Products: SMIQ, AMIQ, WinIQSIM™, SMIQK16, AMIQK16

Generating Signals for Wireless LANs, Part I: IEEE 802.11b

Application Note

With Wireless Local Area Networks (WLAN) already entering the mass markets, generating signals to WLAN standards will become increasingly important. Signal sources are needed in R&D (or production) to test RF modules, to evaluate basic receiver functionality or when new designs are being evolved. This Application Note focuses on the most commonly used standard IEEE 802.11b. Topics covered include technical aspects of the physical layers as well as details on configuring available signal sources.

ROHDE&SCHWARZ

Subject to change – Gernot Bauer 8/2002 – 1GP49_1E

Contents

1 Introduction to Wireless LAN Systems

With Wireless LANs already being widely deployed in offices and homes, numerous manufacturers are offering a variety of solutions. There are still several standards competing in the different license exempt bands. Table 1-1 lists the most common standards existing today for wireless LANs. This list is not totally complete. There are also other standards existing such as the work of the Japanese MMAC, Wireless ATMs, and others.

Table 1-1: The established standards for Wireless LANs

Standard	Related Organization	First Rel.	Used Frequency Bands	Spread Techn.	Modulation Technique	Supported Phy. Rates
802.11	IEEE 802 LMSC	1997	2.4 - 2.4835 GHz	FHSS DSSS	4GFSK, 2GFSK DQPSK, DBPSK	2, 1 Mbps 2, 1 Mbps
802.11b	IEEE 802 LMSC	1999	2.4 - 2.4835 GHz	DSSS	CCK PBCC	11, 5.5 Mbps 11, 5.5 Mbps
802.11a	IEEE 802 LMSC	1999	5.15 - 5.35 GHz & 5.725 - 5.825 GHz[1]	OFDM	BPSK, QPSK, 16QAM, 64QAM	6 - 54 Mbps
HIPERLAN/1	ETSI BRAN	1996	5.15 - 5.30 GHz	-	GMSK FSK	23,529 Mbps 1,470 Mbps
HIPERLAN/2	ETSI BRAN	2000	5.15 - 5.35 GHz & 5.470 - 5.725 GHz[2]	OFDM	BPSK, QPSK, 16QAM, 64QAM	6 - 54 Mbps
HomeRF 1.0	HomeRF WG	1999	2.4 - 2.4835 GHz	FHSS	FSK	1.6, 0.8 Mbps
HomeRF 2.0	HomeRF WG	2000	2.4 - 2.4835 GHz	FHSS	FSK	10, 5 Mbps
Bluetooth	Bluetooth SIG	1999	2.4 - 2.4835 GHz	FHSS	GFSK	1 Mbps

As this is an Application Note on signal generation, we will mainly focus on the physical layers of the standards listed above and how to create compatible signals.

Section 2 gives details on the implementation of the 802.11 and 802.11b physical layers. Devices compatible with 11b are already provided by numerous manufacturers. 802.11b, also known under the brand name Wireless Fidelity (Wi-Fi) is the most wide-spread technique today.

Section 3 describes how to create 802.11 and 11b signals with WinIQSIM™[3]. Setups for the basic receiver tests as well as some more sophisticated examples are discussed.

Part Two of this Application Note [6] (which will be published in the near future) concentrates on the 11a extension to the 802.11 standard. Although 11a was completed before 11b, equipment development has taken longer due to its higher technical complexity and also because of the introduction of a new modulation format, incompatible with 11 and 11b. 11a products are just starting on the market these days.

In parallel to the standards defined by IEEE, ETSI gave life to the Broadband Radio Access Network (BRAN) project and developed the HIPERLAN/1 standard. Although this standard and related products have already been available for a number of years, it has not gained substantial market importance. With the introduction of HIPERLAN/2 and 802.11a products in the 5 GHz band, it is like

[1] The frequency bands given for the 802.11a standard are valid for the U.S., usable bands in other regions may differ.

[2] The frequency bands given for the HIPERLAN/2 standard are valid for Europe, usable bands in other regions may differ.

[3] WinIQSIM™ is a trademark of Rohde & Schwarz GmbH & Co. KG

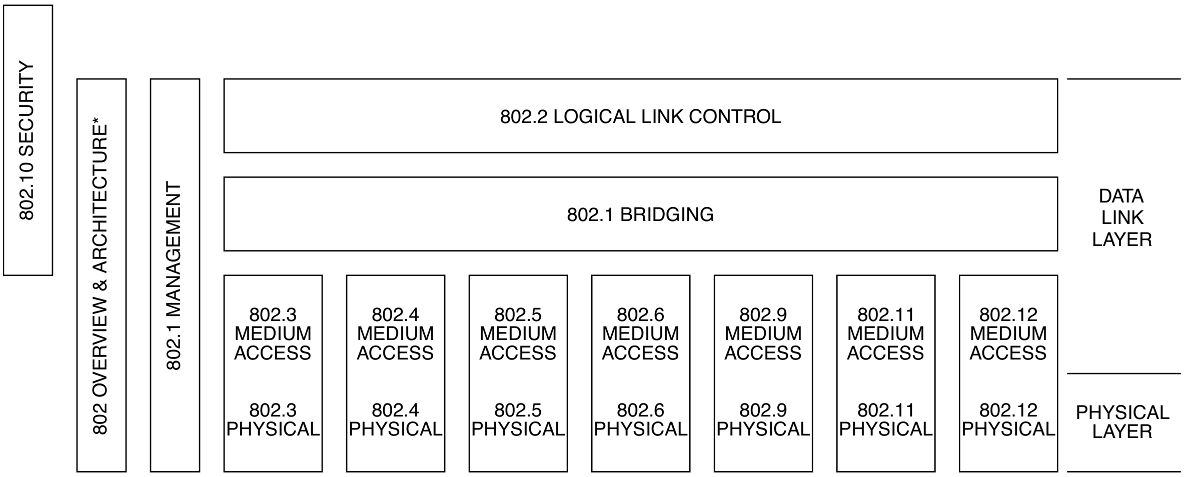
to play only a minor role in the future. We will therefore not cover this standard. The HIPERLAN/2 system also seems to be failing to gain really substantial industry support, with lots of manufacturers supporting 802.11a rather than HIPERLAN/2. Therefore we will discuss HIPERLAN/2 only briefly in Part Two of this Application Note.

Additionally to the work presented by official standardization bodies, the HomeRF™ working group is also promoting products running in the 2.4 GHz band. Devices are already available in the market and competing with Wi-Fi products. In terms of quantity 11b has already overtaken HomeRF™ SWAP products, and due to the much smaller industry support it is unclear whether this standard will succeed in competing with 11b. We therefore will not cover HomeRF™ in this publication.

And finally we also want to mention Bluetooth™. It has been included in Table 1-1 for comparison, although it is considered to be a wireless Personal Area Network (PAN) instead of a LAN. *Bluetooth* products are designed to operate in different user segments, with small, low power handheld devices as the main operating target. For information on how to create *Bluetooth* signals, please refer to Application Notes 1GP38 [7] and 1GP48 [8].

2 The IEEE 802.11 and 11b Standards

In 1990 the IEEE LAN MAN Standards Committee (LMSC) formed the working group 802.11 to develop a wireless networking standard. The first release of the base standard was available in 1997, which covers the definition of the LAN system architecture, the services as well as the Medium Access Control (MAC) protocol and three different physical layers.



* Formerly IEEE Std 802.1A.

Figure 2-1: Relationship between 802 standard family members

In Figure 2-1 the different standard members and its relationship are shown. The most used one today is surely the 802.3, which is the basis for all Ethernet products. All 802 members have different MAC definitions and one or more different physical layers. Any member can use the same Logical Link Control (LLC) protocol 802.2.

When work on the base standard 802.11 was finished, three different physical transmission methods have been specified; a Frequency Hopping Spread Spectrum (FHSS) mode working in the 2.4 GHz ISM band, a Direct Sequence Spread Spectrum (DSSS) mode also for the 2.4 GHz band and an infrared transmission method. The DSSS system and its higher rate extension developed by task group B will be discussed in section 2.1. We will not cover the FHSS mode in this document, as it has never been developed further and still only provides basic data rates of 1 and 2 Mbps. Its significance is expected to decrease with the new high rate modes being introduced. We will also not discuss the infrared transmission method. It is clear that the propagation characteristics of light make it difficult for a widespread LAN to be deployed. Also this mode only allows for transmission at 1 and 2 Mbps.

The 802.11 base standard also defines the MAC protocol layer, which is identical for all different physical layers defined in 802.11 or any of the supplements. To enable the common MAC access to the numerous physical layers - which can be completely incompatible between each other - a Physical Layer Convergence Protocol (PLCP) sublayer has been defined for each Physical Medium Dependent (PMD) sublayer, which in turn provides the radio transmission interface. We will discuss the MAC briefly in section 2.2.

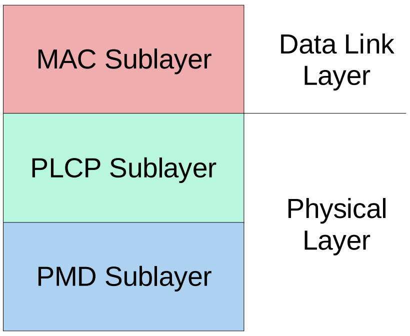


Figure 2-2: Layers defined in the 802.11 standard

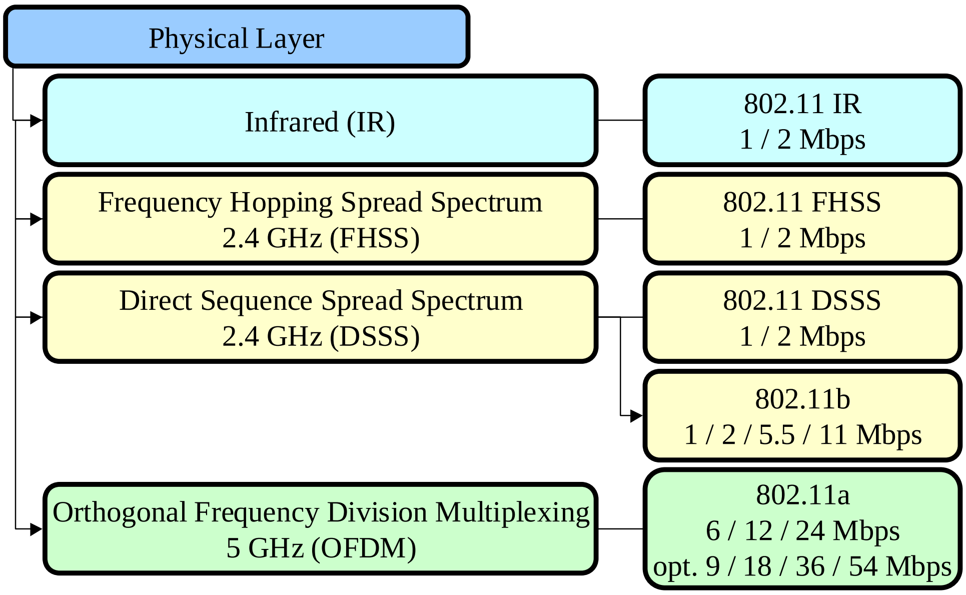


Figure 2-3: The physical layers of 802.11, 11a and 11b

2.1 The 802.11 and 11b PHY

In this section we will go into the details of one of the basic physical layers of the 802.11 standard, the Direct Sequence Spread Spectrum (DSSS) system, defined in [1], chapter 15. This DSSS mode for the 2.4 GHz ISM band has been developed further by task group B into the 802.11b standard, which is backwards compatible with the original DSSS mode of the 802.11 base standard and adds 2 additional higher rate modes. When discussing the PHY modes, we will not differ between 802.11 DSSS and 802.11b, as the 11b also incorporates the original mode.

2.1.1 Defined Transmission Methods

The transmission mode for 11b has four defined data speeds: 1, 2, 5.5 and 11 Mbps. The 1 and 2 Mbps modes have already been set up in the original 802.11 DSSS mode. All modes use direct sequence spread spectrum with a chip rate of 11 Mcps, occupying a bandwidth of about 22 MHz. Channel spacing has been set to 25 MHz for non-overlapping channels.

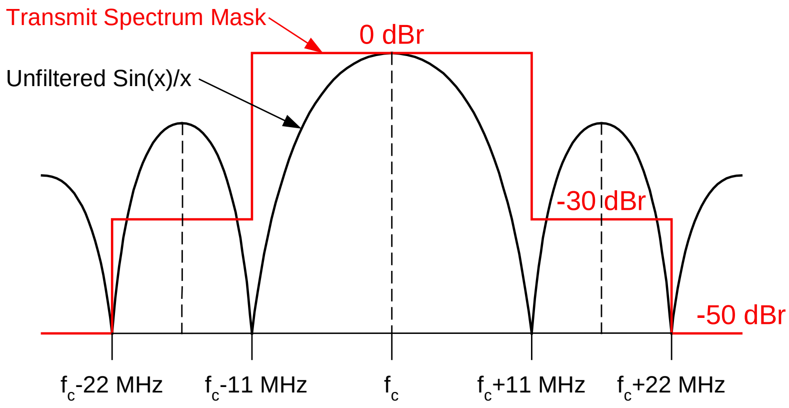


Figure 2-4: Spectrum mask requirements for a DSSS signal

The standard does not prescribe a defined baseband filter, instead a spectrum mask requirement is given which must be fulfilled indirectly by the used filter. The measurements which need to be done to verify the mask shown in Figure 2-4 require a spectrum analyzer with resolution and video bandwidth set to 100 kHz. The given limits are valid for all possible transmission speeds.

Before modulation and spreading, the data coming from the PLCP sublayer (see section 2.1.2) has to be scrambled ([3], section 18.2.4).

2.1.1.1 Low Rate Modulation with Barker Spreading

The scrambled data bits are DBPSK modulated in the 1 Mbps mode and DQPSK modulated in the 2 Mbps mode. The differential phase encoding definitions can be seen in Table 1-1, whereby positive values rotate counterclockwise.

Table 2-1: Phase encoding tables for DBPSK (left) and DQPSK (right)

Bit input	Phase change
0	0
1	π

Dibit pattern (d0, d1) (d0 is first in time)	Phase change
00	0
01	π/2
11	π
10	3π/2 (–π/2)

After modulation, the complex symbols are spread with the following 11 chip Barker sequence, reading left to right:

+1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1

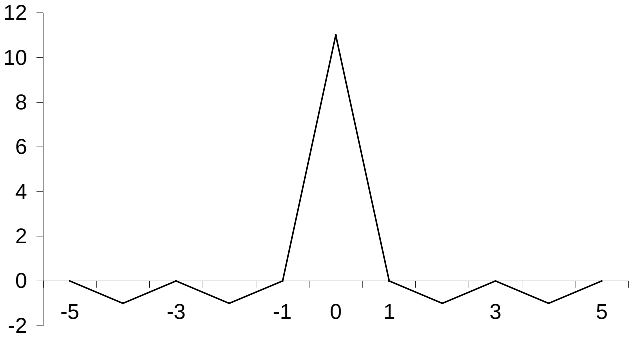


Figure 2-5: The 11 Chip Barker code autocorrelation function

This Barker code has good autocorrelation properties, shown in Figure 2-5. As energy on the sidelobes is very low, the receiver can concentrate on decoding the center peak only. This results in a high immunity of the system to multipath interference and collisions with other DSSS signals. Multipath reception will produce additional peaks in the correlation function. As long as these peaks do not get close to the center, their interference will be ignored. That means multipath delays between 1 and 10 chips (90.9 ns to 909 ns) are not of concern. Assuming a propagation speed of $3{\cdot}10^8$ m/s this will result in a path difference of about 27 to 272 meters. Lower values need to be dealt with using other measures, e.g. antenna diversity.

If the receiver has already synchronized on the center peaks of the Barker codes, any collisions with other frames, even if they are received with the same power will also be ignored, assumed that the spreading code centers of the transmissions will not overlap.

With a code length of 11, this method results in a spreading gain of 10.4 dB. That means all interference, such as microwave oven emissions, are attenuated by this factor. Note that this spreading method is different than the one used in CDMA communication systems, where multiple users overlap with different codes. Here only one code is used by all stations.

2.1.1.2 High Rate CCK Modulation

For the higher rate transmission speeds, two methods have been defined: Complementary Code Keying (CCK) and Packet Binary Convolutional Coding (PBCC). With CCK modulation, 8 chips form a CCK symbol, whereby the nominal chip rate of 11 Mcps is maintained. This yields a symbol rate of 1.375 Msps. The CCK words are based on orthogonal subsets of the code [+1, +1, +1, -1, +1, +1, -1, +1] and are derived by:

$$c = \{e^{j(\varphi_1+\varphi_2+\varphi_3+\varphi_4)}, e^{j(\varphi_1+\varphi_3+\varphi_4)}, e^{j(\varphi_1+\varphi_2+\varphi_4)},$$

$$-e^{j(\varphi_1+\varphi_4)}, e^{j(\varphi_1+\varphi_2+\varphi_3)}, e^{j(\varphi_1+\varphi_3)}, -e^{j(\varphi_1+\varphi_2)}, e^{j\varphi_1}\}$$

The resulting phases of the 8 chips can also be written as:

$$\begin{bmatrix}\theta_1\\\theta_2\\\theta_3\\\theta_4\\\theta_5\\\theta_6\\\theta_7\\\theta_8\end{bmatrix} = \begin{bmatrix}1&1&1&1\\1&0&1&1\\1&1&0&1\\1&0&0&1\\1&1&1&0\\1&0&1&0\\1&1&0&0\\1&0&0&0\end{bmatrix}\begin{bmatrix}\varphi_1\\\varphi_2\\\varphi_3\\\varphi_4\end{bmatrix}$$

This is a form of the generalized Hadamard encoding. φ_1 is added to all chips and rotates the whole symbol. φ_2 is added to all odd chips, φ_3 to all odd pairs of chips and φ_4 to all odd quads of chips. The last chip c7 is indicating the symbol's phase.

The four phases are encoded differently in the 5.5 Mbps and 11 Mbps modes. At 5.5 Mbps, 4 data bits are mapped to one symbol, where at 11 Mbps 8 bits encode one symbol. At both modes, the first two bits of each set encode φ_1 with DQPSK (see Table 2-2), whereby all odd symbols get an extra 180° rotation.

Table 2-2: DQPSK encoding of φ_1

Dibit pattern (d0, d1) (d0 is first in time)	**Even symbols phase change**	**Odd symbols phase change**
00	0	π
01	π/2	3π/2 (–π/2)
11	π	0
10	3π/2 (–π/2)	π/2

The remaining three phases allow 64 possible CCK code words, which are nearly orthogonal by definition. For the 5.5 Mbps mode, we only take 4 of the 64 possible combinations, which have superior coding distance. This results in the remaining two data bits encoding the phases 2 to 4 as follows:

$\varphi_2 = (d2 \bullet \pi) + \pi/2$, $\varphi_3 = 0$, and $\varphi_4 = d3 \bullet \pi$

At 11 Mbps, all 64 CCK words are used by QPSK encoding the phases 2 to 4 with pairs of the remaining 6 data bits.

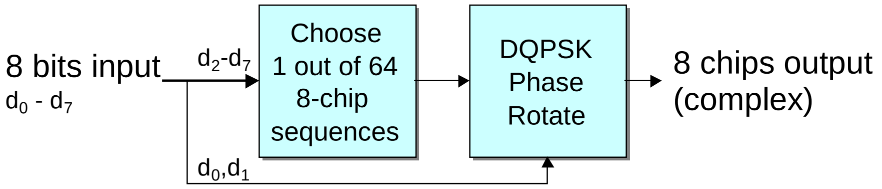


Figure 2-6: Data bit to chip mapping in the 11 Mbps CCK mode.

The overall spreading gain of the CCK modulation equals 11 dB, but transmission ranges are lower than with the Barker spreading method. The CCK method introduces some coding gain, as the E_s/N_0 needed for a correct reception of a code word is lower than that needed if all single chips had to be received correctly.

In multipath environments, CCK sustains delay spreads of up to 100 ns at 11 Mbps and 250 ns at 5.5 Mbps.

2.1.1.3 High Rate PBCC Modulation

For the two higher rates, an additional mode called Packet Binary Convolutional Coding (PBCC) has been introduced. The PBCC mode uses a convolutional code of rate ½ to reach the necessary coding gain. At 5.5 Mbps, BPSK is used for transmission, therefore mapping one data bit to two output chips. With 11 Mbps, a QPSK modulation transmits two bits of the convolutional code, resulting in one data bit per chip. An additional cover code is applied to the obtained complex symbols.

2.1.2 The PLCP

As the MAC defined in 802.11 is the same for all different physical layers existing or being developed in the future, an additional protocol layer has been introduced to enable access to the different PHYs for the MAC. This layer is called Physical Layer Convergence Protocol (PLCP) and is defined differently for each transmission method.

Basically, the PLCP for the DSSS mode of 11b adds a preamble and a header to the PLCP Service Data Unit (PSDU) coming from the MAC layer. There are two formats possible, the long and the short one (see Figure 2-7 and Figure 2-8). The preamble consists of a SYNC and a SFD field and will be transmitted with 1 Mbps Barker spreading in any case. The SYNC field is compiled of 128 scrambled ones for the long preamble and 56 scrambled zeros for the short preamble. It aids the receiver in synchronizing to the signal. The Start Frame Delimiter (SFD) field provides a 16 bit code to help the receiver determine the correct frame start timing. The short preamble format uses a time inverted variant of the long preamble SFD.

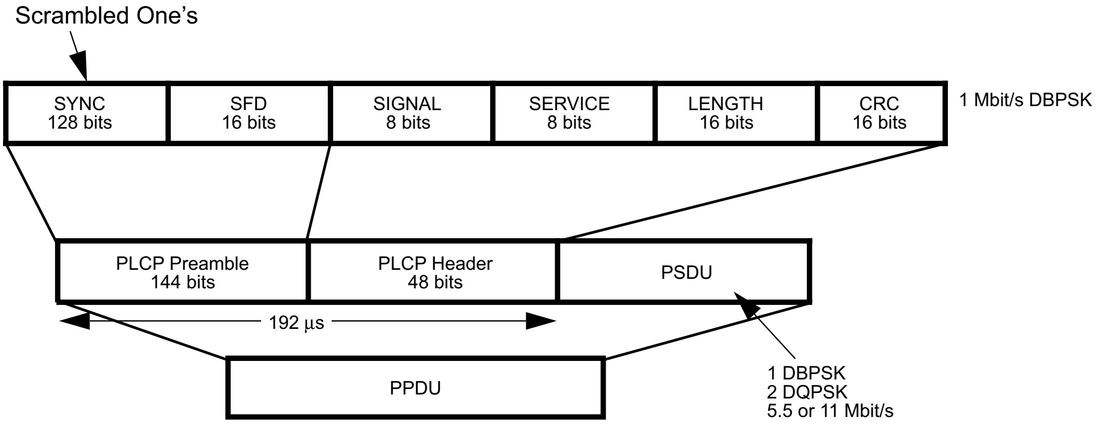


Figure 2-7: The long PLCP PPDU format

The PLCP Header contains 48 bits of information helping the receiver to demodulate the PSDU. The SIGNAL field gives the data rate of the packet's PSDU in 100 kbps steps. The SERVICE field announces the PSDU's modulation as either being CCK or PBCC (for the higher rate modes). It also provides the "Locked clocks bit", which is set when the transmitter's frequency and symbol clocks are locked. The LENGTH field provides the transmission duration of the PSDU in microseconds. Different calculation methods apply for CCK and PBCC, see [3], 18.2.3.5. And finally a CRC is calculated over the header fields.

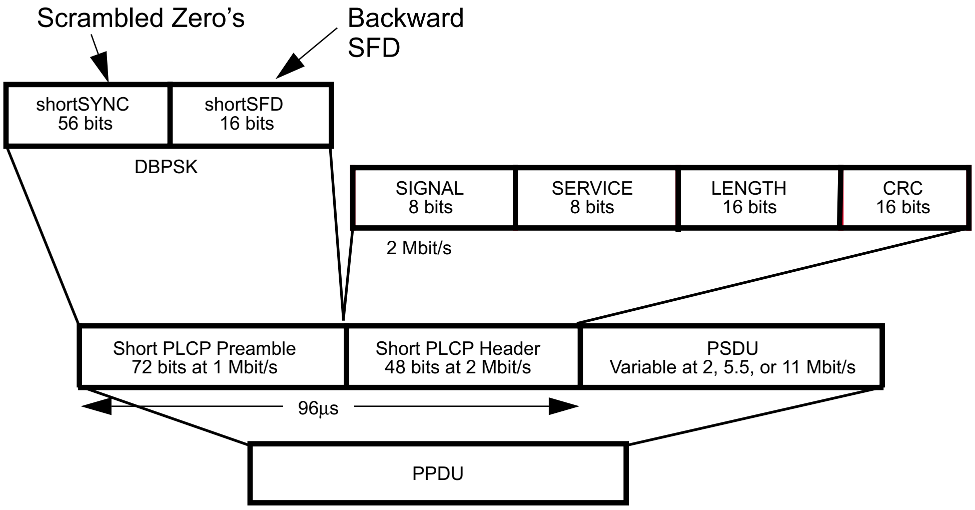


Figure 2-8: The short PLCP PPDU format

The header's content is the same for both the long and short format. The long header is transmitted with 1 Mbps DBPSK, the short one with 2 Mbps DQPSK, both with Barker spreading. The transmission duration of the short PLCP preamble and header format is just half the time of the long format. Devices compatible to the original 802.11 DSSS mode only will not be able to produce or decode the short format.

The following PSDU can then be transmitted on any of the four available data rates with Barker spreading, CCK or PBCC. The long preamble and header format can be combined with any PDSU data rate, the short format is restricted to 2, 5.5 and 11 Mbps.

A complete transmission frame consisting of PLCP preamble, header and PSDU is called PLCP Protocol Data Unit (PPDU).

2.2 The 802.11 MAC

As one might easily imagine, discussing the complete functionality of the MAC layer would be out of proportion for this document. We will therefore concentrate on the different frame formats, which can be found in chapter 7 of [1]. We will need this knowledge when creating such frames in section 3. But studying [1] or an additional reference such as [4] is absolutely necessary for a deeper understanding of the frame exchange procedures.

Figure 2-9 shows the data flow between the protocol layers on the transmission side. The MAC as well as the PLCP provide a transmission service to the next higher layer. On the MAC side, the MAC Service Data Units (MSDUs) are filled with data coming from the LLC. A complete MAC frame with header and Frame Check Sequence (FCS) is known as MAC Protocol Data Unit (MPDU) on the MAC side and will be fed into the PLCP Service Data Unit (PSDU) on the PLCP side. The full frame to be transmitted by the Physical Medium Dependent layer (PMD) is again known as PLCP Protocol Data Unit (PPDU).

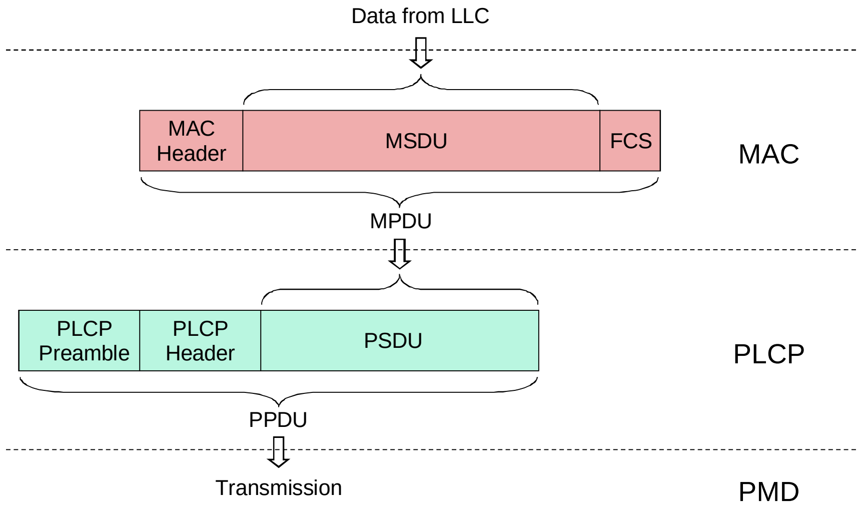


Figure 2-9: Data encapsulation procedure in MAC and PLCP

2.2.1 MAC Frame Formats

As already said, the MAC Protocol Data Units (MPDUs), also called MAC frames, encapsulate the higher layer protocol data or contain MAC management messages.

Octets: 2	2	6	6	6	2	6	0 - 2312	4
Frame Control	Duration/ ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	FCS

MAC Header

Figure 2-10: General MAC frame format

Figure 2-10 displays the general MAC frame format. The fields Address 2, Address 3, Sequence Control, Address 4 and Frame Body are not present in all frame types. We will discuss the meaning of the fields in brief.

Frame Control

B0	B1B2	B3B4	B7 B8	B9	B10	B11	B12	B13	B14	B15
Protocol Version	Type	Subtype	To DS	From DS	More Frag	Retry	Pwr Mgt	More Data	WEP	Order
Bits: 2	2	4	1	1	1	1	1	1	1	1

Figure 2-11: The Frame Control field

The Frame Control field itself is again divided into the subfields displayed in Figure 2-11. The “Protocol Version” field shall always be 0. The valid entries for the fields “Type” and “Subtype” are shown in Table 2-3, which define the actual type of frame.

Table 2-3: Defined frame types

Type value b3 b2	Type description	Subtype value b7 b6 b5 b4	Subtype description
00	Management	0000	Association request
00	Management	0001	Association response
00	Management	0010	Reassociation request
00	Management	0011	Reassociation response
00	Management	0100	Probe request
00	Management	0101	Probe response
00	Management	0110–0111	Reserved
00	Management	1000	Beacon
00	Management	1001	Announcement traffic indication message (ATIM)
00	Management	1010	Disassociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication
00	Management	1101–1111	Reserved
01	Control	0000–1001	Reserved
01	Control	1010	Power Save (PS)-Poll
01	Control	1011	Request To Send (RTS)
01	Control	1100	Clear To Send (CTS)
01	Control	1101	Acknowledgment (ACK)
01	Control	1110	Contention-Free (CF)-End
01	Control	1111	CF-End + CF-Ack
10	Data	0000	Data
10	Data	0001	Data + CF-Ack
10	Data	0010	Data + CF-Poll
10	Data	0011	Data + CF-Ack + CF-Poll
10	Data	0100	Null function (no data)
10	Data	0101	CF-Ack (no data)
10	Data	0110	CF-Poll (no data)
10	Data	0111	CF-Ack + CF-Poll (no data)
10	Data	1000–1111	Reserved
11	Reserved	0000–1111	Reserved

Frames of type Management only contain information for the receiving MAC management entity. Control frames aid in controlling medium access. Data frames contain - as indicated by their name - data from higher protocol layers, but not in all cases. They can either contain only data, combine transmission of data to any station with transmitting control information, contain only Point Coordinator Function (PCF) control information or no data at all. For a deeper understanding of the medium access mechanisms like PCF or Distributed Coordination Function (DCF) please refer to [1], section 9. This knowledge will also be needed for a deep understanding of the details in some of the examples in section 3.

The remaining 8 bits of the Frame Control field contain additional flags. The “To DS” and “From DS” fields indicate whether a frame is intended for the Distribution System (DS) or is originating from it. The “More Fragments” flag will be set to 1 when the current MAC frame is fragmented to several parts and further ones are outstanding. A set “Retry” bit indicates a retransmission of a probably not properly received frame. With the “Power Management” flag the station is indicating its power management status after the frame exchange sequence has been completed. So a set flag indicates that the station will activate its power saving. The “More Data” bit is used to indicate that more outstanding frames are to be transmitted, e.g. to inform a station in power save mode of these buffered frames when it is being polled. The “WEP” flag indicates an applied Wired Equivalent

Privacy (WEP) encryption to the frame body data. The “Order” field is set to 1 whenever the “StrictlyOrdered” service class is used for transmission, that means any reordering of broadcast/multicast frames relative to directed ones is not permitted.

Duration/ID

For most of the frames, the Duration/ID field of the MAC header gives a transmission duration value depending on the transmitted frame type. This value is being used to inform all listening stations of the time needed for transmitting the current MSDU and eventual following ones. This will set the Network Allocation Vector (NAV) in all stations receiving the frame except the one actually addressed. With the NAV the stations know of a busy medium, even if a transmitting node is eventually hidden. This procedure is also known as the virtual carrier-sense mechanism. For a detailed description on the physical and virtual carrier-sense methods please refer to [1], section 9.2.1. The Duration value is set to 32768 during the Contention-Free Period (CFP), when the Point Coordinator (PC) is controlling access of the medium.

In frames of type Power Save Poll, the Duration/ID field carries the Association Identity (AID) of the transmitting station. The 2 most significant bits are set to 1.

Address fields

The four address fields of the MAC header can contain the Basic Service Set Identification (BSSID), the source, destination, transmitting station and receiving station addresses. Note that not all of the frame types use all of the possible address fields.

Sequence Control

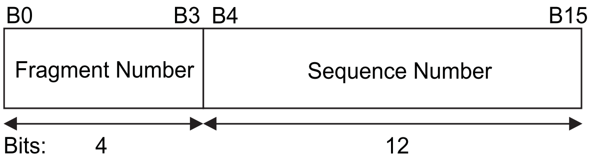


Figure 2-12: Sequence Control field

The Sequence Control field shown in Figure 2-12 contains the Fragment and Sequence Numbers. The Sequence Number starts at 0 and identifies every MSDU with a unique number, but stays the same for all fragments of a frame during fragmented transmission. The Fragment Number counts the fragments, starting at 0. When the transmission of MSDUs is not fragmented, the Fragment Number will always be 0. At retransmission of an MSDU or fragment thereof the whole Sequence Control field will not change.

Frame Body

The Frame Body contains the actual data from the Logical Link Control (LLC) layer, with any length of 0 to 2312 octets.

FCS

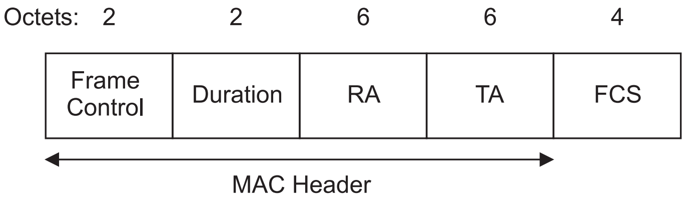
The Frame Check Sequence (FCS) field contains a 32 bit CRC. For calculation details, please refer to [1], section 7.1.3.6.

2.2.2 Some Individual Frame Formats

As can be seen in Table 2-3, the defined MAC frame types are quite numerous. We will therefore only discuss a selection of the most important frame formats.

2.2.2.1 RTS / CTS frames

Exchange of the Request To Send (RTS) and Clear To Send (CTS) packets may considerably improve the performance of the CSMA/CA access method by transmitting the duration of the following data packet and its ACK frame by both the sending and receiving nodes. With the RTS/CTS exchange procedure a fast check of the transmission path is possible, detecting collisions quickly.

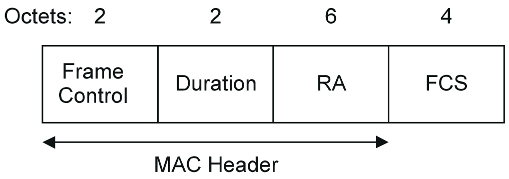


Octets:	2	2	6	6	4
	Frame Control	Duration	RA	TA	FCS

Figure 2-13: The RTS frame format

The Duration value of the RTS frame is set to the transmission duration of the following CTS frame, plus the pending data or management frame, plus the ACK frame plus three Short Interframe Space (SIFS) intervals in microseconds. This will set the NAV of all listening stations accordingly.

The receiver (RA) and transmitter (TA) addresses will be set to the MAC addresses of the receiving and transmitting stations.



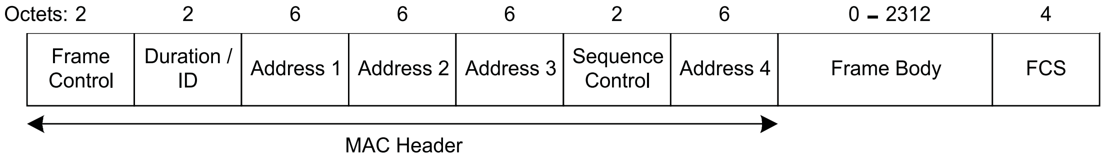
Octets:	2	2	6	4
	Frame Control	Duration	RA	FCS

Figure 2-14: The CTS frame format

The Duration value of the CTS packet is set to the remaining frame exchange duration in microseconds after the CTS packet has been sent, which is the duration of the data or management frame and the ACK frame plus two SIFS periods. This will set the NAVs of all stations listening to the receiver (that is transmitting the CTS packet), which may not be able to receive the original transmitter of the RTS frame.

The RA is set to the receiver of the CTS packet.

2.2.2.2 Data frame



Octets:	2	2	6	6	6	2	6	0 – 2312	4
	Frame Control	Duration / ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	FCS

Figure 2-15: The data frame format

The data frame is intended to transmit data from higher layers. Its Duration value is set to the transmitting duration of the following ACK frame plus one SIFS period, in case of non-fragmented transmission. For fragmented MSDUs, the Duration value will equal to the transmission time of the next fragment, plus two ACK frames, plus three SIFS periods. Data frames always need to be acknowledged. If an acknowledgement is not received, a retransmission needs to be scheduled

The four address fields are set depending on the “To DS” and “From DS” flags of the Frame Control field.

Table 2-4: The data frame address fields

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	1	RA	TA	DA	SA

Address 4 is omitted in the case the “To DS” and “From DS” flags are not both equal to 1. The other fields are set to the Destination Address (DA), Source Address (SA), Transmitter Address (TA), Receiver Address (RA) or Basic Service Set Identity (BSSID).

The Sequence Control field of the frame needs to contain the right sequence and fragment numbers (see 0).

2.2.2.3 ACK frame

As already mentioned, a correctly received data frame needs to be acknowledged. When the DCF is in use, the ACK frame serves this purpose. After receiving a data frame with correct FCS, the receiver needs to send an ACK frame after a SIFS period as a follow-up. Should the received data frame contain errors, sending the ACK frame will be omitted. The original transmitter of the data frame will schedule retransmission of this frame in any case where an ACK frame has not been received correctly or not been received at all. Any station must be able to compensate for duplicate received frames.

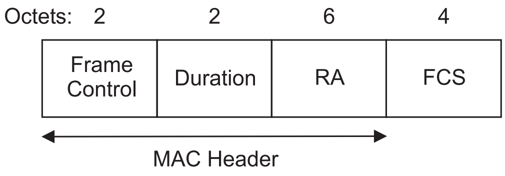


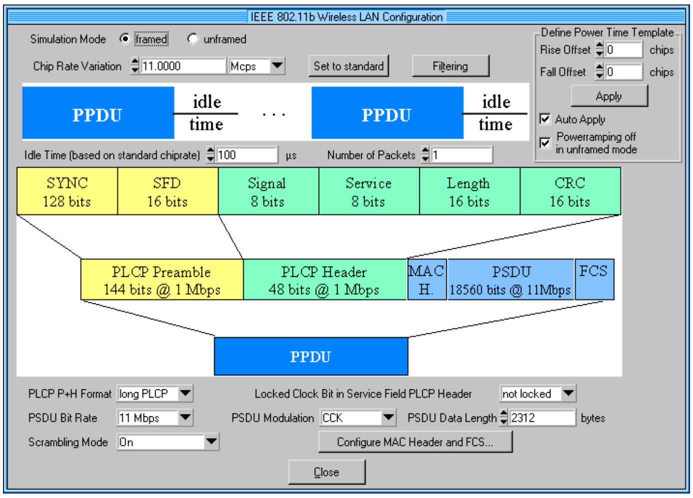
Figure 2-16: The ACK frame format

If the frame acknowledged was the last or only fragment of an MSDU, the Duration value of the ACK frame will be set to 0, as the sender is not intending any further transmission. When the ACK frame is acknowledging a received fragment and more are to follow (“More Fragments” bit in Frame Control field set to 1), the Duration value will show the transmission time of the next fragment, plus one ACK frame, plus two SIFS intervals.

The RA will be equal to the address of the station transmitting the original data frame.

3 Creating 802.11 and 11b Signals

Signals compatible with the 802.11 DSSS and 802.11b modes can be created with WinIQSIM from Rohde & Schwarz from version 3.80. WinIQSIM is free software downloadable from the Rohde & Schwarz website, but to enable the upload of an 802.11b signal, the keycode options either AMIQK16 or SMIQK16 have to be installed in the instruments.



IEEE 802.11b Wireless LAN Configuration

Simulation Mode ● framed ○ unframed

Chip Rate Variation 11.0000 Mcps

Idle Time (based on standard chiprate) 100 µs

Number of Packets 1

Define Power Time Template

Rise Offset 0 chips

Fall Offset 0 chips

☑ Auto Apply

☑ Powerramping off in unframed mode

PLCP P+H Format long PLCP

Locked Clock Bit in Service Field PLCP Header not locked

PSDU Bit Rate 11 Mbps

PSDU Modulation CCK

PSDU Data Length 2312 bytes

Scrambling Mode On

Figure 3-1: The 802.11b extension to WinIQSIM

WinIQSIM supports all possible modulation formats of 802.11b. The PLCP fields can be configured according to the standard. Any MAC header can be defined with WinIQSIM, which calculates the FCS accordingly. The complete signal will be calculated and then uploaded to the ARB memory of an AMIQ (or an SMIQ equipped with option B60).

Table 3-1 shows the maximum signal lengths possible with the different ARB solutions. When calculating the frame numbers, we assume a transmission speed of 11 Mbps with short PLCP format and a data frame of length 8192 bits (that is a data length of 1024 octets including the MAC header). A SIFS of 10 µs is presumed between the frames.

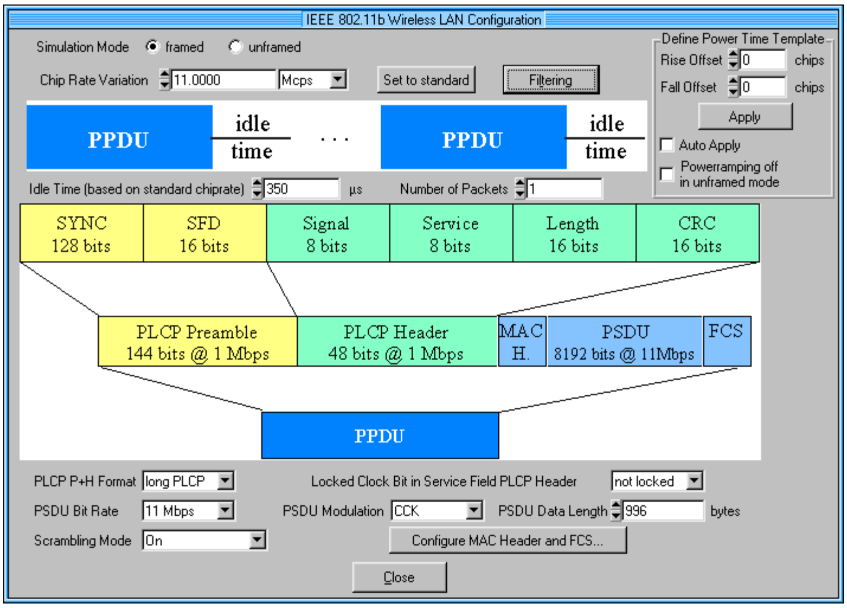
Table 3-1: Available signal lengths with the different ARBs

Over-sampling factor	maximum signal duration			maximum number of frames		
	SMIQB60	AMIQ03	AMIQ04	SMIQB60	AMIQ03	AMIQ04
8	-	45.45 ms	181.82 ms	-	53	213
7	-	51.95 ms	207.79 ms	-	61	244
6	-	60.61 ms	242.42 ms	-	71	284
5	-	72.73 ms	290.91 ms	-	85	341
4	-	90.91 ms	363.64 ms	-	106	427
3	15.52 ms	121.21 ms	484.85 ms	18	142	569

SMIQB60 supports a maximum sampling rate of 40 MHz, that means oversampling rates higher than 3 are not possible. But this fact is not of concern, as the internal digital interpolation filter will take care of any aliasing components automatically, higher oversampling is therefore not needed. Factors lower than 3 are not desirable, the filter will then start to cut off vital components of the signal; at factor 2, suppression starts at 8.25 MHz. An oversampling factor 3 is the right choice for the B60.

3.1 Signals for Receiver Tests

The 11b specification [3], section 18.4.8 specifies the RF parameters, which compliant receivers have to meet. There are four tests given to verify these parameters: Minimum input level sensitivity, maximum input level, adjacent channel rejection and Clear Channel Assessment (CCA). WinIQSIM can generate signals for all of these tests. The receiver has to demodulate the signal and perform FER measurements and CCA according to the standard. For the first three tests the same signal setup is used for the required signal. This setup is provided as “Receiver tests.iqs” in the “1GP49_0E examples.zip” archive (subdirectory “Receiver Tests\”) and shown in Figure 3-2.



IEEE 802.11b Wireless LAN Configuration

Simulation Mode ● framed ○ unframed

Chip Rate Variation 11.0000 Mcps

Define Power Time Template

Rise Offset 0 chips

Fall Offset 0 chips

□ Auto Apply

□ Powerramping off in unframed mode

Idle Time (based on standard chiprate) 350 µs

Number of Packets 1

PLCP P+H Format long PLCP

Locked Clock Bit in Service Field PLCP Header not locked

PSDU Bit Rate 11 Mbps

PSDU Modulation CCK

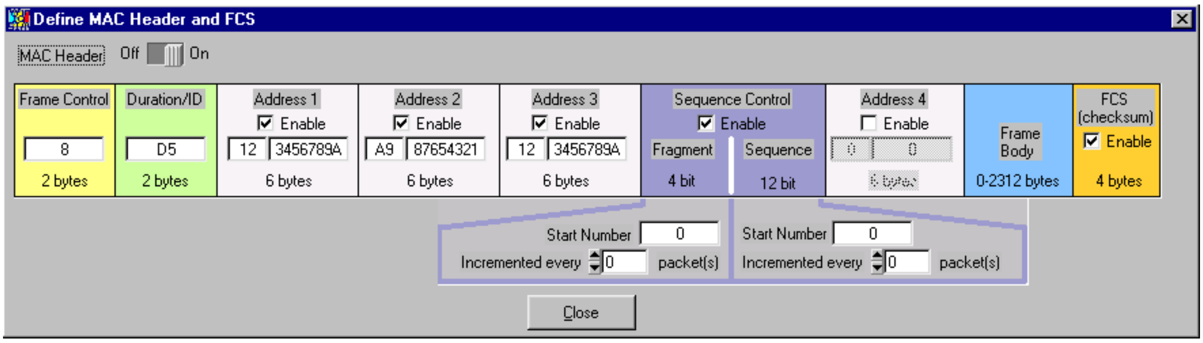
PSDU Data Length 996 bytes

Scrambling Mode On

Figure 3-2: WinIQSIM setup for the receiver tests

The signal uses 11 Mbps CCK modulation - as specified for the receiver tests in [3] - with long PLCP PPDU format and activated scrambling. The baseband filter has been set to Gaussian with B•T=0.3, to meet the transmit spectrum mask requirements of section 18.4.7.3. The oversampling factor is 8, to get optimum results with AMIQ. Set it to factor 3 when using SMIQB60.

The PSDU data is of length 996 octets; with the 28 octets of the activated MAC header this makes a total of 1024 bytes for the PSDU, as prescribed by [3]. The idle time between two frames has been set to 350 µs. This equals the interframe space of the DCF plus a medium backoff time. The Distributed Interframe Space (DIFS) for 11b is specified as 50 µs (SIFS of 10 µs + 2 x Slot Time of 20 µs). The initial backoff window can be between 0 and 31 slots, the mean value of 15 slots makes a backoff time of 300 µs.



Define MAC Header and FCS

MAC Header Off On

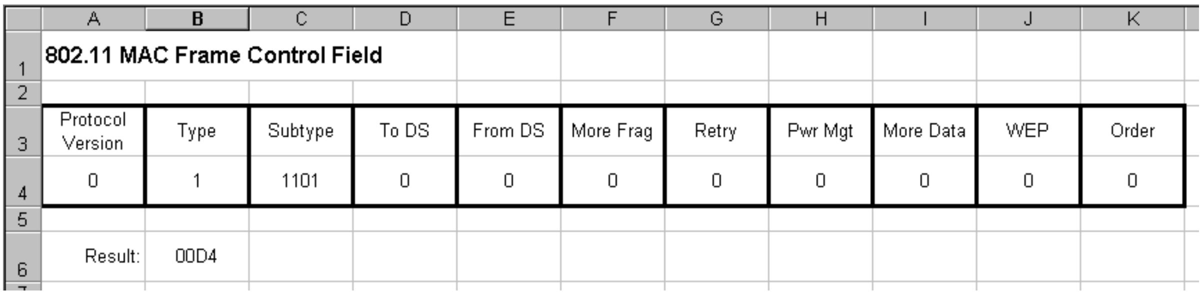
Frame Control	Duration/ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	FCS (checksum)
		☑ Enable	☑ Enable	☑ Enable	☑ Enable	□ Enable		☑ Enable
8	D5	12 3456789A	A9 87654321	12 3456789A	Fragment Sequence	0 0		
2 bytes	2 bytes	6 bytes	6 bytes	6 bytes	4 bit 12 bit	6 bytes	0-2312 bytes	4 bytes

Fragment: Start Number 0, Incremented every 0 packet(s)

Sequence: Start Number 0, Incremented every 0 packet(s)

Figure 3-3: MAC header for the receiver test signal

The MAC header is configured for a frame of type data. The Frame Control field has to be entered in hexadecimal notation in WinIQSIM. To ease the calculation of this field, the MS Excel file “Frame Control Field Calculation Sheet.xls” has been provided in the examples archive. Enter all parameters (see Figure 3-4) in binary notation and they are converted to hexadecimal automatically. Note that the binary values for Type and Subtype have to be entered with the LSB right, exactly as given in Table 2-3.



802.11 MAC Frame Control Field

Protocol Version	Type	Subtype	To DS	From DS	More Frag	Retry	Pwr Mgt	More Data	WEP	Order
0	1	1101	0	0	0	0	0	0	0	0

Result: 00D4

Figure 3-4: The MS Excel file “Frame Control Field Calculation Sheet.xls”

Three of the four address fields are activated, where address 1 specifies the destination address, address 2 the source address and address 3 the BSSID. Dummy numbers have been entered in this fields. To make this setup work, specify the correct addresses here. The destination address is the most important one, as reception will only work with the right address. The BSSID should be set to the address of the AP, if an AP is to be simulated or tested. Otherwise the BSSID shall be the BSSID of an IBSS.

3.1.1 Receiver Minimum Input Level Sensitivity

Any compliant receiver will have to be able to perform reception of the defined high rate CCK signal with a resulting FER lower than $8 \bullet 10^{-2}$, at an input level of -76 dBm. The energy detection threshold has to be set to -76 dBm or less. Use the provided setup “Receiver tests.iqs” and enter the correct destination address. Set the SMIQ to a valid channel frequency (see [3], 18.4.6.7.2) and set the level to -76 dBm. If the cable length is of consideration, measure the cable loss at the desired frequency and increase the SMIQ level by this amount. The DUT now has to receive the frames and an additional software has to count the FER (Frame Error Ratio) by evaluating the FCS of the MAC header. This FER has to be less than $8 \bullet 10^{-2}$ for the DUT to pass the test.

3.1.2 Receiver Maximum Input Level

The same procedure as in 3.1.1 also applies for the maximum input level test, but here the output level of the SMIQ has to be set to -10 dBm. The DUT still needs to provide an FER of less than $8 \bullet 10^{-2}$ to pass this test.

3.1.3 Receiver Adjacent Channel Rejection

For the adjacent channel test an additional signal source is needed. This should be a second SMIQ, and both SMIQs need to be connected to the DUT with a coupler. The levels to be set on the SMIQs have to be corrected for the path loss of the cabling and coupler. This is ideally determined with a power meter at the desired transmission frequencies.

The SMIQ transmitting the required signal should be configured with the given “Receiver tests.iqs” setup with correctly defined destination address. Set the level on this SMIQ to -70 dBm + path loss and the frequency to a valid channel. The second SMIQ has to be configured to transmit the interfering signal, which can be done with the “Adjacent channel.iqs” setup of the examples archive. This is a CCK signal in unframed mode with continuous transmission to provide equal conditions at any time of frame reception. The level of the second SMIQ with this interfering signal has to be set to -35 dBm + path loss. The interferer’s frequency shall be on a valid channel according to [3], 18.4.6.7.2 with a distance of ≥ 25 MHz to the wanted signal.

The DUT has to receive the required signal and count the FER, which must be lower than $8 \cdot 10^{-2}$ under these conditions.

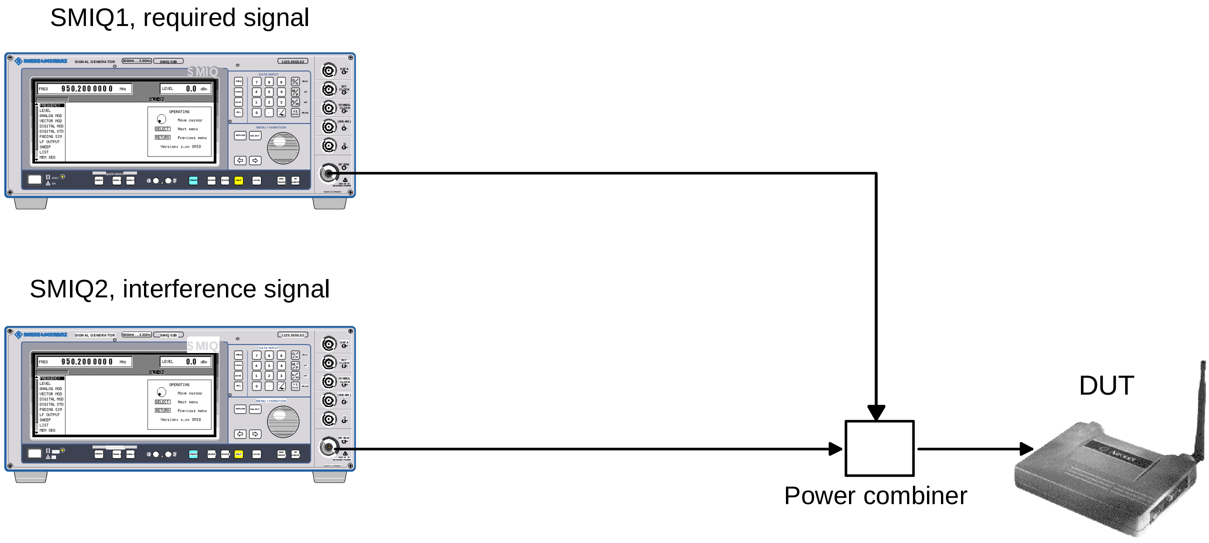


Figure 3-5: Setup for the adjacent channel rejection test

3.1.4 CCA

The CCA indicator shall be TRUE whenever the channel is free and transmission is allowed. The indicator timings have to follow certain rules, which are tested with the CCA test.

To perform this test, a compliant high rate signal has to be applied at the DUT antenna connector with a level above the energy detection threshold. The Energy Detection (ED) threshold depends on the available transmission power of the station, as shown in Table 3-2.

Table 3-2: Energy detection thresholds for different TX powers

TX power	ED threshold
P > 100 mW	≤ -76 dBm
50 mW < P ≤ 100 mW	≤ -73 dBm
P ≤ 50 mW	≤ -70 dBm

A predefined signal setup for this test has been provided with the “CCA test 1.iqs” file. Here, the destination address shall **not** be set to the address of the station to be tested, to avoid any ACK frames being transmitted from it. We will just make sure that the DUT is capable of detecting a busy or clear channel. In the setup file the signal’s oversampling is again set for AMIQ operation, set it to 3 when using SMIQB60.

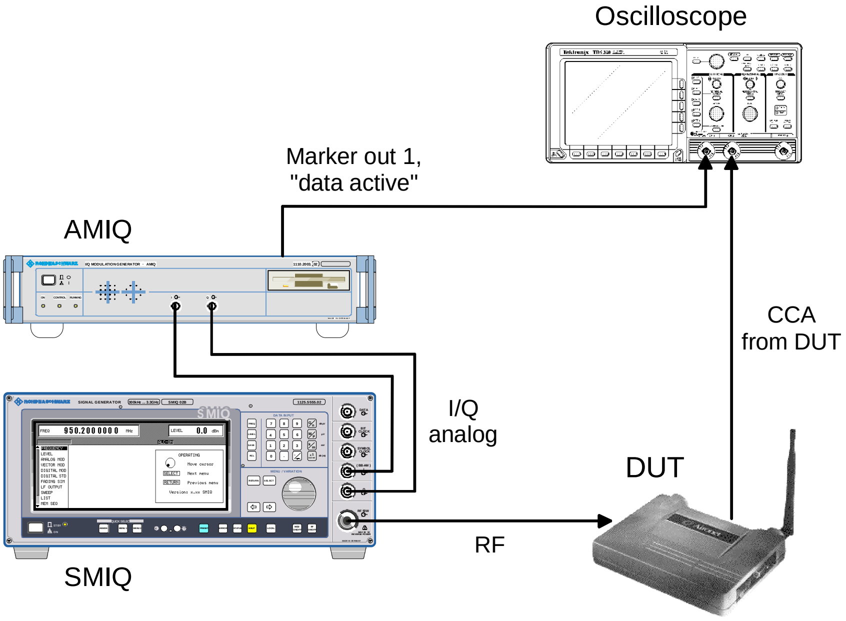


Figure 3-6: Instrument setup for the CCA test when using AMIQ

The first part of this test has to determine if the CCA indicator will show a busy channel early enough. The CCA signal needs to be accessible via an exposed test point and shall be compared to the timing of the transmitted signal. Marker output 1 of AMIQ has been programmed with the “data active” signal and is high whenever transmission is active. The two signals, CCA and data active have to meet the timing requirements shown in Figure 3-7. The CCA must show a busy channel within 15 µs of the next active transmission, when it takes the DUT exactly 5 µs to switch from receive to transmit. Figure 3-7 also shows the timing with respect to the three interframe spaces. The test signal has been designed with 30 µs idle time between frames, which is exactly a PCF Interframe Space (PIFS). Therefore, the DUT in DCF mode must not start any transmission after expiration of its DIFS and backoff timer. The shown 15 µs is the time from the beginning of the new frame to the next MAC slot boundary, and therefore the maximum allowable delay for the CCA to show busy. This value may also be higher, if the DUT’s time to switch from receive to transmit is less than 5 µs.

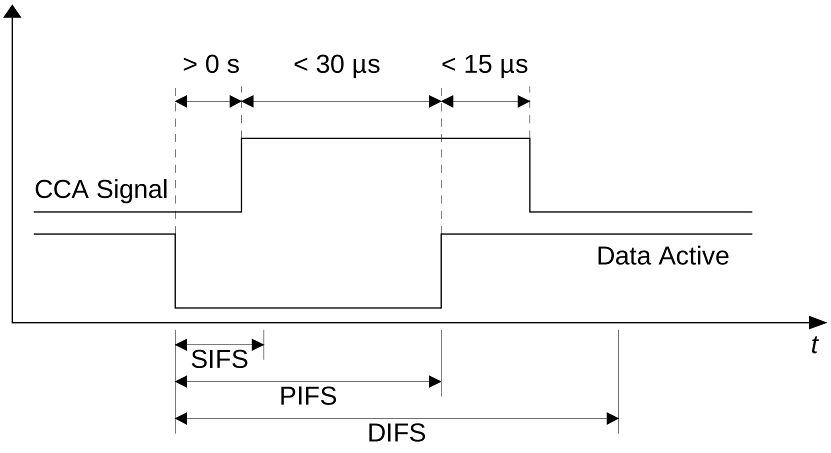


Figure 3-7: CCA timing relationship

When SMIQB60 is used, there is no option to program a data active signal as with AMIQ. But the test can also be performed by connecting the I output to the oscilloscope. The baseband I signal will then be shown, which is 0 during the interframe space. With this method, the timing can also be measured. Triggering of the oscilloscope shall then be done with the CCA signal, otherwise a stable result may not be possible. For troubleshooting purposes, program Trigger Out 1 with the SMIQ internal signal "SEQUENZ", to get an extra trigger signal.

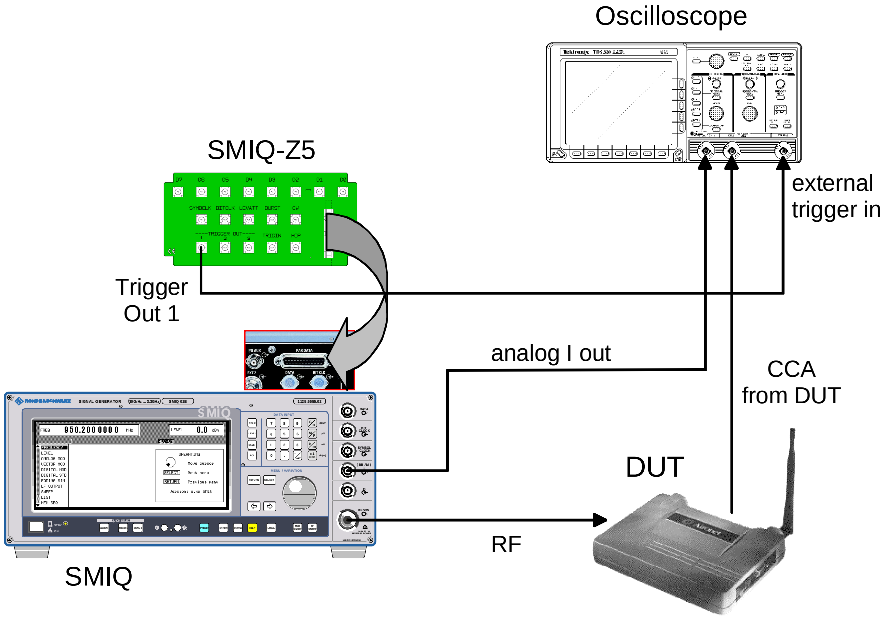


Figure 3-8: Instrument setup for the CCA test when using SMIQB60

The second CCA test has to determine if the LENGTH field of the PLCP header has been evaluated correctly. The CCA shall indicate "busy" for the whole frame length, even if a loss of carrier sense occurs during frame reception. This requires that the PLCP header has been successfully decoded. The provided file "CCA test 2.iqs" is a modification of the previously used test setup, where power ramping has been additionally introduced to cut off the signal after 3000 chips. The data active marker of AMIQ still shows high for the whole intended frame duration.

For this test we use the same connections between the DUT, SMIQ/AMIQ and the oscilloscope as above. At the end of the intended frame transmission, the CCA signal shall not go back to high before the data active signal provided on marker output 1 of the AMIQ reaches low. When SMIQB60 is used, the correct timing can be determined with respect to the transmission start of the next frame. The time between the CCA reaching high and the I output of the SMIQ showing non-zero values again, must not be longer than 30 µs (see Figure 3-7).

3.2 Additional Signal Examples

WinIQSIM can create a lot more 11b compatible signals for all kinds of equipment tests. This subsection gives some more examples. The aim is not to define complete tests or to develop a precise scenario which can be used one to one in a real situation, but to show the capabilities of WinIQSIM and what is additionally possible with a few tricks. With the presented knowledge, the given examples can be modified to match the exact needs in a real life situation.

3.2.1 RTS/CTS example

The basic functionality of WinIQSIM does not include a sequencer to enable concatenation of different signal pieces and so simulate for example a certain frame exchange sequence. But with some additional calculations it is possible to exploit the Multi Carrier Mixed Signal system to achieve exactly the same goal. In this example, we will build up a typical RTS/CTS exchange sequence as it might be received by an additional third station on the network. The goal of the example is to show precisely how the setup can be done and the calculations are carried out. One typical purpose for such a signal could be to test the Network Allocation Vector (NAV) of a station, which should correspond with the calculated timings. The Duration field of all frames has been set such that the NAV timer of any station listening to the sequence reaches zero at the end of the ACK frame.

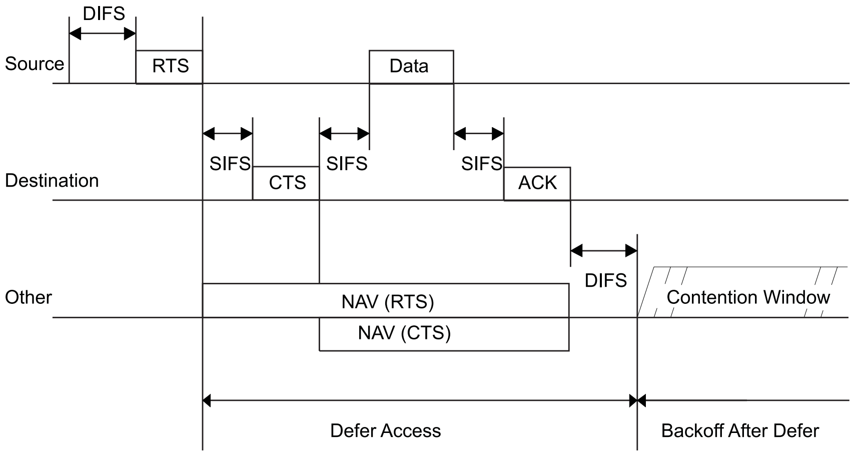


Figure 3-9: Setting the NAV in a typical RTS/CTS sequence

Basis for this setup is Figure 3-9, where a normal exchange of RTS and CTS frames before transmission of the actual Data frame and its acknowledgement is shown. These four frames shall now be generated with WinIQSIM by using the Multi Carrier Mixed Signal system. The basic principle behind this trick is to define all four frames independently and add them to one signal with the mixing option by specifying a carrier offset of 0 Hz and introducing defined time delays for each frame. To accomplish this, the four frames have to be generated with an idle time after each transmission such that every signal has the same number of samples. During the idle period the I and Q samples are zero, so with a correct delay introduced the signals can be added without any overlapping.

For the timing calculations see Figure 3-10, which gives the exact duration values for the complete setup. This is the basis for the definition of the 4 frames.

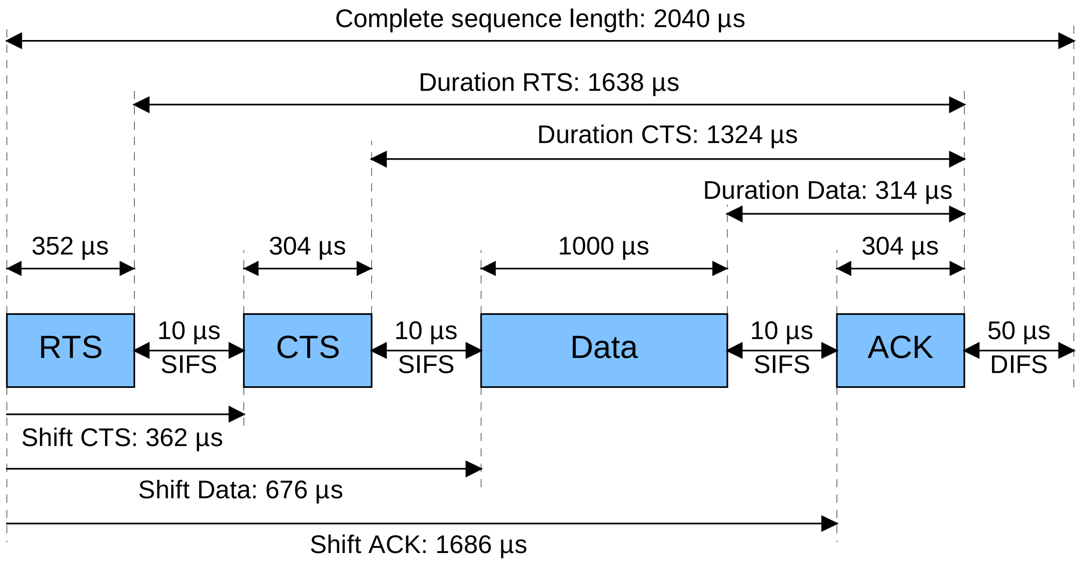


Figure 3-10: Timing relationship for the RTS/CTS example

Table 3-3: The parameters of the 4 frames used in the RTS/CTS example.

Parameter	RTS frame	CTS frame	Data frame	ACK frame
PLCP P+H format	long	long	long	long
PSDU Bit Rate & Modulation	1 Mbit DBPSK	1 Mbit DBPSK	11 Mbit CCK	1 Mbit DBPSK
MAC Frame Control	00 10 1101 0 0 0 0 0 0 0 0	00 10 0011 0 0 0 0 0 0 0 0	00 01 0000 0 0 0 0 0 0 0 0	00 10 1011 0 0 0 0 0 0 0 0
MAC Duration	666 (HEX)	52C (HEX)	13A (HEX)	0 (HEX)
MAC Address 1	123456789A	-	123456789A	-
MAC Address 2	A987654321	A987654321	A987654321	A987654321
MAC Address 3	-	-	ABCDEFABCD	-
MAC Sequence Control	-	-	Start FN: 0, Inc: 0 Start SN: 0, Inc: 0	-
MAC Address 4	-	-	-	-
Frame Body length & data	0	0	1083 bytes, PRBS 9	0
MAC FCS	yes	yes	yes	yes
Frame duration	352 µs	304 µs	1000 µs	304 µs
Idle Time	1688 µs	1736 µs	1040 µs	1736 µs
Frame shift	0 µs	362 µs	676 µs	1686 µs

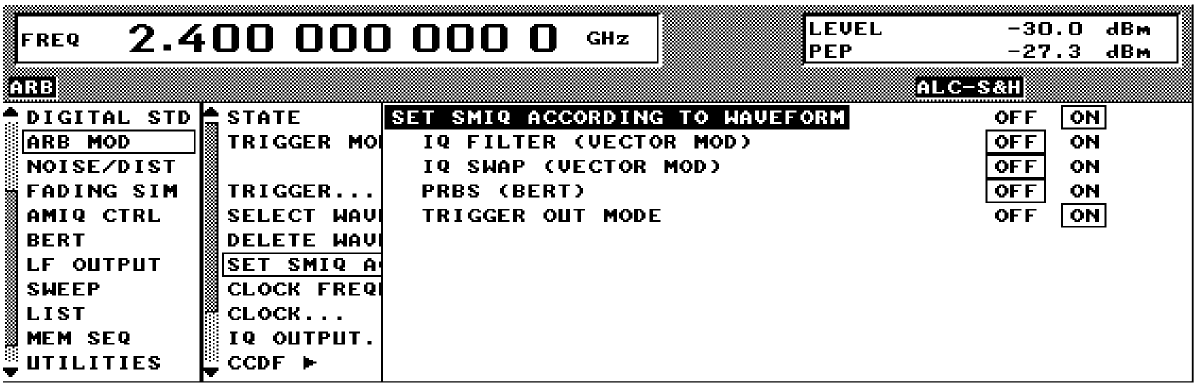
Table 3-3 shows all relevant parameters of the four frames used in the example. These parameters have been entered into four different WinIQSIM setups, which are provided in the examples archive as “RTS frame.iqs”, “CTS frame.iqs”, etc. in subdirectory “RTS-CTS\”. All frames use long PLCP preamble and header format. The control frames are transmitted with 1 Mbps Barker spreading, the data frame uses 11 Mbps CCK. The MAC Frame Control parameters of Table 3-3 are shown with LSB left notation, to enter these parameters in WinIQSIM they just have to be converted to LSB right and hexadecimal notation. The Duration/ID field of the MAC header reads the intended duration in µs for the lasting transmission of the sequence, which shall set the NAV of any listening station accordingly. These parameters can be seen in Figure 3-10, and need to be converted to hexadecimal notation again for WinIQSIM. For the address fields, dummy parameters have been used. Their configuration corresponds to the definitions described in section 2.2.2 of this document. The Sequence Control field is only present in the Data frame and is set to 0. Also only the Data frame contains a frame body field, with 1083 octets of data. This value has been chosen to get an easy to calculate duration of 1000 µs for the data frame.

The frame duration values are derived from the frame parameters discussed above and are needed together with the interframe spaces to calculate the rest of the timing parameters. All frame lengths, together with their interframe spaces, accumulate to a total of 2040 µs for the entire sequence. To enable adding all these signals, every setup needs to include an idle time long enough to hold the rest of the sequence. Therefore, the Idle Time parameter of WinIQSIM equals to the sequence length minus the transmission duration of the particular frame. Table 3-3 shows the result of these calculations in the line “Idle Time”. And last but not least, every frame - except the first one - has to be shifted in time to its desired location. This is just the time of the frame start referenced to the beginning of the sequence. Figure 3-10 again displays the time shifts for these frames.

To create the complete signal with all four frames, “.ibn” waveform files need to be created first. Perform this by loading every single frame setup in WinIQSIM. After loading, make sure that you are using the correct oversampling factor: Select 8 for AMIQ and 3 for SMIQB60. Afterwards, select “Save for Add/Multi Carrier Mixed Signal” from the “File” menu and enter the setup file title as file name. Adding of the four single frames to the complete sequence has been prepared in the “RTS CTS sequence.iqs” setup file. The defined four carriers contain the created frames, whereby the waveform source files are referenced to path “Q:\RTS-CTS”. If these files are in another path, an error message will occur when loading the setup into WinIQSIM. As a countermeasure, one can set the source files for the four channels again, to get them from the right path. Channel 0 contains the RTS frame, channel 1 the CTS frame, channel 2 the Data frame and channel 3 the ACK frame. The

Carrier Spacing has been set to 0, as already mentioned to create one signal with the frames transmitted after each other on the same frequency. The initial delays of these channels have been set to the calculated values of Table 3-3, to produce the desired sequence timing.

Now this complete sequence can for example be used to test the correct functionality of the NAV timer of a station. For this the station must be able to provide the NAV signal on an external port. With an oscilloscope the timing could be verified by comparing it to a sequence restart signal provided by AMIQ or SMIQ. The mentioned WinIQSIM settings include programming of Marker output 4 of AMIQ with a restart signal, which is high for a short period of time at the beginning of each sequence, as well as Trigger Out 1 of SMIQ, which produces the same signal when SMIQB60 is used. To activate this signal on SMIQ, switch on the menu settings "Set SMIQ according to waveform" as well as "Trigger out mode" in the "ARB Mod menu" (See Figure 3-11).



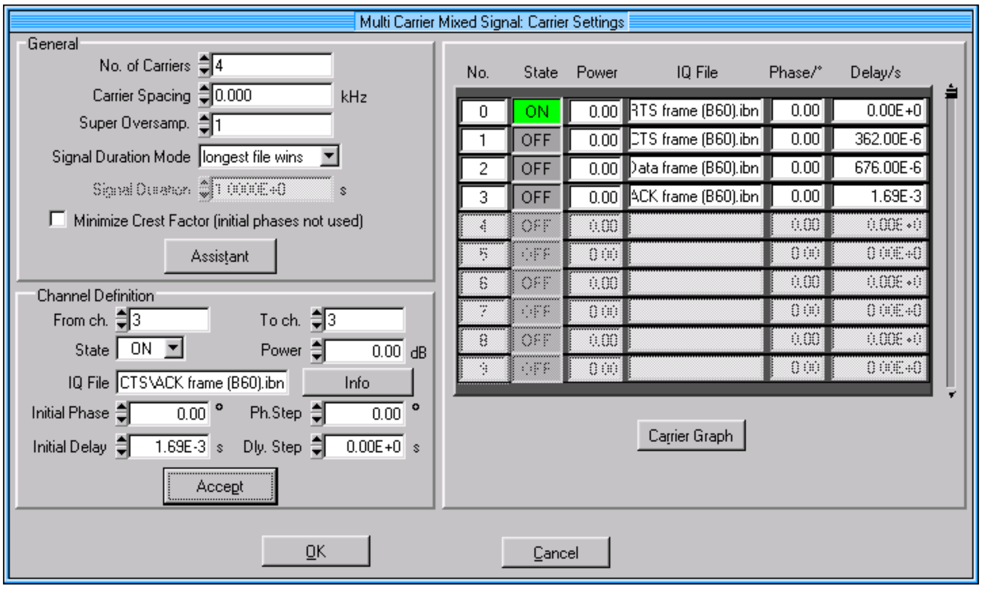
FREQ 2.400 000 000 0 GHz

LEVEL -30.0 dBm
PEP -27.3 dBm

SET SMIQ ACCORDING TO WAVEFORM	OFF	[✓ ON]
IQ FILTER (VECTOR MOD)	[✓ OFF]	ON
IQ SWAP (VECTOR MOD)	[✓ OFF]	ON
PRBS (BERT)	[✓ OFF]	ON
TRIGGER OUT MODE	OFF	[✓ ON]

Figure 3-11: SMIQ settings for outputting the sequence restart signal on Trig Out 1.

When performing the same test under more severe conditions, omit transmission of some of the frames in the sequence. To give an example, the DUT must also show the same NAV timer behavior when only the RTS frame is transmitted. This can be simulated by switching off all channels except channel 0 in the Multi Carrier setup (see Figure 3-12 and "RTS CTS sequence, RTS only.iqs"). Then only the RTS frame will be transmitted, while still setting the NAV to the whole sequence duration. It is also possible to have other combinations - e.g. only the CTS frame or only the Data frame transmitted, the NAV of the listening station shall still behave according to the definitions of [1].



Multi Carrier Mixed Signal: Carrier Settings

General

No. of Carriers: 4
Carrier Spacing: 0.000 kHz
Super Oversamp.: 1
Signal Duration Mode: longest file wins
Signal Duration: 1.000E+0 s
☐ Minimize Crest Factor (initial phases not used)

Channel Definition

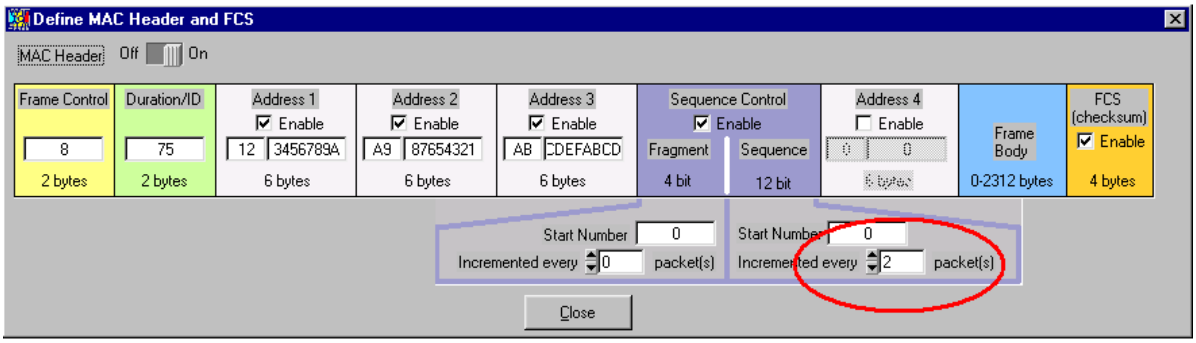
From ch.: 3 To ch.: 3
State: ON Power: 0.00 dB
IQ File: CTS\ACK frame (B60).ibn
Initial Phase: 0.00 ° Ph.Step: 0.00 °
Initial Delay: 1.69E-3 s Dly. Step: 0.00E+0 s

No.	State	Power	IQ File	Phase/°	Delay/s
0	ON	0.00	RTS frame (B60).ibn	0.00	0.00E+0
1	OFF	0.00	CTS frame (B60).ibn	0.00	362.00E-6
2	OFF	0.00	Data frame (B60).ibn	0.00	676.00E-6
3	OFF	0.00	ACK frame (B60).ibn	0.00	1.69E-3
4	OFF	0.00		0.00	0.00E+0
5	OFF	0.00		0.00	0.00E+0
6	OFF	0.00		0.00	0.00E+0
7	OFF	0.00		0.00	0.00E+0
8	OFF	0.00		0.00	0.00E+0
9	OFF	0.00		0.00	0.00E+0

Figure 3-12: Only RTS frame active of the RTS/CTS example

3.2.2 Retransmission example

Another scenario appearing in real world situations is the retransmission of a Data frame. Whenever the original transmitter of a Data frame does not receive an acknowledgement after the SIFS period correctly or does not receive it at all, the Data frame sent before needs to be retransmitted. Such a situation can be simulated with the Sequence Control functions of the MAC Header panel (see Figure 3-13). The Start Number and Sequence Number fields can be set to a defined initial value, and are incremented individually after the specified number of frames. If the start number of the Sequence Number subfield is set to zero and is intended to be incremented every two packets - as specified in this example - the result will be a sequence of two frames containing value 0, two frames containing 1, two frames with 2 and so on. If an increment value of zero packets is specified, all frames will contain the same number.



Define MAC Header and FCS

MAC Header Off / On

Frame Control	Duration/ID	Address 1	Address 2	Address 3	Sequence Control		Address 4	Frame Body	FCS (checksum)
		☑ Enable	☑ Enable	☑ Enable	☑ Enable		□ Enable		☑ Enable
8	75	12 3456789A	A9 87654321	AB CDEFABCD	Fragment	Sequence	0 0		
2 bytes	2 bytes	6 bytes	6 bytes	6 bytes	4 bit	12 bit	6 bytes	0-2312 bytes	4 bytes

Fragment: Start Number 0, Incremented every 0 packet(s)

Sequence: Start Number 0, Incremented every 2 packet(s)

Figure 3-13: MAC Header for the retransmission example

WinIQSIM has been implemented so that whenever more than one frame contains the same Sequence and Fragment numbers, the same data will be transmitted with these frames. Also, the Retry bit of the Frame Control field is automatically set with every retransmission. The initial frame of such a set contains the value originally specified in the Frame Control Field.

So the example to be discussed here is set up as follows. The file “Retransmission.iqs” of subdirectory “Retransmission\” contains the desired settings. This time, short PLCP Preamble and Header format is used together with 11 Mbps CCK modulation. The MAC Header configuration basically equals to the Data frame of the last example, so the destination address has to be set to the address of the receiver again. For the Duration/ID field a value of 117 µs is set, which equals to an SIFS space plus the duration of one ACK frame transmitted at 11 Mbps. The Sequence Control field is prepared with the values already mentioned before, to have the Sequence Number incremented every two frames. After every frame an idle time of 167 µs is inserted, to give the receiver enough time to send its ACK frame. Basis for this value is the assumption of one ACK frame being transmitted at 11 Mbps with short PLCP format (which takes 107 µs), plus one SIFS of 10 µs plus one DIFS of 50 µs. Should the receiver try to send its acknowledgment at a rate lower than 11 Mbps, overlapping with the next frame in the sequence may occur. This can be compensated by selecting a longer idle time between the frames.

The complete signal includes a total of 6 frames with 2000 bytes of user data each. As every frame is transmitted twice, this makes 6000 bytes of data for the entire sequence. The data is taken from the file “PN15 Data.dbi” and is based on a PRBS 15. At the receiver, the MAC layer should detect the duplicate frame transmissions and build up the original data sequence. If appropriate software exists on the receiver, the resulting data can be compared to the transmitted sequence of the given file and an exact match should be indicated.

3.2.3 Fragmented MSDU example

When simulating fragmented MSDUs, set up such a signal the same way as shown in the example before. By specifying a Fragment Number increment value larger than zero and setting up the signal as described in the last example, a sequence of frames with MSDU fragments is obtained. A combination of Sequence Number and Fragment Number increments is also possible and could look like this: Incrementing Fragment Number every frame and incrementing Sequence Number every third frame will produce a sequence with one MSDU fragmented into three frames. That means, always three frames contain the same sequence number with increasing fragment numbers. After one set of three fragments has been transmitted, the Sequence Number will increment and WinIQSIM will automatically set the fragment number of the first frame of the next set to zero, as defined in [1], 9.4.

Although these automatic functions work fine, we will not rely on them in this example. Instead, we use the sequencing trick already presented in section 3.2.1, and build up the individual fragments one by one. This gives us the ability to modify the MAC header individually for each fragment, and thus set the Duration/ID fields to their correct parameters. The automatic function will keep the same MAC header for all frames, which should also work in all cases where updating the NAV of other stations is not too critical.

Table 3-4: The parameters of the three Data frames used in the fragmented MSDU example

Parameter	Fragment 0	Fragment 1	Fragment 2
PLCP P+H format	short	short	short
PSDU Bit Rate & Modulation	11 Mbit CCK	11 Mbit CCK	11 Mbit CCK
MAC Frame Control	00 01 0000 0 0 1 0 0 0 0 0	00 01 0000 0 0 1 0 0 0 0 0	00 01 0000 0 0 0 0 0 0 0 0
MAC Duration	716 (HEX)	716 (HEX)	75 (HEX)
MAC Address 1	123456789A	123456789A	123456789A
MAC Address 2	A987654321	A987654321	A987654321
MAC Address 3	ABCDEFABCD	ABCDEFABCD	ABCDEFABCD
MAC Sequence Control	Start FN: 0, Inc: 0 Start SN: 0, Inc: 0	Start FN: 1, Inc: 0 Start SN: 0, Inc: 0	Start FN: 2, Inc: 0 Start SN: 0, Inc: 0
MAC Address 4	-	-	-
Frame Body length & data	2000 bytes, “PN15 Data Fragment 0.dbi”	2000 bytes, “PN15 Data Fragment 1.dbi”	2000 bytes, “PN15 Data Fragment 2.dbi”
MAC FCS	yes	yes	yes
Frame duration	1571 µs	1571 µs	1571 µs
Idle Time	3563 µs	3563 µs	3563 µs
Frame shift	0 µs	1698 µs	3396 µs

Table 3-4 shows the parameters of the three Data frames, which form the MSDU fragments in this example. We use short PLCP format with 11 Mbps CCK modulation. The Frame Control field is identical to the one of a typical Data frame, except for the first two frames, which have the “More Frag” bit set to indicate that more fragments of the same MSDU will follow. The last frame has this bit cleared. Section 9.2.5.6 of [1] defines the Duration fields of the frames in fragmented mode. Every fragment shall set the NAV of the listening stations to indicate busy until the end of the ACK frame acknowledging the next transmitted fragment. The Sequence Control fields specify the correct Fragment Number, entered as Start Number in the MAC Header panel. As data source the same PRBS 15 based sequence is used as in the last example, but here three different source files need to be specified. The three files include the portion of the complete data set needed for the fragment only. The idle and shift times are again calculated the same way as in the RTS/CTS example.

The setup files can again be found in the examples archive under “Fragmented MSDU\”.

4 Equipment for receiver tests

Several different equipment setups are possible to perform the receiver tests in section 18.4.8 of specification 802.11b. An SMIQ03B or higher can be used with either the internal ARB SMIQB60 or with an external AMIQ. An SMV03 together with an AMIQ is also applicable.

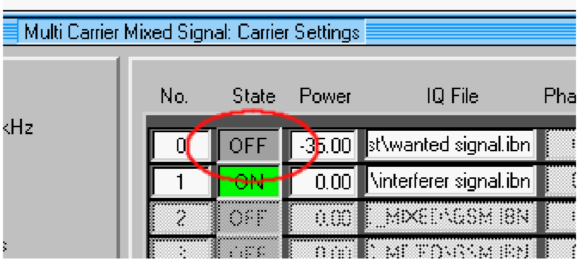
Table 4-1 gives an overview on the possible instrument combinations and their applicability for the receiver tests. In general, using the SMIQB60 ARB is possible: However due to its memory capacity, only 18 different frames with 1024 octets each – as prescribed by the 11b specification – are available. It is not possible to have SMIQ with B60 perform the adjacent channel rejection tests, due to the bandwidth capacity of the SMIQB60 ARB. AMIQ together with an SMIQ or SMV can provide both, the wanted and the interferer signal at once, but an additional calibration has to be performed to ensure optimum accuracy of the wanted signal.

4.1 Setting up the adjacent channel rejection test with one AMIQ

The WinIQSIM Multi Carrier Mixed Signal system can combine both the wanted signal and the 11b modulated interferer to be output simultaneously by one AMIQ. The examples archive includes the setups “wanted signal.iqs” and “interferer signal.iqs” in the directory “Single Box ACR Test\”, as an example setup. The “mixed signal.iqs” setup combines the .ibn files generated with these setups. When transmitting this signal to the DUT, the frequency on the generator needs to be altered by half the channel spacing. So in the example where the interferer is above the wanted signal, set the generator frequency to the desired channel + 12.5 MHz. For channel 1 this would be 2.412 GHz + 12.5 MHz equals 2.4245 GHz.

The following AMIQ calibration procedure is necessary to fulfill the requirements for signal accuracy for the wanted signal: its level has to be at least 35 dB lower than the interferer and is therefore easily affected by inadequate sideband cancellation in an uncalibrated system.

1. Generate the mixed signal with the wanted signal deactivated

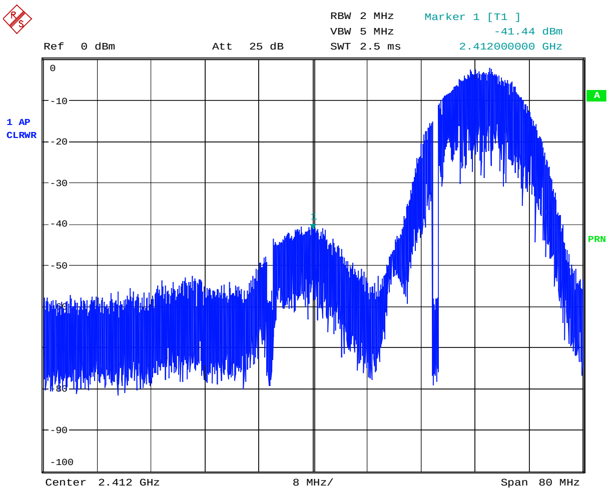


Multi Carrier Mixed Signal: Carrier Settings

No.	State	Power	IQ File	Pha
0	OFF	-35.00	st\wanted signal.ibn	
1	ON	0.00	\interferer signal.ibn	
2	OFF	0.00	_MIXED\GSM.IBN	
3	OFF	0.00	[illegible]	

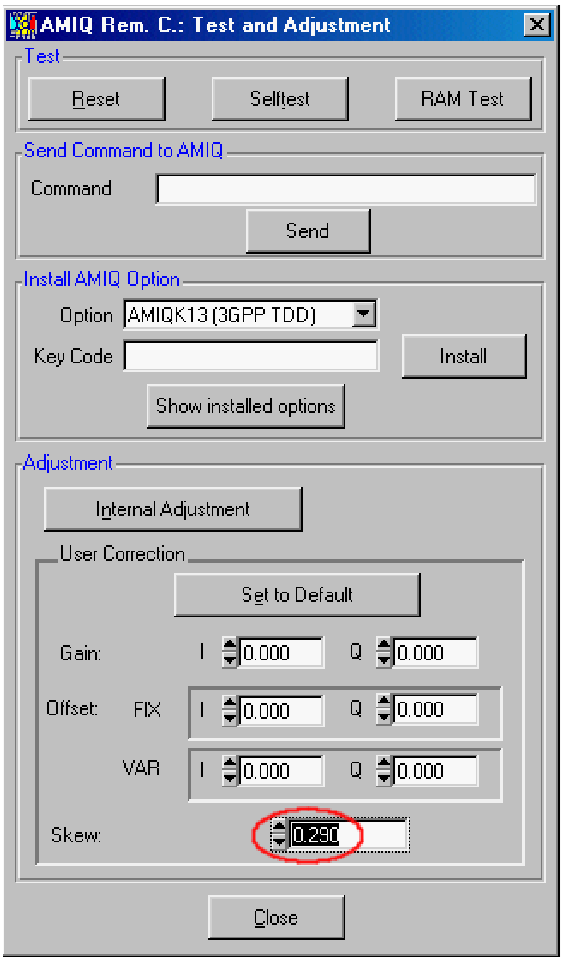
2. Display the signal on a spectrum analyzer

The analyzer shows the improper sideband cancellation right, at the frequency of the wanted signal. This can be reduced by altering the I and Q channel delays of the AMIQ



Date: 30.JUL.2002 17:00:20

3. Adjust the AMIQ Skew


AMIQ Rem. C.: Test and Adjustment

Command:

Option: AMIQK13 (3GPP TDD)

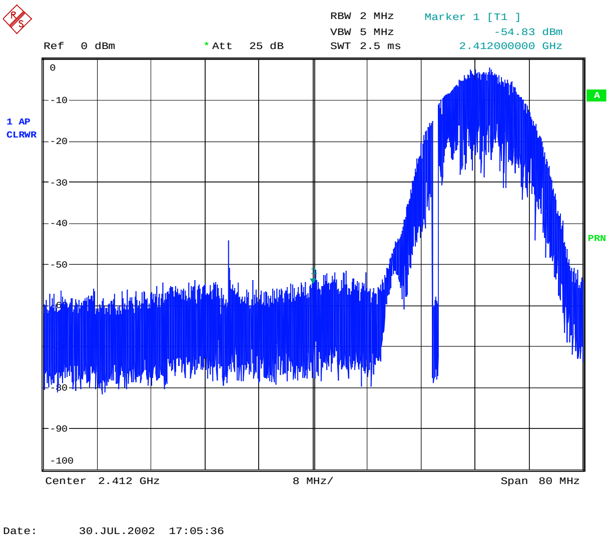
Key Code:

Gain: I 0.000 Q 0.000

Offset: FIX I 0.000 Q 0.000

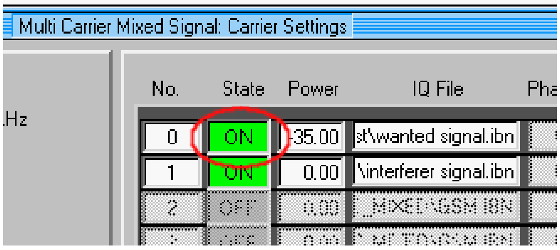
VAR I 0.000 Q 0.000

Skew: 0.290



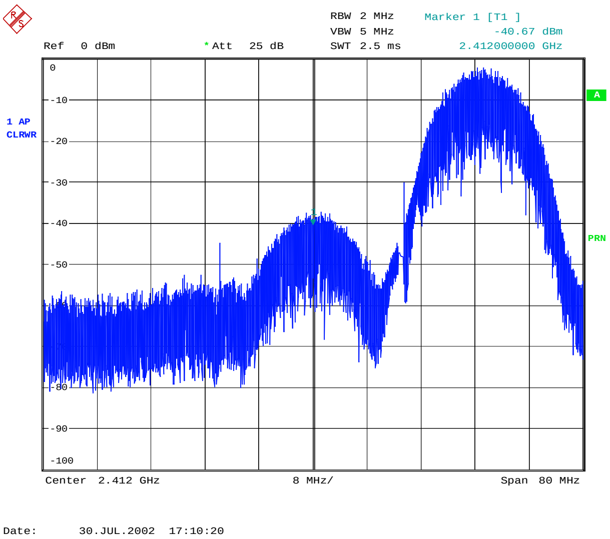
In WinIQSIM under “AMIQ” – “Remote Control and BERT...” select “Test and Adjustment” and adjust the Skew parameter such that the analyzer shows optimum sideband cancellation.

4. Reactivate the wanted signal


Multi Carrier Mixed Signal: Carrier Settings

Hz

```
No.  State  Power   IQ File                  Pha
0    ON     -35.00  st\wanted signal.ibn
1    ON     0.00    \interferer signal.ibn
2    OFF    0.00    ...MIXED\GSM.IBN
```



Reactivate the wanted signal in WinIQSIM and retransmit. The equipment is now ready to perform your tests.

Table 4-1: Equipment setups for the 802.11b receiver tests

	SMIQ + B60	**2x SMIQ + 2x B60**	**SMIQ + AMIQ**	**2x SMIQ + 2x AMIQ**	**SMIQ + B60 + SMIQ + AMIQ**	**SMV + AMIQ**	**2x SMV + 2x AMIQ**
802.11b receiver tests:							
Minimum input level	✓[1]	✓[1]	👍	👍	👍	👍	👍
Maximum input level	✓[1]	✓[1]	👍	👍	👍	👍	👍
Adjacent channel rejection	✗	✓[1]	✓[2]	👍	👍	✓[2]	👍
CCA	👍	👍	👍	👍	👍	👍	👍

👍 Optimum choice

✓ Possible (but not the best choice). The solution has restrictions for the specific application.

✗ Not possible

[1] Low memory (only 18 frames possible)

[2] Additional calibration necessary

5 Abbreviations

ACK	Acknowledgement
AID	Association Identity
ARB	Arbitrary Waveform Generator
BSSID	Basic Service Set Identification
CCA	Clear Channel Assessment
CCK	Complementary Code Keying
CFP	Contention-Free Period
CSMA/CA	Carrier Sense Multiple Access / Collision Avoidance
CTS	Clear To Send
DA	Destination Address
DBPSK	Differential Binary Phase Shift Keying
DCF	Distributed Coordination Function
DIFS	Distributed Interframe Space
DQPSK	Differential Quadrature Phase Shift Keying
DS	Distribution System
DSSS	Direct Sequence Spread Spectrum
ED	Energy Detection
FCS	Frame Check Sequence
FER	Frame Error Ratio
FHSS	Frequency Hopping Spread Spectrum
IBSS	Independent Basic Service Set
LAN	Local Area Network
LLC	Logical Link Control
LMSC	LAN MAN Standards Committee
MAC	Medium Access Control
MPDU	MAC Protocol Data Unit
MSDU	MAC Service Data Unit
NAV	Network Allocation Vector
PAN	Personal Area Network
PBCC	Packet Binary Convolutional Coding
PC	Point Coordinator
PCF	Point Coordinator Function
PHY	Physical Layer
PIFS	Point (Coordination Function) Interframe Space
PLCP	Physical Layer Convergence Protocol
PMD	Physical Medium Dependent
PPDU	PLCP Protocol Data Unit
PSDU	PLCP Service Data Unit
RA	Receiver Address
RTS	Request To Send
SA	Source Address
SFD	Start Frame Delimiter
SIFS	Short Interframe Space
TA	Transmitter Address
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network

6 References

[1] ANSI/IEEE Std 802.11 [ISO/IEC 8802-11:1999(E)], Part 11: Wireless LAN MAC and PHY Specifications, LAN/MAN Standards Committee of the IEEE Computer Society, 1999 Edition

[2] IEEE Std 802.11a-1999 [ISO/IEC 8802-11:1999/Amd 1:2000(E)], Part 11: Wireless LAN MAC and PHY Specifications, High-Speed Physical Layer in the 5 GHz Band, LAN/MAN Standards Committee of the IEEE Computer Society, 1999

[3] IEEE Std 802.11b-1999, Part 11: Wireless LAN MAC and PHY Specifications, Higher-Speed Physical Layer Extension in the 2.4 GHz Band, LAN/MAN Standards Committee of the IEEE Computer Society, 1999

[4] High-Speed Wireless ATM and LANs, Benny Bing, Artech House, 2000

[5] Achieving Ethernet Rates in Wireless LANs, Carl Andren and Mark Webster, Harris Semiconductor

[6] Signals for Wireless LANs, Part II: 802.11a, Application Note 1GP53, Rohde & Schwarz, 2002

[7] Creating Test Signals for Bluetooth with AMIQ / WinIQSIM and SMIQ, Application Note 1GP38, Rohde & Schwarz, 1999

[8] Generating Bluetooth Signals with SMIQ and the Application Software SMIQ-K5, Application Note 1GP48, Rohde & Schwarz, 2001

7 Ordering information

I/Q Modulation Generator

AMIQ03	4 Msamples	1110.2003.03
AMIQ04	16 Msamples	1110.2003.04

Options:

AMIQB1	BER Measurement	1110.3500.02
AMIQK16	Digital Standard IEEE 802.11b	1122.2903.02

Vector Signal Generator:

SMIQ03B	300 kHz to 3.3 GHz	1125.5555.03
SMIQ04B	300 kHz to 4.4 GHz	1125.5555.04
SMIQ06B	300 kHz to 6.4 GHz	1125.5555.06
SMV03	9 kHz to 3.3 GHz	1147.7509.13

Options:

SMIQB11	Data Generator	1085.4502.04
SMIQB12	Memory Extension	1085.2800.04
SMIQB14	Fading Simulator	1085.4002.02
SMIQB15	Second Fading Simulator for two channel or 12 path fading	1085.4402.02
SMIQB17	Noise Generator and Distortion Simulator	1104.9000.02
SMIQB20	Modulation Coder	1125.5190.02
SMIQB21	BER Measurement	1125.5490.02
SMIQB60	Arbitrary Waveform Generator	1136.4390.02
SMIQK16	Digital Standard IEEE 802.11b	1154.7700.02

IQ Simulation Software:
WinIQSIM^{TM} can be downloaded from the Rohde&Schwarz website:
http://www.rohde-schwarz.com

ROHDE & SCHWARZ GmbH & Co. KG · Mühldorfstraße 15 · D-81671 München · P.O.B 80 14 69 · D-81614 München ·
Telephone +49 89 4129 -0 · Fax +49 89 4129 - 13777 · Internet: http://www.rohde-schwarz.com