generation function (sg) takes the following inputs, provided by the caller:

- K: An input key that is used only for signature generation.
- M: A message of Mlen bits to be signed.

It returns the following values:

- Signature S.

The function performs the following operation:

$$S = CMAC(K, M, 64)$$

The K and M parameters are passed to the CMAC MAC Generation function. The output from the MAC Generation function is then returned to the caller as the signature.

6.4.10.2 Signature Verification Function (sv)

The Signature Verification Function (sv) takes a message, its signature and returns whether signature is valid or invalid.

The signature verification function (sv) takes the following inputs, provided by the caller:

- K: An input key that is used to verify the signature.
- M: A message of Mlen bits to be verified.
- S: The signature to be verified.

It returns the following values:

- VALID if the provided signature S matches the locally calculated signature, or INVALID.

The function performs the following operation:

r = VER(K, M, S)

The K, M and S parameters are passed to the CMAC MAC Verification function. The output from the MAC Generation (r) function indicating whether signature is valid or not is returned to the caller.

6.4.11 Cryptographic Overhead

6.4.11.1 Encryption and Integrity Overhead

The total cryptographic overhead per message for an acknowledged channel is equal to the MIC size of 4 bytes (32 bits).

The total cryptographic overhead per message for an unacknowledged channel is equal to the MIC size of 4 bytes (32 bits) plus the counter size of 2 bytes (16 bits), therefore the total overhead is 6 bytes (48 bits).

6.4.11.2 Key Wrap Overhead

The AES Key Wrap Specification adds a 64-bit overhead to the key that is being transported. All the keys transported with Weightless are 128-bit AES keys. Therefore the total size of a key protected for transport is 192 bits.

6.4.11.3 Signature Overhead

The CMAC algorithm used for signatures does not modify the data being signed; it does however ever generate a signature that needs to be transported to the recipient. The overhead therefore is the size of the signature which is 64 bits per signature.

7 REGULATION COMPLIANCE

7.1 INTRODUCTION

Weightless-P physical layer and frame structure are designed to accommodate various regulatory frameworks, and in particular:

1. Operation in band **IV** (779-787MHz) in China (SRRC 423 [2005])
2. Operation in band **V** (863-870MHz) in Europe (ETSI EN 300 220 v2.4.1)
3. Operation in band **V bis** (870-875.6MHz) in Europe (Draft ETSI EN 303 204 v1.1.0)
4. Operation in band **VI** (902-928MHz) in US (Part 15.247 of Title 47 of the Code of Federal Regulations)

The following sections describe deployment scenarios for each of these cases.

7.2 BAND IV IN CHINA (779-787MHZ)

SRRC 423 [2005] limits the transmit power to 10mW/10dBm and does not mandate any particular spectrum usage technique. In such deployment, it is recommended to use Frequency Hopping and to apply Listen Before Talk only for End Device Contention Access.

7.3 BAND V IN EUROPE (863-870MHZ)

Under ETSI EN 300 220 v2.4.1, it is recommended to use Weightless-P with Listen Before Talk (LBT) and either Frequency Hopping Spread Spectrum (FHSS) or Adaptive Frequency Agility (AFA), or a combination of both. When deployed in 100kHz with FHSS, it is mandated to use at least 47 hopping channels in the frequency range 863MHz to 870MHz, except for the ranges dedicated to alarms (868.600-868.700, 869.200-869.400 and 869.650-869.700).

The dwell time cannot exceed 400ms, that is 16 DL_ALLOC or 8 UL_ALLOC timeslots.

The minimum Tx off-time is 100ms, so it is recommended to interleave resource allocations from neighboring Base Stations.

The accumulated Tx on-time over any 200kHz cannot exceed 100 seconds per 1 hour. With 48 hopping channels of 100kHz each, this implies a maximum Tx on-time of 2,400 seconds per hour. Given the TDD half-duplex nature of Weightless-P and the expectation that more resources are allocated to UL_ALLOC than DL_ALLOC, this should not constrain Weightless-P networks.

The maximum transmit power is normally limited to 25mW/14dBm. There is the possibility to use the 869.400-869.650MHz sub-band to carry the SIBs and/or DL_RA/UL_RA, which allow a transmit power of up to 500mW/27dBm.

Depending on their expected traffic type, the End Devices may elect not to implement LBT, except for Contention Access. In such case the duty cycle limitations apply, but there is more flexibility in the choice of Contention Access LBT parameters.

7.4 BAND V BIS IN EUROPE (870-875.6MHZ)

Under Draft ETSI EN 303 204 v1.1.0, the transmit power is limited to 500mW/27dBm. Channel spacing is 25kHz minimum and 200kHz maximum.

In the absence of ER-GSM, the duty cycle limitation is 2.5% for End Devices, and 10% for Base Stations provided they are individually licensed.

An Automatic Power Control scheme is mandatory. It is expected that open-loop power control is sufficient, especially if Frequency Hopping is not in use. In case Frequency Hopping is in use, the RRM Power Control procedure may need to be used.

For use in 873-875.6MHz with ER-GSM protection, the duty cycle limit of 0.01% and maximum on-time of 5ms/1s are too restrictive, and it is recommended to implement either a coordination procedure with the railway operator or a cognitive procedure in order to avoid ER-GSM channels.

7.5 BAND VI IN US (902-928MHZ)

Operation in the 902-928MHz band is recommended under the rules of FCC Part 15.247. Although operation without hopping (under FCC Part 15.249) is possible, it restricts the transmit power to -1dBm.

It is required to use at least 50 hopping channels (with a minimum 25kHz channel spacing or 20dB bandwidth, whichever is greater) and the dwell time is limited to 400ms, and maximum on-time on any channel to 400ms in a 20 seconds period.

Output power is restricted to 1W/30dBm and can be combined with p to 6dBi of directional antenna gain. Above 6dBi of directional antenna gain, the conducted output power needs to be decreased accordingly.