Keysight Technologies

IEEE 802.11 Wireless LAN PHY Layer (RF) Operation and Measurement

Application Note

KEYSIGHT TECHNOLOGIES

Introduction

This application note is written for those who desire an understanding of the test system configuration and testing of Wireless LAN (WLAN) devices and some of the issues that arise in connection with it. Further detail on many of the topics covered herein may be found in the Appendices.

The use of wired Local Area Networks has become ever more commonplace, even in situations where only a few computers need to be connected together. Price reductions have helped stimulate use and so have easier system configuration and increasing robustness.

A number of applications can benefit from the removal of the cable connections needed by a fixed LAN. Remote database access is a good example – from warehouses to retail stores to college campuses. WLAN cards will also be used soon for public Internet access in certain "hotspots," such as airports and hotels, where users are largely stationary and need access to a variety of medium- and high-speed digital services.

The IEEE 802.11 Wireless LAN specification was written to extend the functionality provided by the IEEE 802.3 Wired LAN standard. A radio interface adds considerable complexity; however, advances in highly integrated radio circuitry have made it possible to bring the cost of wireless devices down to affordable levels.

The ETSI BRAN HiperLAN/2 is an alternative specification for WLAN, with more extensive services, but diminishing commercial support. Its radio frequency (RF) operates in a similar way to 802.11a, although the allocation of transmission time-slots is quite different. Increasing collaboration is now taking place between those involved in the two standards.

While wired LAN already uses numerous techniques to deal with multiple users who must access a central server, additional steps must be taken to deal with the vagaries of WLAN links. A WLAN link has many less-than-ideal transmission characteristics, such as the dependency of signal errors on physical position and the ability of nearby RF devices to "eavesdrop" or interfere.

Security is always an important issue in radio transmissions. Considerable effort is being made to ensure that security for WLAN is both adequate and straightforward to apply.

This application note begins with a brief description of an IEEE 802.11 Wireless LAN system, emphasizing the radio or physical layer. Consistency at this level provides the basis for widespread device interoperability.

Comparisons are made to cellular radio systems to highlight the significant differences in the operation of the two links. Transmitter and receiver measurements needed to verify conformance with the IEEE specification are described, along with information on how to set up the Device Under Test (DUT) and the test equipment. Appropriate equipment from Keysight Technologies, Inc. is highlighted in Appendix A. Finally, Appendices B and E provide a wide range of reference and learning material.

Table of Contents

1. Basic Concepts Of IEEE 802.11 Wireless Lan

As the name implies, Wireless LAN was designed to extend the data transfer function of a Wired LAN. The heritage is important—standards which define how it works continue to evolve, but at its heart, WLAN is a system for transferring packets of digital data wirelessly and without error whenever an originating computer can send them. In this respect, it is like an asynchronous Bluetooth link but unlike a synchronous cellular voice connection, which is based on analog transmission. Transmissions take place after a device has first listened to make sure the channel is clear, a method called Carrier Sense Multiple Access/with Collision Avoidance (CSMA/CA). It is fundamentally different from the rigorous timeslot allocations used in cellular and cordless phones. This may cause confusion for engineers migrating from other technologies.

Software is used to adapt LAN packets for transmission over the radio path, which, of course, is far less predictable than a wired path. This protocol is called Logical Link Control (LLC) and Medium Access Control (MAC). User data is encoded, headers are added, and longer packets are broken up (fragmented) before transmission.

–

The most widely used WLAN systems involve Network Interface Cards (NICs, also referred to as STAtions), and Access Points (APs). These allow the users to create individual wireless-to-wired LAN links, called Infrastructure Basic Service Sets, or BSS. An Extended Service Set (ESS) entails the construction of a complete network. The access point acts not only to transfer data from wired to wireless devices, but is also responsible for allocation of the radio channel to the clients it serves.

In the absence of other users in the license-exempt bands used by WLAN, a BSS can be configured to make efficient use of the radio spectrum. Even in this situation, throughput for individual users is usually only a fraction of the peak data rates which WLAN systems are known by. Typically, the maximum throughput is half the nominal peak rate and drops even more as clients are added (there may be no predetermined limit), or as the NIC moves away from the Access Point. Coverage depends on both the physical environment and the frequency band; however, in many cases the transfer time for a file over WLAN will be as low as that of a wired LAN because of bottlenecks occurring elsewhere.

Two other WLAN schemes exist. A Peer-Peer (ad hoc) Independent Basic Service Set, or IBSS, involves the use of two NICs. Interoperability between such cards may be limited due to different vendor designs, but otherwise this can be one of the most straightforward ways of effecting wireless data transfer between mutually friendly devices. Extenders are more specialized system components which deal with radio propagation problems while not acting as specific network end-points.

Table 1: System frequency bands, data rates, and modulation schemes

			Transmit Scheme			Modulation			
System	Frequency Band	Max Data Rate (Mbps)	CCK	PBCC	OFDM	BPSK	QPSK	16 QAM	64 QAM
802.11b	2.4 GHz	11		OPTION		DIFF	DIFF		
802.11g	2.4 GHz	54		OPTION		DIFF	DIFF		
802.11a,h	5 GHz	36, Opt to 54							
HiperLAN/2	5 GHz	54							
HiSWAN	5 GHz	54							

NOTE: DIFF=differential modulation encoding.
802.11g includes an option for mixed CCK-OFDM.

1.1 Use of Radio Carriers and Modulation

Radio is not the only medium addressed by the 802.11 specification, but it will be the focus of this application note.

Data must be applied to a radio carrier before transmission. The carrier can be used in several ways:

1.1.1 Modes of Carrier Operation

- FHSS – Frequency Hopping Spread Spectrum
  A single carrier switches frequency to reduce the likelihood that it will interfere with, or be interfered by, other carriers.

- DSSS – Direct Sequence Spread Spectrum
  The energy in a single carrier is spread over a wider spectrum by multiplying data bit(s) with a special 11-bit pattern, called a Barker key. This is done at a chip rate of 11 MHz. This technique can help reduce interference from narrow-band sources. The IEEE 802.11b-1999 specification uses an 8-bit key.

  Two schemes are used by 802.11b to spread the spectrum of a single carrier. CCK (Complementary Code Keying) is mandatory, while PBCC (Packet Binary Convolutional Coding) may be added. Channel agility may also be added as an option.

- CCK – Complementary Code Keying
  This is used to increase IEEE 802.11b's peak data rate from 2 to 11 Mbps, while still using QPSK (Quadrature Phase Shift Keying) modulation. It does this by first increasing the data clock rate (symbol rate) from 1 Mbps to 1.375 Mbps, then taking data in 8-bit blocks (8*1.375 = 11). Six of the 8 bits are used to choose 1 of 64 complementary codes, which are 8 chips long and clocked out at 11 MHz. Thus all 8 chips are "used up" in (1/1.375) µs – the time before another byte is ready. The other 2 bits are combined with the code in the QPSK modulator.

- PBCC – Packet Binary Convolutional Coding
  This scheme is optional for IEEE 802.11b and g. It makes use of Forward Error Correction to improve the link performance when noise is the limitation. Scrambled data is fed into a convolutional encoder. The encoder consists of a 6-stage memory, with specific taps combined to give two outputs. The four possible output states (00,01,10,11) are mapped into two possible QPSK states (11 Mbps). A codeword controls how the chosen state alternates over time. The RF modulator is driven from this point.

  IEEE 802.11a, HiperLAN/2 and HiSWAN use OFDM.

- OFDM – Orthogonal Frequency Division Multiplexing
  OFDM uses multiple carriers, of which there are 52, spaced 312.5 kHz apart. Data is sent on 48 carriers simultaneously, with 4 used as pilots. The time to transmit each bit increases in proportion to the number of carriers. This makes the system less sensitive to multi-path interference, a major source of distortion.

  This note concentrates only on DSSS and OFDM systems. Some systems, such as 802.11g, may use both methods during the same RF burst, making them more compatible with 802.11b systems.

- Modulation
  The RF carrier(s) must be modulated. All the WLAN systems described in this note use a form of phase-shift keying for the preamble. More complex schemes, such as 64QAM (Quadrature Amplitude Modulation) give faster bit rates for user data, but

require better radio performance and less noise to work to their full potential. BPSK (Phase Shift Keying), QPSK, and QAM are described in standard RF texts.

Often, the modulation format changes during the transmission. This is because the early part of the burst contains important information about the burst, including analog characteristics such as frequency, and digital information such as burst length. Simpler modulation formats are less prone to bit errors, and thus are more suitable to use early in a burst.

1.1.2 Frequency Bands and Power Levels

WLAN systems operate in one of the frequency bands shown in Figure 1 below. The maximum transmit powers are also shown. Transmit Power Control and Dynamic Frequency Selection, part of the HiperLAN/2 specification, will be added to 802.11a operation to satisfy European regulatory requirements.

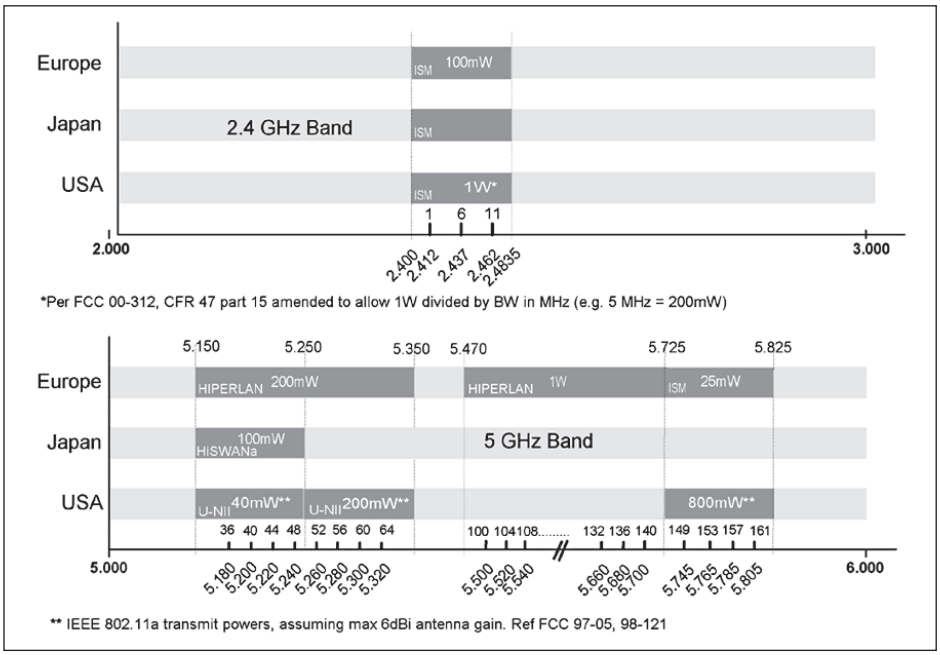

Figure 1: Major channel allocations and power levels

1.2 Anatomy of a WLAN device

Physically, the most common format of a WLAN device is that of a PC Card (PCMCIA), suitable for direct connection to a laptop computer. Access points may simply have a PC Card mounted on a motherboard.

Electrically, the WLAN card is split into two major sections: the analog RF (PHY layer) and digital Baseband (MAC, or Medium Access Control) processing. The connection to the host computer is generally through the PC Card or Compact Flash interface.

In an access point, additional digital circuitry is used for the interface with a wired LAN (i.e., via Cat 5/Cat 6 cabling). Some designs provide power from the LAN wiring rather than from a separate power supply.

1.2.1 Description of Operation

Figure 2 below is a generic block diagram of a radio system. As with most electronic systems, newer radio designs have higher levels of integration, although performance trade-offs must be made. This applies particularly to the receiver. Some systems will not use, or provide access to, the intermediate signals discussed in this note. Readers are advised to carefully study the block diagram of the system they must test.

The Local Oscillators (LOs) share both transmit and receive functions. Frequency doubling or tripling is used (although not shown in the diagram) to give better Voltage Controlled Oscillator (VCO) performance and to isolate the RF output from other signals.

1.2.2 Data Reception

Diversity reception is used to reduce the effect of nulls on signal levels. A Receive Signal Strength Indication (RSSI) test, made during the short training sequence, determines which path is switched in for a particular burst. The chosen signal is fed through an amplifier/downconversion chain before being mixed into a pair of quadrature signals which are digitized. Analog gain control means that 6 to 8 bits is usually sufficient for the A/D conversion. Some hybrid schemes use DSP (Digital Signal Processing) for the IQ (In-phase Quadrature) separation and therefore need only a single connection from the analog circuit.

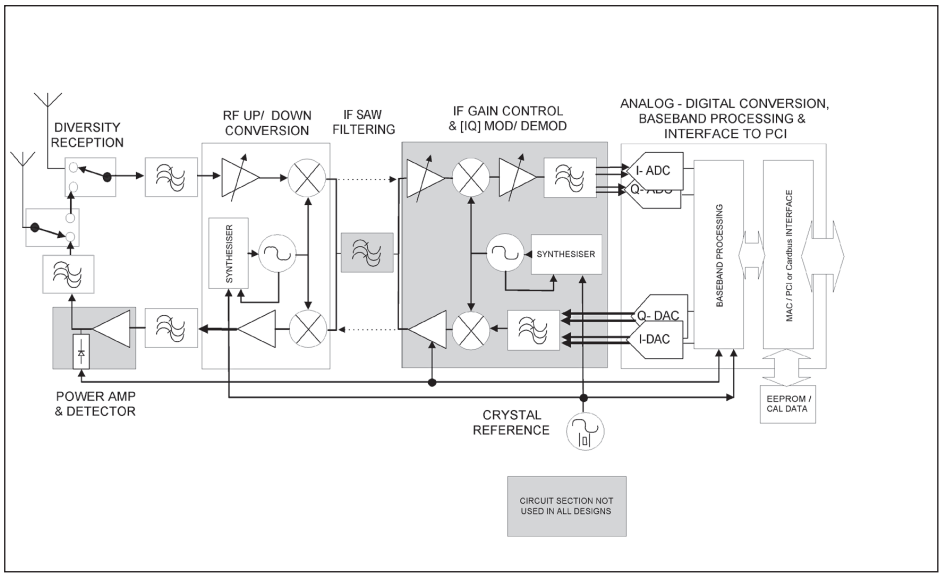

Figure 2: Block diagram of a WLAN card

An equalizer and other components of digital circuits are able to reduce the effect of distortions such as frequency error or amplitude variations, but the design itself must ensure that others errors—such as high-frequency local oscillator phase noise—are low enough to guarantee the needed link performance.

The RF portion of 802.11b, which is difficult to make small and inexpensive, is not so challenging in terms of Bits/Hz. However, the higher data rates of 802.11a and the doubling of channel frequency make it far more difficult to design and manufacture.

Receiver sensitivity is important because it determines the maximum range over which a WLAN link can operate. There are secondary system benefits as well. If one link completes a transmission faster than another because the Packet Error Rate is lower, battery consumption will be reduced and less interference will occur to other users. In a real-world Industrial, Scientific and Medical (ISM) or Unlicensed National Information Infrastructure (UNII) environment, interference suppression and linearity will directly affect the performance of the radio. They are therefore important test parameters. It may be more difficult to distinguish between causes of poor performance as hardware becomes more and more integrated and if special test modes are not available.

1.2.3 Data Transmission

Transmitter performance requirements usually necessitate an external power amplifier (PA). Cost, current consumption, and linearity combine to demand considerable attention to detail in this choice. Pre-distortion of the signal from Baseband processing may allow less stringent PA design, but it may also limit the choice of devices used if it relies heavily on a particular performance characteristic. Diversity transmission may also be applied (the switching in Figure 2 does not allow for this).

Designs with SAW (Surface Acoustic Wave) or Dielectric Bandpass filtering in the IF (Intermediate Frequency) are suited to normal TDD (Time Division Duplex) operation, but also have fewer options for internal loop-back paths for testing and self-calibration. Self-calibration becomes important when the performance of the analog circuit is affected by temperature.

Differential signal paths are becoming more common as power supply and signal voltages decrease and background noise becomes more prominent. Balun transformers can be used when single-ended signals are needed.

Although the analog hardware can be tested in isolation, it needs to be combined with DSP (Digital Signal Processing) of the Baseband circuit in order to comprise a complete transceiver. Care is needed when modeling total system performance because a number of error contributions may not be just simple arithmetic additions, but result from analog and other phenomena.

Algorithms within the DSP play an essential role in both transmission and reception. Figure 3 shows an example of the main processing blocks needed for 802.11a/ OFDM system.

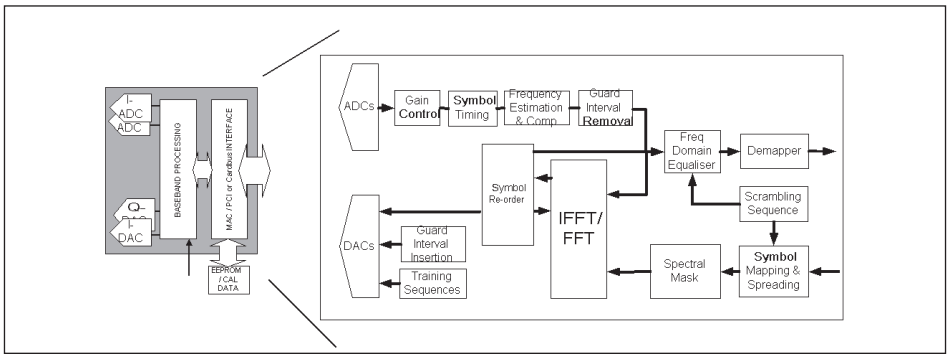

Figure 3: Digital processing blocks for an OFDM transceiver

1.3 Time Division Duplex and Frame Structure

A WLAN device can only transmit or receive at a single time. Transmissions occur as bursts (frames) which vary in length and spacing, usually in the range of a few hundred microseconds to one millisecond. The 802.11b CCA (Clear Channel Assessment) receiver test specifies the longest possible 5.5 Mbps frame–3.65 ms.

The basic structure of the frames is shown in Figures 4 and 5. The preamble is used by the receiver to adapt to the input signal. This may involve frequency and phase error equalizing, as well as time alignment. The header contains a wealth of information, including the destination address and the format of the remainder of the burst. User data is transferred from the original packets, which are fed into the MAC layer. Long packets may be fragmented (broken up) if the radio determines that this will improve link performance.

Five time periods in the 802.11 specification determine the spacing between transmissions. The physical values vary according to the standard used and are shown in Table 2.

The combined effect of using CSMA/ CA, data which is sent when ready and different time intervals between frames, is to produce seemingly random spacing between bursts.

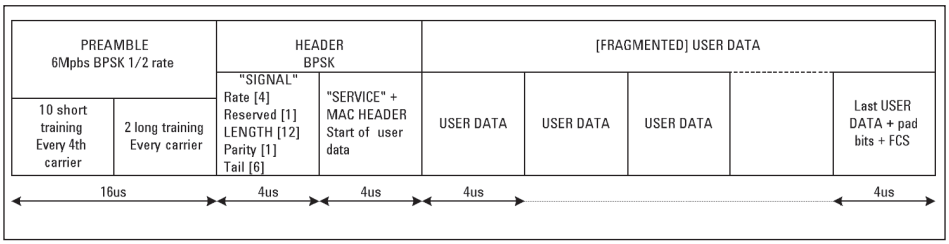

Figure 4: IEEE 802.11a frame structure

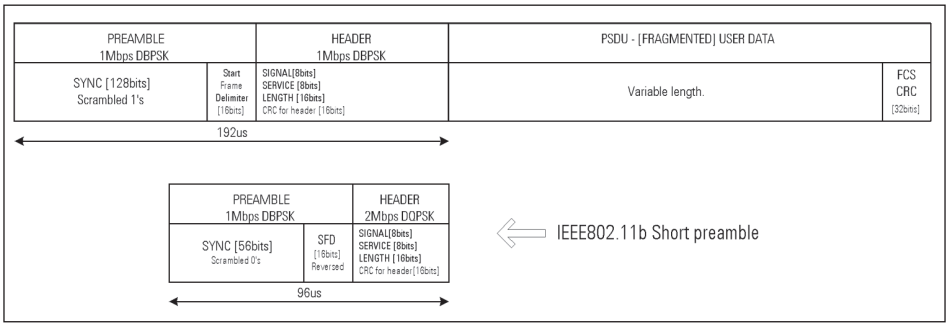

Figure 5: IEEE 802.11b frame structure with short/long sync

1.4 The Medium Access Control Layer

The Medium Access Control (MAC) layer provides an asynchronous data packet delivery service to the LLC software that uses it. This means that it is impossible to predict exactly when transmissions will take place. The MAC software takes the data and, identifying the PHY layer with which it is working, transports the data to the MAC layer software in the client's receiver. Three types of MAC Frames are used to provide this service:

- Management Frames
  Eleven sub-frame types are used for link management. They provide the means for establishing and terminating a link—beacon transmission and probe requests, authentication, and association.

- Control Frames
  Six sub-frame types are used to make sure the link functions correctly: Request To Send, Clear To Send, ACKnowledged, Power Save, Contention Free, and CF – End + CF–Ack.

- Data Exchange Frames
  Eight sub-frame types are used and all except one contain user data. Most of them make the link more efficient by adding link control information.

Figure 6a (below) shows how these frames are used (not to scale). Figure 6b shows the major frame timing options.

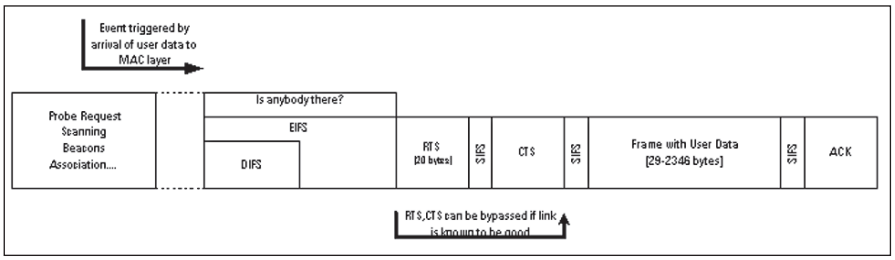

Figure 6a: Outline process to send data (IEEE 802.11)

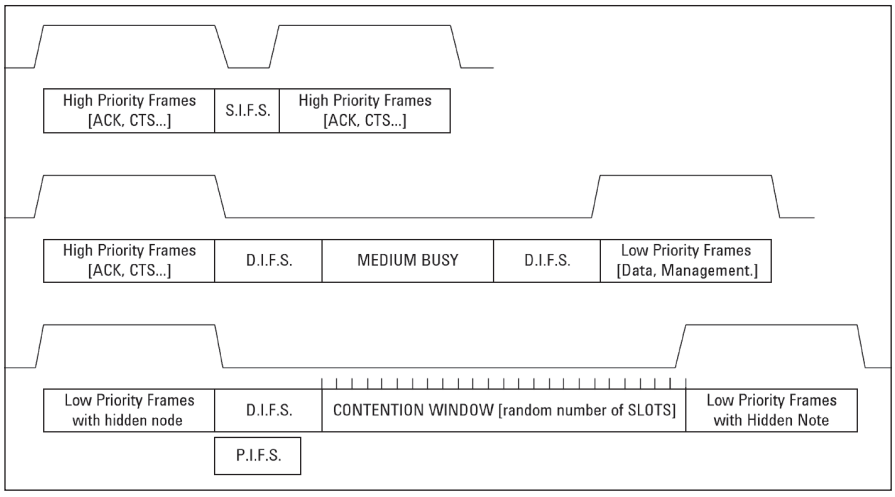

Figure 6b: Frame timing (IEEE 802.11)

1.5 Establishing Contact

Starting when a device is powered up, software above the MAC layer must stimulate the device to establish contact. Either active or passive scanning is used. The IEEE specification allows for different implementations, so characteristics may differ between devices.

Table 2: IEEE 802.11 Timing Intervals

Time Interval	802.11a	802.11b
SIFS - Short Inter Frame Space	16 µs	10 µs
SLOT	9 µs	20 µs
Priority IFS = SIFS + SLOT	25 µs	30 µs
Distributed IFS = SIFS + 2 SLOTS	50 µs	50 µs
Contention Window Min	15 slots	31 slots
Extended FS - much longer	Variable	Variable

1.5.1 Active Scanning

Active Scanning is the fastest way to establish contact, but consumes more battery power. Listening for a clear channel, the device which seeks to establish contact sends a Probe Request. If the Service Set IDentity matches, the recipient then sends a Probe Response. The scanning device uses this information to decide whether or not it will join the (I)BSS, but there is no further transmission at this point.

1.5.2 Passive Scanning

In Passive Scanning, Beacons and Probe Requests are used. After selecting a channel, the scanning device listens for Beacons or Probe Requests from other devices. A Beacon is transmitted from an Access Point in a BSS or ESS. It contains information about the AP and a timing reference. Beacon transmissions occur on a 1024µs time grid, spaced roughly every 100ms. Like other transmissions, they are subject to a clear channel test and so may be delayed.

1.5.3 Authentication

Before any user data is transferred, the Sender and Receiver must agree that they are ready to talk. These are processes of authentication (which happens first) and association. There are several others (e.g., random exponential transmission back-off) which can be used if a device finds that the channel is not clear when it is ready to transmit.

Earlier, a list of modulation rates was shown for the different 802.11 standards. The specifications do not define exactly how these are selected. Different designs will employ different proprietary algorithms. Currently, there is no "quality of service" standard in the MAC frames. However, the transmitting device is able to gauge the fidelity of the link based on the regularity of ACK frames coming back from the device it is seeking to contact.

1.6 Exchanging Data: Two Methods

When two WLAN devices are ready to exchange data, they must choose one of two methods. The decision depends on the expected performance of the radio link.

1.6.1 Two-step Exchange

Two-step data exchange is simply the sequence:
- Send
- Acknowledge

This is good for short packets or a sparsely-used RF environment.

1.6.2 Four-step Exchange

More typically, however, exchange is a four-step process:
- Request To Send (RTS)
- Clear To Send (CTS)
- Send
- Acknowledge

This is used for long frames, where there is a higher likelihood of interference with, or from, an RF-noisy environment. A special MAC signal (dot11RTSThreshold) is used to choose between frame lengths.

2. Phy Layer (Rf) Test Suite

The measurements described below are used mainly to determine if a WLAN device conforms to a relevant standard. The only mandatory RF testing is in the regulatory statutes of various countries.

Transmissions using an antenna or live network may be unpredictable. While a number of tests described here can be performed live, a screened RF connection and/or environment is normally used. This is essential for repeatable receiver measurements. Signals at 2.4 GHz and 5 GHz act very differently from the audio and digital signals with which most people are familiar.

Readers are encouraged to seek competent technical advice if they wish to perform RF measurements and are new to the subject.

Table 3: Summary of IEEE 802.11a,b transmitter tests and configurations

IEEE Ref.#	Test	Packet Type	Payload	Instrument Configuration
18.4.7.1 18.4.7.2 17.3.9.1	Transmit Power Average	Longest Framed ≥1024 byte payload	PN9(15)	Edge Trigger, using Trigger hold off (set to frame length)
	Transmit Power Peak	Longest	PN9(15)	Measurement BW ≥18 MHz to capture peak or “Properly adjusted” for limitations in measurement BW
	Power Density 802.11a	Longest	PN9(15)	RBW 1 MHz Detector type, Sweep Time: See notes
18.4.7.6	Power Rise/Fall 802.11b	Longest		RBW ≥18 MHz, VBW ≥1 MHz, to suit <2 µs rise time
18.4.7.3	Spectrum Mask	Longest Use unframed Test mode signal or time-gating	PN15 Scrambler ON	802.11b:RBW 100 kHz, VBW 100 kHz Detector type, Sweep Time: See notes
17.3.9.2				802.11a: RBW 100 kHz, VBW 30 kHz Detector type, Sweep Time: See notes
18.4.7.7	RF Carrier Suppression 802.11b	Longest Framed	0101 DPSK Scrambler OFF	RBW 100 kHz, VBW 100 kHz Detector type: See notes
17.3.9.6.1	Center Frequency Leakage 802.11a	Longest Framed		Reference and result both measured during channel estimation part of burst
17.3.9.6.2	Spectral Flatness 802.11a	Longest	PN9(15) Scrambler ON	Use Channel Estimation from pre-measurement equalizer.
18.4.6.8	Transmission Spurious	Longest	PN9(15) Scrambler ON	RBW > 1 MHz. If smaller, integrate result to be equivalent of 1 MHz [Quasi] peak detector
17.3.9.4 18.4.7.4	Center Freq. Tolerance	Longest Framed	PN9(15) Scrambler ON	802.11a requires Tx clock & symbol clock to come from the same oscillator. Method depends on Test Mode
17.3.9.5	Symbol Clock Freq. Tolerance			802.11a Tested by inference from RF Center Frequency
17.3.9.6.3	Constellation Error 802.11a	802.11a 20 frames ≥16 OFDM symbols	PN9(15) Scrambler ON	An equalizer is used before the measurement. Works on Short or Long training sequence
18.4.7.8	Error Vector Magnitude 802.11b	Unframed	1111 Scrambler ON	Equalizer removes frequency error before measurement

Note: Packet types, payloads, and measurement configurations, shown in italics, are recommendations for testing where a specification is unclear. Test refrence numbers which start with 17 apply to IEEE 802.11a. Test refrence numbers which start with 18 apply to IEEE 802.11b.

3. Transmitter Measurements

If not controlled, many transmitter parameters can reduce the performance of WLAN systems, or even prevent RF devices from working together. Tests have been devised to prevent this from happening. Table 3 provides a summary.

Transmitter tests are described first because some transceiver problems can be found quickly by analyzing transmitted output first. Examination of the diagram in Figure 2 (pg 5) shows why this is the case: The local oscillator(s) (LOs) for frequency up- and down-conversion are shared, so many impairments on an LO which could affect the receiver will be immediately evident in the transmissions.

3.1 Test Conditions and Measurement Setup

Two main configurations are used for testing the transmitter path. They are distinguished by the signal interfaces and the way the device is controlled. One is suitable for only RF/analog circuitry, while the other is applicable to a complete WLAN device. Figure 7 (right) shows the configuration for the RF/analog case. Control of the circuit requires proprietary hardware, but the IQ Baseband signal for driving the transmit path can be provided by an ESG-C signal generator.

Some WLAN designs have an intermediate signal available, usually in the 100s of MHz range. It may be useful for selecting a signal analyzer/signal generator with coverage at this frequency.

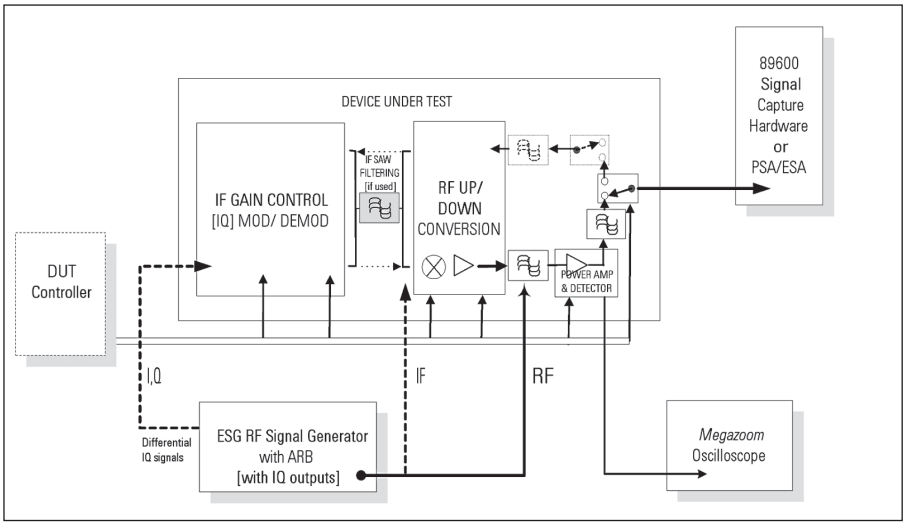

Figure 7: Transmitter test configuration for RF/analog circuitry

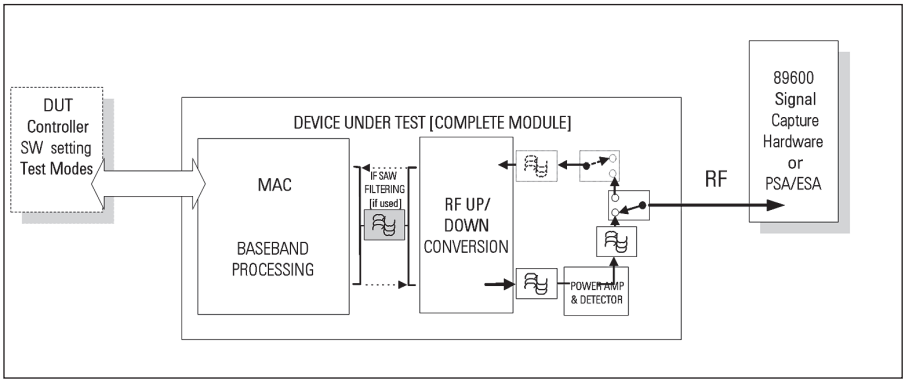

Figure 8: Transmitter test configuration for a complete WLAN card

The antenna in a real-world system is often designed to focus transmit power in a certain direction and will have a radiation efficiency that depends on the exact implementation. This can make it difficult to compare the performance of different pieces of RF hardware. Thus some measurements refer to Effective Isotropic Radiated Power (EIRP). Physical measurements involve the use of a remote antenna for testing, which can be very impractical. Instead, theoretical calculations can be used to provide a correction coefficient for measurements made over a direct cable connection.

3.1.1 Measurement Triggering

Measuring framed RF signals requires the use of a trigger signal. Many test instruments have this as an internal feature. In 802.11a, HiperLAN/2, and 802.11b, a complication occurs because of significant variation in signal level due to modulation. Careful selection of the trigger level may solve the problem. Alternatively, the Trigger Hold-off function may be used if the frame period is fairly regular. Trigger Hold-off acts to disable the trigger circuit for a defined period of time after a trigger signal has been acted on.

3.1.2 Interaction with DSP

Often, a complete WLAN card must be tested. It is only at this point that problems of interaction between the Digital Signal Processing (DSP) and analog circuitry are uncovered. These can be as straightforward as power supply de-coupling or as complex as electromagnetic coupling. Figure 8 shows the configuration needed to test a complete WLAN device. It is simpler than Figure 7 because the MAC processor provides the stimulus. The results are therefore the combined effect of DSP control in the MAC and the analog circuit performance that follows it. Tests may be constrained, in run time as well as circuit evaluation, by MAC control software available to the user.

3.2 Test Modes

The IEEE 802.11 specification describes various Test Modes, which control the operational state of the radio and a number of transmit parameters. These are more likely to be used when testing a complete WLAN Card. They are shown in Table 4. Other parameter options may become available for 802.11a.

The IEEE 802.11 specification does not include any over-the-air control of Test Mode functions. Hence it is often not a straightforward task to provide the complex, integrated testing expected of modern wireless devices. Proprietary device control software may also be needed. If Test Modes are supported, a second WLAN device, shown in Figure 8, is usually not needed. However, it may be a useful addition to handle operational (functional) testing.

A secondary effect of the independence of test equipment and device control is that system control software must pay special attention to the triggering and timing of measurements.

3.3 Transmitter Power

The power measurements described below will be affected by loss and the Voltage Standing Wave Ratio (VSWR) of cables and other RF components used in measurement. It is important, both at 2.4 GHz and 5 GHz, to use components suitable for the frequency range.

The 802.11 standard does not specify a tolerance limit for the impedance of the antenna ports or the frequency range to be tested. A port match of 10 dB (VSWR~2:1) is often used, representing an impedance variation of between 25 and 100 ohms. Combined with at the antenna, but no other losses, this can produce signal variations of up to ±1 dB. In addition, mismatches at harmonic frequencies may cause amplifier non-linearity and produce modulation quality problems. These should be analyzed during design.

Table 4: Description of 802.11 test modes

Name	Type	Valid Range	Description
TEST_ENABLE	Boolean	True, false	True enables test mode
TEST_MODE	Integer	1,2,3	01 - Transparent Receive 02 - Continuous Transmit 03 - 50% Duty Cycle
SCRAMBLE_STATE	Boolean	True, false	True turns scrambler ON
SPREADING STATE	Boolean	True, false	True turns spreading ON Not applicable for 802.11a
DATA TYPE	Integer	1,2,3	Selects between undefined data patterns, e.g. 111,000,random
DATA TYPE	Integer	02,04,11,22	Value represents half the transmitted bit rate, e.g. 22 = 11 Mbps
PREAMBLE TYPE	Boolean	Null,0,1	0 - Long 1 - Short
MODULATION CODE TYPE	Boolean	Null,0,1	0 - CCK 1 - PBCC

3.3.1 Average Output Power

If a device's transmitter and receiver are working correctly in all other respects, then average transmit power will be the main factor affecting the WLAN's coverage area.

All normal WLAN transmissions are framed (bursted). If a fixed mark-space ratio can be generated by the test software, it is possible to perform a power measurement using detectors with average responses. A correction factor can be used to correct the lower reading obtained. This technique can be a little laborious, however. The measurement in Figure 9 was triggered from the burst edge and is thus simpler to make.

It is common to make just an average power reading using unframed data. This gives an indication of the operating level of the device, but removes all information about the dynamic performance of the transmitter path, unless done in conjunction with a modulation quality or spectrum test.

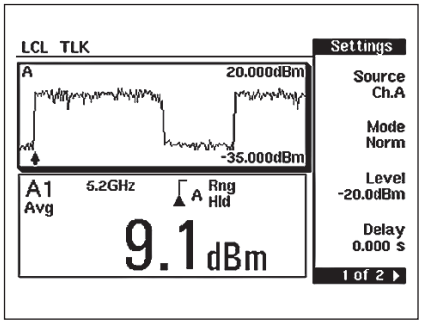

Figure 9: Average power measurement of IEEE 802.11a, using EPM-P

3.3.2 Peak Output Power, Complementary Cumulative Distribution Function (CCDF)

In a system using bursted RF, power peaks are often associated with turn-on spikes. As Figure 10 shows, for IEEE 802.11a and HiperLAN/2, significant peaks can be seen during the entire burst. In a standard signal, the peaks can be as much as 11 dB higher than average over a single frame. If the peaks are not transmitted correctly, the receiver will record Bit Errors or Packet Errors. Thus the overall link quality will be reduced.

IEEE 802.11b also uses modulation formats which cause variations of 2-3 dB above average power throughout the burst. These variations can be very short, so a wide measurement bandwidth is needed to accurately characterize the signal. If the measurement bandwidth is less than the signal bandwidth, it is impossible to track peaks accurately. For example, if we assume that signal power distribution is Gaussian and that video measurement bandwidth is 5 MHz, the peak power level will read low by 2-3 dB. The average power, however, will be correct to within 0.5 dB. Regulatory requirements usually stipulate a "true peak measurement for the emission in question over the full bandwidth of the channel." This implies a minimum capture-bandwidth of 18 MHz.

Fortunately, measurement methods have been developed to deal with the variable amplitude formats of 802.11. If we look at the Power vs. Time plot in Figure 10, we can see that the highest powers occur relatively infrequently. The probability that the signal will exceed a certain value decreases as the power threshold increases. If some peaks are clipped, it is useful to know how often this happens in order to allow adjustment of amplifier bias currents.

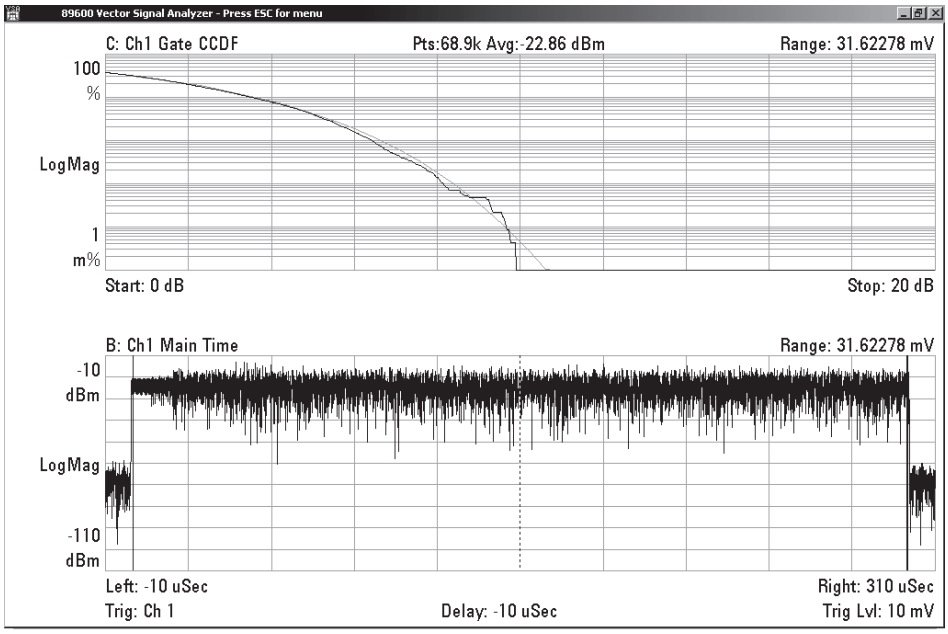

Figure 10: Combined display plot, including IEEE 802.11a CCDF measurement

Note: Measurement gating must be used to avoid including a zero power reading between bursts.

Figure 10 also shows a plot of Power Level (horizontal axis) vs. Probability (vertical axis). This is known as a Complementary Cumulative Distribution Function (CCDF) plot. The left-hand power reference is automatically set to the average of the measured signal—in this case, -22.858 dBm.

The gray curve is the equivalent of Gaussian distributed noise and serves as a guide to possible problems.

When required, calibration of the absolute power level of the signal analyzer may be carried out using a CWRF (Continuous Wave Radio Frequency) signal and power meter. Automated functions may be available in the test equipment and software.

3.3.3 Transmitter Power Control

Control of the transmit power level is part of the HiperLAN/2 specification and of IEEE 802.11b for transmit powers greater than 100mW. It is not part of 802.11a, but will be introduced with the 802.11h specification. This is to meet European Dynamic Transmit Control requirements, which are intended to address some of the needs of other users operating at 5 GHz.

HiperLAN/2 has different requirements for the Access Point and the Mobile Terminal (MT). The AP has 16 power levels, ranging from +30 dBm to –15 dBm, in 3dB steps. The MT has transmit power intervals of –15 dBm to -9 dBm, -9 dBm to +9 dBm, +9 dBm to +18 dBm, and +18 dBm to +30 dBm.

The configuration for testing power control is the same as for output power, with the addition of trigger signals to ensure that measurements are made only after the device has settled at a new power level.

Note: WLAN systems may not have the high-speed power control algorithms of some cellular systems. Separate test control may be required for design and manufacture.

3.4 Transmit Output Spectrum

3.4.1 Input Attenuation Settings

The measurement bandwidths used for swept spectrum measurements are considerably less than the signal bandwidth—100 kHz, as compared to 18MHz. This has the effect of reducing the readings displayed for normal markers. However, the full signal power is fed to the input mixer of the signal analyzer, which will introduce distortion if it is overloaded. Therefore, when using manual control of input attenuation, adjustments should be made on the basis of total signal power. This may be shown as Channel Band (or Total) Power on the instrument.

3.4.2 Transmitter Spectrum Mask

This test is used to ensure that multiple WLAN devices do not unduly interfere with each other. It is associated with the adjacent channel receiver tests in section 6.6.

The need for a linear transmitter path was described earlier. Inevitably, a designer has to make a trade-off between average transmit power and distortion. While not a direct measure such as Packet Error Rate, the spectrum test can be a good indicator of deteriorating performance. Visible changes in the spectrum are likely to occur well before Packet Errors occur, due to modulation errors. A spectrum test may be combined with Error Vector Magnitude measurements to get to the root cause of a problem, but note that some EVM errors get worse as the spectrum improves.

The IEEE 802.11 standards do not specify a transmit modulation filter function; however, filtering is implied in the spectrum mask. Figure 11 shows an 802.11b signal where the modulation filtering is correct, but where the designer has forgotten to include an anti-alias (reconstruction) function.

Signal Framing

The IEEE 802.11b spectrum mask is that of a continuous signal. The drawback with configuring a transmitter for continuous output is that the final result may not be representative of actual performance under burst conditions. Some standards are explicit in the need to use framed signals.

Several options are available for measuring the spectrum in practice:
- The transmission may be modified to produce a continuous (unframed) signal
- A slow sweep period can be used to give a complete display of a framed signal
- Some form of gated spectrum analysis may be performed on the burst using a vector signal analyzer
- Detector Type, Sweep Time, Signal Payload, Reference Level Setting

Spectrum masks are relative, based on a reference level measurement. Fast sweep times can cause variations in the reference level taken from one sweep to the next. This happens if the display point does not include all the level variations seen through the burst (see notes in Peak Power measurement, section 3.3.2). If the payload data varies from one frame to the next, it will increase the likelihood of reference level variations.

A 500 ms sweep was used for the reference measurements in Figures 11 and 12.

The IEEE 802.11 standard does not specify the type of measurement detector to be used. Empirically, the shape of the spectrum (for an unframed signal) is similar using either a swept spectrum analyzer or vector signal analyzer.

A number of other communication standards, including GSM and Bluetooth, now use zero-span, multiple offset measurements for adjacent channel testing. An average detector is used. A continuous sweep, using a relatively slow sweep time, will give similar results.

A swept spectrum analyzer with an average detector was used for Figures 11 and 12. The measurement is not gated. The spectrum response to the complete transmission is measured, but note that the absolute level will vary for a framed signal, depending on the mark-space ratio of the signal. The Average Detector function in the PSA/ESA spectrum analyzer supercedes the technique previously offered by Video Filtering.

Note: Manually setting the Video Bandwidth too low when using Average Detector will cause an Uncal error message to appear.

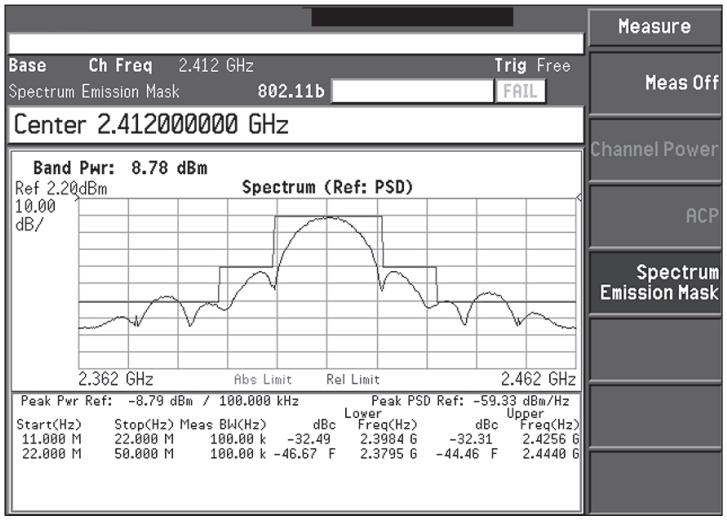

Figure 11: IEEE 802.11b signal failing spectrum test mask. Regulatory tests effect outer limit line levels.

A peak detector will produce a similar-looking plot if there are no short transient effects. The absolute level will be higher, plus it is more sensitive to changes in the reference level setting due to different data patterns.

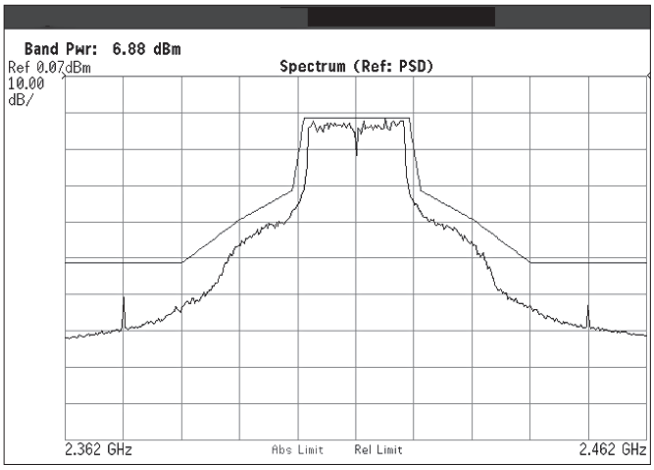

Figure 12: IEEE 802.11a signal measured using Keysight performance spectrum analyzer

A vector signal analyzer can also provide good results, and can be programmed to synchronize the measurements with specific points in the frames. This can result in more stable reference level readings.

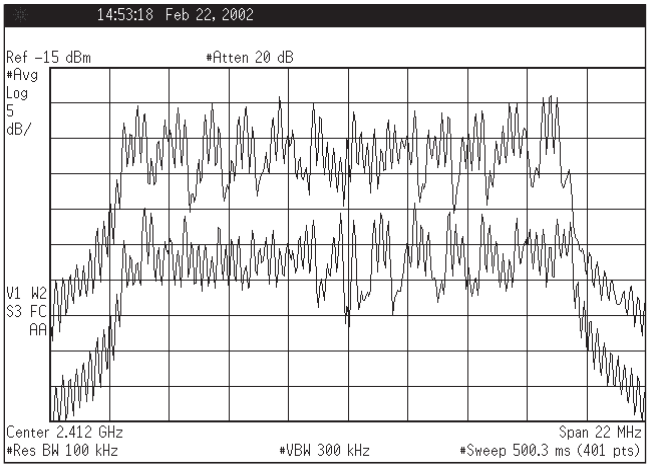

Figure 13: Power spectral density measurement made on an IEEE 802.11a signal with 01 pattern and scrambling off, showing ripple due to data pattern

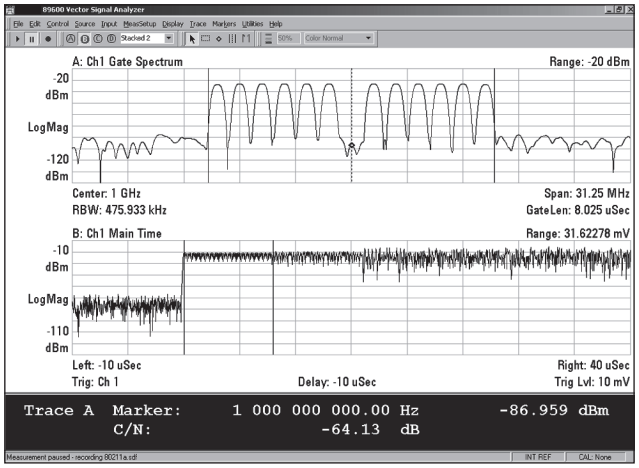

Figure 14: Plot showing center frequency leakage of an IEEE 802.11a signal

Note: If variations in individual channel powers are suspected, they can be separately identified with the gated channel response measurement in section 3.4.6.

3.4.3 Power Density

Given the "noisy" nature of IEEE 802.11a, some measurements like the reference measurement for the spectrum test are defined as power spectral density. Expressed as power within a specified bandwidth, the result is nominally independent of the measurement bandwidth. The measurement should generally be made under realistic operating conditions. Variations will occur if the signal level varies with frequency because of the data pattern being transmitted. The data pattern or scrambling state should be specified. In Japan, the maximum transmitted power is expressed as 10 mW/MHz. In the United States, a conversion factor of 16 is used to go from a power density of, say, 2.5 mW/MHz to 40 mW/MHz.

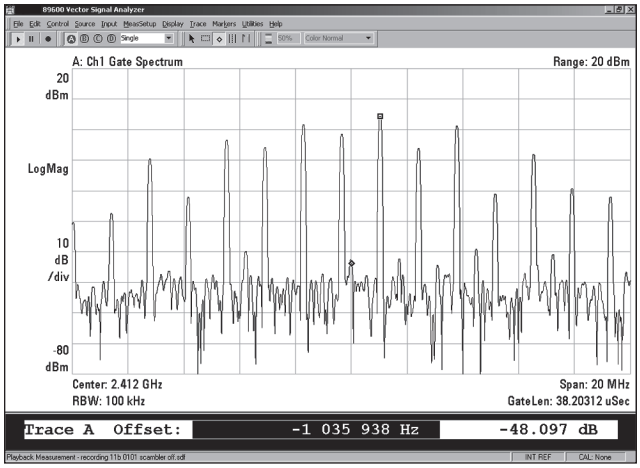

Figure 15: Plot showing RF carrier suppression of an IEEE 802.11b signal

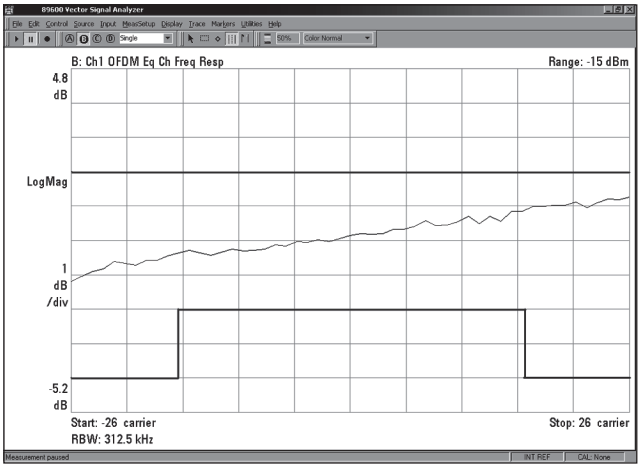

Figure 16 IEEE 802.11a spectral flatness plot

3.4.4 IEEE 802.11a Center Frequency Leakage

Energy at the center frequency of the carrier can cause problems with receiver designs which use zero frequency intermediate signals. IEEE 802.11a specifically avoids using the center carrier for transmission. The measurement is gated over the 8 µs-channel estimation section of the preamble. This is the part of the waveform when every 4th carrier is turned on.

3.4.5 IEEE 802.11b Carrier Suppression

The normal spectrum for an 802.11b signal may not show a noticeable level reduction at the center frequency. A "01" test pattern, with scrambling off, is used to create the right conditions. The reference is defined as the value of the highest signal found. The carrier must be at least 15 dB below the highest signal found.

3.4.6 Spectral Flatness

This test applies only to the OFDM signals in IEEE 802.11a and HiperLAN/2. Variations in carrier flatness will reduce demodulation margins and degrade link performance. It is measured during the 8 µs-channel estimation phase of the burst, with all 52 carriers are turned on. It is 8 µs after the start of a normal burst.

Note: Filters in the measurement path may affect spectral flatness. Calibration or normalization may be used to remove linear errors.

3.5 Modulation Tests

3.5.1 Constellation Error

Directly referred to only in IEEE 802.11a, the constellation error is measured as under EVM, described below. It is reported as a decibel (dB) value, dependent on the modulation rate being tested. Interaction may occur between problems which cause high constellation errors and those which cause Spectrum Mask failures. Many modulator errors cause different effects when using OFDM rather as opposed to a single carrier. For more detailed information, see the References.

3.5.2 Error Vector Magnitude

IEEE 802.11 uses a metric called Error Vector Magnitude (EVM) as a measure of modulation quality. It has become an industry standard for a wide variety of applications, from cellular phones to cable television. The basic concept of EVM is that any impaired signal (usually a complex one) can be represented as the sum of an ideal signal and an error signal. Since an error signal cannot be measured directly, test instrumentation determines the error signal by reconstructing the ideal signal based on received data and then subtracting it from the actual signal.

The error signal encompasses all sources of error, including:

- Additive Noise
- Nonlinear Distortion
- Linear Distortion, e.g., frequency response
- Phase Noise
- Spurious Signals
- Other Modulation Errors, e.g., quantization errors, offsets

At any time, the error signal is represented as a complex vector extending from where we are in the IQ plane to where we want to be. Every chip has its own error vector. EVM is defined as the root mean square (rms) over 1000 chips.

Combining EVM Readings

The list below shows that some error sources are noiselike, while others are systematic. EVM is the combination of many factors, so it is not possible to define an exact mathematical relationship between EVMs coming from different components in a transmitter or receiver. However, non-coherent errors will usually add in on a root-sum-of-squares basis. Device simulation is therefore needed to perform accurate analysis.

New techniques are being developed to more readily isolate the causes of distortions. Up-to-date information may be obtained from the Keysight web site, **www.keysight.com/ find/wlan**, or from your local Keysight sales representative.

The EVM specification of IEEE 802.11b is a very generous 35%. This would be poor for a QPSK signal, but is reasonable for DSSS given because of the coding gain due to spectrum spreading. The situation is very different for 802.11a,g. Table 5 shows how the EVM specification varies with bit rate. Data rates above 24Mbps are optional for IEEE 802.11a.

In the same way a Power vs. Time or a Gated Spectrum plot give a lot more diagnostic information than a numeric power reading, so EVM vs. Time and Channel (for 802.11a) can also provide more information about the cause of problems. Figure 18 is a combination display indicating characteristics of a timing error. The solid lines across the bars show the RMS (Root Mean Square) EVM value at each point.

Center Frequency Tolerance

The method for measuring center frequency tolerance depends on the availability of test modes. If modulation is turned off, it may be as simple as using a frequency counter, but a more accurate and realistic result would be gained from a normal modulated signal. This is because changes in current consumption due to analog or digital circuits changing state can cause transient changes in the local oscillator frequencies. The equalizer in the receiver of a real device has to use part of the transmitted preamble, so it is important that this be correct.

In Figure 19a the frequency error is reported as a by-product of the demodulation process. The binary data shown is the content of the preamble. Spaces represent carrier 0. Figure 19b shows how the frequency may change during the frame.

HiperLAN/2 and future 802.11 specifications have requirements for Dynamic Frequency Selection. This allows the WLAN system to adapt to the presence of RADARs. The carrier must switch within 1ms in HiperLAN/2.

The IEEE 802.11b specification allows for a Channel Agility option. The method of operation is not mandated. As an indication of the settling time required, the operating channel frequency has ≤ 224 µs to settle within ±60 kHz of its final value.

Table 5: Constellation error and EVM equivalent for IEEE 802.11a

Data Rate (Mbit/ sec)	**Relative Constellation Error (db)**		**EVM (%rms)**
	HiperLAN/2	802.11a	
6	-19	-5	56.2
9	-19	-8	39.8
12	-19	-10	31.6
18	-19	-13	22.3
24	-19	-16	15.8
36	-19	-19	11.2
48	N/A	-22	7.9
54	-24	-25	5.6

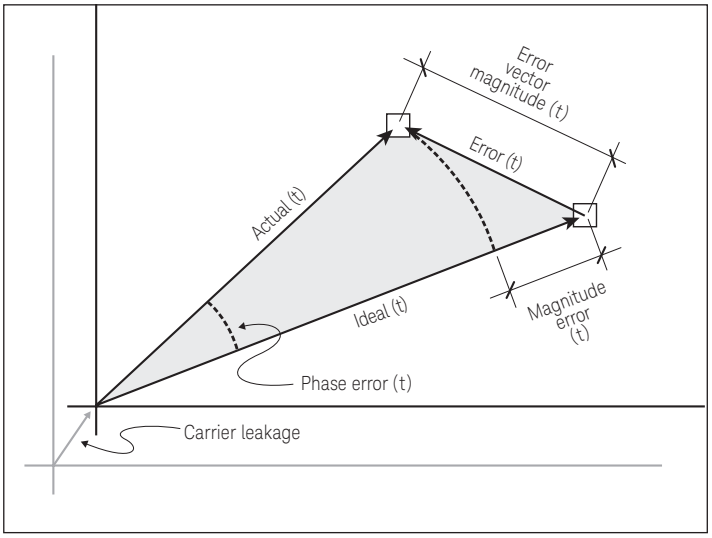

Figure 17 The elements used to define EVM measurement

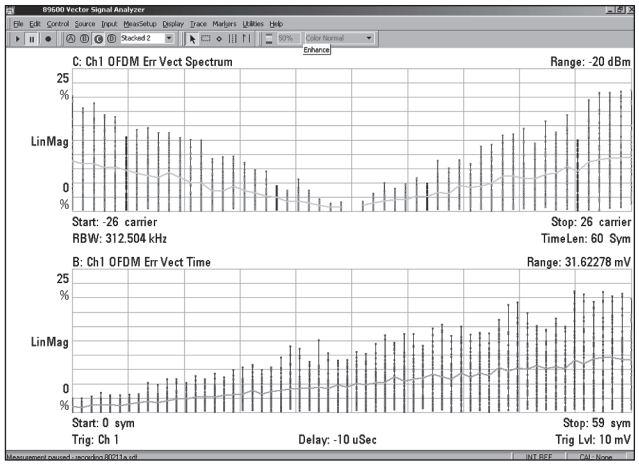

Figure 18: EVM vs. Time and vs. Channel for an IEEE 802.11a signal with timing error

3.6 Transmitter Bit Error and Packet Error Rates

The modulation tests described so far require wide-band measurement equipment. An alternative transmitter test involves making Packet Error Rate (PER) or Bit Error Rate (BER) tests with a good "golden" reference receiver. While this test may be simple and convenient, it has a number of serious limitations:

- The result depends on the receiver's analog circuit performance, which may be difficult to reproduce in low-cost hardware.
- The result depends on the receiver's data recovery algorithms (e.g., Viterbi), which may vary from one design to the next.
- Packet Errors indicate that all other performance margins have been used up. This is not a good way to get a warning of performance deterioration!

EVM and spectrum measurements provide far more information about transmitter performance. For these reasons, this application note will not provide further detail on Transmitter PER or BER measurements.

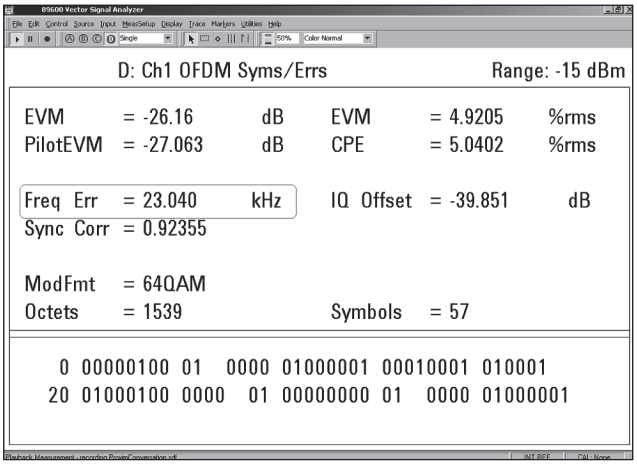

Figure 19a: Frequency error from an IEEE 802.11a device

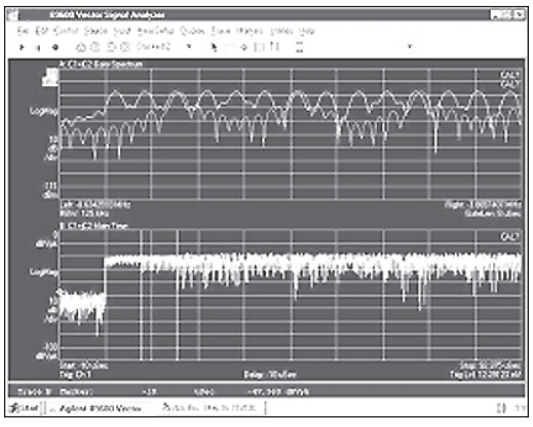

Figure 19b: Frequency change during frame

4. Timing Tests

WLAN systems are Time Division Duplex (TDD), so switching goes from transmit to receive. The use of Clear Channel Assessment means that the transition from one state to another needs to be short and well-controlled.

Every individual station starts with its own timing reference. This is used to establish both transmission and reception intervals. To work effectively within a network, stations need to synchronize their timers. This is done prior to association and then for as long as the stations are within the BSS.

The interaction between analog circuitry and Baseband processing is critical. A combination of test equipment may be used to measure signals in both domains simultaneously. An oscilloscope or logic analyzer will allow complex triggering configurations to be defined. Figure 27 (pg. 30) shows an example of useful signal connections.

4.1 Power vs. Time

IEEE 802.11a does not specify a Power vs. Time template, but this is an important measurement for all radio standards. The wide modulation bandwidth of WLAN signals reduce the likelihood of spectrum mask failures due to switching, even with sub-microsecond rise times. However, an 802.11a receiver has to adjust to the incoming signal using only 16µs of the burst. Problems have arisen in other standards because of having no definition of what happens before the burst. The plots in Figures 20 and 21 show two effects in 802.11b that could cause interoperability problems.

In Figure 20, a short power burst appears before the main burst. In Figure 21, a clear step in RF level occurs at the beginning of the burst. Further analysis of this device showed that the Power Amplifier was turned on before data transmission began.

HiperLAN/2 has more explicit requirements for the shape of the burst. These are shown in Figure 22.

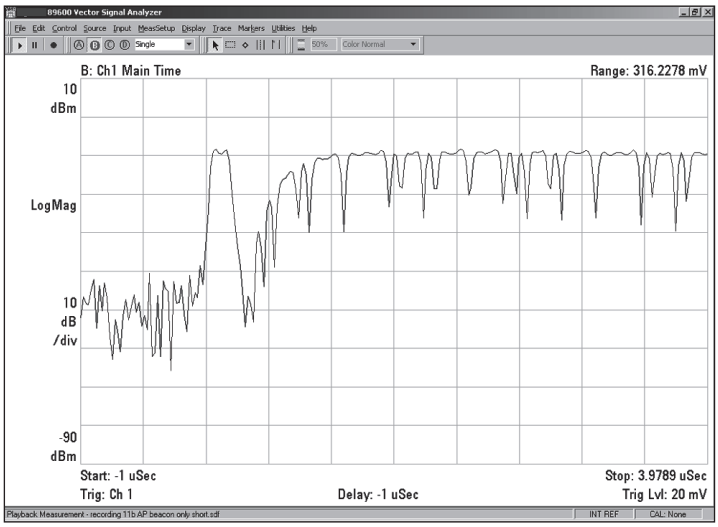

Figure 20: Example of unusual ramp conditions in IEEE 802.11b devices

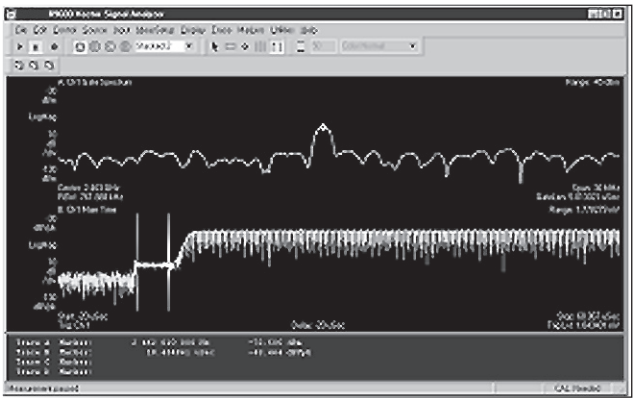

Figure 21: Example of unusual ramp conditions in IEEE 802.11b devices

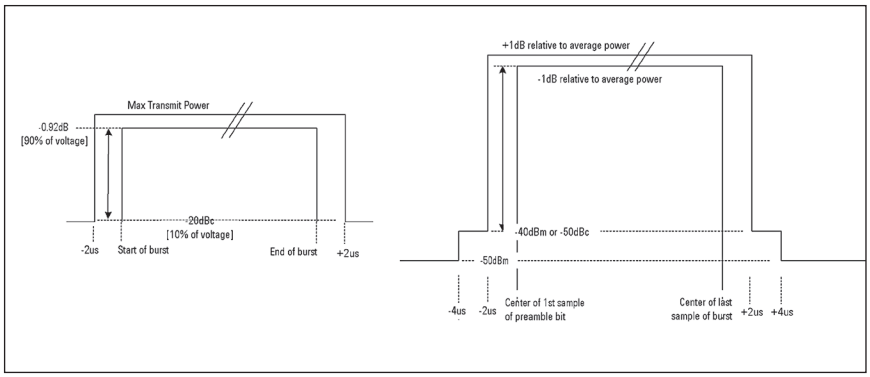

Figure 22: Power vs. Time mask for 802.11b and HiperLAN/2

4.2 Spectrogram Testing

Spectrogram tests offer a fast way to detect anomalies in complex signals. Color or gray-scale is added to the display to express amplitude. Using time-capture in a signal analyzer, suspect signals can be replayed more slowly to fully examine amplitude, frequency, and modulation transitions.

This application note does not offer a full representation of the spectrogram signal. Please contact your local Keysight representative for a demonstration, or visit **www.keysight.com/find/wlan** for details.

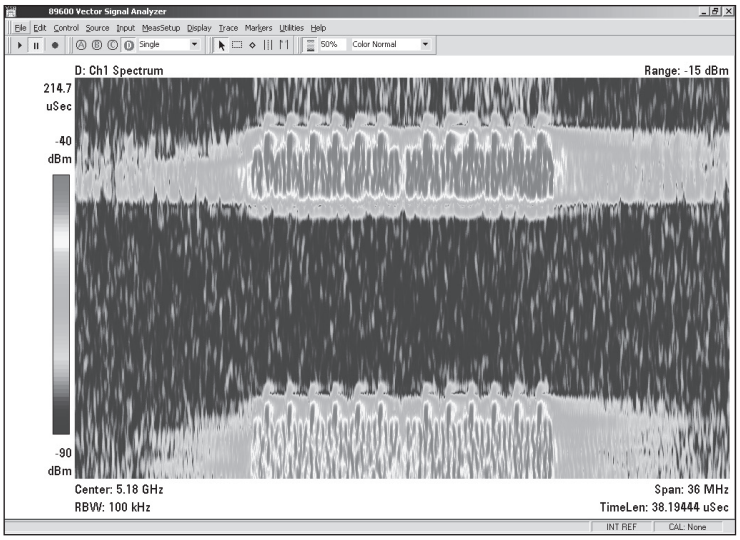

Figure 23: Spectrogram showing change in use of carriers at the start of an IEEE 802.11a frame

4.3 Transmitter-Receiver, Receiver-Transmitter Turnaround Time

Tx-Rx, Rx-Tx Turnaround Time tests are significant in the operation of a WLAN system, but they require detailed knowledge of the device being tested as well as access to internal test points. The equipment configuration for the Clear Channel Assessment test can be adapted to make these tests.

5. Transceiver Spurious Tests

The use of high-speed digital circuitry means that overall system emissions are often a combination of analog and digital effects. The tests, described only briefly here, are often time-consuming and require close attention to measurement configuration. Control lines that are nominally digital can easily become unintended antennas when RF signals couple into them. Unexpected variations in results often indicate that RF signals are present on cables.

Transceiver measurements consist of performing out-of-band spurious emissions tests. These confirm that the WLAN radio is operating within regulatory limits.

Two types of emissions tests are performed—conducted and radiated. Conducted emissions are a measure of the unwanted signals generated by the DUT from its output connector or from any cabling the device uses. Special signal coupling techniques are required for some measurements.

Radiated emissions are those emanating from the device and picked up on external antennas. Official RFI testing often involves the use of an anechoic chamber to remove background disturbances.

Separate standards are specified according to the region in which the equipment is to be used. The United States follows Federal Communications Commission (FCC) standard, parts 15.205, 15.209, 15.247, and 15.407. European countries follow the European Technical Standards Institute (ETSI) ETS 300 328 standard. In Japan, TELEC defines operating limits.

Spurious emission testing can be performed using a spectrum analyzer. Tests requiring compliance with International Special Committee on Radio Interference (CISPR) Publication 16 may require electromagnetic compatibility (EMC) spectrum analyzers with quasi-peak detectors. These tests are not covered in this application note. Please contact your local Keysight sales representative for more information on Keysight's EMC products.

6. Receiver Measurements

Receiver design is often difficult because the designer has to allow for many different input signal conditions, some of which are difficult to predict. This is especially true when operating in an unlicensed band. This publication covers only the more common tests needed by application engineers; however, details of more sophisticated techniques can be found in Appendices B and E. One such technique is to record a live RF signal, save it, and then replay it on demand, as shown in Figure 24.

Contact your local Keysight sales representative for more information on such specialized tests.

6.1 Test Conditions and Setup

Two basic receiver test configurations are described below. The first is a test of the analog circuit alone, while the second embraces the complete receiver.

Testing in IEEE 802.11a and 802.11b is generally done using a one-way signal path, while HiperLAN/2 designs may include options for signal loop-backs. This allows external test equipment to demodulate the returned signal and do its own BER measurement.

A one-way signal path has the potential for faster testing, because data does not have to be returned; however, it places a greater burden on the device supplier and system integrator. Care is needed in the triggering and sequencing of the measurement, since changes in level of the signal source require time to settle before further measurements are begun.

6.2 Bit Error Rate

The WLAN standards do not directly refer to Bit Error Rate (BER) measurements. Unlike cellular (voice) systems, WLAN transmissions do not normally send unprotected bits. Of course, Packet Errors are caused by Bit Errors, so the longer a packet is, the less likely it will be successfully recovered if the signal propagation path is poor.

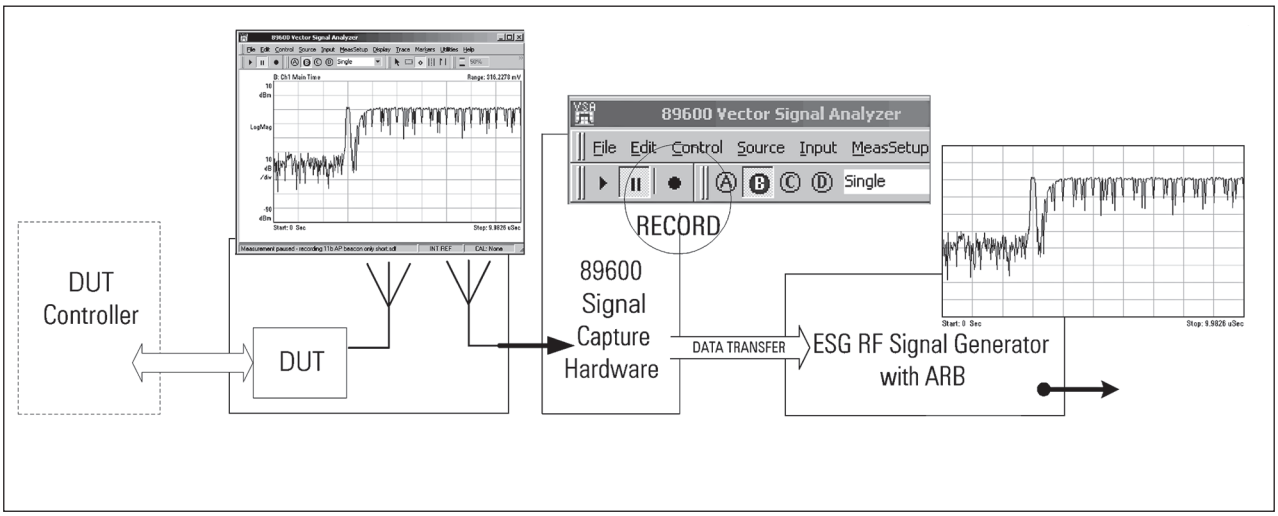

Figure 24: Signal record/replay of suspect signal using Keysight 89600 Vector Signal Analyzer and ESG

6.2.1 Bit Errors and RF

Bit Errors are created when the signal vector is not at the right place on the IQ plane when the receiver reaches a decision point. There are many reasons why the constellation becomes distorted, some of which are discussed in the transmitter modulation tests in section 3.5. Figure 25 shows an IQ constellation for a 5% EVM signal with Bit Errors occurring. The actual BER depends on the type of distortion.

The correlation between modulation errors and bit errors becomes more complex when multiple carriers (OFDM) are used. All WLAN standards discussed here use techniques which reduce the probability of bit errors caused by poor signal-to-noise ratios (energy per bit/noise, or Eb/No). In IEEE 802.11b, this includes spectrum spreading; in 802.11a, forward error correction is applied.

DSP algorithms, such as Viterbi, improve receiver performance by using a short amount of data history to predict what was most likely sent. The DSP then knows the difference between what it received as a raw bit and what it calculates as the correct bit. This correction process also provides signal quality information as a by-product.

Table 6: Summary of WLAN receiver performance tests

IEEE Ref.	Test	Payload	Test Configuration
18.4.8.1 18.4.8.2	Receiver minimum Input Sensitivity Max Input Level 1000 frames	PN9(15)11Mbps CCK	802.11b: 1024byte PSDU, -76 dBm,1 -10 dBm2
17.3.10.1 17.3.10.4		PN9(15) Scrambling ON	802.11a: 1000byte PSDU (see table 7),1 -30 dBm2 HiperLAN/2: 54byte PDU (see table 7),1 -20 dBm2 (class 1 receiver), -30 dBm2 (class 2 receiver)
18.4.8.3	Adjacent Channel rejection	PN9(15) 1000 frames	802.11b: Test all other channels within the band Interferer -35 dBm, Wanted -70 dBm, test as Min. Input Interferer is unsynchronized with wanted signal.
17.3.10.2			802.11a: See table 8 for levels. Interferer is unsynchronized with wanted signal.
17.3.10.3	802.11a Non-adjacent Channel rejection	PN9(15) 1000 frames	As above. Test all other channels within the band, on a 20 MHz spacing from wanted signal. Interferer is unsynchronized with wanted signal.
18.4.8.4	Clear Channel Assessment [CCA]		802.11b: Multiple test conditions apply.
17.3.10.5			802.11a: 1. With input signal -82 dBm, >90% (within 4 µs) probability of Carrier Sense showing Signal Busy. 2. Signal Busy shown for any signal above -62 dBm.

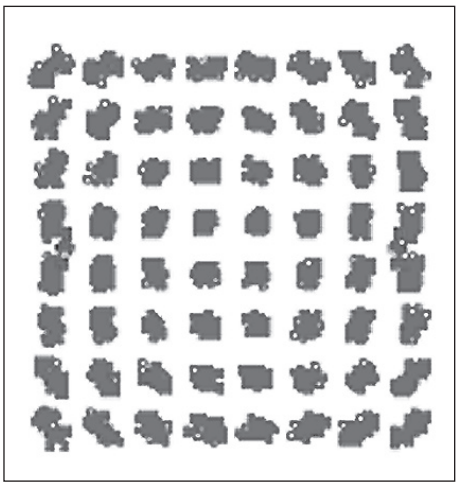

Figure 25: IQ constellation when bit errors occur

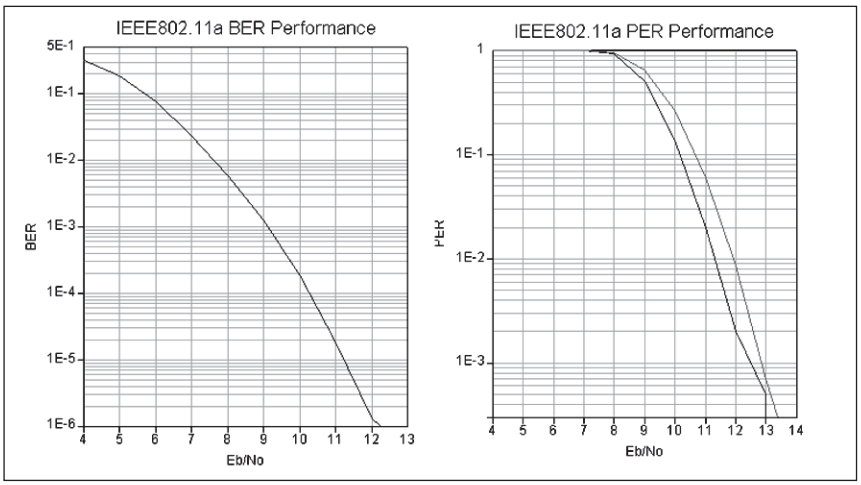

Figure 26: Plot showing variations on BER and PER vs. Input level, with 1024 byte payload, 24Mbps

The result of these techniques is that Bit Error measurements are a very strong function of RF signal level. Figure 26 shows how quickly Bit Error and Packet Error deteriorate with a reduction in Eb/No. The plots were generated using Keysight Advanced Design System software.

6.2.2 Bit Error vs. Packet Error

A Bit Error Rate measurement is possible with a WLAN system and may give an indication of performance more quickly than Packet Error Rate. The test configuration of Figure 27 (pg.29) is used. A typical setup is with a PN 9 or PN15 sequence in a repeating frame having a 1024-byte payload. Scrambling should be on. Vendor (proprietary) software would then recover the bit pattern and synchronize it to the PN sequence.

The Keysight ESG can run this BER test itself, if decoded data, clock, and frame signals are available from the Baseband circuit.

In practice, repeatable measurements can be made only if care is taken in setting the signal level for the test.

The performance of the modulator in the test source may also affect the PER reading. The usual practice is to use a high-quality test source to remove this variable. Impairments may be deliberately added, if required.

6.3 Receiver EVM Measurements

Analog measurements of the output of the receiver downconversion chain can provide much more information than BER and PER about the impairment suffered by a recovered signal. The same techniques described in transmitter modulation measurement in section 3.5 apply. Some options of the Keysight 89600 Vector Signal Analyzer are specifically designed to address a situation where the RF signal is downconverted to DC.

Figure 27 shows the configuration for this test. Further details on this type of measurement may be obtained by contacting your local Keysight sales representative.

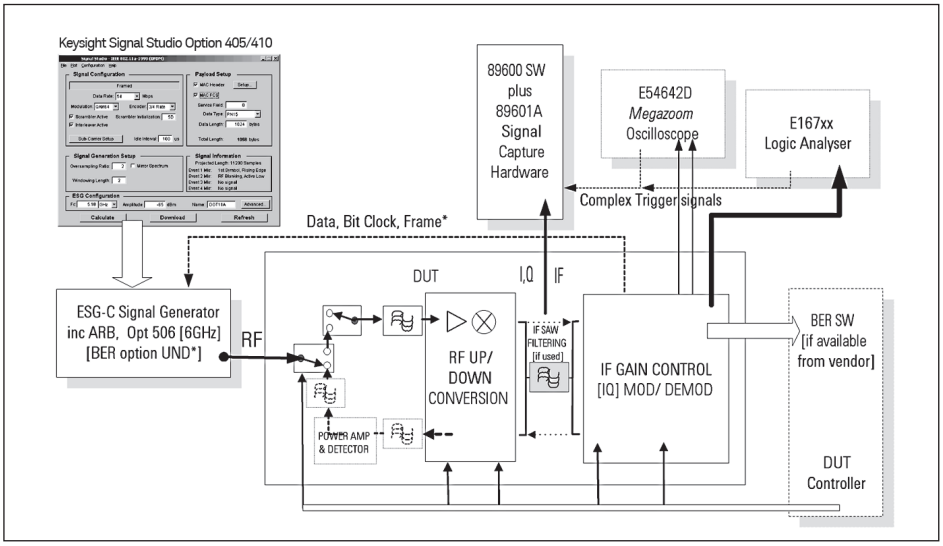

Figure 27: Diagram of analog-only receiver measurement paths

6.4 Frame Error Rate, Packet Error Rate

WLAN systems operate on a positive acknowledgement-based technique. When a frame is sent, it incorporates extra data to allow the receiver to determine if any bit errors have occurred. This is the role of the Cyclic Redundancy Check (CRC) and Frame Check Sequence (FCS). A receiver uses the payload data it recovers to calculate a CRC, employing exactly the same algorithm as the transmitting device. The two CRCs are then compared. Any differences between them mean that one or more bit errors have occurred in the payload data. If this is the case, the ACKnowledge frame is not sent. The CRCs are themselves error-protected, so they will not suffer bit errors unless the performance of the data content of the frame is very poor.

Frame Error Rate (802.11b) and Packet Error Rate (802.11a) use the same measurement configuration. Figure 28 shows the necessary connections.

Actual test operation will depend on the software used for the receiver measurements. The term for IEEE 802.11b testing is Frame Error Rate (FER). This measurement relies on the detection of failures in the Cyclic Redundancy Checks, which in 802.11b are used in both header and payload.

FER is defined as:

$$\left(1 - \frac{\text{No. of Frames Correctly Received}}{\text{No. of Frames Transmitted}}\right) * 100\%$$

In normal operation, an Acknowledge packet is sent from the receiving station only if the CRCs are correct. It is possible that the sending station may not correctly receive the ACK signal itself. For this reason, the Retry field is set to 1 to mark re-transmissions and other changes with adjacent frames.

As described in section 1.5.3, Random Back-off intervals may be applied in normal use if Acknowledgement packets are not delivered. This is one of the functions which should be overridden by a proper test mode to avoid problems in test sequencing.

Similarly, the effect of re-transmission requests could cause problems if not dealt with by the signal source. Again, available test modes should allow these functional requirements to be disabled.

HiperLAN/2 and IEEE 802.11a also use a frame-based receiver performance test called Packet Error Rate (PER). Unlike Frame Error Rate in 802.11b, CRCs are not used, but there is a frame check sequence after the user data, by which the receiver determines if the data was corrupted. If a frame is not detected at all by the receiver, the FER/PER reading will be low. The test software used must have a way to determine the number of frames sent.

6.5 Minimum Input Sensitivity, Maximum Input Level

This test is run according to the description and configuration in Figure 28. The test limits for the different standards are shown in Table 7.

Table 7: Receiver sensitivity standards

Data Rate Mbps	Sensitivity Level dBm	
	HiperLAN/2	802.11a
	PER <10%	
6	-85	-82
9	-85	-82
12	-85	-82
18	-85	-82
24	-85	-82
36	-85	-82
48	-85	-82
54	-85	-82
	802.11b, FER <8%	
11	-76	

6.6 Adjacent Channel, Non-Adjacent Channel Rejection

These tests verify that the receiver can deal with other WLAN signals within the same band. Figure 29 shows the test configuration. The RF isolator prevents high-level signals from one source from creating intermodulation products in the other. If both generators have 40 dB or more of internal attenuation applied, the isolator may not be required.

IEEE 802.11 explicitly states that the interference source must not be synchronous with the wanted signal. One reason for this is to test the way a ZIF (Zero Intermediate Frequency) receiver deals with the effect of an RF burst that appears in the middle of a

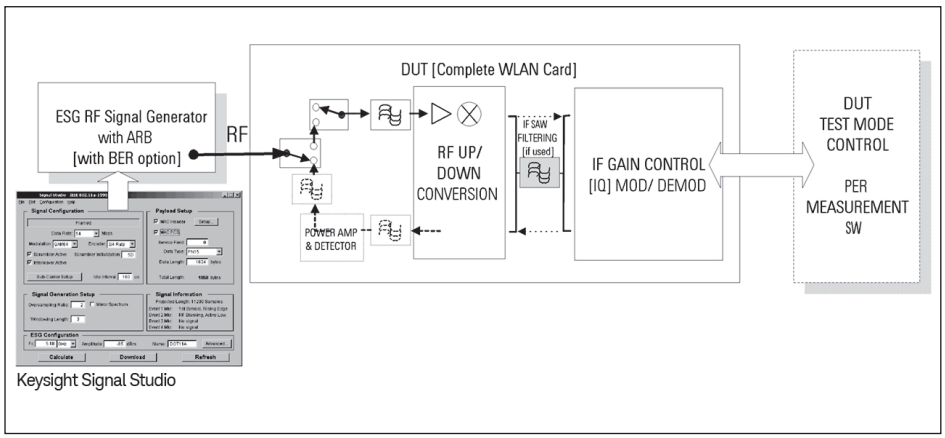

Figure 28: Diagram of complete receiver measurement path

wanted signal frame. It is difficult to specify a single timing/frequency relationship between the wanted and interfering signals. Choosing a short idle period for the interferer is one approach. During design it is recommended that the test configuration lock the reference frequencies of the two signal sources and make use of external triggering for the interferer. The trigger delay function should be used to adjust frame timing. Stepping the delay through the frame period will highlight problems within a design. Frequency offsets can also be entered for the interference source within the operational limits of the WLAN device.

The combination of these techniques will improve the reproducibility of the test.

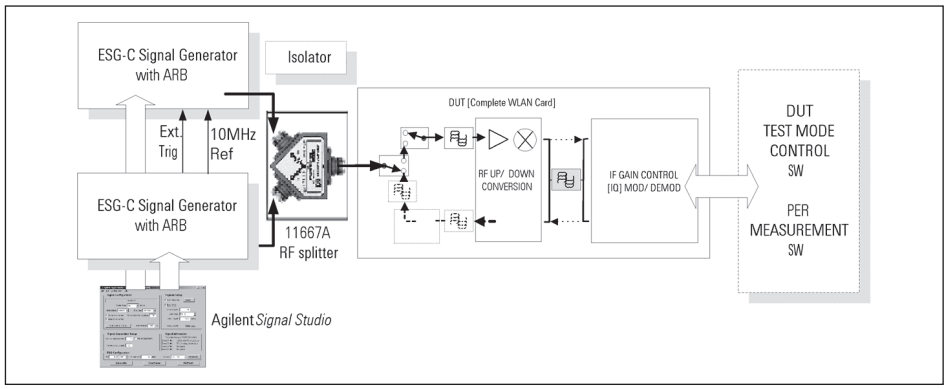

Figure 29: Test configuration for receiver adjacent channel and blocking tests

6.7 HiperLAN/2 Receiver Blocking Performance

A blocking test is designed to check the performance of the receiver when signals originating outside the WLAN system are present. Only HiperLAN/2 includes such tests in the specification. When a system is operating in a license-exempt frequency band, it may be considered appropriate to carry out some form of blocking test—at minimum, this may identify issues with a particular design.

The test configuration is similar to that shown for the adjacent channel rejection tests. The signal source should be replaced with one having higher frequency coverage if needed.

Note: F^C in Table 9 is the operating frequency of the test device. Testing in the 2.4 GHz ISM band would have to be adapted to suit the operation of 802.11b devices.

6.8 Clear Channel Assessment, RSSI

Clear Channel Assessment detection times are specified as < 4 µs for 802.11a and <25 µs (5 µs plus one MAC slot length) for 802.11b. Access to the carrier sense signal is needed. An oscilloscope triggered from the signal generator can be used to perform the test. Figure 30 (page 32) indicates the appropriate connection points.

The Receive Signal Strength Indicator (RSSI) is measured during the preamble. The only performance stipulation is that it be monotonic. The result is reported only to the receiver's MAC processor, not to the transmitter of the signal. RSSI is frequently found in end-user software to provide signal strength graphics to help in system configuration.

Some receiver characteristics which are important to the operation of a WLAN device, such as Clear Channel Assessment, are complex and difficult to measure without the appropriate software from the supplier of the device.

Table 8: Receiver adjacent channel test limits

Data Rate Mbps	Adjacent Channel Rejection (dB)	Non-Adjacent Channel Rejection (dB)
802.11a		
6	16	32
9	15	31
12	13	29
18	11	27
24	8	24
36	4	20
48	0	16
54	-1	15
802.11b		
11	35	

Table 9: HiperLAN/2 blocking signal limits

Frequency Range of Blocking Signal	Test Limit (dBm)
0.1 – >2500 MHz	0
2.5 – >4.5 GHz	-10
4.5 – >5.15 GHz	-30
5.15 GHz – >FC-50 MHz	-30
FC+50 MHz – >5.35 GHz	-30
5.35 – >5.47 GHz	-30
5.47 GHz – FC-50 MHz	-30
FC+50 MHz – >5.725 GHz	-30
5.725 – >7 GHz	-30
7 – >13 GHz	-20

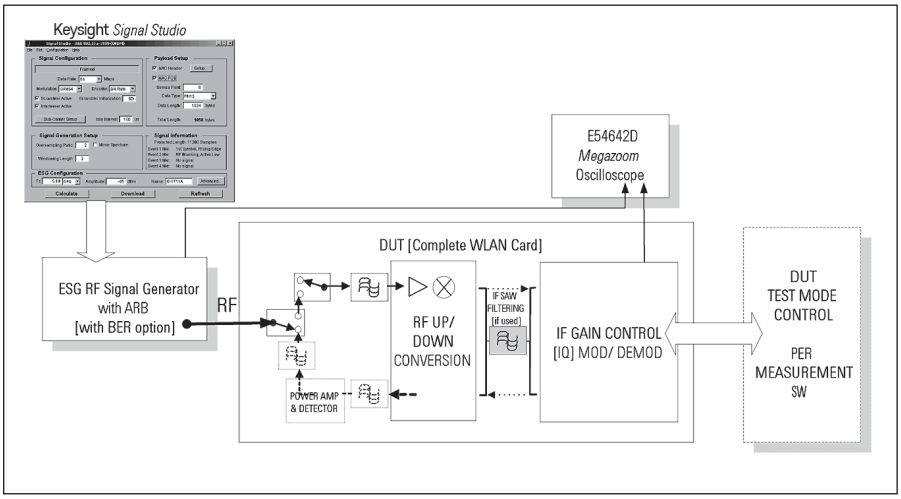

Figure 30: Test configuration for clear channel assessment tests

Additional receiver tests may be required to address the European Dynamic Frequency Selection requirements. A number of RADAR systems operate in the upper 5 GHz bands.

HiperLAN/2 also has an RSSI measurement requirement. The value, between 0 (-91 dBm) and 62 (> -20 dBm) recorded by the receiver, is transmitted to the Access Point for system transmission power management.

7. Power Supply Measurements

All equipment designs need to be tested at extremes of supply voltage, even if specifications do not require it. Operating limits will vary according to the conditions imposed by the host device, whether a PC or a combination cell phone.

Other power supply measurements can also be very informative. These include the current consumption as a function of the operational state of the device. Receiver Power Management (RPM) is part of the specification, because current consumption for listening is similar to that for transmitting. Careful timing of the receiver's active periods is required. The longer oscillators and digital circuitry are turned off, the longer the battery life will be.

Monitoring power supply current relative to the timing of radio transmission or reception helps ensure that firmware and hardware work together as expected. It is also straightforward to make before and after comparisons following firmware updates to ensure that no unwanted changes have occurred. Battery emulation allows repeatable testing of a DUT under realistic conditions.

Keysight offers a complete line of DC power supplies for these tests. These include general-purpose instruments as well as instruments specifically tailored to the demands of mobile communication. These DC voltage supplies also offer low-current measuring capability, which is useful for evaluating battery consumption during standby operation.

Appendix A: Keysight Solutions for Wireless LAN

Keysight Equipment for Wireless LAN PHY Layer (RF) Testing

● Full measurement capability
♦ Some measurement limitations

IEEE 802.11 RF LAYER TESTS	IEEE REFERENCE	89600 Series VECTOR SIGNAL ANALYZERS	PSA, ESA Series SPECTRUM ANALYZERS	ESG-C Series SIGNAL GENERATORS	EPM-P SERIES POWER METERS
Transmitter Tests					
Output Power	18.4.7.1.2 17.3.9.1	●	♦[1]		●[2]
Power Rise/Fall	18.4.7.6	●			
Spectrum Mask	18.4.7.3 17.3.9.2	♦	●		
Carrier Suppression	18.4.7.7	●	●		
Center Frequency Leakage	17.3.9.6.1	●			
Spectral Flatness	17.3.9.6.2	●	♦		
Transmission Spurious	18.4.6.8	♦	●		
Center Frequency Tolerance	17.3.9.4 18.4.7.4.5	●	♦		
Symbol Clock Frequency Tolerance	17.3.9.5	●	♦		
Constellation Error	17.3.9.6.3	●			
Error Vector Magnitude	18.4.7.8	●			
Transceiver Tests					
Out-of-band Spurious Emission	17.3.8.4 18.4.6.9		●		
Receiver Tests					
Sensitivity	18.4.8.1 17.3.10.1			●	
Max Input Level	18.4.8.2 17.3.10.4			●	
Adjacent Channel Rejection	18.4.8.3 17.3.10.2			●[3]	
Non-adjacent Channel Rejection	17.3.10.3			●[3]	
Clear Channel Assessment	18.4.8.4 17.3.10.5			●	

1. Channel power measurement indicates Average transmit power
2. Thermal sensor gives true rms power reading. Peak detector under-reads peak-average result when OFDM/modulation is applied.
3. Use second source as interferer. CW interference (for blocking tests) can be generated using Keysight E8241A Microwave Signal Generator.

Test Equipment with WLAN Capability

1. Vector Signal Analyzers, 89600 Series

Versatile and precise signal analysis, with 36 MHz capture bandwidth for 802.11a turbo modes. In-depth analysis of IEEE 802.11 transmitter and receiver chains. Automatic detection and demodulation of 802.11a formats. Provides modulation quality analysis for IEEE 802.11a OFDM signals, including EVM versus time & EVM versus sub-carrier.

Recommendation for 802.11a:

89641A, with dc-6 GHz tuner
Opt. AYA/B7R: Vector Signal Analysis and OFDM demodulation
Opt. 105: Dynamic links to EESof/ADS

2. Signal Generators, ESG-D Series (3-4 GHz), E4438C with Signal Studio

Generate IEEE 802.11 signals for transmitter and component tests, send formatted packets for receiver PER testing, generate Baseband signals for direct input to MAC or Analog circuits.

Recommendation for 802.11a, b:

E4438C, with Signal Studio
Opt. 410: IEEE 802.11a
Opt. 405: IEEE 802.11b
Opt. 506: 6 GHz operation
Opt. UNJ: Enhanced Phase noise
Opt. 002: Internal Baseband Generator
Opt. 005: 6 Gbyte hard-drive
Opt. UN7: Internal BER Tester (measurement capability dependent on vendor test configuration)

3. Spectrum Analyzer, PSA (6.7-50 GHz) and ESA-A Series

Automated "one button" test execution for Swept Spectrum transmitter measurement. Performs a broad range of spectrum measurements.

Recommendation:

E4440A PSA, 26.5 GHz
Opt H70: 70 MHz IF for use with 89611A VSA

4. EPM-P Power Meter, 8482A Thermal Sensor, E9327 Peak Power Sensor

Make accurate average power measurements with thermal sensor. Measure and inspect framed signals with the Peak Power Sensors.

5. Simulation Software, ADS with E8874A WLAN Design Guides

Essential software tool for design and simulation of custom WLAN systems. Pre-defined WLAN component models speed the simulation process. Can be linked with the ESG-D and 89600 Series.

Other Test Equipment

1. RF Shielded Enclosure

Allows repeatable RF measurements to be made, without interference from external environment.

2. DC Sources, 66319, 66321 B/D

Fast, programmable dynamic
DC power sources with battery emulation.

3. Logic Analyzers – 1680/1690 Series

Comprehensive system-level debugging for digital hardware design and verification

4. Logic Analyzers – 16700 Series

Provides comprehensive system-level debugging for multiple processor/ bus designs. Use E5904B with Emulation Trace Macrocell port for ARM processor triggering.

5. Mixed Signal Oscilloscopes – 54600 Series

Use for verification and debugging of IEEE 802.11 baseband signals.

6. Network Analyzers – 8753E Series

Provides measurement of Antenna VSWR and performance of PA, LNA and RF switch.

7. Function Generator, 33250A, 80 MHz Function/Arbitrary Waveforms

Generate clock signals and noise, or combine with an oscilloscope to reproduce baseband waveforms.

Accessories

1. Oscilloscope Probe–54006A

Passive probes with very low capacitance (0.25 pF).

2. Close Field Probe–11940A

Measures magnetic field radiation up to 1 GHz.

3. Splitter–11667A

Use for ratio measurements and equal power splitting.

4. Directional coupler–773D

Use for monitoring one RF waveform (2-18 GHz) while two IEEE 802.11 devices are connected by cables.

5. Dual directional coupler–772D

Useful for monitoring both RF waveforms (2-18 GHz) while two IEEE 802.11 devices are connected by cables.

Appendix B: Recommended Reading

Web Links:

1. Keysight WLAN Application and Product information:
http://www.keysight.com/find/wlan/

2. Keysight Web Training: **www.keysight.com/find/education**

   – Measurement Challenges for OFDM Systems, ENEN archive, 18 September 2001.

   – Wireless LAN – A Unified Physical Layer Design and Measurement Environment, ENEN archive, 6 March 2002

3. IEEE 802.11 Home Page: **http://www.ieee802.org/11/**

4. WECA Home Page: **http://www.wirelessethernet.org/**

5. ETSI Technical Home Page **www.etsi.org/technologies-clusters/**

Demo Software:

1. Keysight 89600 demo software available on CD, or downloadable (95 Mbytes)

2. Keysight Signal Studio software, downloadable (6.5 Mbytes)

Application Notes:

1. RF Testing Of Wireless LAN Products, Application Note 1380-1, literature number 5988-3762EN

2. Eight Hints for Making Better Measurements Using RF Signal Generators, Application Note 1306-1, literature number 5967-5661E

3. Eight Hints for Making Better Spectrum Analyzer Measurements, Application Note 1286-1, literature number 5965-7009E

5. Spectrum Analysis, Application Note 150, literature number 5952-0292

5. Testing and Troubleshooting Digital RF Communications Receiver Designs, Application Note 1314, literature number 5968-3579E

6. Testing and Troubleshooting Digital RF Communications Transmitter Designs, Application Note 1313, literature number 5968-3578E

Articles:

1. The Design and Verification of IEEE 802.11a 5 GHz Wireless LAN Systems, Keysight article, web only http://www.chipcenter.com/networking/ technote019.html

Product Overviews:

1. ***Bluetooth***™ & Wireless LAN Test Products, Systems and Services, lit. number 5988-4438EN

2. Keysight EPM-P Series Single- and Dual-Channel Power Meters Demo Guide, literature number 5988-1605EN

Product Notes:

1. Keysight 89600 Series Wide Bandwidth Vector Signal Analyzers, literature number 5980-0723E

2. Keysight 89640A dc to 2700 MHz Vector Signal Analyzer Technical Specifications, literature number 5980-1258E

3. Using Vector Modulation Analysis in the Integration, Troubleshooting and Design Of Digital RF Communications Systems, Product Note 89400-8., literature number5091-8687E

4. Ten Steps to a Perfect Digital Demodulation Measurement, Product Note 89400-14A, literature number 5966-0444E

5. 802.11a WLAN Signal Studio Software, Option 410 for the E4438C ESG Signal Generator, literature number 5988-5765EN

6. 802.11b WLAN Signal Studio Software, Option 405 for the E4438C ESG Signal Generator, literature number 5988-5766EN

7. Customizing Digital Modulation with the Keysight ESG-D Series Real-Time I/Q Baseband Generator, Option UN8, literature number 5966-4096E

8. Generating and Downloading Data to the Keysight ESG-D RF Signal Generator for Digital Modulation, literature number 5966-1010E

9, Generating Digital Modulation with the Keysight ESG-D Series Dual Arbitrary Waveform Generator, Option UND, literature number 5966-4097E

Appendix C: Glossary

Acknowledgement:

The short frame sent by a receiver when it is able to correctly decode a frame.

Beacon:

A regular RF transmission used by stations to discover if there are other devices within its operating range. Beacons are also used for coarse timing alignment.

Carrier Sense Multiple Access/Collision Avoidance:

The term used to describe the way 802.11 devices listen for other RF signals before transmitting.

Hidden Node:

A station that is not "heard" directly when another station listens as part of the CSMA/CA process.

Medium Access Control:

The function of the software that adapts wired LAN transmissions, making them suitable for sending over an RF link.

Network Allocation Vector:

A timing variable used to let each station know how long it has to wait before transmitting.

Station:

The Access Point or Network Interface card that interfaces between the host device and the RF link

Appendix D: Symbols and Acronyms

ACK	Acknowledgement
ADS	Advanced Design System
AP	Access Point
BER	Bit Error Rate
bps	Bits Per Second
BPSK	Binary Phase Shift Keying
BRAN	Broadband Radio Access Network
BSS	(Infrastructure) Basic Service Set
CCA	Clear Channel Assessment
CCDF	Complementary Cumulative Distribution Function
CCK	Complementary Code Keying
CRC	Cyclic Redundancy Check
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CTS	Clear To Transmit
CW	Contention Window
DCF	Distributed Coordination Function
DFS	Dynamic Frequency Selection
DIFS	Distributed (Coordination Function) Interframe Space
DQPSK	Differential Quadrature Phase Shift Keying
DSSS	Direct Sequence Spread Spectrum
DUT	Device Under Test
ED	Energy Detect
EFS	Extended Frame Space
EIRP	Equivalent Isotropic Radiated Power
ESG	(Electronic) Signal Generator
ESS	Extended Service Set
ETSI	European Technical Standards Institute
EVM	Error Vector Magnitude
FCS	Frame Check Sequence
FER	Frame Error Rate
FHSS	Frequency Hopping Spread Spectrum
HiperLAN	High Performance Local Area Network
HiSWAN	High Speed Wireless Access Network
IBSS	Independent Basic Service Set
IF	Intermediate Frequency
ISM	Industrial, Scientific, and Medical
LLC	Logical Link Control
LO	Local Oscillator
MAC	Medium Access Control
MT	Mobile Terminal
NIC	Network Interface Card
OFDM	Orthogonal Frequency Division Multiplexing
PBCC	Packet Binary Convolutional Coding
PDU	Protocol Data Unit
PER	Packet Error Rate
PHY	Physical (layer)

PIFS	Priority Interframe Space
PLCP	Physical Layer Convergence Protocol
PLL	Phase Locked Loop
PMD	Physical Medium Dependent
PN9,15	Pseudo Random Number
PSDU	PLCP Service Data Unit
QAM	Quadrature Amplitude Modulation
RBW	Resolution Bandwidth
RSS0	Receive Signal Strength 0 (Zero)
RSSI	Receive Signal Strength Indication
RTS	Ready To Send
RX	Receiver
SAW	Surface Acoustic Wave (Filter)
SIFS	Short Interframe Space
STA	Station (in HiperLAN/2)
TDD	Time Division Duplex
TPC	Transmit Power Control
TX	Transmitter
UNII	Unlicensed National Information Infrastructure
VBW	Video Bandwidth
VCO	Voltage Control Interface
VSA	Vector Spectrum Analyzer
VSWR	Voltage Standing Wave Ratio
WECA	Wireless Ethernet Compatibility Alliance
WLAN	Wireless Local Area Network

Appendix E: References

1. Supplement to IEEE Standard for Information Technology, IEEE Std 802.11a–1999 (supplement to IEEE Std 802.11-1999)

2. Higher Speed Physical Layer in the 2.4 GHz Band, IEEE Std 802.11b/D8.0,Sept 2001 (draft supplement to IEEE Std 802.11-1999)

3. Broadband Radio Access Networks (BRAN); HiperLAN Type 2; Physical Layer ETSI TS 101 475 V1.1.1 (2000-04)

Formerly known as Application Note 1380-2.

KEYSIGHT TECHNOLOGIES

Published in USA, December 5, 2017
5988-5411EN
www.keysight.com