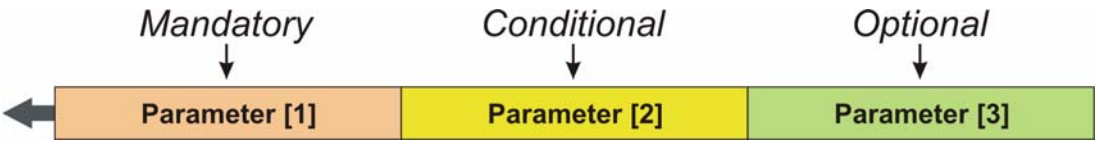
WIMAX from A-Z
-
reloaded

INACON GmbH
Kriegsstrasse 154
76133 Karlsruhe
Germany
www.inacon.com
e-mail: inacon@inacon.de

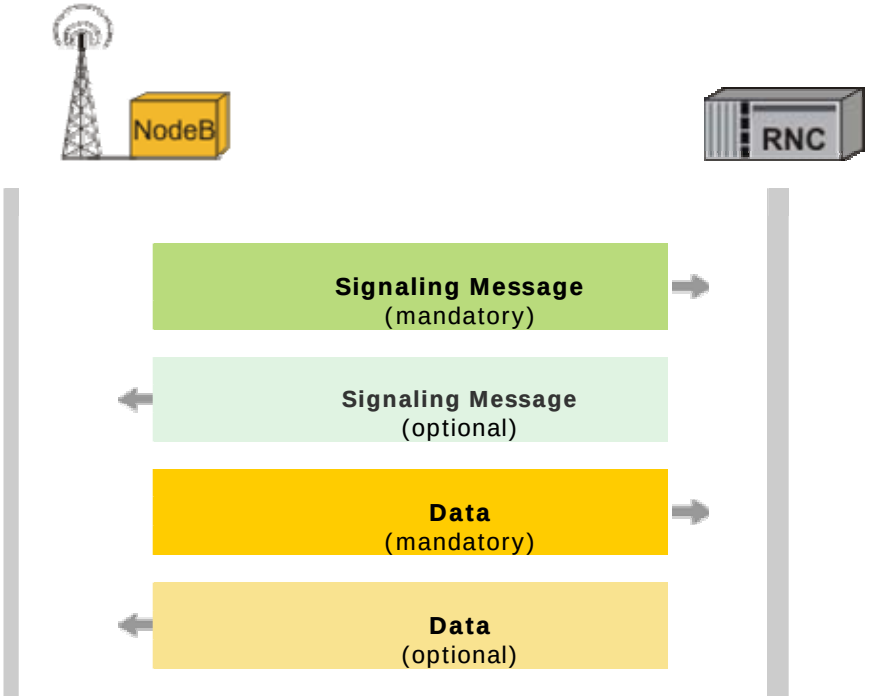
Legend:

All INACON publications use the same color codes to distinguish mandatory from optional or conditional parts in frame formats or optional from mandatory data blocks or signaling messages in scenarios. The different color codes are explained underneath:

- **Color Codes in Frame Formats:**



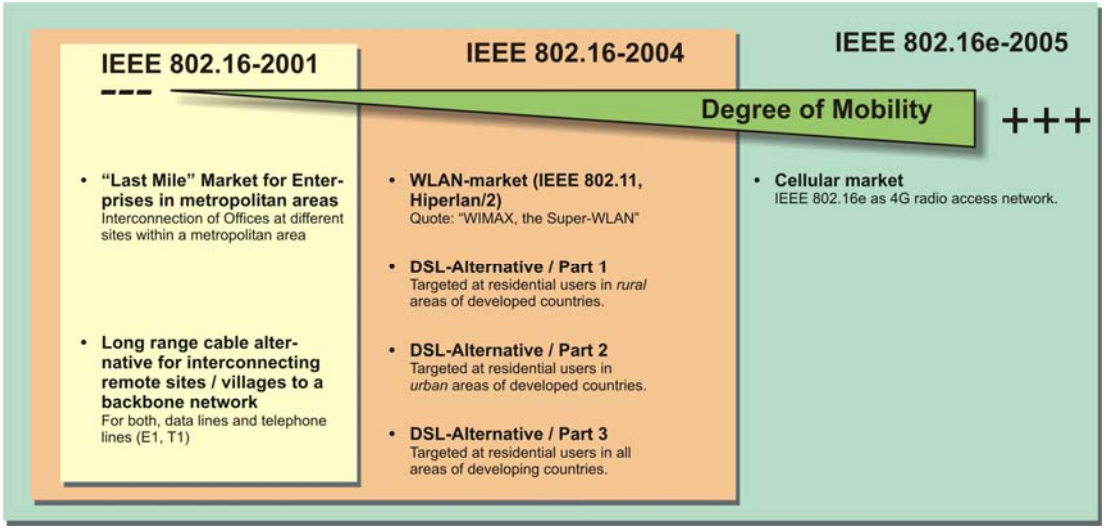
- **Color Codes in Scenarios:**



1

1.1 What is WIMAX?

1.1.1 Evolution of a Standard's Business Targets



The objective of this section is to illustrate the evolution of the business targets of IEEE 802.16.

Key point of this section is that this genealogy of WIMAX manifests itself in many physical and MAC-layer specific procedures. Some of them cannot hide their origin in a PTP-technology.

Image Description
The center of the image is represented by the three rectangles.

- The yellow rectangle is historically the oldest one and the text inside represents the applications that this version of the standard (Release IEEE 802.16-2001) was targeted at.
- Most important is that IEEE 802.16-2001 was a plain PTP-technology without consideration of OFDM or OFDMA and solely meant for the frequency range 10 – 66 GHz.
- The red rectangle represents the next major release of the standard, IEEE 802.16-2004.
- It incorporates updates like 802.16a and 802.16d.
- However, more important for this section's considerations is the fact that IEEE 802.16-2004 is really a completely new technology, addressing completely different applications.
- Important technical aspects of this change are the new support for the NLOS-frequency range 2 – 11 GHz and the support of OFDM, OFDMA, AMC and HARQ.

- These changes enable IEEE 802.16-2004 to address the requirements of new markets, mainly to become the wireless DSL-alternative.

It is noteworthy that most vendors claim to “not be interested in IEEE 802.16-2004-products”. Yet, most features that they support with 802.16e have already been inserted into the 802.16-2004 variant of the standard.

- The previous statement already paved the way to the next change: The green rectangle represents the latest update of the applications to be supported.
- IEEE 802.16e-2005 represents the “real” WIMAX, technically amending IEEE 802.16-2004 by scalable OFDMA and support for mobility features.
- These technical amendments enable WIMAX to address and attack the cellular market.

Very important: The red rectangle contains the yellow rectangle and the green rectangle contains the red rectangle. Each newer standard version contains the previous versions.

Room for your Notes

- **Abbreviations of this Section:**

4G	4th Generation …	**NLOS**	Non Line Of Sight
AMC	Adaptive Modulation and Coding	**OFDM**	Orthogonal Frequency Division Multiplexing
DSL	Digital Subscriber Line	**OFDMA**	Orthogonal Frequency Division Multiple Access
GHz	Giga Hertz (10^9 Hertz)	**PTP**	Point to Point
HARQ	Hybrid ARQ (3GTS 25.212)	**WIMAX**	Worldwide Interoperability for Microwave Access (IEEE 802.16)
IEEE	Institute of Electrical and Electronics Engineers	**WLAN**	Wireless Local Area Network (IEEE 802.11)

1.2.2 IEEE 802.16 X, Y Z – the ABC of a Standard

The objective of this section is the provision of an overview of the nomenclature and terminology of the various working groups, standard versions and amendments of IEEE 802.16.

Key point of this section is to understand that 802.16-standardization is still ongoing and therefore, various amendments like 802.16g are still underway and will eventually be incorporated into the core document.

Image Description

- The image uses the metaphor of IEEE 802.16 being a house which is built from the various pieces of the standard.
- We tried to walk along this metaphor as far as possible. Example: The fundament and major piece of the standard is the IEEE 802.16-2004 edition. IEEE 802.16e-2005 only adds a roof to the basic building.
- Not all amendments are illustrated in the image but all versions and amendments are described in the text. For a detailed description of the targets and work of all working groups please refer to the IEEE 802.16 website at http://www.ieee802.org/16/.

1.2.2.1 IEEE 802.16.1

This is the original “seed” of WIMAX. IEEE 802.16.1 put together the original system requirements list.

1.2.2.2 IEEE 802.16.2

The coexistence working group (IEEE 802.16.2) should investigate how 802.16 would coexist in the RF-area with other nearby systems (e.g. LMDS or MMDS).

1.2.2.3 IEEE 802.16a

Founded in January 2000 and complemented by 802.16b, the 802.16a working group should investigate if and how the new MAN-standard could be interesting in frequency ranges underneath 10 GHz ("Sub-10 Study Group"). The effort of the 802.16a and b working groups was merged into the mainstream standard and resulted in the release of the IEEE 802.16a-2003 standard (which includes the genuine IEEE 802.16-2001 standard).

1.2.2.4 IEEE 802.16b

Responsible for the Wireless HUMAN PHY-layer option that allows using WIMAX in the license free frequency ranges between 5 GHz and 6 GHz.

Room for your Notes

- **Abbreviations of this Section:**

GHz	Giga Hertz (10^9 Hertz)	**MAN**	Metropolitan Area Network
HUMAN	High-speed Unlicensed Metropolitan Area Network	**MMDS**	Multipoint Microwave Distribution System or Multi-channel Multi-point Distribution System
IEEE	Institute of Electrical and Electronics Engineers	**RF**	Radio Frequency
LMDS	Local Multipoint Distribution Services	**WIMAX**	Worldwide Interoperability for Microwave Access (IEEE 802.16)

1.2.2.5 IEEE 802.16c

The 802.16c working group focuses on interoperability and testing and releases their own standards to complement the mainstream 802.16 standard. The 802.16c-1 contains the PICS (Protocol Implementation Conformance Statement), the 802.16c-2 the test suite structure and the 802.16c-3 contains (Radio Conformance Tests). Note that all three are limited to the 10-66 GHz frequency range. The 802.16c-4 shall expand the coverage to 2-11 GHz.

1.2.2.6 IEEE 802.16-2001

IEEE 802.16-2001 represents the first release of the 802.16 standard. It only covered the frequency range 10 – 66 GHz (LOS-operation) and did only include single carrier operation (no OFDM).

1.2.2.7 IEEE 802.16.2-2001

IEEE 802.16.2-2001 represents the results of the work of the coexistence working group (see 1.2.2.2).

1.2.2.8 IEEE 802.16d

The work of the 802.16d working group had the following major targets: The addition of use profiles for the 2-11 GHz frequency range and the addition of subchannelization to the OFDM PHY-layer option. In addition, the 802.16d working group added means for AAS and MIMO to the standard.

1.2.2.9 IEEE 802.16-2004

IEEE 802.16-2004 represents the aggregated output of the work of all working groups including .16a, b, c and d. IEEE 802.16-2004 is also the basis for the amendments added by .16e ff (including m!) and already includes OFDM with FFT-size = 256, OFDMA with FFT-size = 2048.

1.2.2.10 IEEE 802.16e-2005 with CORRIGENDUM 1 for IEEE 802.16-2004

The .16e working group had to give into the enormous pressure to release a mobile operation amendment still in 2005. The consequence is IEEE 802.16e-2005 which also contains the first corrections for errors within IEEE 802.16-2004.
Unfortunately, the time was not there to merge the mobile amendments and the corrections with 802.16-2004. Consequentially, IEEE 802.16e-2005 only provides the delta subclauses and paragraphs and requires the parallel reading of IEEE 802.16-2004 and IEEE 802.16e-2005.

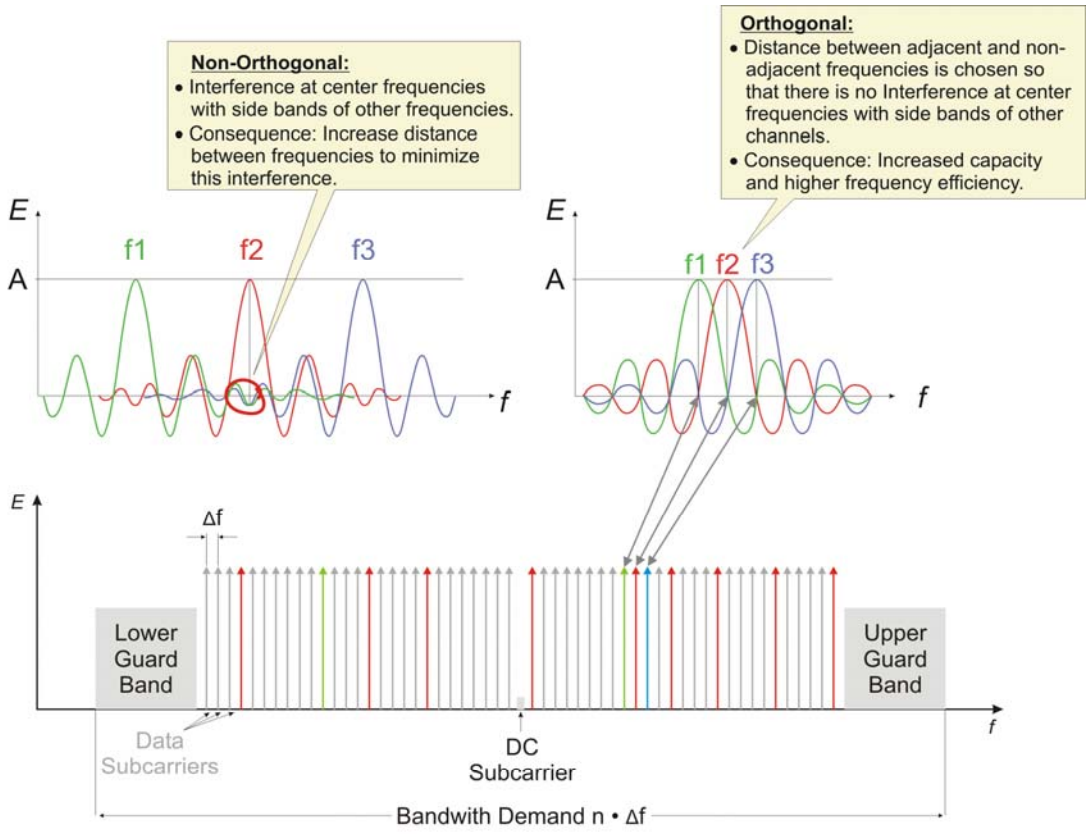
1.2.2.11 CORRIGENDUM 2 for IEEE 802.16-2004

There is a second update for the fundamental specification 802.16-2004 that is currently (summer 2007) a work in progress. It corrects numerous errors of corrigendum 1 and adds numerous new bits and pieces. However, there are no new major features added through corrigendum 2.

1.2.2.12 IEEE 802.16f

This amendment of 802.16-2004 adds a MIB to the base standard. This MIB contains, among other things, database object definitions for managed BS's and MS's that can be used to convey configuration information from a central database to these devices. Note that 802.16f does not cover any mobile specific database objects.
And as for most amendments, 802.16f will be merged into the baseline documents as soon as more stable.

1.4.2 OFDMA – Fast Review



The objective of this section is to provide a broad overview of the assets of an OFDMA-system.

Key points of this section are to:
1. Realize the meaning of the word “orthogonal” with respect to FDM. It relates to the distance between adjacent carriers.
2. Understand how multiple users may simultaneously access an OFDM-system.

Image Description

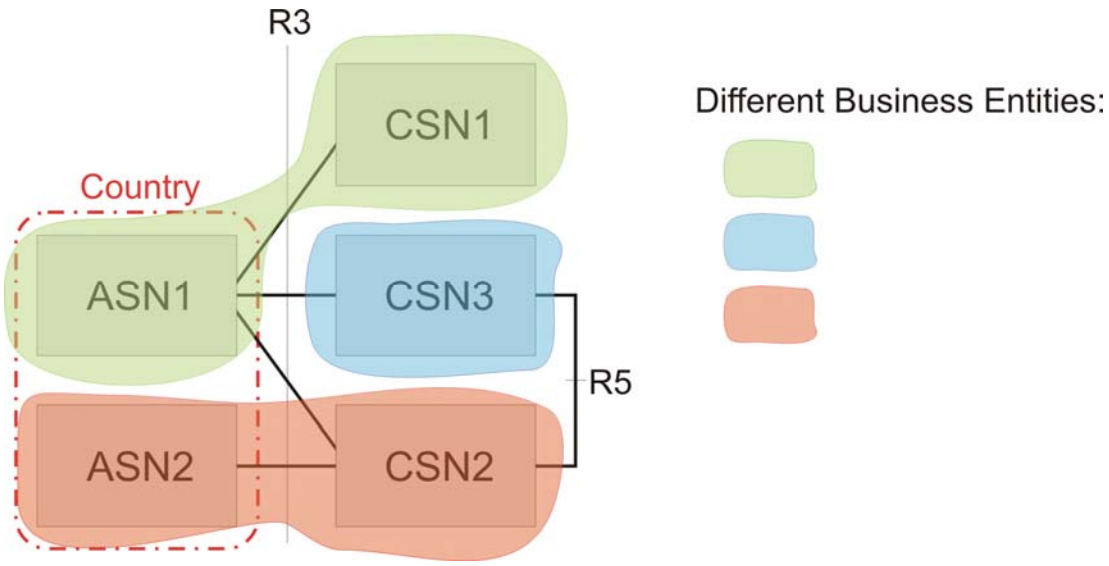
- The image illustrates in the upper part two FDM-systems.
- The left one is non-orthogonal and hence, there are interferences among the different carriers.
- The FDM-system on the right side is orthogonal because the distance among the frequencies F1, F2 and F3 is selected in the illustrated way to provide for zero interference.
- Underneath this detailed view, the image illustrates the typical brickwall view of an OFDM-system with the two guardbands on the left and on the right side without any transmission and the DC-subcarrier in the middle, also without any transmission.
- Some subcarriers are colored to illustrate the multiple access dimension of this system. Three users A, B and C are using the resources for their specific purposes and applications (see legend).

Room for your Notes

- **Abbreviations of this Section:**

DC	Direct Current	**OFDMA**	Orthogonal Frequency Division Multiple Access
FDM	Frequency Division Multiplexing	**SMS**	Short Message Service (3GTS 24.011, 3GTS 23.040)
OFDM	Orthogonal Frequency Division Multiplexing		

2.1.4 Possible Relationships between ASN and CSN



The objective of this section is to illustrate possible business relationships between the two ASN's on one hand, covering different geographic regions, and the related CSN's on the other hand.

Key point of this section is that access network sharing and unbundled access / core network operation are standard features of WIMAX.

Image Description

- The image illustrates two ASN's which cover the two different geographic regions of one country (red border).
- The image also illustrates the three CSN's which are using the two ASN's.
- ASN 1 and CSN1 belong to the same business entity. Similarly, ASN 2 and CSN 2 belong to the same business entity.
- CSN 3 has no own access network and uses ASN 1 and 2 through different roaming agreements.
- The meaning of the R3- and R5-interfaces will be introduced in a later section.

2.1.4.1 Assessing the Situation of CSN 1 and NSP 1

The operator of CSN 1 (NSP 1) also owns ASN 1 and has the right to use the necessary frequencies. However, NSP 1 is only a regional WIMAX network operator as he or she has no access within the region that is covered by ASN 2.

2.1.4.2 Assessing the Situation of CSN 2 and NSP 2

The operator of CSN 2 (NSP 2) also owns ASN 2 and has the right to use the necessary frequencies. Opposed to NSP 1, the NSP 2 can provide service within the entire country through a roaming agreement with the operator of ASN 1.

2.1.4.3 Assessing the Situation of CSN 3 and NSP 3

NSP 3 as operator of CSN 3 owns no own WIMAX access resources within this country. Still, NSP 3 can offer a nationwide WIMAX-service through two different types of roaming agreements with the operators of ASN 1 and ASN 2.

2.1.4.4 Conclusions

The total unbundling between access network and core network allows for new and different business models and relationships than what was possible in the past.

Examples:

- Business entities like coffee retailers or energy suppliers may act as “front men” and as CSN while *some* access network is providing the local coverage.
- Incumbent GSM- / UMTS- or CDMA-network operators may take WIMAX as alternative radio access technology on board without the need to actually install a WIMAX-network of thousands of base stations.

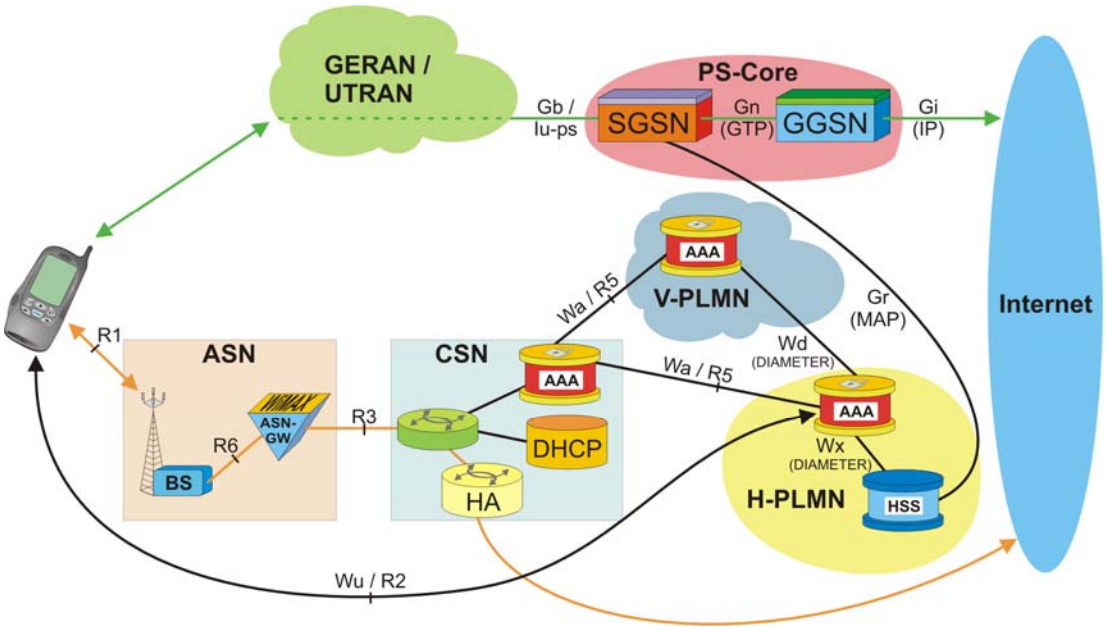
[WIMAX-Forum NWG Stage 2 Part 1 (6.4)]

Room for your Notes

- **Abbreviations of this Section:**

ASN	Access Service Network	**NSP**	Network Service Provider
CDMA	Code Division Multiple Access	**NWG**	Network Working Group (WIMAX Forum)
CSN	Connectivity Service Network	**UMTS**	Universal Mobile Telecommunication System
GSM	Global System for Mobile Communication	**WIMAX**	Worldwide Interoperability for Microwave Access (IEEE 802.16)

2.7.5 Network Architecture in case of I-WLAN Direct IP-Access



The objective of this section is to illustrate the combined 3GPP- / WIMAX-network architecture in case of the "I-WLAN Direct IP-Access" interworking.

Key point of this section is that the 3GPP-network contribution is primarily related to authentication issues. The entire traffic bypasses the 3GPP-network.

Image Description

- The image illustrates in the top half the standard 3GPP-access network resources together with the standard packet-switched core.
- The green arrows shall highlight the data and information flow, if the MS on the left side attached to the packet-switched core through GERAN/UTRAN.
- The lower half of the image is dedicated to the alternative WIMAX-based access, considering the split into ASN and CSN.
- Very interesting: In the illustrated example, the H-PLMN which is a 3GPP-network becomes the H-CSN of the mobile station.
- The orange and black lines indicate the information flow in case of WIMAX-based network access.
- In that respect, the orange line illustrates the data flow while the black lines illustrate the flow of control information (e.g. AAA or DHCP).

- The image illustrates two PLMN's, a V-PLMN and the H-PLMN. There will only be a V-PLMN involved in the illustrated case, if the WIMAX CSN-operator has only a roaming agreement with the V-PLMN operator which in turn will involve the H-PLMN operator of the mobile user.
- Whenever applicable, the image lists the interface names from both terminologies, 3GPP and WIMAX-forum.
- The mobile user will identify him- or herself through a SIM- or USIM-card.

[WIMAX-Forum NWG Stage 2 3GPP-WIMAX Interworking, 3GTS 22.234, 3GTS 23.234, 3GTS 24.234, 3GTS 43.318, 3GTS 44.318]

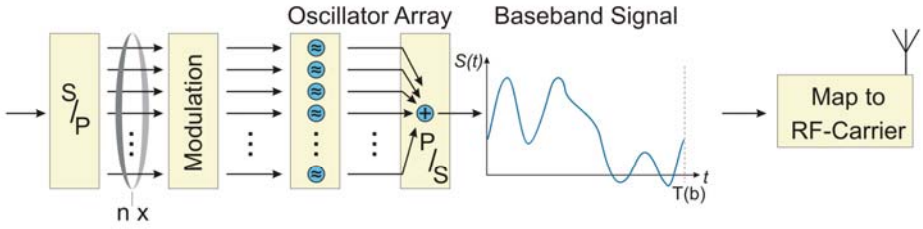
- **Abbreviations of this Section:**

3GPP	Third Generation Partnership Project (Collaboration between different standardization organizations (e.g. ARIB, ETSI) to define advanced mobile communications standards, responsible for UMTS)	**I-WLAN**	Interworking WLAN (Wireless Local Area Network) (3GTS 23.234)
3GTS	3rd Generation Technical Specification	**MAP**	Mobile Application Part (3GTS 29.002)
AAA	Authentication, Authorization and Accounting	**MS**	Mobile Subscriber Station (IEEE 802.16e)
ASN	Access Service Network	**NWG**	Network Working Group (WIMAX Forum)
BS	Base Station (IEEE 802.16)	**PLMN**	Public Land Mobile Network
CSN	Connectivity Service Network	**PS**	Packet Switched
DHCP	Dynamic Host Configuration Protocol (RFC 2131)	**SGSN**	Serving GPRS Support Node
GERAN	GSM EDGE Radio Access Network	**SIM**	Subscriber Identity Module
GGSN	Gateway GPRS Support Node	**USIM**	Universal Subscriber Identity Module (3GTS 31.102)
GTP	GPRS Tunneling Protocol (3GTS 29.060)	**UTRAN**	UMTS (Universal Mobile Telecommunication System) Terrestrial Radio Access Network
H-PLMN	Home PLMN	**V-PLMN**	Visited PLMN
HA	Home Agent (Mobile IP / RFC 3344)	**WIMAX**	Worldwide Interoperability for Microwave Access (IEEE 802.16)
HSS	Home Subscriber Server (3GTS 23.002). HSS replaces the HLR with 3GPP Rel. 5		

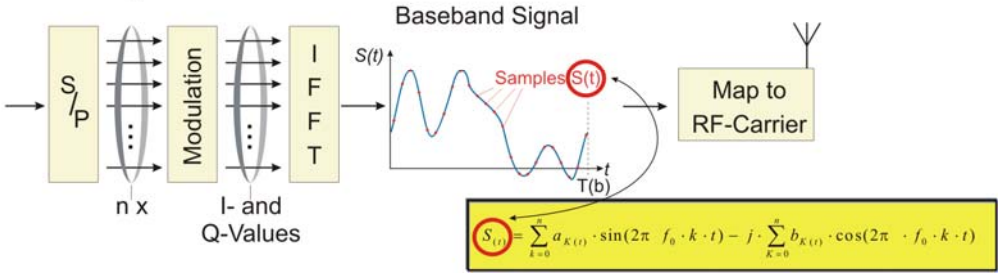
3.2 Advanced Issues of OFDM / OFDMA

3.2.1 OFDM / OFDMA and IFFT

1. Implementation Option: Discrete Technology



2. Implementation Option: Inverse FFT



The objective of this section is to illustrate how IFFT maps so perfectly to the requirements of an OFDM system.

Key point of this section is that IFFT provides nothing else but the digital recipe to produce perfectly orthogonal sine waves and to burn the formula into silicon.

Image Description

- The image illustrates two implementation options.
- The upper option 1 is analog and operates by producing the single orthogonal subcarriers within an oscillator array.
- Option 2 goes a different way and applies the IFFT formula within the yellow box. The most important asset of this IFFT-formula is the factor 'k' that inherently provides harmonic, orthogonal frequencies.

Please note that in both cases, the resulting S(t) is a baseband signal that needs to be mapped to the respective RF-carrier frequency.

3.2.1.1 Considering the Discrete Oscillator Array Option

This option is unrealistic for large scale deployments as it scales very poorly and since it is very expensive to implement.

3.2.1.2 Details of the IFFT Option

- The illustrated formula may be real numbered only (sin) or complex numbered (sin + cos).
- The number of samples S(t) over one symbol duration T(b) depends on the highest OFDM frequency which is k x f(0).
- According to Nyquist, we therefore need 2 x k x f(0) different samples S(t) per symbol period T(b) to provide for an error-free signal processing.

Please calculate for a bandwidth of 10 MHz with an FFT-size = 1024, how many samples are required within which symbol duration.

- Obviously, for each sample S(t(x)), all different k-values need to be applied.
- We provided the aforementioned details to illustrate the enormous processing power that is required for OFDM.

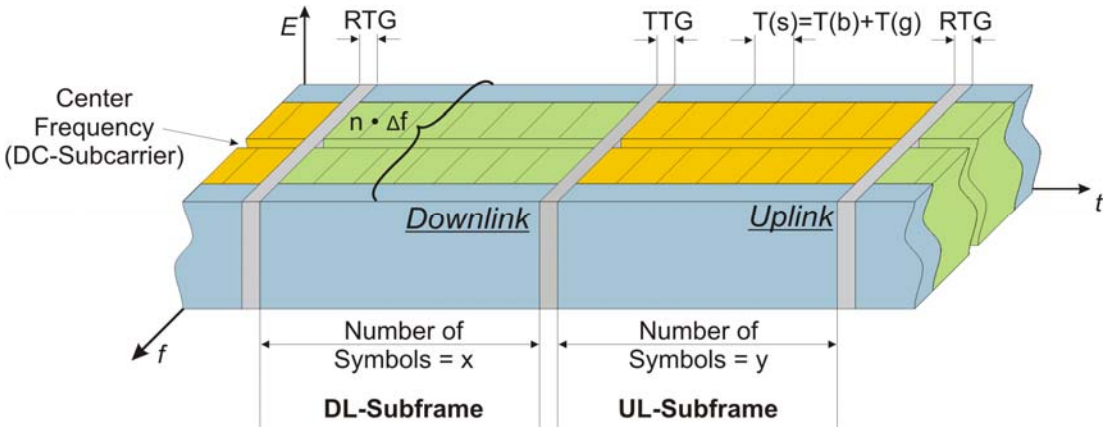
3.2.1.2.1 Why is it called F a s t Fourier Transformation?

- The difference between fast and regular Fourier transformation is that fast Fourier transformation uses a special algorithm for the fast calculation of the single values of a Fourier series.
- This algorithm was officially published in 1965 but was applied already by Carl Friedrich Gauss in 1805.
- Obviously, this algorithm is also optimal for chip based calculations. The only disadvantage of FFT is that the FFT-size = n needs to be a 2^k value (e.g. 64, 128, 256, 512, 1024 …). Values like n = 66, 214 or similar are therefore forbidden.

- **Abbreviations of this Section:**

FFT	Fast Fourier Transformation	**OFDM**	Orthogonal Frequency Division Multiplexing
IFFT	Inverse Fast Fourier Transformation	**OFDMA**	Orthogonal Frequency Division Multiple Access
MHz	Mega Hertz (10^6 Hertz)	**RF**	Radio Frequency

3.2.5.2 View of a TDD-Implementation



The objective of this section is to illustrate how an OFDM/OFDMA-system looks like in case of TDD as duplex scheme.

Image Description

- The image illustrates how an OFDM-system will look like if TDD is used as duplex scheme.
- The relationship between T(s), T(b) and T(g) is obviously the same as in the FDD-form.
- Opposed to FDD there is only one center frequency.
- Duplex transmission is achieved by defining time frames which in turn are split into downlink and uplink subframes.
- The duration of these subframes is measured in multiples of symbol durations T(s) as illustrated in the image.

Important properties of TDD-systems are:

- Simultaneous transmission in uplink and downlink is not possible but the opposite transmission direction needs to wait for “its” subframe.
- Asymmetric uplink and downlink traffic can well be supported as the subframe durations can be adjusted.
- Channel reciprocity is there which means that the same RF-conditions can be assumed for both directions. Uplink measurement results can therefore be input for downlink RF-tuning.
- No paired frequency bands are required.
- Base stations must be finely synchronized to minimize interference among each other. The implementation of GPS-receivers is typical.

Note that the WIMAX-Forum has mandated TDD-operation initially for WIMAX [WIMAX Forum Mobile System Profile (4.1.1.2)].

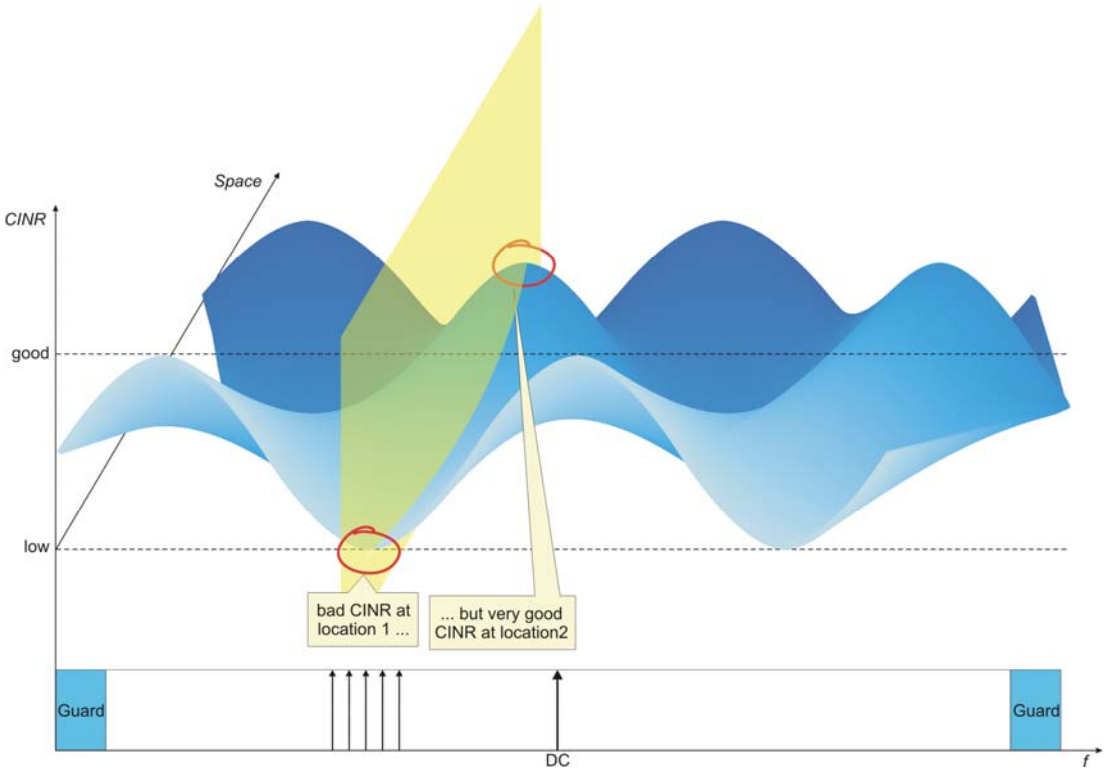
Room for your Notes

- **Abbreviations of this Section:**

DC	Direct Current	**RF**	Radio Frequency
DL	Downlink	**RTG**	Receive transmit Transition Gap (IEEE 802.16 (3.45)) the time between an uplink subframe and the subsequent downlink subframe in a TDD-system
FDD	Frequency Division Duplex	**TDD**	Time Division Duplex
GPS	Global Positioning System	**TTG**	Transmit receive Transition Gap (IEEE 802.16 (3.63)) the time between a downlink subframe and the subsequent uplink subframe in a TDD-system
OFDM	Orthogonal Frequency Division Multiplexing	**UL**	Uplink
OFDMA	Orthogonal Frequency Division Multiple Access	**WIMAX**	Worldwide Interoperability for Microwave Access (IEEE 802.16)

3.3.3 Distributed vs. Adjacent Subcarrier Allocation (DSCA/ASCA)

3.3.3.1 Location- and Frequency-Selective Fading CINR



The objective of this section is to illustrate why two different subcarrier allocation strategies, adjacent and distributed, are used, taking into the consideration the interference situation on the wireless channel.

Key point of this section is that ASCA and DSCA can coexist within a single OFDMA-frame but are beneficial for clients in different situations, mobile or fixed and with or without use of smart antennas.

What is the space distance between two adjacent hills or two adjacent valleys?

Image Description

- The image tries to illustrate in 3D the CINR (vertical axis) in dependency of frequency (horizontal axis) and space or location (3D axis).
- The yellow area shall emphasize that the indicated subcarriers will perform pretty poor at location 1 but very well at location 2.

Consequence: The interference pattern is space- and frequency-selective and looks similar to the surface of a pond into which stones have been thrown.

3.3.3.2 Advantageous Use of DSCA

The image already implies that DSCA-use makes sense when the user is moving because good and bad frequencies should be equally distributed as the user moves along the areas where good and bad reception conditions change continuously.

3.3.3.3 Advantageous Use of ASCA

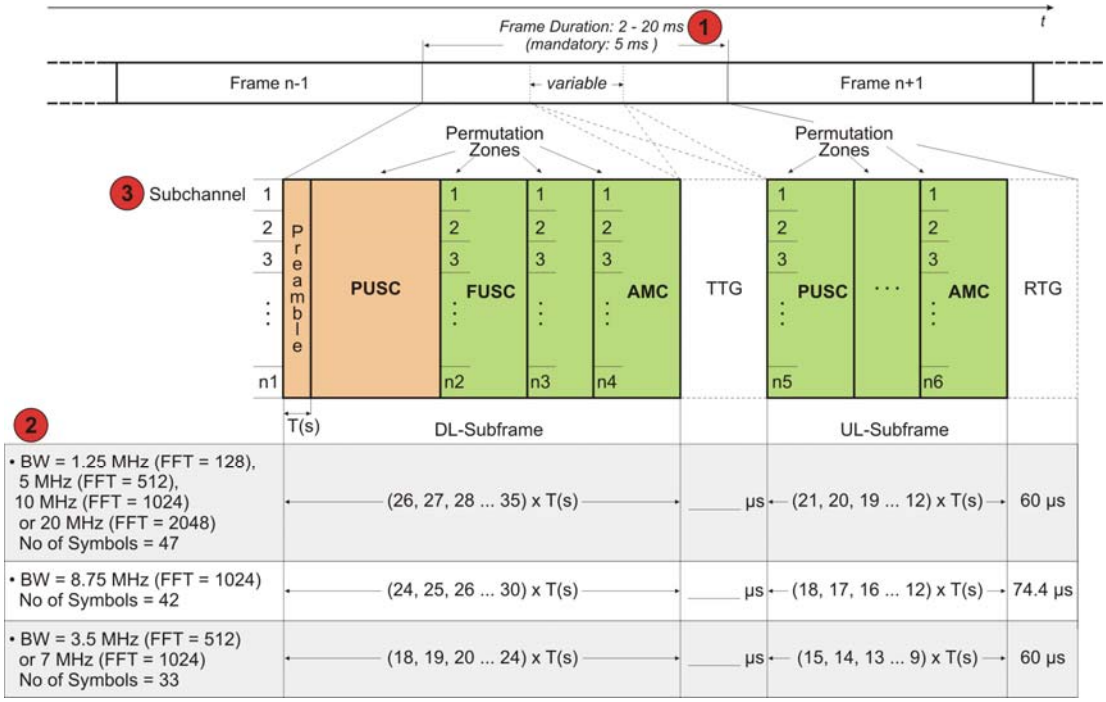
Use of ASCA permutation makes sense when a user is not moving or when beamforming shall be applied.

Room for your Notes

- **Abbreviations of this Section:**

ASCA	Adjacent Subcarrier Allocation	**DSCA**	Diversity / Distributed Subcarrier Allocation
CINR	Carrier to Interference and Noise Ratio	**OFDMA**	Orthogonal Frequency Division Multiple Access

3.4 OFDMA-Frame Structure (TDD)



The objectives of this section are to illustrate the time and subchannel domains of the WIMAX OFDMA-frame and to provide an overview of its internal structure.

Image Description

- The image illustrates at the top three successive OFDMA-frames in TDD-mode.
- The frame N is described in more detail in the lower parts of the image.
- Each OFDMA-frame consists of a downlink and an uplink part. These two parts are termed downlink and uplink subframe.
- The image also illustrates the already introduced RTG and TTG to allow the MS/SS the switch between receive and transmit.
- The different permutation zones are timely aligned inside the two subframes.

3.4.1 Frame Duration and other Time Constraints

The frame duration may vary according to the standard between 2 ms and 20 ms. However, the WIMAX-forum has mandated support for 5 ms frame duration [WIMAX-Forum Mobile System Profile (4.1.1.5)] and therefore all the following parameters are tailored to this overall frame duration.

Please add the missing TTG-values in the image.

Very interesting is the possibility to vary the duration of the individual downlink and uplink subframes within certain limits. These variations are presented in the table at the bottom of the image, depending on the Δf and T(b) of the different bandwidths and FFT-sizes. These variations have been predefined by the WIMAX-forum in [WIMAX-Forum Mobile System Profile (4.1.1.6), (4.1.1.7)].

3.4.2 No of Subchannels

The number of subchannels is variable with the FFT-size and the current permutation scheme and therefore varies even within a single subframe if the permutation changes (see n1, n2, n3 …).

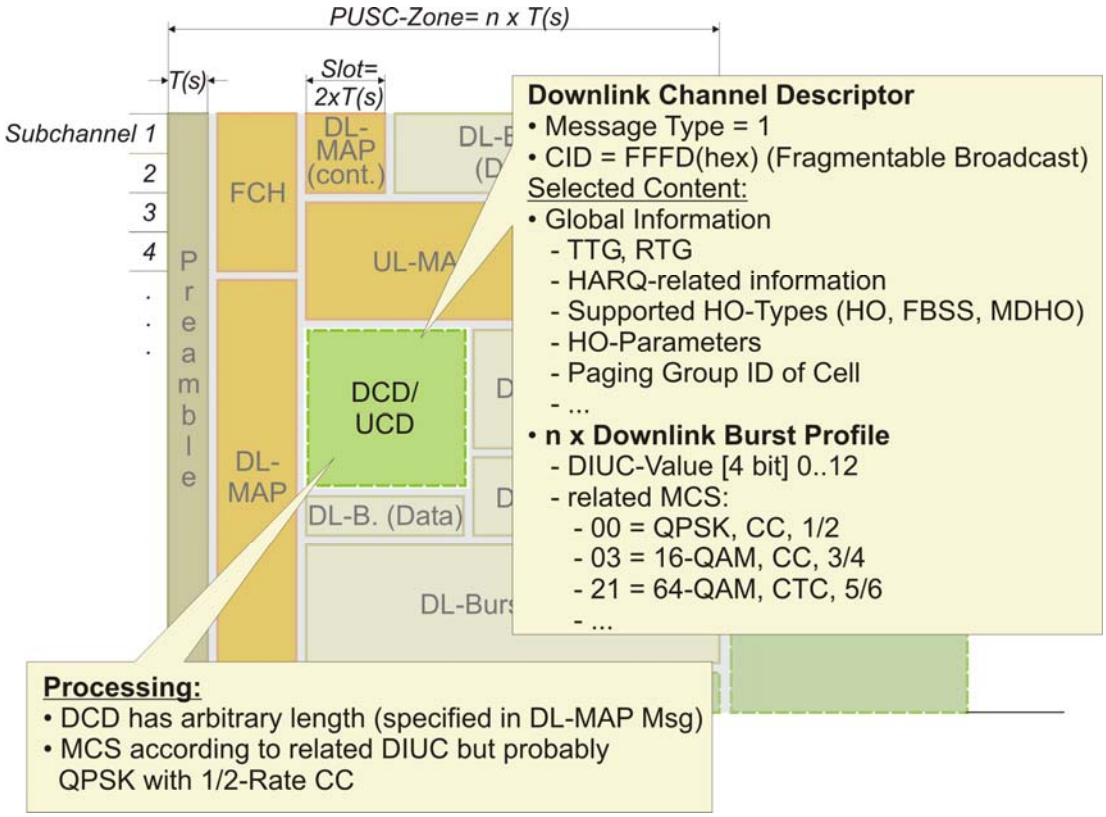
3.4.3 Permutation Zones and Preamble

Each frame may contain different permutation zones but shall start with the DL-PUSC zone. The preamble is necessary for layer 1 synchronization and broadcasts a predefined bit pattern.
There is a maximum of eight different zones within one DL-subframe [IEEE 802.16e-2005 (8.4.4.2)].
Very interesting: Only the PUSC-zone within the DL-subframe is mandatory within the entire frame. Without uplink traffic of any kind, there will be no instance of an UL-subframe.
[IEEE 802.16-2004, IEEE 802.16e-2005 (8.4.6.1.2.2.2)]

- **Abbreviations of this Section:**

AMC	Advanced Modulation and Coding	**RTG**	Receive transmit Transition Gap (IEEE 802.16 (3.45)) the time between an uplink subframe and the subsequent downlink subframe in a TDD-system
BW	Bandwidth	**SS**	Subscriber Station (IEEE 802.16)
FFT	Fast Fourier Transformation	**TDD**	Time Division Duplex
FUSC	Full Usage of Subchannels	**TTG**	Transmit receive Transition Gap (IEEE 802.16 (3.63)) the time between a downlink subframe and the subsequent uplink subframe in a TDD-system
MS	Mobile Subscriber Station (IEEE 802.16e)	**UL**	Uplink
OFDMA	Orthogonal Frequency Division Multiple Access	**WIMAX**	Worldwide Interoperability for Microwave Access (IEEE 802.16)
PUSC	Partial Usage of Subchannels		

4.1.1.3 DCD-Message



The objective of this section is to illustrate the meaning, coding, mapping and content of the DCD-Message.

Key point of this section is that the DCD-message does not occur in every DL-subframe. The maximum time between consecutive DCD-messages (and UCD-messages) is 10 s.

Image Description
The image repeats the presentation of the DL-subframe but emphasizes the content and processing of the DCD-Message.

[IEEE 802.16e-2005 (6.3.2.3.1), (11.4)]

4.1.1.3.1 Header Section

- The DCD-message represents a regular MAC-management message with a normal header section.
- The CID inside a DCD-message shall be FFFD(hex).

4.1.1.3.2 Content

The content of the DCD-message can roughly be separated into two parts: global information and downlink burst profiles.

4.1.1.3.2.1 Global Information

This information relates to downlink related broadcast information that is important for all mobiles operating in a cell [IEEE 802.16e-2005 (6.3.2.3.1), (11.4.1)]. In addition to the indicated parameters the DCD-message contains among others an identification of the DL-center frequency and of the overall frame length (5 ms).

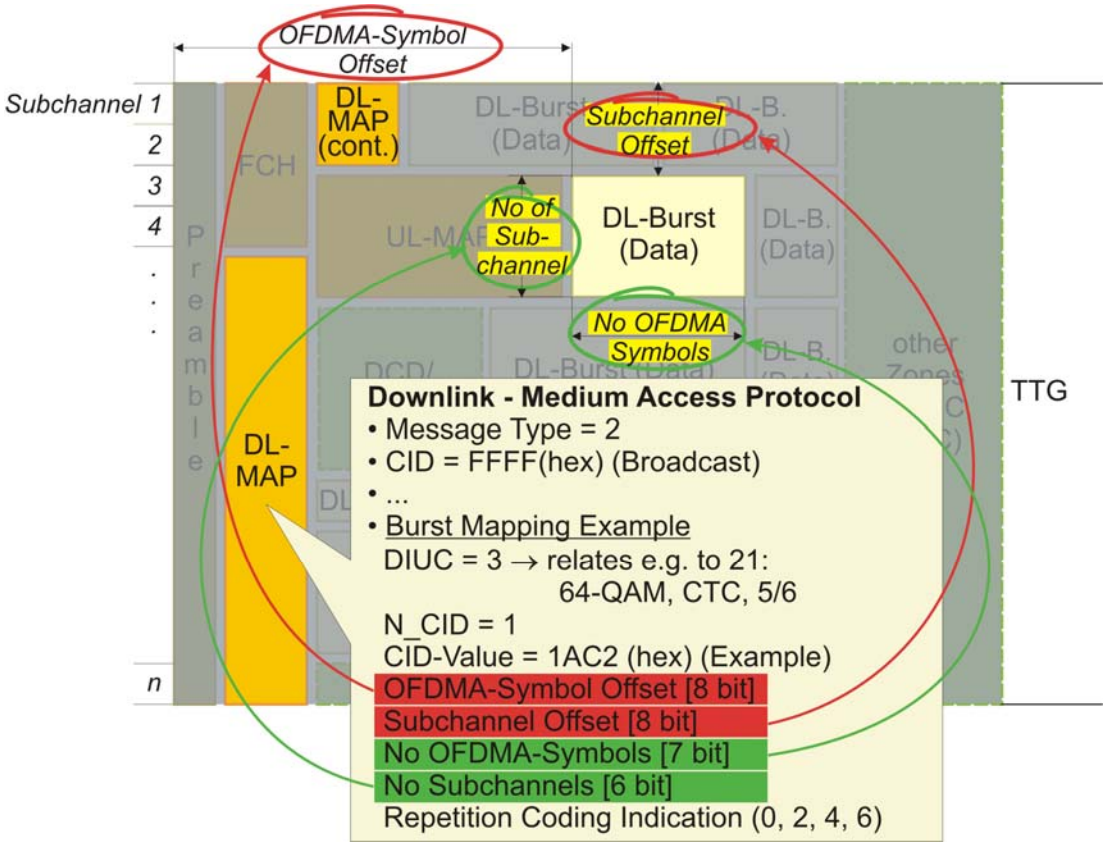
4.1.1.3.2.2 Downlink Burst Profiles

The downlink burst profiles represent integer pointer values that relate to processing instructions used on downlink bursts. For DL-burst processing, only DIUC-values 0 – 12 are available. These processing instructions relate to modulation scheme (QPSK, 16-QAM or 64-QAM), coding scheme (CC or CTC) and code rate. Various pointer values have been predefined in [IEEE 802.16e-2005 (11.4.2)]. The definition of the downlink burst profiles enables the fast tagging of a DL-burst through a pointer to enable the MS/SS to process that burst. More details will be provided in a subsequent section.

- **Abbreviations of this Section:**

16-QAM	16 symbols Quadrature Amplitude Modulation	**HARQ**	Hybrid ARQ (3GTS 25.212)
64-QAM	64 symbols Quadrature Amplitude Modulation	**MAC**	Medium Access Control
AMC	Adaptive Modulation and Coding	**MCS**	Modulation and Coding Scheme
CC	Convolutional Coding	**MDHO**	Macro-Diversity Handover
CID	Connection Identifier (WIMAX)	**MS**	Mobile Subscriber Station (IEEE 802.16e)
CTC	Convolutional Turbo Coding	**PUSC**	Partial Usage of Subchannels
DCD	Downlink Channel Descriptor (WIMAX Message)	**QPSK**	Quadrature Phase Shift Keying
DIUC	Downlink Interval Usage Code (WIMAX Term)	**RTG**	Receive transmit Transition Gap (IEEE 802.16 (3.45)) the time between an uplink subframe and the subsequent downlink subframe in a TDD-system
DL-MAP	Downlink-Medium Access Protocol (MAC-Message in WIMAX / IEEE 802.16)	**SS**	Subscriber Station (IEEE 802.16)
FBSS	Fast Base Station Switching	**TTG**	Transmit receive Transition Gap (IEEE 802.16 (3.63)) the time between a downlink subframe and the subsequent uplink subframe in a TDD-system
FCH	Frame Control Header	**UCD**	Uplink Channel Descriptor (WIMAX Message)

4.2 Resource Allocation in DL-Direction



The objective of this section is to illustrate how the burst mappings within the DL-MAP-message are used for downlink resource allocation.

DL-allocations are always rectangular regions. During normal operation, MS's and SS's shall listen to all DL-MAP-messages to detect DL-resource allocations for themselves.

Image Description
The image illustrates again the already known DL-subframe but emphasis is on the allocation of the yellow DL-burst to a specific user through the burst mapping example [IEEE 802.16e-2005 (8.4.5.3)].

4.2.1 Burst Mapping Example
The image illustrates one example how the allocation may look like.

4.2.1.1 DIUC-Allocation

The DIUC-allocation tells the MS how the data has been processed inside the BS. In the example, DIUC = 3 relates through DCD-mapping e.g. to burst profile 21 with 64-QAM modulation etc. [IEEE 802.16e-2005 (11.3.1)].

4.2.1.2 CID-Relation

Within a given burst mapping, the MS will search for one of its own CID-values to understand whether it must process the respective DL-burst.

The example illustrates that the burst mapping allows for one burst mapping to be related to several CID's, e.g. in case of multicast (N_CID > 1). However, multicast may also be achieved through multicast CID's. Please refer to section 5.2.2.3.

4.2.1.3 Definition of Frequency and Time Dimension

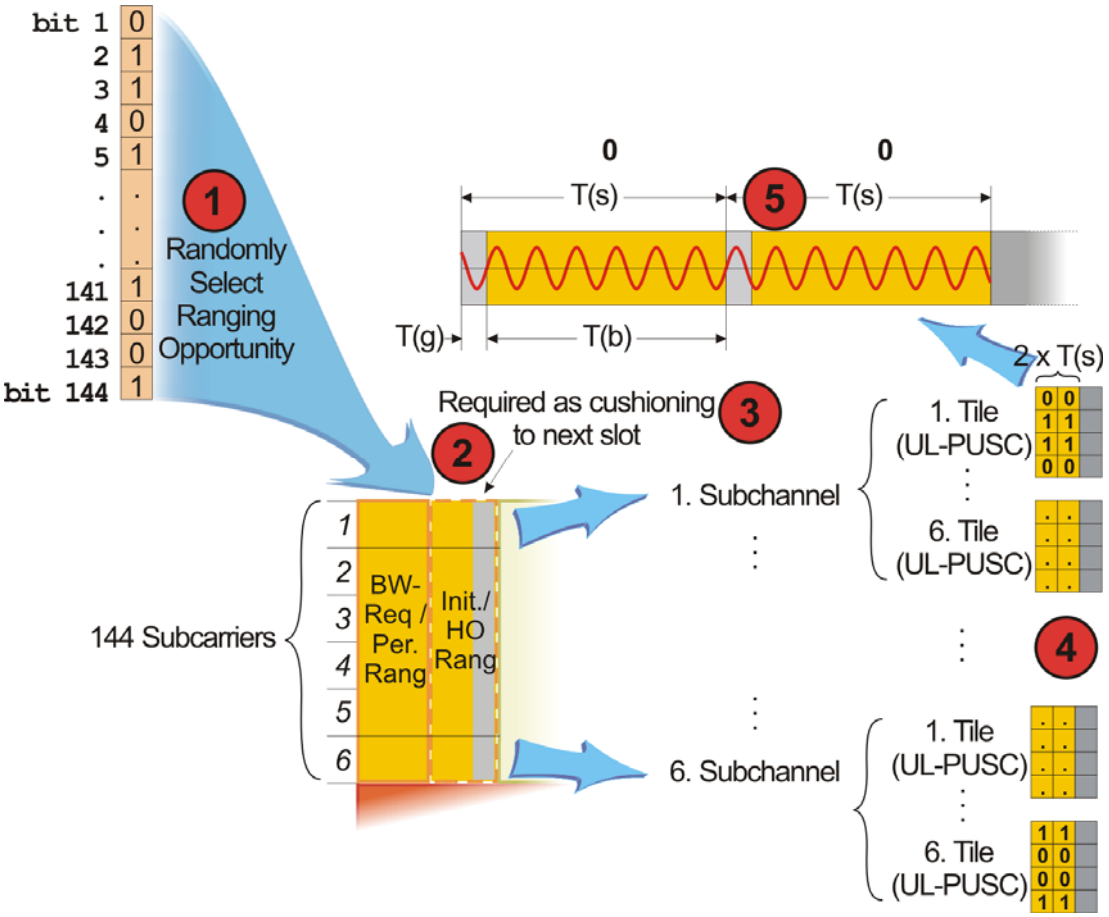
The actual resource allocation is done by:

1. Pointing to the start of an allocation through an "OFDMA-symbol offset"-value (for time dimension) and a "subchannel offset"-value (for the frequency dimension). These values are highlighted in red color.
2. Scaling the allocation through the green highlighted parameters "No of OFDMA-symbols" and "No of Subchannels" which together unambiguously identify a region inside the DL-subframe.

- **Abbreviations of this Section:**

64-QAM	64 symbols Quadrature Amplitude Modulation	**FCH**	Frame Control Header
AMC	Adaptive Modulation and Coding	**MS**	Mobile Subscriber Station (IEEE 802.16e)
BS	Base Station (IEEE 802.16)	**OFDMA**	Orthogonal Frequency Division Multiple Access
CID	Connection Identifier (WIMAX)	**QAM**	Quadrature Amplitude Modulation
CTC	Convolutional Turbo Coding	**TTG**	Transmit receive Transition Gap (IEEE 802.16 (3.63)) the time between a downlink subframe and the subsequent uplink subframe in a TDD-system
DCD	Downlink Channel Descriptor (WIMAX Message)	**UCD**	Uplink Channel Descriptor (WIMAX Message)
DIUC	Downlink Interval Usage Code (WIMAX Term)	**UL**	Uplink
DL-MAP	Downlink-Medium Access Protocol (MAC-Message in WIMAX / IEEE 802.16)		

4.4.4.3 Mapping of Ranging Codes to Ranging Opportunities



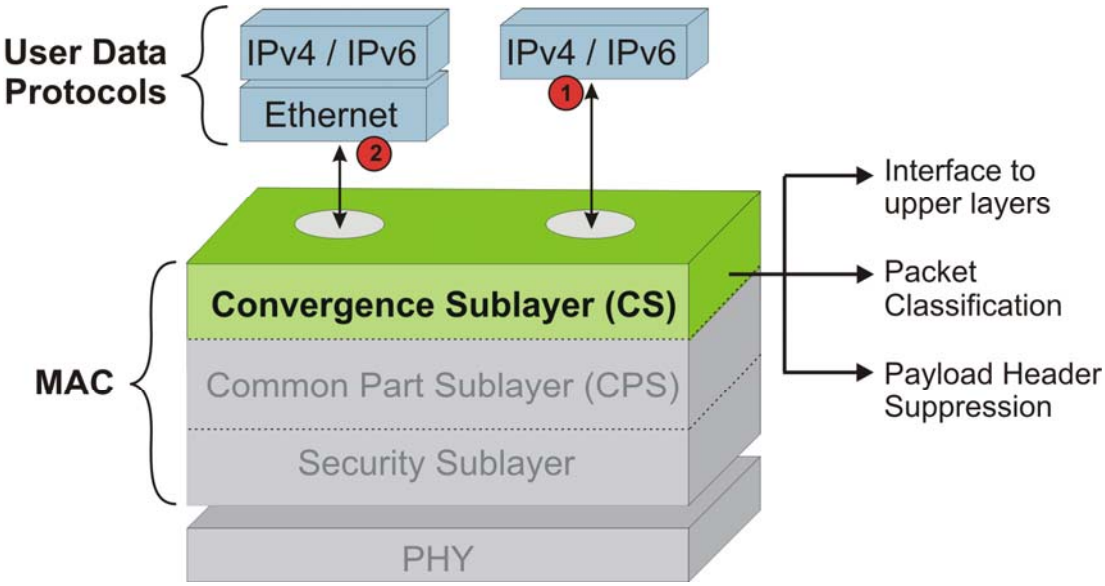
The objective of this section is to illustrate how a randomly selected 144 bit long initial ranging code is mapped to a ranging opportunity.

Image Description

- The image illustrates how an MS maps an initial ranging code to a ranging subchannel which consists itself of 6 subchannels (each with 6 x 4 subcarriers).
- In the second step, the image illustrates how the 144 bit are mapped to the 6 x 6 x 4 = 144 subcarriers.
- In case of initial ranging, the same ranging code shall be sent in two consecutive symbols which is illustrated through the sine waves at the right top of the image.

5.2 The MAC-Layer of IEEE 802.16e

5.2.1 Tasks and Functions



The objectives of this section are to illustrate the relations of the MAC-CS and to introduce its tasks and functions.

Image Description

- The image illustrates the center part of the WIMAX-protocol stack within the MS or the BS.
- The top part illustrates which user application protocols are supported by WIMAX according to [WIMAX-Forum Mobile System Profile (5.1.2)].

1
- Support for both IPv4 and IPv6 is mandatory.

2
- Support for Ethernet (IEEE 802.3) and VLAN-tagging and its interpretation (IEEE 802.1P/Q) are optional.

5.2.1.1 Convergence Sublayer (MAC-CS)

The tasks and functions of the MAC-CS are listed and described in the following text. [IEEE 802.16-2004 (5.2)]

5.2.1.1.1 Packet Classification

Packet classification is typically based on IP-addresses and port numbers. Through packet classification incoming PDU's can be assigned to the appropriate service flows.

5.2.1.1.2 Payload Header Suppression (PHS)

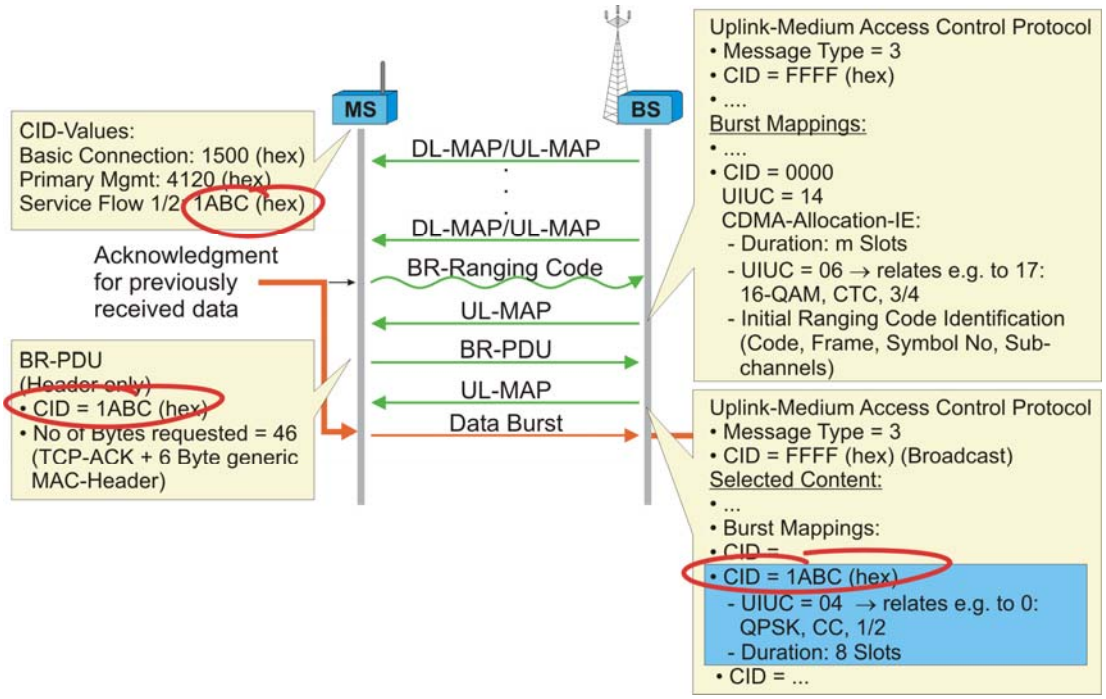
PHS is mandatory according to [WIMAX-Forum Mobile System Profile (5.1.1)]

Room for your Notes

- **Abbreviations of this Section:**

BS	Base Station (IEEE 802.16)	**MS**	Mobile Subscriber Station (IEEE 802.16e)
IEEE	Institute of Electrical and Electronics Engineers	**PHS**	Payload Header Suppression (IEEE 802.16)
IPv4	Internet Protocol (version 4)	**PHY**	Physical Layer
IPv6	Internet Protocol (version 6)	**VLAN**	Virtual LAN
MAC	Medium Access Control	**WIMAX**	Worldwide Interoperability for Microwave Access (IEEE 802.16)

5.2.7.2.1 Data to be transferred in UL-Direction



The objective of this section is to continue the presentation of the previous section, assuming that the MS intends to send a TCP-ACK as acknowledgment of the previous DL-data transfer.

Key point of this section is that uplink data transfer takes tendentiously more time to begin, because the MS has to start from BR-ranging if no uplink resources are currently active.

Image Description

- Consider that the image continues the presentation from the previous section.
- All DL-data has been transferred and is currently processed within the MS or beyond.
- Therefore, the MS fell back to listening to the downlink broadcast messages.
- Eventually, the MS receives a TCP-ACK (40 Octets) from its application. Of course, for the MS these are simply 40 Octets worth of UL-data to be transmitted.
- As before, the MAC-CS determines the respective CID (again 1ABC(hex)) based on the aforementioned packet classification rules.
- Since there are no UL-resources allocated to that MS at this time, the MS has to pick one ranging slot and code and transmit it to the BS.

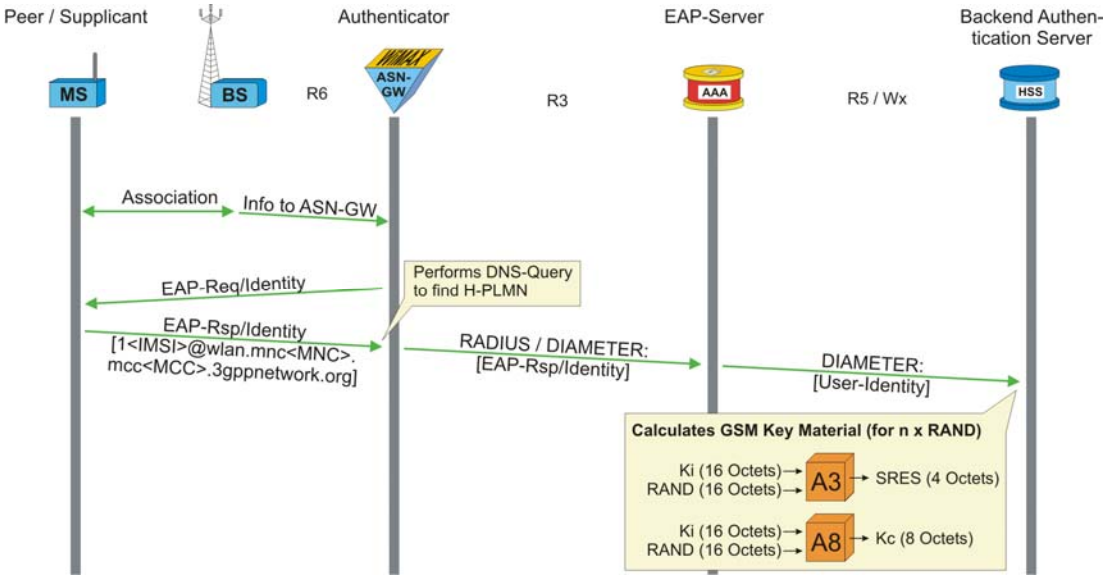
- Provided that the BS properly received the BR-code, it will use the UL-MAP-message to allocate enough uplink resources to the MS so that it can transmit a BR-PDU to the BS, indicating CID and number of resources required.
- Note that this allocation is related to CID = '0000' (initial ranging) but identifies the MS based on used BR-code and time parameters.
- Now the MS transmits the BR-PDU to the BS which identifies the CID to which the BR pertains and it identifies the number of octets to be transmitted (46 Octets = TCP-ACK (40 Octets) + Generic MAC Header (6 Octets)).
- The BS responds with a second UL-MAP allocation but in this case, the BS identifies the MS with the CID ('1ABC'(hex)) which was included in the BR-PDU.
- The MS processes the TCP-ACK according to the requested coding scheme and modulation and transmits it in the related UL-burst.

Room for your Notes

- **Abbreviations of this Section:**

16-QAM	16 symbols Quadrature Amplitude Modulation	**DL-MAP**	Downlink-Medium Access Protocol (MAC-Message in WIMAX / IEEE 802.16)
BR	Bandwidth Request (WIMAX Term)	**MAC**	Medium Access Control
BS	Base Station (IEEE 802.16)	**MS**	Mobile Subscriber Station (IEEE 802.16e)
CC	Convolutional Coding	**PDU**	Protocol Data Unit or Packet Data Unit
CDMA	Code Division Multiple Access	**QAM**	Quadrature Amplitude Modulation
CID	Connection Identifier (WIMAX)	**QPSK**	Quadrature Phase Shift Keying
CS	Convergence Sublayer	**TCP**	Transmission Control Protocol
CTC	Convolutional Turbo Coding	**UIUC**	Uplink Interval Usage Code (WIMAX Term)

6.2 EAP-SIM-Procedure



The objective of this section is to illustrate how EAP-SIM-based mutual authentication and key generation [RFC 4186] are performed between an MS with SIM-card and a 3GPP-AAA server that is termed EAP-server.

The key point of this section is that the MS selects EAP-SIM authentication by prefixing a '1' in front of its user identity (⇔ "1<IMSI>@wlan.mnc<MNC>.mcc<MCC>. 3gppnetwork.org).

6.2.1 Initial Conditions

- The MS has no own security means and depends on the SIM-card of the user (no USIM).

6.2.2 Applicability of this Procedure

- The presented EAP-SIM-procedure applies in different cases; The presented procedure is related to "I-WLAN Direct IP-Access".

6.2.3 Detailed Description

- The mobile station initially associates with the WIMAX BS. The related messages are illustrated in section 6.1.
- In the presented case the BS relays an EAP-Request/Identity-message from the ASN-GW through PKMv2-messaging to retrieve the mobile station's NAI (its user identity).

- To relay its NAI to the ASN-GW, the mobile station embeds its NAI (⇔ 1<IMSI>@wlan.mnc<MNC>.mcc<MCC>.3gppnetwork.org) into an EAP-Respone/Identity-message which in turn is embedded into a PKMv2-message
- An example of such an NAI is:
  1262033110005936@wlan.mnc03.mcc262.3gppnetwork.org.

The presented example includes the string “wlan” which directly translates into the mobile station’s selection to using the “I-WLAN Direct IP-Access” option.
Other NAI-formats exist to indicate GAN/UMAN-access or “I-WLAN 3GPP IP-Access”.
The 3GPP-network acts in this case as H-CSN.

- **Abbreviations of this Section:**

AAA	Authorize Authenticate Answer (DIAMETER message type)	**MCC**	Mobile Country Code
ASN	Access Service Network	**MNC**	Mobile Network Code
ASN-GW	Access Service Network-Gateway	**MS**	Mobile Subscriber Station (IEEE 802.16e)
BS	Base Station (IEEE 802.16)	**NAI**	Network Access Identifier (RFC 2486)
CSN	Connectivity Service Network	**PKMv2**	Privacy Key Management Version 2
DNS	Domain Name System	**PLMN**	Public Land Mobile Network
EAP	Extensible Authentication Protocol (RFC 3748)	**RADIUS**	Remote Authentication Dial In User Service (RFC 2865)
EAP-AKA	Extensible Authentication Protocol method for 3rd generation Authentication and Key Agreement (RFC 4187)	**RAND**	Random Number
EAP-SIM	Extensible Authentication Protocol method for gsm Subscriber Identity Module (RFC 4186)	**SIM**	Subscriber Identity Module
GAN	Generic Access Network	**SLF**	Subscriber Locator Function
GSM	Global System for Mobile Communication	**SRES**	Signed Response
H-PLMN	Home PLMN	**UMAN**	Unlicensed Mobile Access Network
HSS	Home Subscriber Server (3GTS 23.002). HSS replaces the HLR with 3GPP Rel. 5	**USIM**	Universal Subscriber Identity Module (3GTS 31.102)
I-WLAN	Interworking WLAN (Wireless Local Area Network) (3GTS 23.234)	**WIMAX**	Worldwide Interoperability for Microwave Access (IEEE 802.16)
IMSI	International Mobile Subscriber Identity	**WLAN**	Wireless Local Area Network (IEEE 802.11)

6.2 EAP-SIM-Procedure

6.2.3 Detailed Description (continued)

- Note that the leading '1' indicates the desire of the MS to use EAP-SIM rather than another procedure like EAP-AKA.
- In the presented case we assume that the WIMAX-ASN is able to connect to the H-PLMN as H-CSN directly but this is not necessarily true in which case the mobile station would need to use a so called "Decorated NAI" rather than a "Root NAI" which we illustrate above.
- With the help of a DNS-server the ASN-GW resolves the NAI into the IP-address of the AAA-server of the H-PLMN of the subscriber.
- In our example, the ASN-GW relays the EAP-Response/Identity-message together with the NAI directly towards a AAA-server within the H-PLMN.
- The AAA-server may need to query the SLF to determine the very HSS that serves this subscriber (only if there is more than one HSS in that PLMN).
- In the next step, DIAMETER-messages are used to retrieve authentication information from the HSS of the subscriber. As illustrated, the HSS selects a sequence of random numbers RAND and uses the specific subscriber key Ki as input for the GSM-security algorithms A3 and A8 to calculate a sequence of SRES- and Kc-values [3GTS 43.020].

Room for your Notes