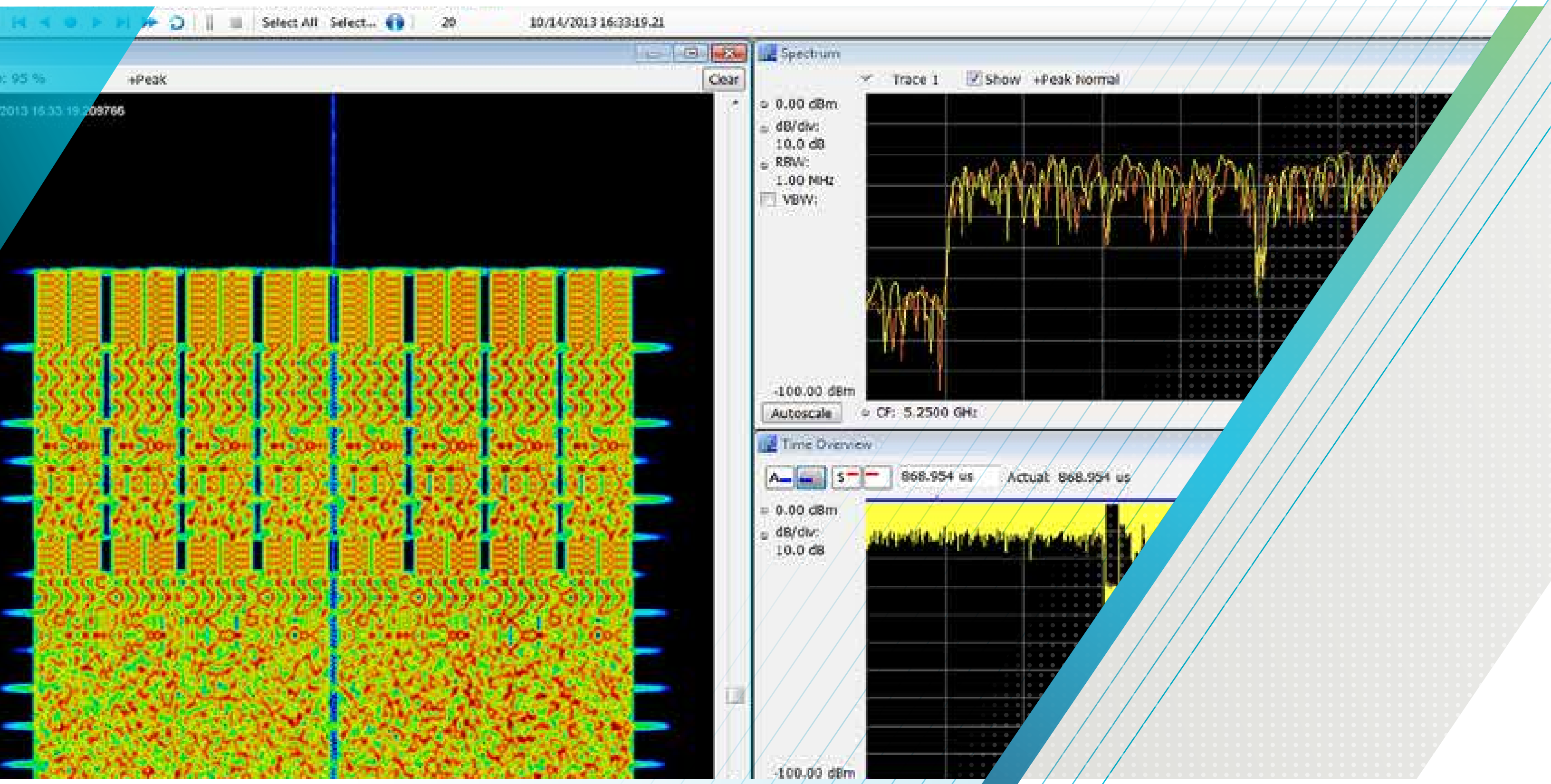
Wi-Fi: Overview of the 802.11 Physical Layer and Transmitter Measurements

PRIMER



10/14/2013 16:33:19.21

0.00 dBm

dB/div: 10.0 dB

RBW: 1.00 MHz

□ VBW:

-100.00 dBm

CF: 5.2500 GHz

868.954 us

0.00 dBm

dB/div: 10.0 dB

-100.00 dBm

Tektronix®

Table of Contents

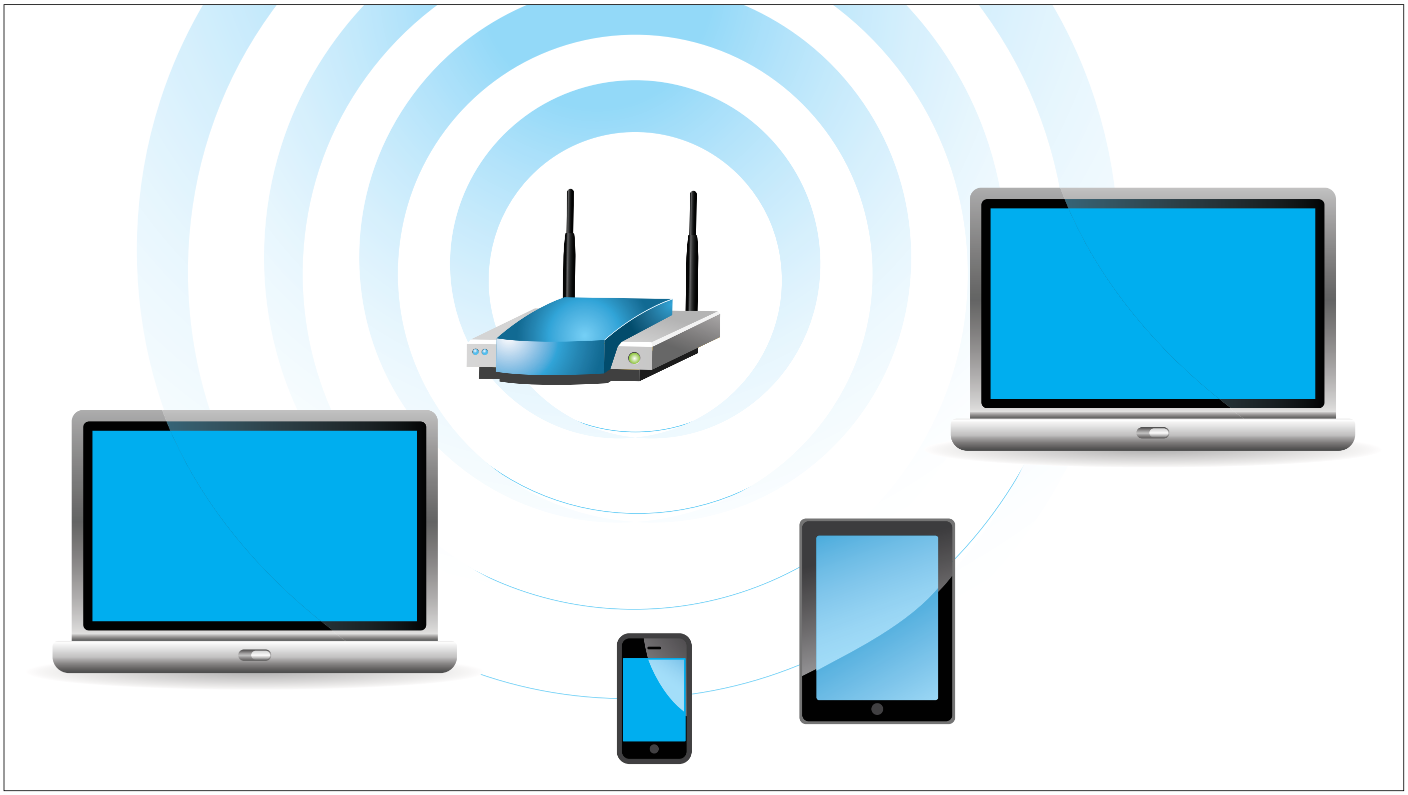


Figure 1. The 802.11 standards have enabled millions of electronic devices to exchange data or connect to the internet wirelessly using radio waves.

Introduction

Wi-Fi is a technology that allows many electronic devices to exchange data or connect to the internet wirelessly using radio waves. The Wi-Fi Alliance defines Wi-Fi devices as any "Wireless Local Area Network (WLAN) products that are based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards".

The key advantage of IEEE 802.11 devices is that they allow less-expensive deployment of Local Area Networks (LANs). For places where running cables to every device is not practical, such as outdoor areas and airports, they can host wireless LANs. Products from every brand name can inter-operate at a basic level of service thanks to their products being designated as "Wi-Fi Certified" by the Wi-Fi Alliance.

Today, millions of IEEE 802.11 devices are in use around the world and they operate in the same frequency bands, this makes the need for their coexistence critical. Even though over time older devices will be retired, some consumers and businesses will still be using the old standards for years. For some businesses the original 802.11b devices meet their needs and the need to change has not occurred. Wider bandwidth 802.11 deployments must therefore be able to "play nicely" with the older standards, both by limiting their impact on nearby legacy WLANs and by enabling communication with legacy stations.

This primer provides a general overview for each of the 802.11 standards, their PHY layer characteristics and their testing requirements. In this document, we use 802.11 and IEEE 802.11 interchangeably.

IEEE 802.11 Standard and Formats

IEEE 802 refers to a family of IEEE standards dealing with Local Area Networks and Metropolitan Area Networks (Table 1). The IEEE 802 family of standards is maintained by the IEEE 802 LAN/MAN Standards Committee (LMSC). An individual Working Group provides the focus for each area.

IEEE 802.11 is a set of medium access control (MAC) and physical layer (PHY) specifications for implementing Wireless Local Area Network (WLAN) communication. The 802.11 family is a series of over-the-air modulation techniques that share the same basic protocol (Table 2). These standards provide the basis for wireless network products using the Wi-Fi brand. The segment of the radio frequency spectrum used by 802.11 varies between countries.

IEEE 802.11-1997 or Legacy Mode

The original version of the standard IEEE 802.11 was released in 1997, but is basically obsolete today. It specified bit rates of 1 or 2 megabits per second (Mbit/s). It specified three alternative physical layer technologies:

- Diffuse infrared operating at 1 Mbit/s
- Frequency-hopping spread spectrum operating at 1 Mbit/s or 2 Mbit/s
- Direct-sequence spread spectrum operating at 1 Mbit/s or 2 Mbit/s

The latter two radio technologies used microwave transmission over the Industrial Scientific Medical (ISM) frequency band at 2.4 GHz. Its specified data rate was to be transmitted via infrared (IR) signals or by either frequency hopping or direct-sequence spread spectrum (DSSS) radio signals. IR remains a part of the standard but has no actual implementations.

A weakness of this original specification was that it offered so many choices that interoperability was sometimes challenging. It is really more of a "beta-specification" than a rigid specification, initially allowing individual product vendors the flexibility to differentiate their products but with little to no inter-vendor operability.

IEEE 802 Standards	
802.1	Bridging & Management
802.2	Logical Link Control
802.3	Ethernet - CSMA/CD Access Method
802.4	Token Passing Bus Access Method
802.5	Token Ring Access Method
802.6	Distributed Queue Dual Bus Access Method
802.7	Broadband LAN
802.8	Fiber Optic
802.9	Integrated Services LAN
802.10	Security
802.11	Wireless LAN
802.12	Demand Priority Access
802.14	Medium Access Control
802.15	Wireless Personal Area Networks
802.16	Broadband Wireless Metro Area Networks
802.17	Resilient Packet Ring

Table 1. 802 Family of Standards.

The DSSS version of legacy 802.11 was rapidly supplemented (and popularized) by the 802.11b amendment in 1999, which increased the bit rate to 11 Mbit/s. Widespread adoption of 802.11 networks only occurred after the release of 802.11b. As a result few networks were implemented using the original 802.11-1997 standard. In this document several sections do not provide further detail about the original legacy mode for this reason.

IEEE 802.11b

802.11b has a maximum raw data rate of 11 Mbit/s and uses the same media access method defined in the original legacy standard. 802.11b products appeared on the market in early 2000 and it is a direct extension of the modulation technique defined in the original standard. The dramatic increase in throughput of 802.11b (compared to the original standard) along with substantial price reductions led to the rapid acceptance of 802.11b as the definitive wireless LAN technology.

IEEE 802.11 PHY Standards						
Release Date	Standard	Frequency Band (GHz)	Bandwidth (MHz)	Modulation	Advanced Antenna Technologies	Maximum Data Rate
1997	802.11	2.4 GHz	20 MHz	DSSS, FHSS	N/A	2 Mbits/s
1999	802.11b	2.4 GHz	20 MHz	DSSS	N/A	11 Mbits/s
1999	802.11a	5 GHz	20 MHz	OFDM	N/A	54 Mbits/s
2003	802.11g	2.4 GHz	20 MHz	DSSS, OFDM	N/A	542 Mbits/s
2009	802.11n	2.4 GHz, 5 GHz	20 MHz, 40 MHz	OFDM	MIMO, up to 4 spatial streams	600 Mbits/s
2013	802.11ac	5 GHz	40 MHz, 80 MHz, 160 MHz	OFDM	MIMO, MU-MIMO, up to 8 spatial streams	6.93 Gbits/s

Table 2. IEEE 802.11 PHY Standards.

One disadvantage of 802.11b devices is that they may have interference issues with other products operating in the 2.4 GHz band. Devices operating in the 2.4 GHz range include microwave ovens, cordless phones, Bluetooth devices, baby monitors and some amateur radio equipment. Interference issues and user density problems within the 2.4 GHz band have become a major issue as the popularity of Wi-Fi has grown.

IEEE 802.11a

The 802.11a standard was added to the original standard and was ratified in 1999. The 802.11a standard uses the same core protocol as the original standard and was the first of the 802.11 family to operate in the 5 GHz band. It uses a 52-subcarrier orthogonal frequency-division multiplexing (OFDM) with a maximum raw data rate of 54 Mbit/s, which typically yields a throughput in the mid-20 Mbit/s. Today, many countries around the world are allowing operation in the 5.47 to 5.725 GHz Band. This will add more channels to the overall 5 GHz band enabling significant overall wireless network capacity. 802.11a is not interoperable with 802.11b since they operate on different frequency bands. However, most enterprise class Access Points have multi-band capability today.

Using the 5 GHz band gives 802.11a a significant advantage, since the 2.4 GHz ISM band is heavily used. Degradation caused by such conflicts can cause frequently dropped connections and degradation of service. However, the higher 5 GHz frequency also brings a slight disadvantage as the effective range of 802.11a is slightly less than that of 802.11b/g. 802.11a signals cannot penetrate as far as those for 802.11b because they are absorbed more readily by walls and other solid objects in their path and because the path loss in signal strength is proportional to the square of the signal frequency. On the other hand, OFDM has fundamental propagation advantages in a high multipath environment, such as an indoor office, and the higher frequencies enable the use of smaller antennas with higher RF system gain, which counteracts the disadvantage of a higher band of operation. The increased number of usable channels and the near absence of other interfering systems (microwave ovens, cordless phones, baby monitors) give 802.11a a significant bandwidth and reliability advantage over 802.11b/g.

Confusion on the release time of 802.11a and 802.11b is common. The 802.11a products started shipping late, lagging 802.11b products due to 5 GHz components being more difficult to manufacture. In addition, first generation product performance was poor and plagued with problems. When second generation products started shipping, 802.11a was not widely adopted in the consumer space primarily because the less-expensive 802.11b was already widely adopted. However, 802.11a later saw significant penetration into enterprise network environments, despite the initial cost disadvantages, particularly for businesses which required increased capacity and reliability over 802.11b/g-only networks. Sections in this document often lead with 802.11b for this reason.

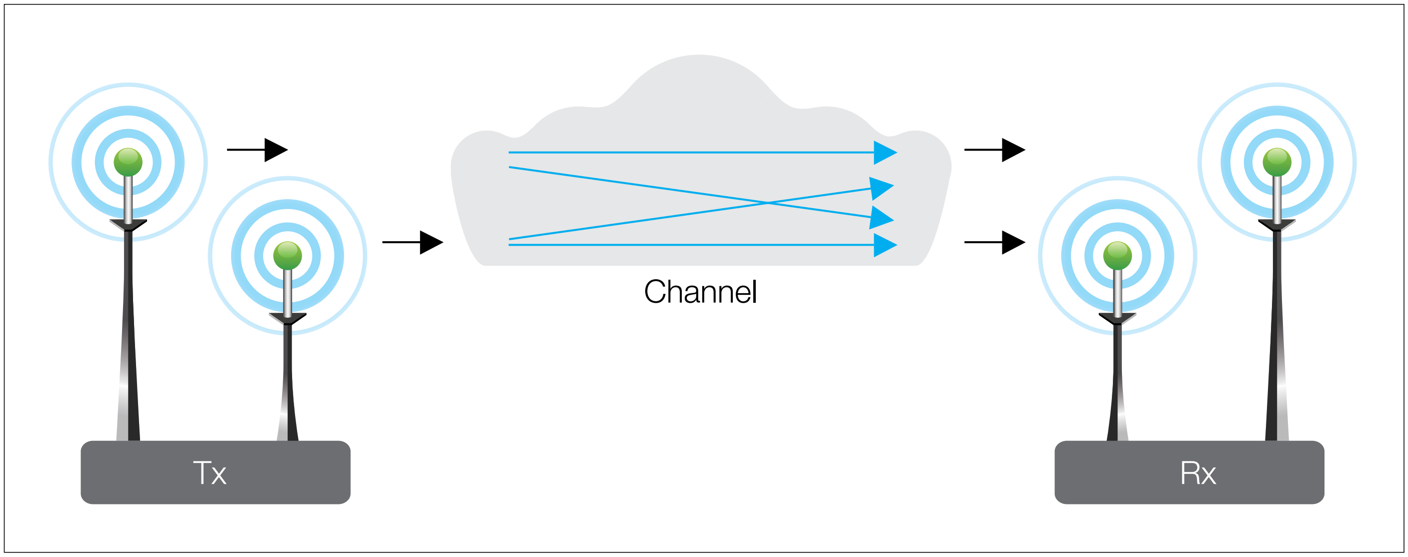


Figure 2. MIMO uses multiple antennas to coherently resolve more information than possible using a single antenna.

IEEE 802.11g

The 802.11g standard was rapidly adopted by consumers starting in January 2003, well before ratification, due to the desire for higher speeds and reductions in manufacturing costs. By summer 2003, most dual-band 802.11a/b products became dual-band/tri-mode, supporting 802.11a and b/g in a single mobile adapter card or Access Point (AP).

802.11g works in the 2.4 GHz band (like 802.11b), but uses the same OFDM based transmission scheme as 802.11a. It operates at a maximum physical layer bit rate of 54 Mbit/s, exclusive of forward error correction codes. 802.11g hardware is fully backwards compatible with 802.11b hardware. In an 802.11g network, however, the presence of a 802.11b device will significantly reduce the speed of the overall 802.11g network.

Despite its major acceptance, 802.11g suffers from the same interference as 802.11b in the already crowded 2.4 GHz range. Additionally, the success of the standard has caused usage/density problems related to crowding in urban areas. To prevent interference, there are only three non-overlapping usable channels in the U.S. and other countries with similar regulations (channels 1, 6, 11, with 25 MHz separation), and four in Europe (channels 1, 5, 9, 13, with only 20 MHz separation). Even with such separation, some interference due to side lobes exists, though it is considerably weaker.

IEEE 802.11n

The 802.11n amendment includes many enhancements that improve WLAN range, reliability, and throughput. At the physical (PHY) layer, advanced signal processing and modulation techniques have been added to exploit multiple antennas and wider channels. At the Media Access Control (MAC) layer, protocol extensions make more efficient use of available bandwidth. Together, these High Throughput (HT) enhancements can boost data rates up to 600 Mbps – more than a ten-fold improvement over 54 Mbps 802.11a/g.

802.11n operates on both the 2.4 GHz and the 5 GHz bands. Support for 5 GHz bands is optional. IEEE 802.11n builds on previous 802.11 standards by adding multiple-input multiple-output (MIMO) and 40 MHz channels to the PHY layer, and frame aggregation to the MAC layer.

Behind most 802.11n enhancements lies the ability to receive and/or transmit simultaneously through multiple antennas. 802.11n defines many "M x N" antenna configurations, ranging from "1 x 1" to "4 x 4". MIMO uses multiple antennas to coherently resolve more information than possible using a single antenna. One way it provides this is through Spatial Division Multiplexing, which spatially multiplexes multiple independent data streams, transferred simultaneously within one spectral channel of bandwidth. MIMO can significantly increase data throughput as the number of resolved spatial data streams is increased. Each spatial stream requires a discrete antenna at both the transmitter and the receiver.

Figure 3. The broad acceptance and success of 802.11 devices have created the need for new usage models which require higher throughput.

The number of simultaneous data streams is limited by the minimum number of antennas in use on both sides of the link. However, the individual radios often further limit the number of spatial streams that may carry unique data. The M x N : Z notation helps identify the capability of a given radio. The first number M is the maximum number of transmit antennas that can be used by the radio. The second number N is the maximum number of receive antennas that can be used by the radio. The third number Z is the maximum number of data spatial streams the radio can use. For example, a radio that can transmit on two antennas and receive on three, but can only send or receive two data streams would be 2 x 3 : 2.

Another optional 802.11n feature is 40 MHz channels. Prior 802.11 products use channels that are approximately 20 MHz wide. 802.11n products have the option to use 20 or 40 MHz wide channels, providing the AP has 40 MHz capability as well. Channels operating with a bandwidth of 40 MHz provide twice the PHY data rate available over a single 20 MHz channel. The wider bandwidth can be enabled in either the 2.4 GHz or the 5 GHz mode, but must not interfere with any other 802.11 or non-802.11 (such as Bluetooth) system using the same frequencies.

IEEE 802.11ac

The early standards for wireless LAN were designed primarily to connect a laptop PC in the home or office, and to allow connectivity “on the road”. The broad acceptance and success of WLAN has created the need for new usage models which would require higher throughput, such as:

- Wireless display
- In-home distribution of HDTV and other content
- Rapid upload/download of large files to/from servers
- Backhaul traffic (mesh, point-to-point, etc.)
- Campus and auditorium deployments
- Manufacturing floor automation

IEEE 802.11ac (aka VHT, Very High Throughput) is a standard that provide throughput in the 5 GHz band. 802.11ac leverages 802.11n (and 802.11a) structure where possible. This is advantageous for ensuring backwards compatibility and co-existence and also allows the 802.11ac developers to focus on the new features that are needed to achieve the throughput requirements.

The 802.11ac specification has expected multi-station WLAN throughput of at least 1 Gbps and a single link throughput of at least 500 Mbps. This is accomplished by extending the air interface concepts embraced by 802.11n:

- Wider RF bandwidth (up to 160 MHz)
- More MIMO spatial streams (up to 8)
- Multi-user MIMO
- High-density modulation (up to 256-QAM).

The standard was developed from 2011 through 2013 and approved in January 2014.

All 802.11ac devices are required to support 20, 40, and 80 MHz channels and 1 spatial stream, as a phase1 of deployment. In addition, several features are also defined in 802.11ac phase 2:

- Wider channel bandwidths (80+80 MHz and 160 MHz)
- Higher modulation support (optional 256QAM)
- Two or more spatial streams (up to 8)
- Multi-User MIMO (MU-MIMO)
- 400 ns short guard interval
- Space Time Block Coding (STBC)
- Low Density Parity Check (LDPC)

802.11ac devices making use of only the mandatory parameters (80 MHz bandwidth, 1 spatial stream, and 64-QAM 5/6) are capable of a data rate of approximately 293 Mbps. Devices that take advantage of the phase 2 parameters (8 spatial streams, 160 MHz of bandwidth and 256-QAM 5/6 with a short guard interval) can achieve almost 7 Gbps.

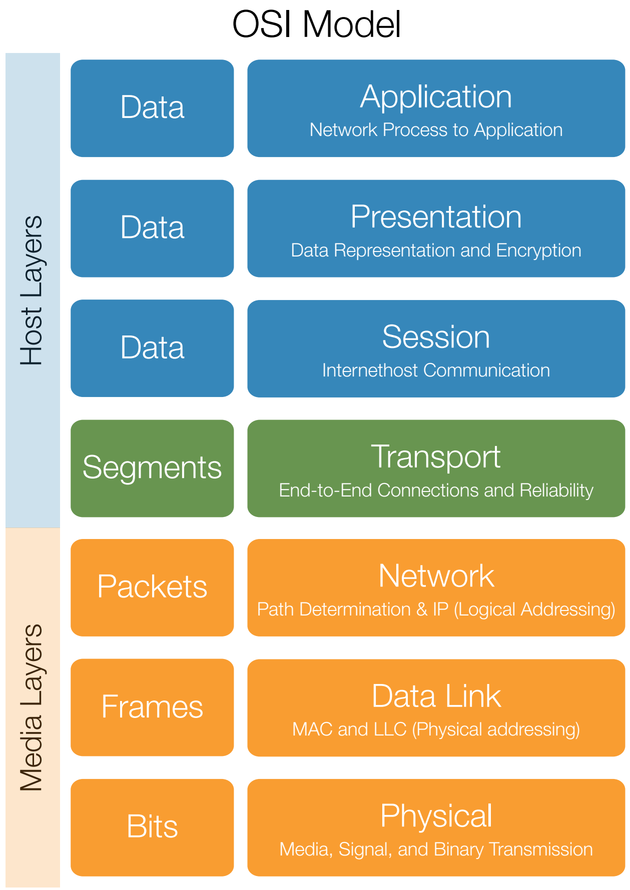

OSI Model
Host Layers
Media Layers
Data
Application
Network Process to Application
Data
Presentation
Data Representation and Encryption
Data
Session
Internethost Communication
Segments
Transport
End-to-End Connections and Reliability
Packets
Network
Path Determination & IP (Logical Addressing)
Frames
Data Link
MAC and LLC (Physical addressing)
Bits
Physical
Media, Signal, and Binary Transmission

Figure 4. The OSI model describes how information moves from an application program running on one networked computer to an application program running on another networked computer.

Protocol Architecture Overview

The Open Systems Interconnection Reference Model, or the OSI model, was developed by the International Organization for Standardization, which uses the abbreviation of ISO. The OSI model is a layered model that describes how information moves from an application program running on one networked computer to an application program running on another networked computer. In essence, the OSI model prescribes the steps to be used to transfer data over a transmission medium from one networked device to another. The OSI model defines the network communications process into seven separate layers as shown in Figure 4.

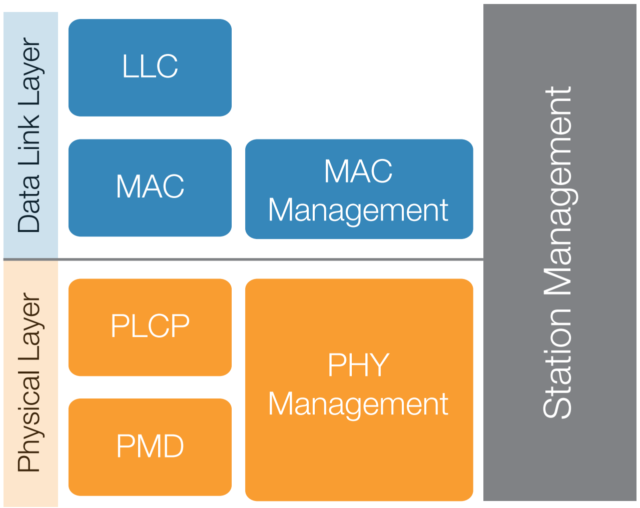


Figure 5. The 802.11 standards focus on the Data Link and Physical Layers of the OSI reference model.

Practical, connectionless LANs began with the pre-IEEE Ethernet specification, which is the ancestor of IEEE 802.3. The Standard 802.11 covers protocols and operation of wireless networks. It only deals with the two lowest layers of the OSI reference model, the physical layer and the Data Link layer (or Media Access Control layer). The goal is for all the 802.11 series of standards to be backward compatible and to be compatible at the Medium Access Control (MAC) or Data Link layer. Each of the 802.11 standards should therefore only differ in physical layer (PHY) characteristics (Figure 5).

The MAC layer provides the functional and procedural means to transfer data between network entities and to detect and possibly correct errors that may occur in the physical layer. It provides access to contention based and contention-free traffic on different kinds of physical layers. In the MAC layer the responsibilities are divided into the MAC sub-layer and the MAC management sub-layer. The MAC sub-layer defines access mechanisms and packet formats. The MAC management sub-layer defines power management, security and roaming services.

The Physical Layer defines the electrical and physical specifications for devices. In particular, it defines the relationship between a device and a transmission medium. The major functions and services performed by the physical layer are the following:

- Establishment and termination of a connection to a communications medium.
- Participation in the process where the communication resources are effectively shared among multiple users. For example, contention resolution and flow control.
- Modulation or conversion between the representation of digital data in user equipment and the corresponding signals transmitted over a communications channel. These are signals operating over the physical cabling (such as copper and optical fiber) or over a radio link.

The Physical layer is divided into three sub layers.

1. The Physical Layer Convergence Procedure (PLCP) acts as an adaption layer. The PLCP is responsible for the Clear Channel Assessment (CCA) mode and building packets for different physical layer technologies.
2. The Physical Medium Dependent (PMD) layer specifies modulation and coding techniques.
3. The PHY management layer takes care of the management issues like channel tuning.

The Station Management sub-layer is responsible for coordination of interactions between the MAC and PHY layers.

This primer focuses on the PHY layer as this is where the design requirements for the device hardware using the different techniques of the 802.11 standards are realized.

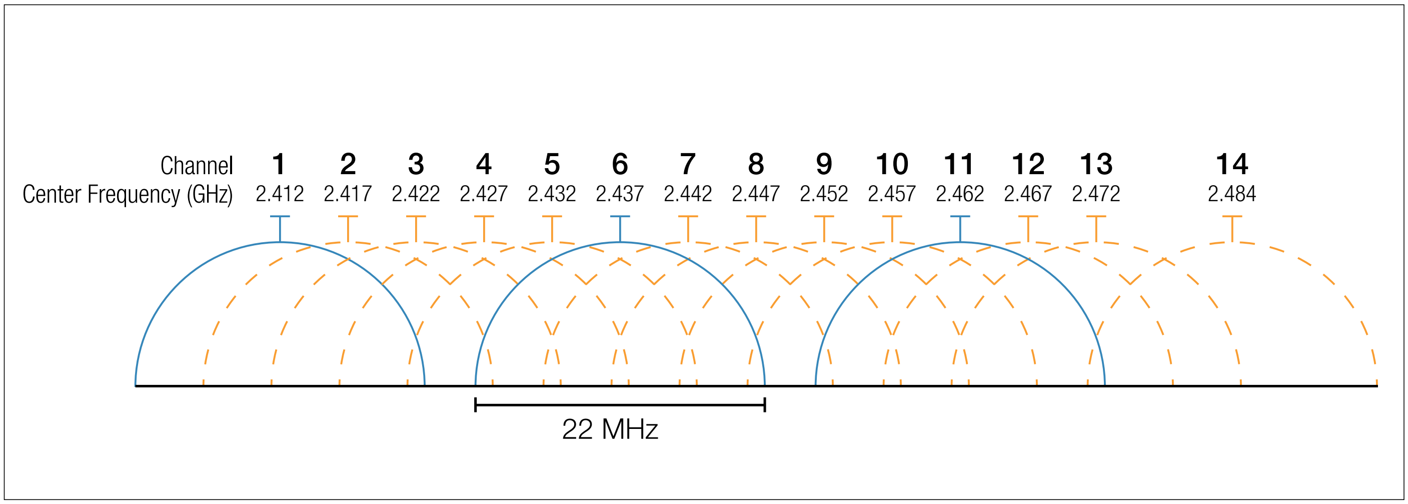


Figure 6. The 2.4 GHz band is divided into 14 overlapping channels.

Channel Allocations and Spectral Masks

The 802.11b, 802.11g, and the low-frequency part of the 802.11n standards utilize the 2.400 – 2.500 GHz spectrum located in the ISM band. The 802.11a, 802.11n and 802.11ac standards use the more heavily regulated 4.915 – 5.825 GHz band. These are often referred to as the "2.4 GHz and 5 GHz frequency bands". Each of these spectrums are sub-divided into channels with a center frequency and bandwidth, similar to the way commercial spectrums are sub-divided.

The 2.4 GHz band is divided into 14 channels spaced 5 MHz apart, beginning with channel 1 which is centered on 2.412 GHz (Figure 6). The channel numbering of the 5.725 – 5.875 GHz spectrum is less intuitive due to the differences in regulations between countries.

Channel Bandwidths

Early 802.11 products use channels that are approximately 20 MHz wide. In the US, 802.11b/g radios use one of eleven 20 MHz channels (three non-overlapping: 1, 6, 11) within the 2.4 GHz ISM frequency band. When the OFDM PHY was introduced to 802.11, the channel bandwidth was 20 MHz with later amendments adding support for 5 and 10 MHz bandwidths. 802.11a radios use one of twelve non-overlapping 20 MHz channels in the 5 GHz Unlicensed National Information Infrastructure (UNII) band. 802.11n products can use 20 or 40 MHz wide channels in either the ISM or UNII band.

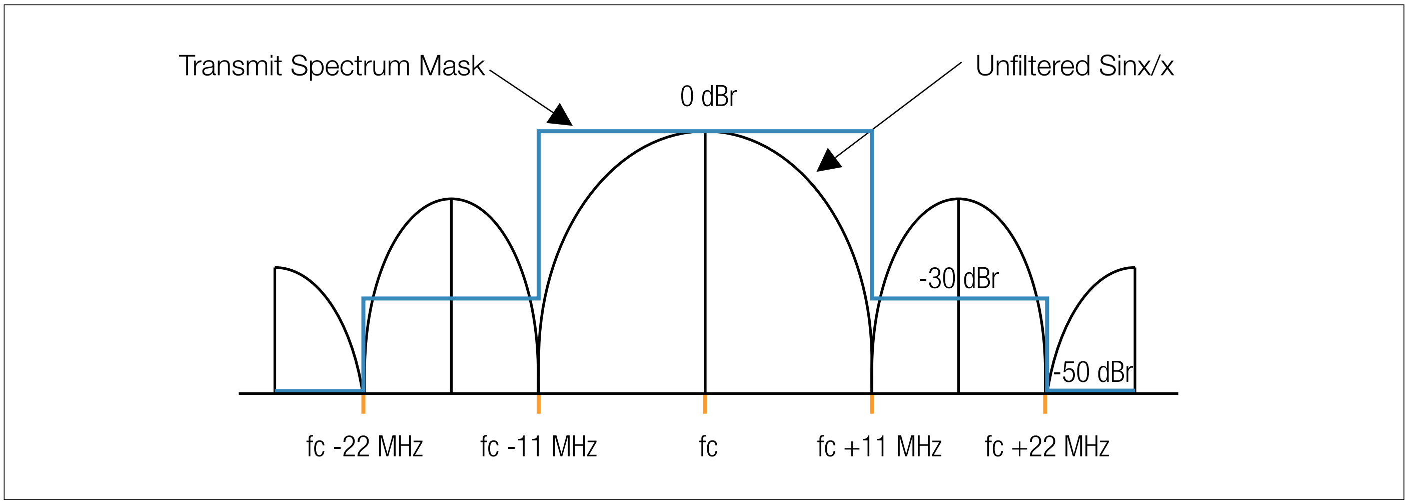


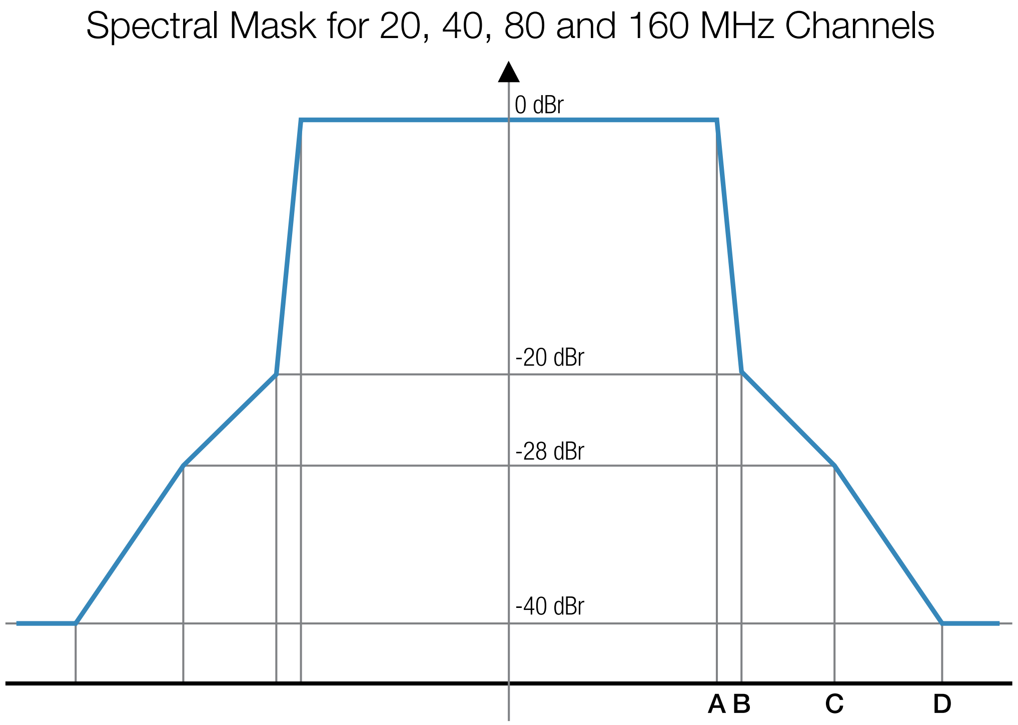
Figure 7. Spectral mask for 802.11b standard.

802.11ac includes support for 80 MHz bandwidth in phase1 and 160 MHz bandwidth in phase 2. The 802.11ac device is required to support 20, 40, and 80 MHz channel bandwidth reception and transmission. The 80 MHz channel consists of two adjacent, non-overlapping 40 MHz channels. The 160 MHz channels are formed by two 80 MHz channels which may be adjacent (contiguous) or non-contiguous. With the newer standards, they are allowed to use a wider bandwidth to boost throughput.

However, it is important to realize that the 2.4 and 5 GHz frequency bands did not get any bigger. Products from all of the 802.11 standards are required to share the same bandwidth. Only if there is spectrum available can the wider bandwidths be used. This is why many 802.11n WLANs may end up using 40 MHz channels only in the 5 GHz band.

Spectral Masks

The 802.11 standard specifies a spectral mask which defines the permitted power distribution across each channel. The spectral mask requires the signal be attenuated to certain levels (from its peak amplitude) at specified frequency offsets. Figure 7 shows the spectral mask used for the 802.11b standard. While the energy falls off very quickly from its peak, it is interesting to note the RF energy that is still being radiated at other channels. This will be discussed further in our next section.



Channel Size	A	B	C	D
20 MHz	9 MHz	11 MHz	20 MHz	30 MHz
40 MHz	19 MHz	21 MHz	40 MHz	60 MHz
80 MHz	39 MHz	41 MHz	80 MHz	120 MHz
160 MHz	79 MHz	81 MHz	160 MHz	240 MHz

Figure 8. OFDM spectral mask used for 802.11a/g/n/ac.

The 802.11a, 802.11g, 802.11n and 802.11ac standards that use the OFDM encoding scheme, have a spectral mask that looks completely different (Figure 8). OFDM allows for a more dense spectral efficiency, thus it gets higher data throughput than the BPSK/QPSK techniques in 802.11b.

Overlapping Channels

The 802.11 use of the term “channel” can often lead to confusion. For radio and TV channels, they are allocated specific frequency spectrums in which to operate. As shown in Figure 6 and from the 802.11 spectral masks it is apparent that plenty of RF energy is going into adjacent channels. Since the spectral mask only defines power output restrictions at specific frequency offsets, it is often assumed that the energy of the channel extends no further than these limits. It is more correct to say that, given the separation between channels, the overlapping signal on any channel should be sufficiently attenuated to minimally interfere with a transmitter on any other channel.

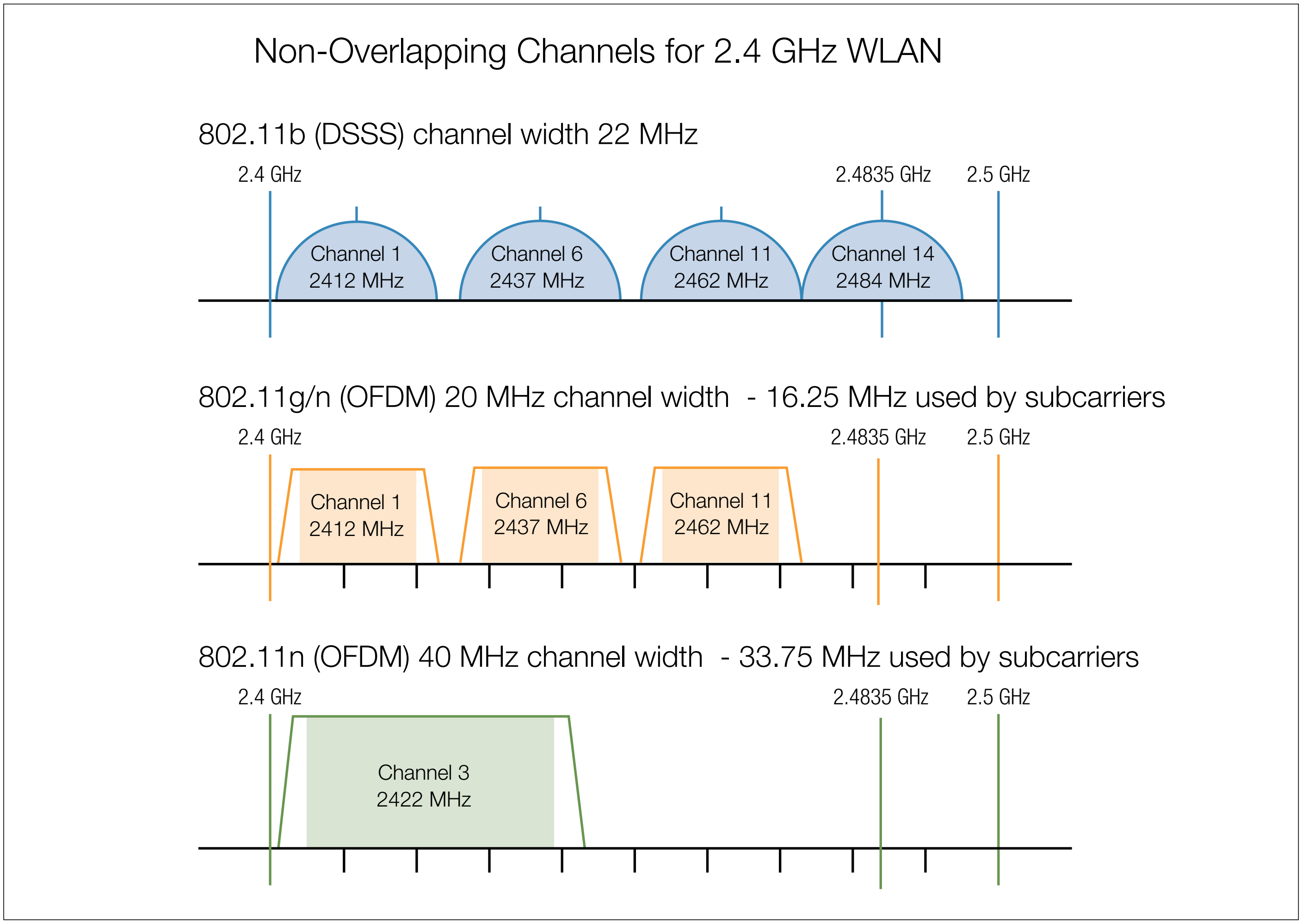

Non-Overlapping Channels for 2.4 GHz WLAN
802.11b (DSSS) channel width 22 MHz
2.4 GHz
2.4835 GHz
2.5 GHz
Channel 1
2412 MHz
Channel 6
2437 MHz
Channel 11
2462 MHz
Channel 14
2484 MHz
802.11g/n (OFDM) 20 MHz channel width - 16.25 MHz used by subcarriers
2.4 GHz
2.4835 GHz
2.5 GHz
Channel 1
2412 MHz
Channel 6
2437 MHz
Channel 11
2462 MHz
802.11n (OFDM) 40 MHz channel width - 33.75 MHz used by subcarriers
2.4 GHz
2.4835 GHz
2.5 GHz
Channel 3
2422 MHz

Figure 9. For the 802.11 standards there are only a few channels that are considered non-overlapping.

Confusion often arises over the amount of channel separation required between transmitting devices. The 802.11b standard was based on DSSS modulation and utilized a channel bandwidth of 22 MHz, resulting in three "non-overlapping" channels (1, 6 and 11). 802.11g was based on OFDM modulation and utilized a channel bandwidth of 20 MHz. This occasionally leads to the belief that four "non-overlapping" channels (1, 5, 9 and 13) exist for 802.11g, although this is not the case. Figure 9 highlights the potential non-overlapping channels in the 2.4 GHz bands. Although the "non-overlapping" channels are limited to spacing or product density, the concept has some merit in limited circumstances. Special care must be taken to adequately space AP cells since overlap between the channels may cause unacceptable degradation of signal quality and throughput.

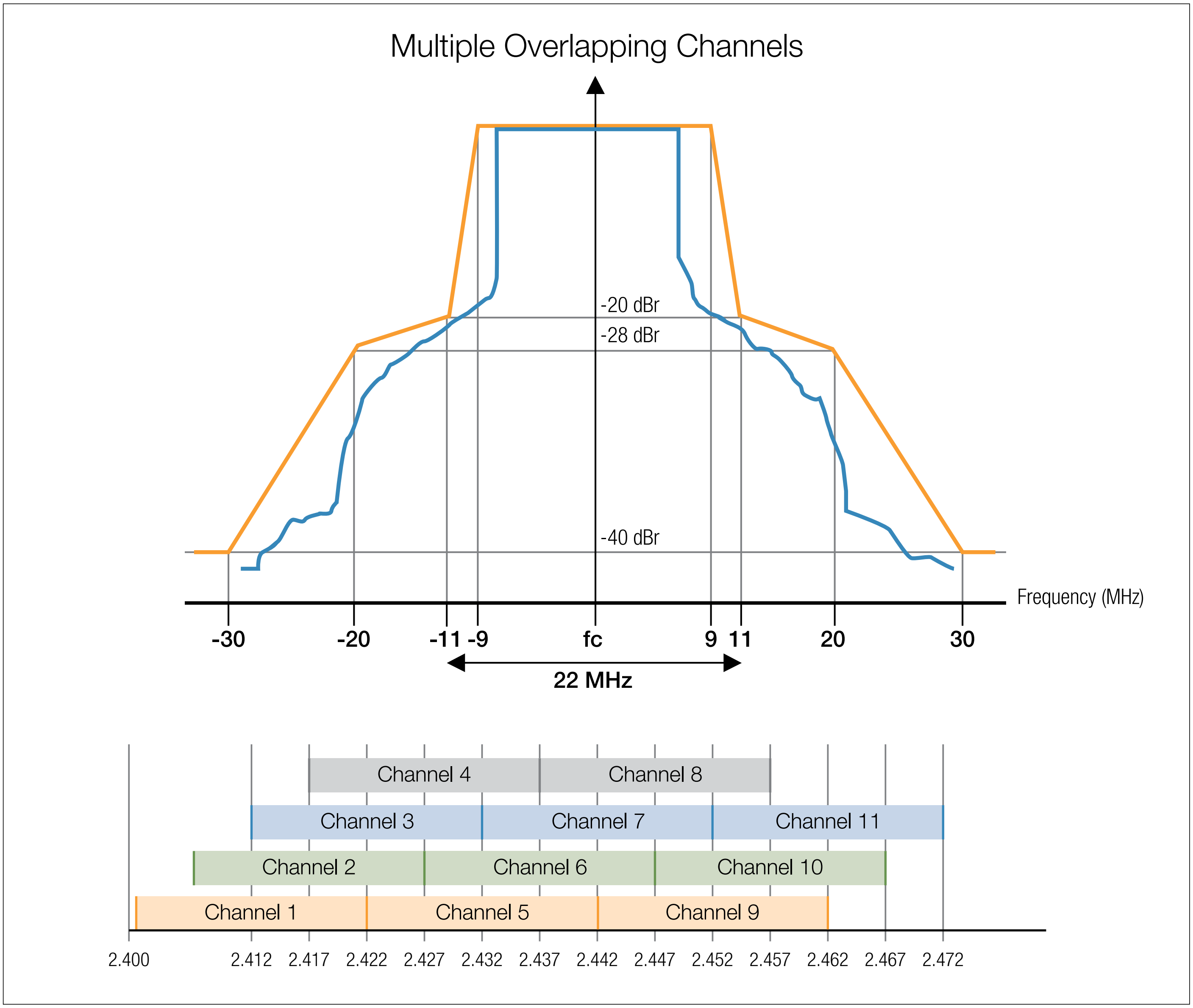


Figure 10. RF energy "bleeds" into frequencies for several adjacent channels, resulting in access points that may actually consume multiple overlapping channels.

ISM use is further complicated by 802.11b/g/n channel overlap. When an 802.11b/g/n radio transmits, the modulated signal is designed to fall within its bandwidth from the channel center frequency. However, RF energy ends up "bleeding" into frequencies for several adjacent channels. As a result, each 802.11b/g/n access point actually consumes multiple overlapping channels (see Figure 10). Transmitting on a 40 MHz 802.11n channel in the ISM band would exacerbate this scarcity by consuming 9 channels: the center frequency plus four channels on the left and four on the right. Finding adjacent unused channels in the congested ISM band is rare; thus, 40 MHz 802.11n operation would very likely interfere with existing 802.11b/g APs. To mitigate this, 802.11n APs using 40 MHz channels are required to listen for legacy (or other non-40 MHz HT) devices and provide coexistence mechanisms.

Country Regulations

Availability of 802.11 channels is regulated by each country, constrained in part by how they each allocate radio spectrum to various services (Table 3 and Table 4). For example, Japan permits the use of all 14 channels for 802.11b, and 1–13 for 802.11g/n-2.4. Other countries such as Spain initially allowed only channels 10 and 11, and France only allowed 10, 11, 12 and 13. They now allow channels 1 through 13. North America and some Central and South American countries allow only 1 through 11. In the US, 802.11 standards operating in the ISM band may be operated without a license, as allowed in Part 15 of the FCC Rules and Regulations.

The regulatory parameters are sent in the PHY Management Layer and are used along with the channel starting frequency given in the Country Information and Regulatory Classes Annex of the 802.11 standard. IEEE uses the phrase "regdomain" to refer to a legal regulatory region. Different countries define different levels of allowable transmitter power, time that a channel can be occupied, and different available channels. Domain codes are specified for the United States, Canada, ETSI (Europe), Spain, France, Japan, and China. The regdomain setting is often made difficult or impossible to change so that the end users do not conflict with local regulatory agencies such as the USA's Federal Communications Commission.

802.11 2.4 GHz Channels Available by Country

Channel	Center Frequency (MHz)	North America	Japan	Most of the World
1	2412	Yes	Yes	Yes
2	2417	Yes	Yes	Yes
3	2422	Yes	Yes	Yes
4	2427	Yes	Yes	Yes
5	2432	Yes	Yes	Yes
6	2437	Yes	Yes	Yes
7	2442	Yes	Yes	Yes
8	2447	Yes	Yes	Yes
9	2452	Yes	Yes	Yes
10	2457	Yes	Yes	Yes
11	2462	Yes	Yes	Yes
12	2467	No	Yes	Yes
13	2472	No	Yes	Yes
14	2484	No	11b only	No

Table 3. 802.11 2.4 GHz band available channels by country (22 MHz wide).

802.11 5 GHz Channels Available by Country

Channel	Center Frequency (MHz)	U.S.	Europe	Japan		Singapore	China	Israel	Korea	Turkey	Australia	South Africa	Brazil
		40/20 MHz	40/20 MHz	40/20 MHz	10 MHz	40/20 MHz	20 MHz	20 MHz	20 MHz	40/20 MHz	40/20 MHz	40/20 MHz	40/20 MHz
183	4915	No	No	No	Yes	No	No	No	No	No	No	No	No
184	4920	No	No	Yes	Yes	No	No	No	No	No	No	No	No
185	4925	No	No	No	Yes	No	No	No	No	No	No	No	No
187	4935	No	No	No	Yes	No	No	No	No	No	No	No	No
188	4940	No	No	Yes	Yes	No	No	No	No	No	No	No	No
189	4945	No	No	No	Yes	No	No	No	No	No	No	No	No
192	4960	No	No	Yes	No	No	No	No	No	No	No	No	No
196	4980	No	No	Yes	No	No	No	No	No	No	No	No	No
7	5035	No	No	No	Yes	No	No	No	No	No	No	No	No
8	5040	No	No	No	Yes	No	No	No	No	No	No	No	No
9	5045	No	No	No	Yes	No	No	No	No	No	No	No	No
11	5055	No	No	No	Yes	No	No	No	No	No	No	No	No
12	5060	No	No	No	No	No	No	No	No	No	No	No	No
16	5080	No	No	No	No	No	No	No	No	No	No	No	No
34	5170	No	No	client only	No	Yes	No	Yes	Yes	Indoors	No	Indoors	Indoors
36	5180	Yes	Indoors	Yes	No	Yes	Yes	Yes	Yes	Indoors	Yes	Indoors	Indoors
38	5190	No	No	client only	No	Yes	No	Yes	Yes	Indoors	No	Indoors	Indoors
40	5200	Yes	Indoors	Yes	No	Yes	Yes	Yes	Yes	Indoors	Yes	Indoors	Indoors
42	5210	No	No	client only	No	Yes	No	Yes	Yes	Indoors	No	Indoors	Indoors
44	5220	Yes	Indoors	Yes	No	Yes	Yes	Yes	Yes	Indoors	Yes	Indoors	Indoors
46	5230	No	No	client only	No	Yes	No	Yes	Yes	Indoors	No	Indoors	Indoors
48	5240	Yes	Indoors	Yes	No	Yes	Yes	Yes	Yes	Indoors	Yes	Indoors	Indoors
52	5260	DFS	Indoors/DFS/ TPC	DFS/TPC	No	Yes	DFS/TPC	Yes	Yes	Indoors	DFS/TPC	Indoors	Indoors
56	5280	DFS	Indoors/DFS/TPC	DFS/TPC	No	Yes	DFS/TPC	Yes	Yes	Indoors	DFS/TPC	Indoors	Indoors
60	5300	DFS	Indoors/DFS/TPC	DFS/TPC	No	Yes	DFS/TPC	Yes	Yes	Indoors	DFS/TPC	Indoors	Indoors
64	5320	DFS	Indoors/DFS/TPC	DFS/TPC	No	Yes	DFS/TPC	Yes	Yes	Indoors	DFS/TPC	Indoors	Indoors
100	5500	DFS	DFS/TPC	DFS/TPC	No	No	No	No	Yes	DFS/TPC	DFS/TPC	Yes	DFS
104	5520	DFS	DFS/TPC	DFS/TPC	No	No	No	No	Yes	DFS/TPC	DFS/TPC	Yes	DFS
108	5540	DFS	DFS/TPC	DFS/TPC	No	No	No	No	Yes	DFS/TPC	DFS/TPC	Yes	DFS
112	5560	DFS	DFS/TPC	DFS/TPC	No	No	No	No	Yes	DFS/TPC	DFS/TPC	Yes	DFS
116	5580	DFS	DFS/TPC	DFS/TPC	No	No	No	No	Yes	DFS/TPC	DFS/TPC	Yes	DFS
120	5600	No	DFS/TPC	DFS/TPC	No	No	No	No	Yes	DFS/TPC	No	Yes	DFS
124	5620	No	DFS/TPC	DFS/TPC	No	No	No	No	Yes	DFS/TPC	No	Yes	DFS
128	5640	No	DFS/TPC	DFS/TPC	No	No	No	No	Yes	DFS/TPC	No	Yes	DFS
132	5660	DFS	DFS/TPC	DFS/TPC	No	No	No	No	No	DFS/TPC	DFS/TPC	Yes	DFS
136	5680	DFS	DFS/TPC	DFS/TPC	No	No	No	No	No	DFS/TPC	DFS/TPC	Yes	DFS
140	5700	DFS	DFS/TPC	DFS/TPC	No	No	No	No	No	DFS/TPC	DFS/TPC	Yes	DFS
149	5745	Yes	SRD (25 mW)	No	No	Yes	Yes	No	Yes	No	Yes	No	Yes
153	5765	Yes	SRD (25 mW)	No	No	Yes	Yes	No	Yes	No	Yes	No	Yes
157	5785	Yes	SRD (25 mW)	No	No	Yes	Yes	No	Yes	No	Yes	No	Yes
161	5805	Yes	SRD (25 mW)	No	No	Yes	Yes	No	Yes	No	Yes	No	Yes
165	5825	Yes	SRD (25 mW)	No	No	Yes	Yes	No	Yes	No	Yes	No	Yes

Table 4. 802.11 5 GHz band available channels by country. Center Frequencies are given for 20 MHz or 40 MHz wide channels. 80 MHz channels are built with adjacent 40 MHz channels. 160 MHz channels are built with adjacent 80 MHz channels. Center Frequencies for 80 MHz and 160 MHz will differ from the ones provided here.

Dynamic Frequency Selection (DFS) - The objective is to achieve maximum system spectral efficiency in bit/s/Hz/site by means of frequency reuse, but still assure a certain grade of service by avoiding co-channel interference and adjacent channel interference among nearby channels.

Indoors – Channel is allowed for indoor use only.

Client Only – Channel is allowed when used in a client mode only.

Transmit Power Control (TPC) - The intelligent selection of transmit power in a communication system to achieve good performance within the system.

Short Range Devices (SRD) – Regulation of the allowed power level of devices using this channel.

Yes/No – Each country defines which channels are allowed.

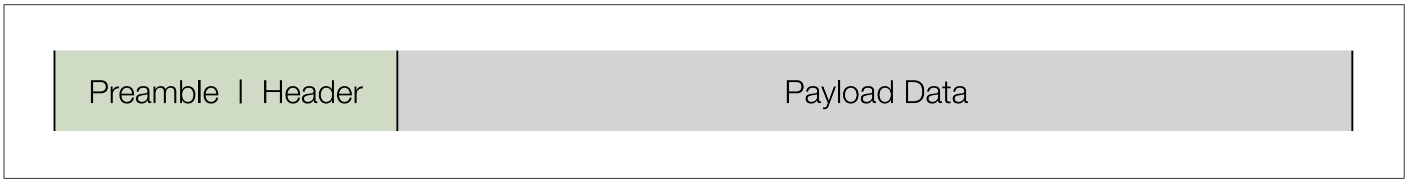


Figure 11. Each PHY packet contains a preamble, header and payload data.

Physical Layer (PHY) Frame Structure

The 802.11 Physical Layer uses bursted transmissions or packets. Each packet contains a Preamble, Header and Payload Data (Figure 11). The Preamble allows the receiver to obtain time and frequency synchronization and estimate channel characteristics for equalization. It is a bit sequence that receivers watch for to lock onto the rest of the transmission. The Header provides information about the packet configuration, such as format, data rates, etc. Finally the Payload Data contains the user's payload data being transported.

The 802.11 standards define "frame" types for use in transmission of data as well as management and control of wireless links. At the top level these frames are divided into three functions: Management Frames, Control Frames and Data Frames. Each frame consists of an MAC header, payload and frame check sequence (FCS). Some frames may not have a payload. The first two bytes of the MAC header form a frame control field specifying the form and function of the frame. The frame control field is further subdivided into the following sub-fields:

- **Protocol Version:** Two bits representing the protocol version. Currently used protocol version is zero. Other values are reserved for future use.
- **Type:** Two bits identifying the type of WLAN frame. Control, Data and Management are various frame types defined in IEEE 802.11.
- **Sub Type:** Four bits providing addition discrimination between frames. Type and Sub type work together to identify the exact frame.
- **ToDS and FromDS:** Each is one bit in size. They indicate whether a data frame is headed for a distribution system. Control and management frames set these values to zero. All the data frames will have one of these bits set. However communication within an IBSS network always sets these bits to zero.
- **More Fragments:** The More Fragments bit is set when a packet is divided into multiple frames for transmission. Every frame except the last frame of a packet will have this bit set.
- **Retry:** Sometimes frames require retransmission, and for this there is a Retry bit which is set to one when a frame is resent. This aids in the elimination of duplicate frames.
- **Power Management:** This bit indicates the power management state of the sender after the completion of a frame exchange. Access points are required to manage the connection and will never set the power saver bit.
- **More Data:** The More Data bit is used to buffer frames received in a distributed system. The access point uses this bit to facilitate stations in power saver mode. It indicates that at least one frame is available and addresses all stations connected.
- **WEP:** The WEP bit is modified after processing a frame. It is toggled to one after a frame has been decrypted or if no encryption is set it will have already been one.
- **Order:** This bit is only set when the "strict ordering" delivery method is employed. Frames and fragments are not always sent in order as it causes a transmission performance penalty.

The next two bytes are reserved for the Duration ID field. This field can take one of three forms: Duration, Contention-Free Period (CFP), and Association ID (AID). An 802.11 frame can have up to four address fields. Each field can carry a MAC address. Address 1 is the receiver, Address 2 is the transmitter, Address 3 is used for filtering purposes by the receiver.

The Sequence Control field is a two-byte section used for identifying message order as well as eliminating duplicate frames. The first 4 bits are used for the fragmentation number and the last 12 bits are the sequence number. There is an optional two-byte Quality of Service control field which was added with 802.11e. The Frame Body field is variable in size, from 0 to 2304 bytes plus any overhead from security encapsulation and contains information from higher layers. The Frame Check Sequence (FCS) is the last four bytes in the standard 802.11 frame. Often referred to as the Cyclic Redundancy Check (CRC), it allows for integrity check of retrieved frames. As frames are about to be sent the FCS is calculated and appended. When a station receives a frame it can calculate the FCS of the frame and compare it to the one received. If they match, it is assumed that the frame was not distorted during transmission.

Management Frames

Management Frames allow for the maintenance of communication. Some common 802.11 subtypes include:

- **Authentication Frame:** 802.11 authentication begins with the wireless network interface controller (WNIC) sending an authentication frame to the access point containing its identity. With an open system authentication the WNIC only sends a single authentication frame and the access point responds with an authentication frame of its own indicating acceptance or rejection. With shared key authentication, after the WNIC sends its initial authentication request it will receive an authentication frame from the access point containing challenge text. The WNIC sends an authentication frame containing the encrypted version of the challenge text to the access point. The access point ensures the text was encrypted with the correct key by decrypting it with its own key. The result of this process determines the WNIC's authentication status.
- **Association Request Frame:** Sent from a station it enables the access point to allocate resources and synchronize. The frame carries information about the WNIC including supported data rates and the SSID of the network the station wishes to associate with. If the request is accepted, the access point reserves memory and establishes an association ID for the WNIC.
- **Association Response Frame:** Sent from an access point to a station containing the acceptance or rejection to an association request. If it is an acceptance, the frame will contain information such an association ID and supported data rates.
- **Beacon Frame:** Sent periodically from an access point to announce its presence and provide the SSID, and other parameters for WNICs within range.
- **Deauthentication Frame:** Sent from a station wishing to terminate connection from another station.
- **Disassociation Frame:** Sent from a station wishing to terminate connection. It's an elegant way to allow the access point to relinquish memory allocation and remove the WNIC from the association table.
- **Probe Request Frame:** Sent from a station when it requires information from another station.
- **Probe Response Frame:** Sent from an access point containing capability information, supported data rates, etc., after receiving a probe request frame.
- **Reassociation Request Frame:** A WNIC sends a reassociation request when it drops from range of the currently associated access point and finds another access point with a stronger signal. The new access point coordinates the forwarding of any information that may still be contained in the buffer of the previous access point.
- **Reassociation Response Frame:** Sent from an access point containing the acceptance or rejection to a WNIC reassociation request frame. The frame includes information required for association such as the association ID and supported data rates.

Control Frames

Control frames facilitate the exchange of data frames between stations. Some common 802.11 control frames include:

- **Acknowledgement (ACK) Frame:** After receiving a data frame, the receiving station will send an ACK frame to the sending station if no errors are found. If the sending station doesn't receive an ACK frame within a predetermined period of time, the sending station will resend the frame.
- **Request to Send (RTS) Frame:** The RTS and CTS frames provide an optional collision reduction scheme for access points with hidden stations. A station sends a RTS frame as the first step in a two-way handshake required before sending data frames.
- **Clear to Send (CTS) Frame:** A station responds to an RTS frame with a CTS frame. It provides clearance for the requesting station to send a data frame. The CTS provides collision control management by including a time value for which all other stations are to hold off transmission while the requesting stations transmits.

Categorization of Data Frame Types

Frame Type	Contention-based Service	Contention-free Service	Carries Data
Data	X		Yes
Data+CF-Ack		X	Yes
Data+CF-Poll		AP only	Yes
Data+CF-Ack+CF-Poll		AP only	Yes
Null	X	X	No
CF-Ack		X	No
CF-Poll		AP only	No
CF-ACK+CF-Poll		AP only	No

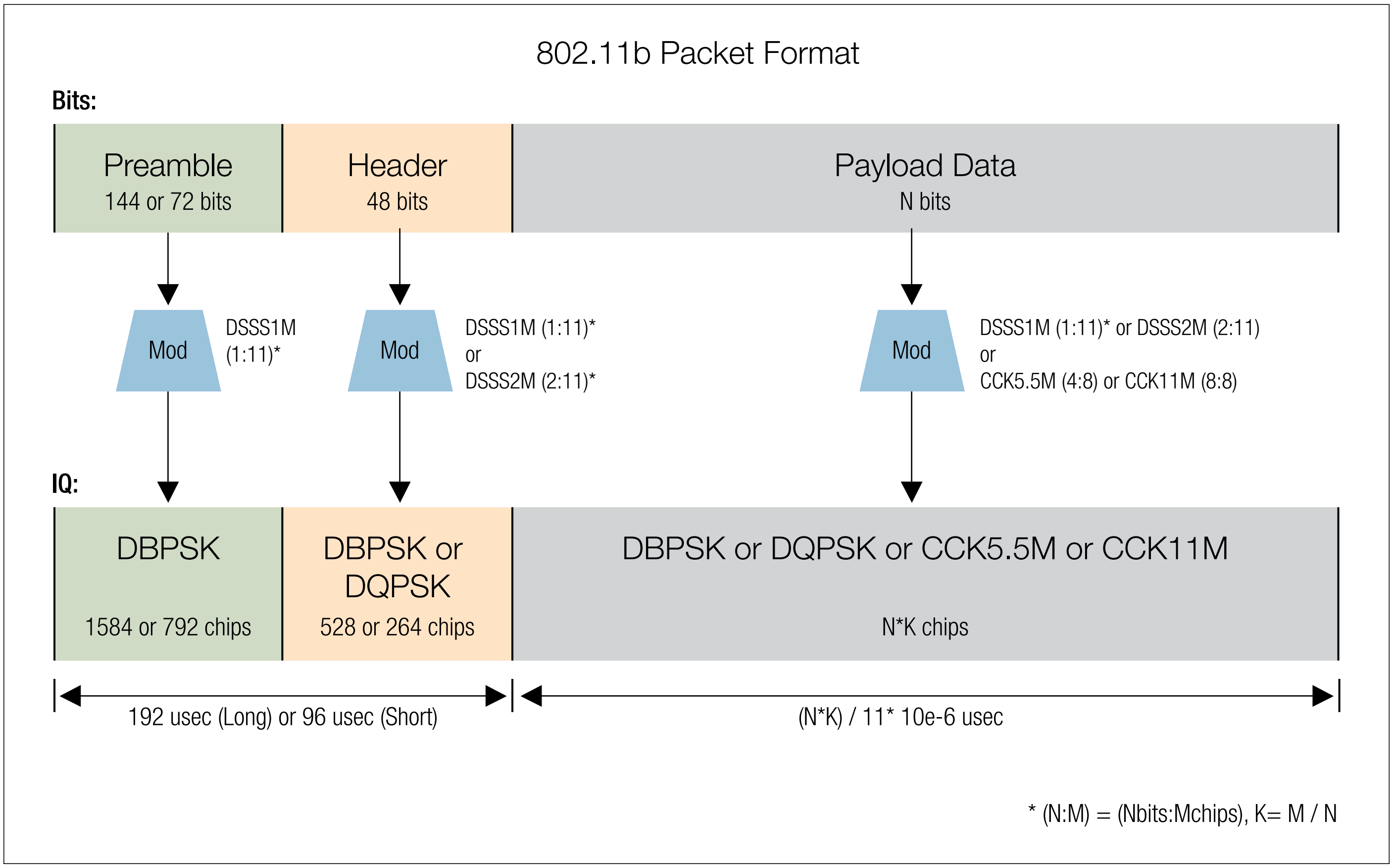
Table 5. Categorization of data frame types.

Data Frames

Data frames carry higher-level protocol data in the frame body. Depending on the particular type of data frame, some of the fields in the figure may not be used. The different data frame types can be categorized according to function. One such distinction is between data frames used for contention-based service and those used for contention-free service. Any frames that appear only in the contention-free period can never be used in an independent basic service set (IBSS). Another possible division is between frames that carry data and frames that perform management functions. Table 5 shows how frames may be divided along these lines.

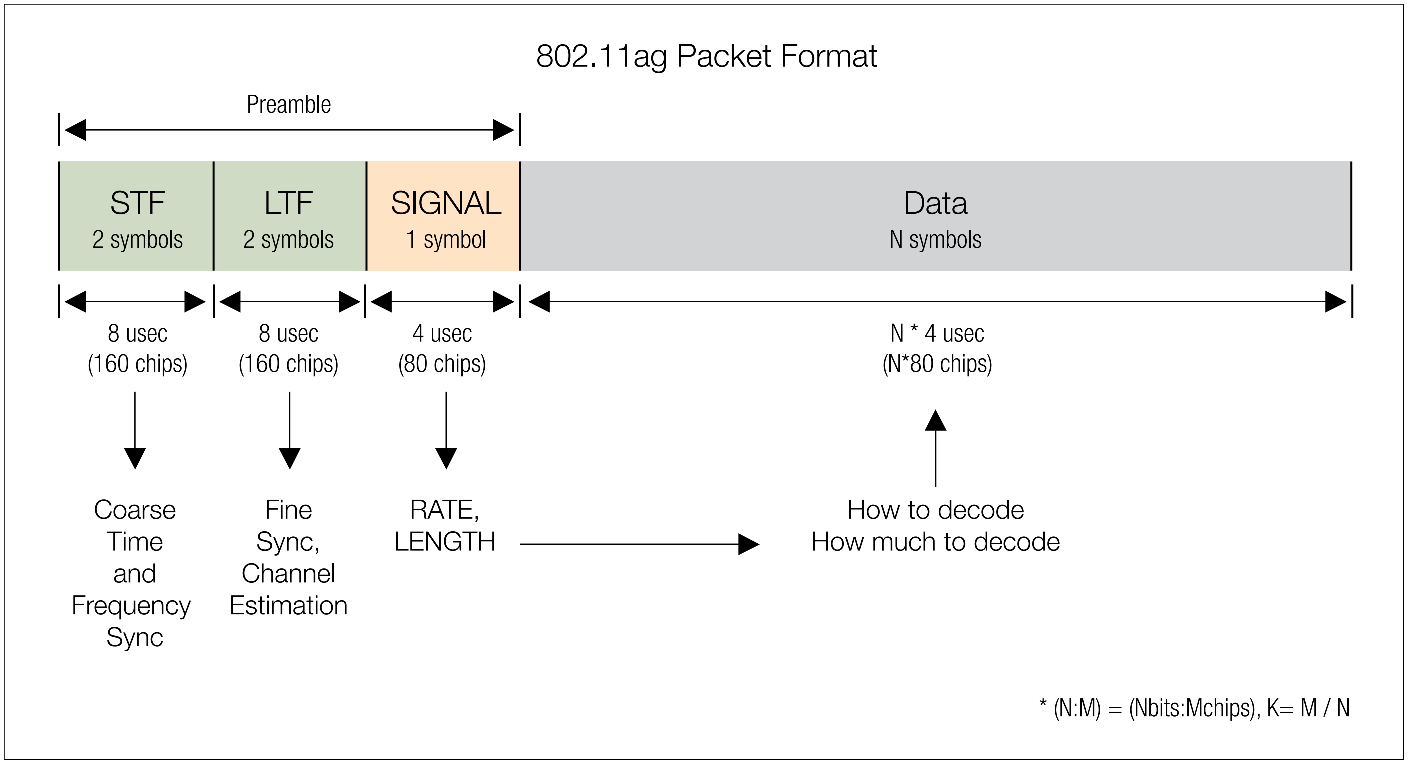
802.11b Packet Format

802.11b Packet Format (refer to figure below)	
Preamble and Header	**Long** (required in original) **Short** (optional in "b")
Preamble	Always uses DSS1M Long Preamble contains 144 bits (128 scrambled 1's + 16 SFD marker bits) Short Preamble contains 72 bits (56 scrambled 0's + 16 SFD marker bits)
Header	Long Header uses DSSS1M, Short Header uses DSSS2M Contains 48 bits indicating configuration: SIGNAL (8 bits): indicates payload data rate (1, 2, 5.5 or 11 Mbps) SERVICE (8 bits): additional HR configuration bits LENGTH (16 bits): length of data Payload in microseconds CRC (16 bits): Protects header data contents
Payload	Payload data modulated with DSSS1M, DSSS2M, CCK5.5M, or CCK11M



802.11a/g Packet Format

802.11a/g Packet Format (refer to figure below)	
Preamble	**STF:** Short Training Field (2 symbols) - Uses on 1/4 of subcarriers. Repeats every 16 chips. - Initial timing sync and frequency estimate. **LTF:** Long Training Field (2 symbols) - Uses all 52 subcarriers (same as Data symbols). - Fine timing and frequency sync, and channel response estimation. **SIGNAL:** (1 symbol) - Encoded similar to a Data symbol, but always uses BPSK modulation. 24 bits of configuration data. - Fields: - RATE (4 bits): Indicates Data FEC coding and modulation (8 combinations), aka "MCS" - LENGTH (12 bits): Number of octets (bytes) carried in Payload - PARITY (1 bit): Even parity-check on RATE+LENGTH data - TAIL (7 bits): Used for SIGNAL symbol FEC decoding
Payload	52 subcarriers, 48 Data + 4 Pilot Data subcarriers use BPSK, QPSK, 16QAM or 64QAM modulation. Same in all symbols Pilots subcarriers (BPSK only) are used to track frequency/phase and amplitude variations over the burst



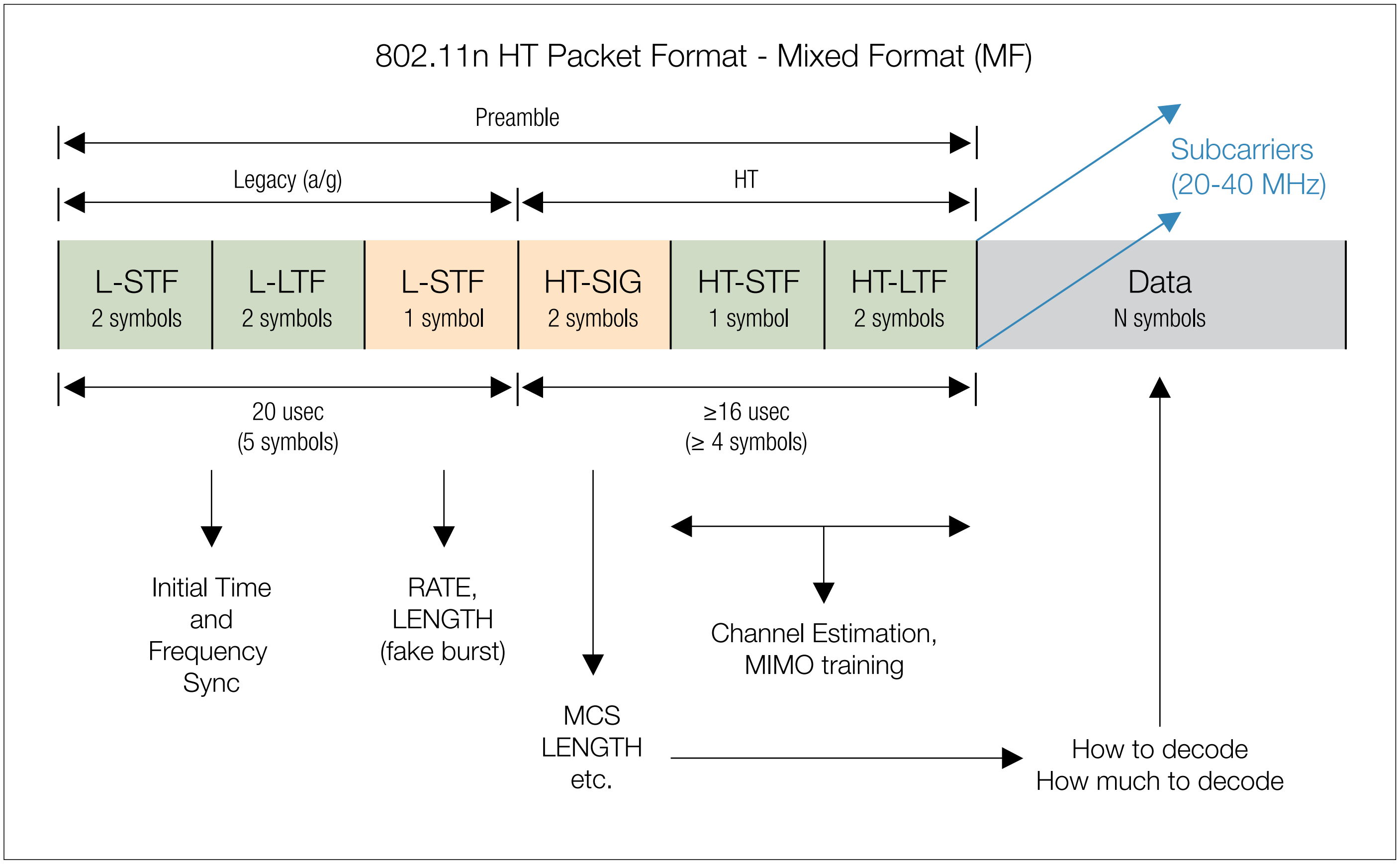
802.11n Packet Format

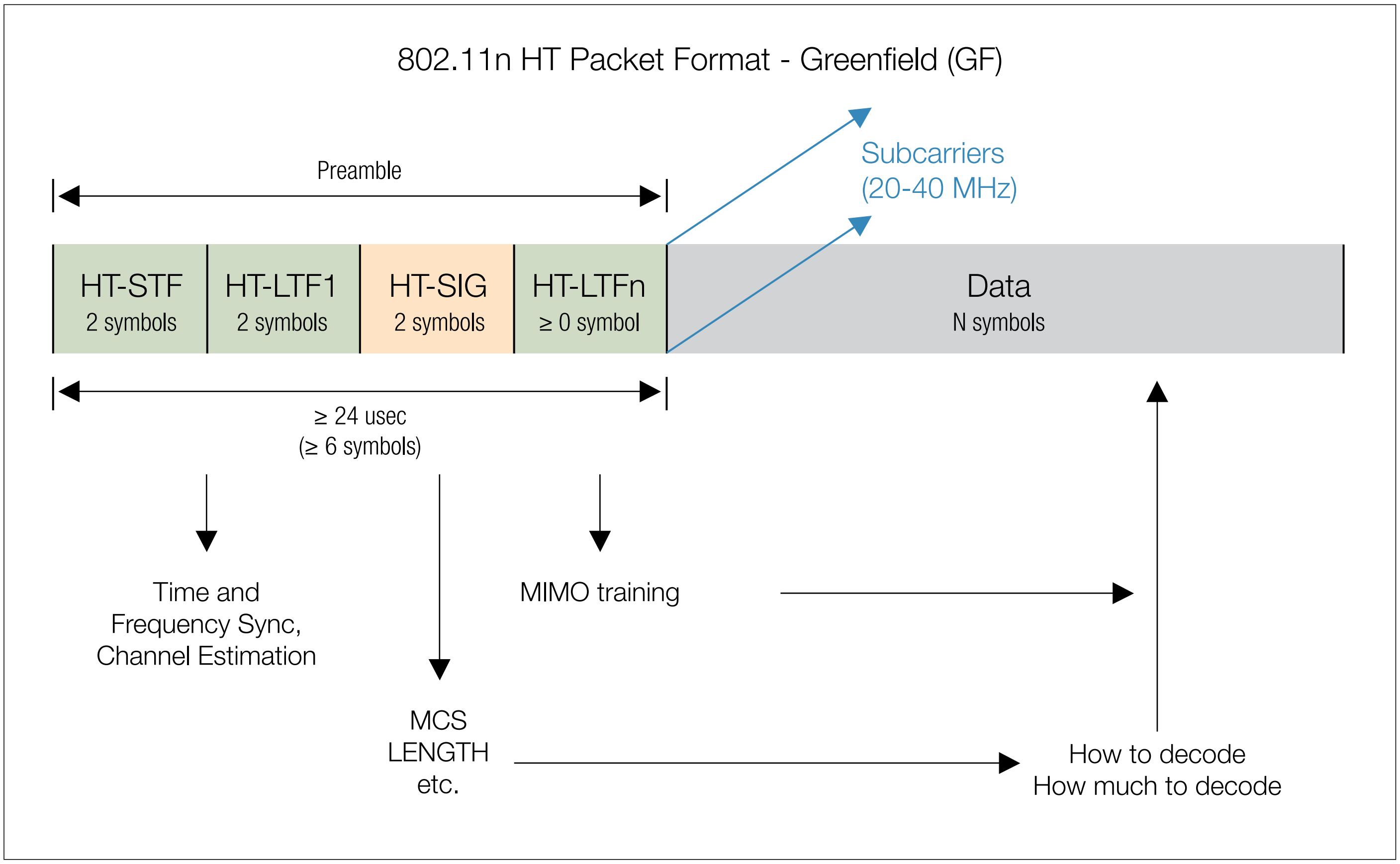
There are two 802.11n operating modes: Greenfield (HT) and Mixed (Non-HT). Greenfield can only be used where no legacy systems exist. HT systems will not switch between Greenfield and Mixed, they will only use one or the other.

An 802.11n AP using Non-HT mode sends all frames in the old 802.11a/g format so that legacy stations can understand them. That AP must use 20 MHz channels and none of the new HT features described in this paper. All products must support this mode to ensure backward compatibility, but an 802.11n AP using Non-HT delivers no better performance than 802.11a/g.

The mandatory HT Mixed mode will be the most common 802.11n AP operating mode. In this mode, HT enhancements can be used simultaneously with HT Protection mechanisms that permit communication with legacy stations. HT Mixed mode provides backwards compatibility, but 802.11n devices pay significant throughput penalties as compared to Greenfield mode.

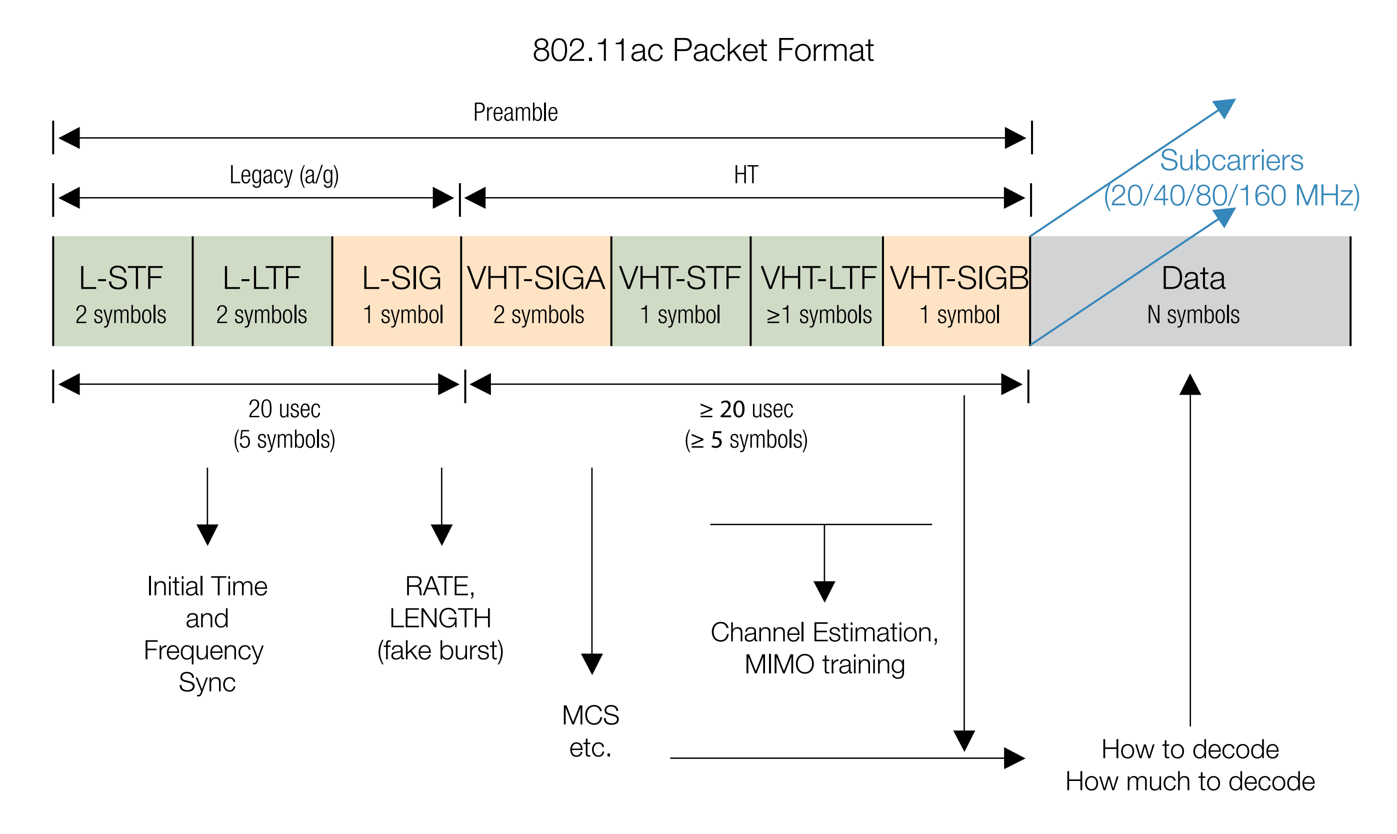
802.11n Packet Format (refer to figures on page 23)	
Preamble Mixed Mode	**Non-HT Legacy** L-STF, L-LTF, L-SIG are backward compatible to a/g systems L-SIG contains RATE and LENGTH values that inform Legacy systems how long to hold off next Tx attempt **HT Mixed Mode** HT-SIG (2 symbols): Indicates MCS (Modulation and Coding Scheme), Length, and other HT-specific parameters HT-STF (1 symbol), HT-LTF (≥1 symbol): Allow sync and channel estimation on HT bandwidth (more subcarriers than L-LTF). Additional HT-LTF symbols are included for MIMO modes to "sound" the multiple channels (paths)
Greenfield Mode	L-STF, L-LTF, L-SIG are dropped, HT-STF and HT-LTF replace L-STF/LTF Otherwise similar to MF Preamble - Fields: - RATE (4 bits): Indicates Data FEC coding and modulation (8 combinations), aka "MCS" - LENGTH (12 bits): Number of octets (bytes) carried in Payload - PARITY (1 bit): Even parity-check on RATE+LENGTH data - TAIL (7 bits): Used for SIGNAL symbol FEC decoding
Payload	56 (20 MHz) or 114 (40 MHz) subcarriers Data subcarriers use BPSK, QPSK, 16QAM, or 64QAM modulation. Same in all symbols Pilots subcarriers (BPSK only) are used to track frequency/phase and amplitude variations over the burst Optional Short Guard Interval can be used if multipath environment allows


802.11n HT Packet Format - Mixed Format (MF)
Preamble
Legacy (a/g)
HT
Subcarriers
(20-40 MHz)
L-STF
2 symbols
L-LTF
2 symbols
L-STF
1 symbol
HT-SIG
2 symbols
HT-STF
1 symbol
HT-LTF
2 symbols
Data
N symbols
20 usec
(5 symbols)
≥16 usec
(≥ 4 symbols)
Initial Time
and
Frequency
Sync
RATE,
LENGTH
(fake burst)
Channel Estimation,
MIMO training
MCS
LENGTH
etc.
How to decode
How much to decode


802.11n HT Packet Format - Greenfield (GF)
Preamble
Subcarriers
(20-40 MHz)
HT-STF
2 symbols
HT-LTF1
2 symbols
HT-SIG
2 symbols
HT-LTFn
≥ 0 symbol
Data
N symbols
≥ 24 usec
(≥ 6 symbols)
Time and
Frequency Sync,
Channel Estimation
MIMO training
MCS
LENGTH
etc.
How to decode
How much to decode

802.11ac Packet Format

802.11ac Packet Format (refer to figure below)	
Preamble	Single Preamble format, no Greenfield type
Legacy Mode	L-STF, L-LTF, L-SIG are backward compatible to a/g systems L-SIG contains RATE and LENGTH values that inform Legacy systems how long to hold off next Tx attempt
VHT Mode	VHT-SIGA (2 symbols): Indicates MCS (Modulation and Coding Scheme), and other VHT-specific parameters VHT-STF (1 symbol), VHT-LTF (≥1 symbol): Allow sync and channel estimation on VHT bandwidth (more subcarriers than L-STF/L-LTF). Additional VHT-LTF symbols are included for MIMO configs to "sound" the multiple channels (paths) VHT-SIGB (1 symbol): Length parameters, MU-MIMO support
Payload	56/114/242/484 (20/40/80/160 MHz) subcarriers (Data + Pilot) Data subcarriers use BPSK, QPSK, 16QAM, 64QAM or 256QAM modulation. Same in all symbols Pilots subcarriers (BPSK only) are used to track frequency/phase and amplitude variations over the burst Optional Short Guard Interval can be used if multipath environment allows



Physical Layer Modulation Formats

The physical layer modulation formats and coding rates determine how the 802.11 data is sent over the air and at what data rates. For example, Direct-Sequence Spread Spectrum (DSSS) was used in the early 802.11 standards, while Orthogonal Frequency Division Multiplexing (OFDM) is being used by many of the later standards. The newer modulation methods and coding rates are generally more efficient and sustain higher data rates, but older methods and rates are still supported for backwards compatibility. Table 6 highlights modulation formats for each of the 802.11 standards. This section discusses in more detail the two primary modulation techniques used today – DSSS and OFDM.

Modulation Techniques Used by the 802.11 Standards	
Legacy	DSSS - DBPSK (1M) DSSS - DQPSK (2M)
802.11b	HR/DSSS - CCK (5.5M, 11M) HR/DSSS - PBCC (5.5M, 11M) (obsolete)
802.11g	ERP - PBCC (22M, 33M) (obsolete) DSSS - OFDM (6-54M) (deprecated)
802.11a/g	OFDM (6-54M)
802.11n	HT20/40 (6.5 - 150M) (SISO 1x1:1) HT20/40 (13 - 600M) (MIMO, up to 4x4:4)
802.11ac	VHT20/40/80/160 (6.5 - 867M) (SISO 1x1:1) VHT80+80 (58.5 - 867M) (SISO 1x1:1) VHT20/40/80/160 (13 - 6933M) (MIMO, up to 8x8:8) VHT80+80 (117 - 6933M) (MIMO, up to 8x8:8)

Table 6. Modulation techniques used by the 802.11 standards.

Direct-Sequence Spread Spectrum

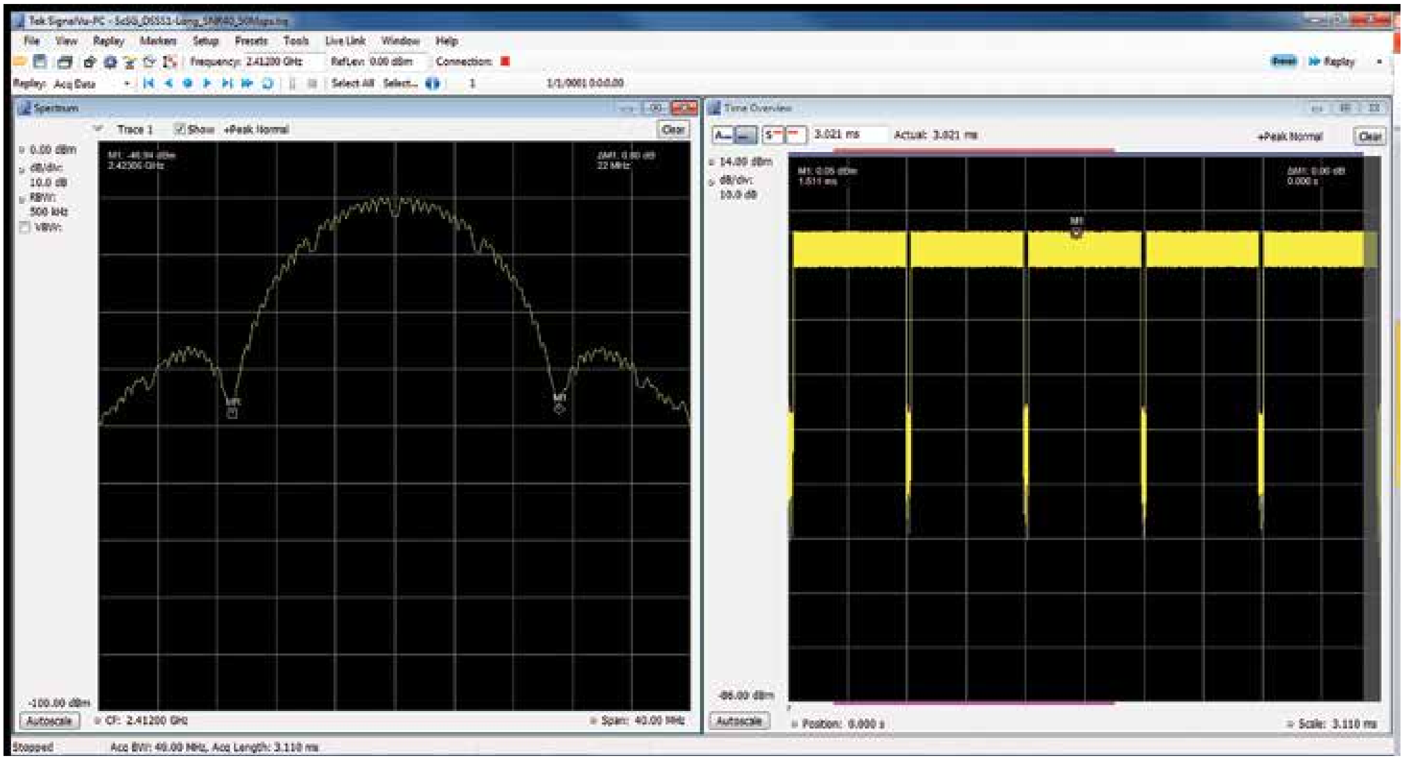
For the original legacy 802.11 and 802.11b standards they make use of Direct-Sequence Spread Spectrum (DSSS) modulation techniques. As with other spread spectrum technologies, the transmitted signal takes up more bandwidth than the information signal that modulates the carrier or broadcast frequency. The name 'spread spectrum' comes from the fact that the carrier signals occur over the full bandwidth (spectrum) of a device's transmitting frequency.

Direct-Sequence Spread Spectrum transmissions multiply the data being transmitted by a "noise" signal. This noise signal is a pseudorandom sequence of 1 and –1 values, at a frequency much higher than that of the original signal.

The resulting signal resembles white noise, similar to an audio recording of "static". This noise-like signal can then be used to exactly reconstruct the original data at the receiving end, by multiplying it by the same pseudorandom number (PN) sequence (because 1 × 1 = 1, and –1 × –1 = 1). This process, known as "de-spreading", mathematically constitutes a correlation of the transmitted PN sequence with the PN sequence that the receiver believes the transmitter is using.

The resulting effect of enhancing signal to noise ratio on the channel is called process gain. This effect can be made larger by employing a longer PN sequence and more chips per bit, but physical devices used to generate the PN sequence impose practical limits on attainable processing gain.

If an undesired transmitter transmits on the same channel but with a different PN sequence (or no sequence at all), the de-spreading process results in no processing gain for that signal. This effect is the basis for the code division multiple access (CDMA) property of DSSS, which allows multiple transmitters to share the same channel within the limits of the cross-correlation properties of their PN sequences.


Tek SignalVu-PC - ScSG_DSSS1-Long_SNR40_50Msps.tiq
File View Replay Markers Setup Presets Tools Live Link Window Help
Preset Replay
Select All Select...
Spectrum
Trace 1
Show
Clear
M1
ΔM1
Time Overview
Clear
M1
Autoscale
Autoscale

Frequency: 2.41200 GHz
RefLev: 0.00 dBm
Connection:
Replay: Acq Data
1
1/1/0001 0:0:0.00

+Peak Normal
0.00 dBm
dB/div: 10.0 dB
RBW: 500 kHz
VBW:
M1: -46.94 dBm 2.42306 GHz
ΔM1: 0.00 dB 22 MHz
-100.00 dBm
CF: 2.41200 GHz
Span: 40.00 MHz

3.021 ms
Actual: 3.021 ms
+Peak Normal
14.00 dBm
dB/div: 10.0 dB
M1: 0.05 dBm 1.511 ms
ΔM1: 0.00 dB 0.000 s
-86.00 dBm
Position: 0.000 s
Scale: 3.110 ms

Stopped
Acq BW: 40.00 MHz, Acq Length: 3.110 ms

Figure 12. The 802.11b DSSS transmitted waveform has a roughly bell-shaped envelope centered on the carrier frequency.

Figure 12 shows the plot of an 802.11b DSSS transmitted waveform. It has a roughly bell-shaped envelope centered on the carrier frequency, just like a normal AM transmission, except that the added noise causes the distribution to be much wider than that of an AM transmission.

DSSS is different from frequency-hopping spread spectrum (FHSS) transmission, that pseudo-randomly re-tunes the carrier, instead of adding pseudo-random noise to the data. DSSS transmissions result in a uniform frequency distribution whose width is determined by the output range of the pseudorandom number generator.

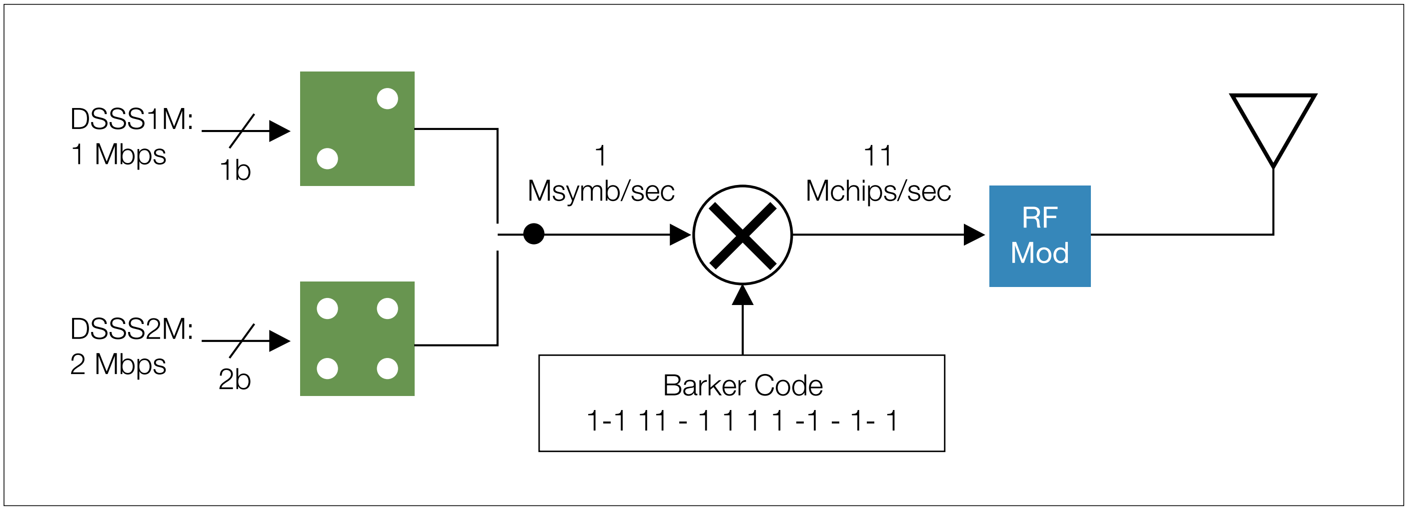


Figure 13. BPSK/QPSK modulation techniques used in the 802.11b standard.

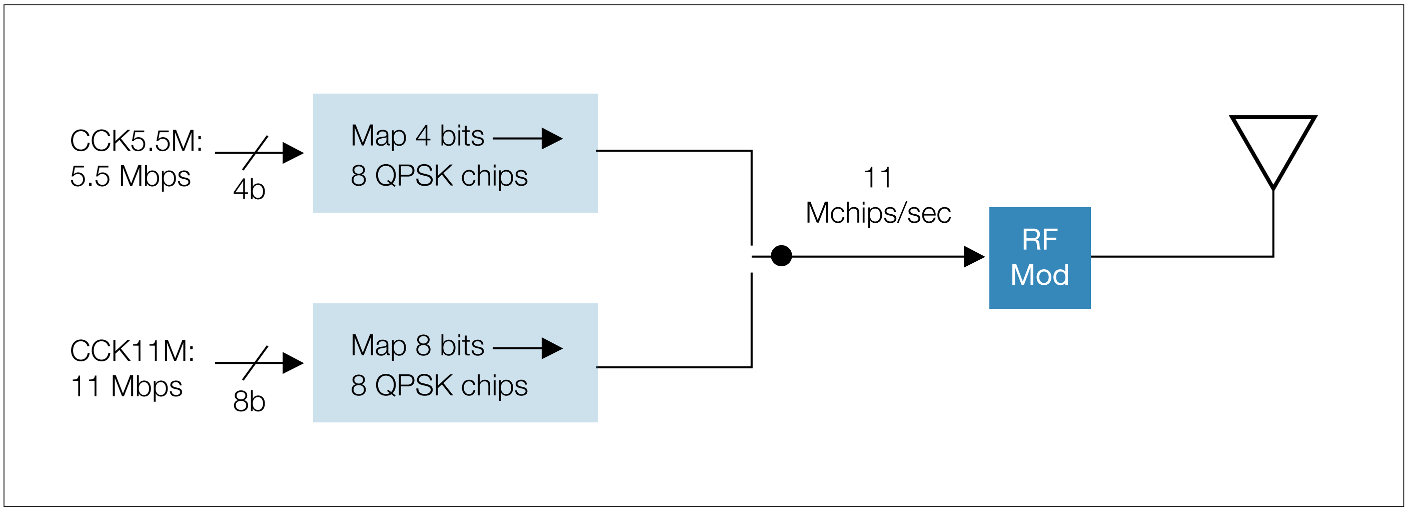


Figure 14. QPSK/QPSK modulation techniques used in the 802.11b standard.

802.11 DSSS modulation uses a two stage process. In the first stage, 1 or 2 bits of data are encoded using a Differential BPSK (DBPSK) or Differential QPSK (DQPSK) method. Both encoding methods produce complex-valued IQ symbols at a rate of 1 Msymbol/sec. Since DBPSK carries 1 bit per symbol, it results in 1 Mbps data throughput, while DQPSK results in 2 Mbps throughput, effectively doubling the capacity of DBPSK. DQPSK uses the spectrum more efficiently, but has reduced immunity to noise and other interference. Following the differential encoding, the 11 chip Barker code spreading is applied, converting the 1 Msymb/sec symbols into 11 Mchip/sec chip sequences. These chips are then modulated on an RF carrier for transmission (Figure 13).

In order to increase the data rate beyond 2 Mbps, 802.11b also specifies complementary code keying (CCK) techniques, which consists of a set of eight-chip code words for the 5.5 Mbps and 11 Mbps data rates. CCK code words have unique mathematical properties that allow them to be correctly distinguished from one another by a receiver even in the presence of substantial noise and multi-path interference. The 5.5 Mbps rate uses CCK to encode four bits per symbol and the 11 Mbps rate encodes eight bits per symbol. Both speeds use QPSK as the modulation technique, which allows for higher data rates (Figure 14).

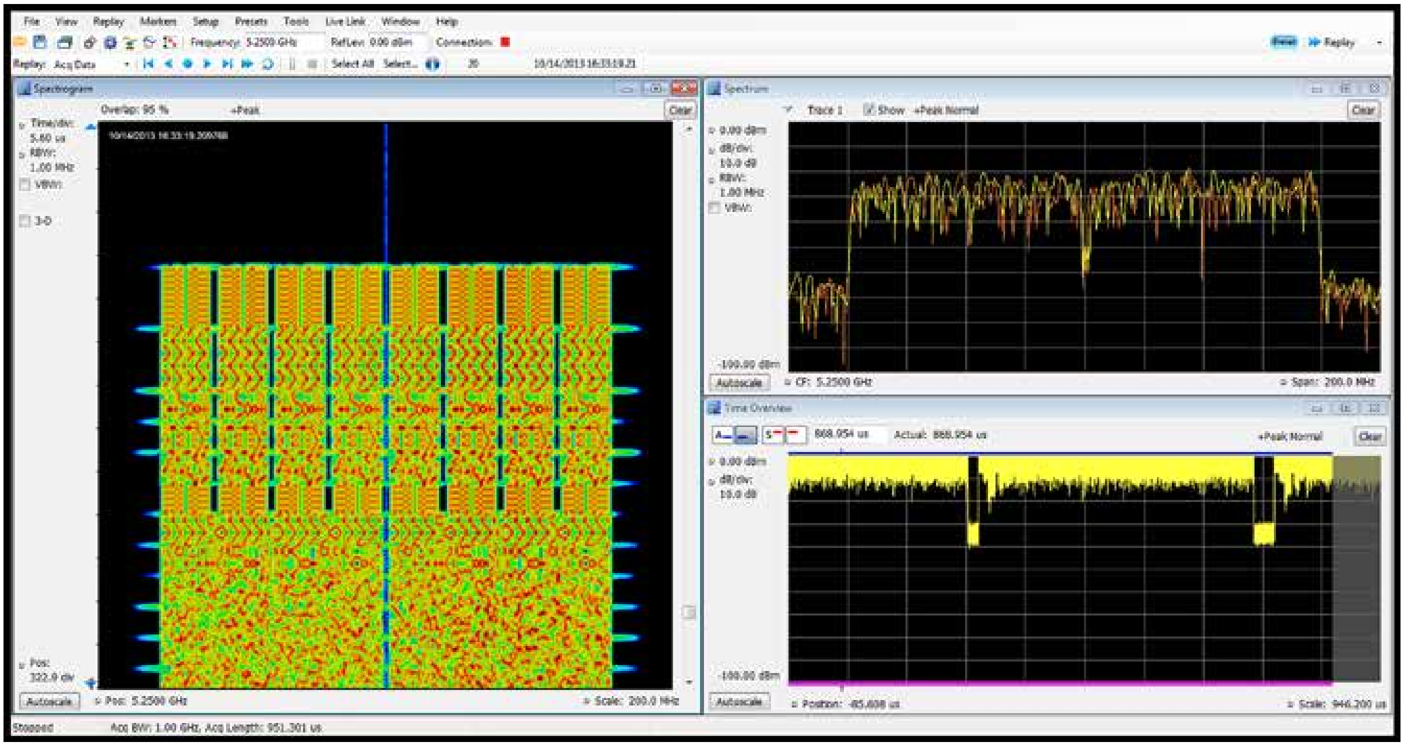


Figure 15. OFDM modulation techniques offer a multitude of choices to allow the system to adapt to the optimum data rate for the current signal conditions.

Orthogonal Frequency Division Multiplexing (OFDM)

Orthogonal Frequency-Division Multiplexing (OFDM) is a method of encoding digital data on multiple sub-carrier frequencies. OFDM enables the transmission of broadband, high data rate information by dividing the data into several interleaved, parallel bit streams modulated on a separate sub-carrier. This modulation technique is a robust solution to counter the adverse effects of multipath propagation and inter-symbol interference (ISI). With the ability to offer several modulation and coding alternatives it can easily adapt to improve the channel quality. The multitude of choices allows the system to adapt the optimum data rate for the current signal conditions. An example of the 802.11ac OFDM signal is shown in Figure 15.

In the past, the spacing between channels was often greater than the symbol rate to avoid overlapping the spectrums. However, in OFDM systems, the sub-carriers overlap, which conserves bandwidth. Keeping the sub-carriers orthogonal to each other controls sub-carrier interference. Orthogonality means there is a mathematical relationship between the sub-carriers.

With OFDM, the high rate data signal is divided equally across the sub-carriers. This reduces the data rate and increases the symbol duration for the sub-carriers, thus reducing the relative amount of dispersion in time caused by multi-path delay spread. Phase noise and non-linear distortion contribute the most to loss of orthogonality, which results in inter-carrier interference (ICI). A guard interval is added to help prevent ICI, as well as ISI. A signal with a slower data rate is more resistant to multi-path fading and interference.

The primary advantage of OFDM over single-carrier schemes is its ability to cope with severe channel conditions (for example frequency-selective fading due to multipath) without complex equalization filters. Channel equalization is simplified because OFDM may be viewed as using many slowly modulated narrowband signals rather than one rapidly modulated wideband signal. The low symbol rate makes the use of a guard interval between symbols affordable, making it possible to eliminate inter symbol interference (ISI) and utilize echoes and time-spreading to achieve a diversity gain, i.e. a signal-to-noise ratio improvement.

Data Modulation and Coding (FEC) Combinations

Forward Error Correction (FEC) or channel coding is a technique used for controlling errors in data transmission over unreliable or noisy communication channels. The central idea is the sender encodes their message in a redundant way by using an error-correcting code (ECC). The redundancy allows the receiver to detect a limited number of errors that may occur anywhere in the message, and often to correct these errors without retransmission. FEC gives the receiver the ability to correct errors without needing a reverse channel to request retransmission of data, but at the cost of a fixed, higher forward channel bandwidth.

In digital communications, a chip is a pulse of a direct-sequence spread spectrum (DSSS) code. The chip rate of a code is the number of pulses per second (chips per second) at which the code is transmitted (or received). The chip rate is larger than the symbol rate, meaning that one symbol is represented by multiple chips.

Modulation and Coding Scheme (MCS): A specification of the high-throughput (HT) physical layer (PHY) parameters that consists of modulation order (e.g.,BPSK, QPSK, 16-QAM, 64-QAM) and forward error correction (FEC) coding rate (e.g.,1/2, 2/3, 3/4, 5/6).

802.11b		
Modulation	Symbol/Chip Ratio	Data Rate (Mbps)
DBPSK	1/11	1
DQPSK	1/5	2
DQPSK	1/2	5.5
BPSK	1/2	5.5
DQPSK	1	11
QPSK	1/2	11
8PSK	1	22
8PSK	1	33

802.11a/g			
RATE	Modulation	FEC Rate	Data Rate (Mbps)
1101 (13)	BPSK	1/2	6
1111 (15)	BPSK	3/4	9
0101 (5)	QPSK	1/2	12
0111 (7)	QPSK	3/4	18
1001 (9)	16QAM	1/2	24
1011 (11)	16QAM	3/4	36
0001 (1)	64QAM	2/3	48
0011 (3)	64QAM	3/4	54

Modulation Coding Scheme and Forward Error Correction Rate for 802.11n

MCS	Modulation	FEC Rate	Data Rate	
			20 MHz (Mbps)	40 MHz (Mbps)
0	BPSK	1/2	7.2	15.0
1	QPSK	1/2	14.4	30.0
2	QPSK	3/4	21.7	45.0
3	16QAM	1/2	28.9	60.0
4	16QAM	3/4	43.3	90.0
5	64QAM	2/3	57.8	120.0
6	64QAM	3/4	65.0	135.0
7	64QAM	5/6	72.2	150.0

Modulation Coding Scheme and Forward Error Correction Rate for 802.11ac

MCS	Modulation	FEC Rate	Data Rate			
			20 MHz (Mbps)	40 MHz (Mbps)	80 MHz (Mbps)	160 MHz (Mbps)
0	BPSK	1/2	7.2	15.0	32.5	65.0
1	QPSK	1/2	14.4	30.0	65.0	130.0
2	QPSK	3/4	21.7	45.0	97.5	195.0
3	16QAM	1/2	28.9	60.0	130.0	260.0
4	16QAM	3/4	43.3	90.0	195.0	390.0
5	64QAM	2/3	57.8	120.0	260.0	525.0
6	64QAM	3/4	65.0	135.0	292.5	585.0
7	64QAM	5/6	72.2	150.0	325.0	650.0
8	256QAM	3/4	86.7	180.0	390.0	780.0
9	256QAM	5/6	N/A	200.0	433.3	866.7

WLAN Operational Process

To connect to a WLAN network, a device has to be equipped with a wireless network interface controller. The combination of computer and interface controller is called a station (STA). All stations share a single radio frequency communication channel. Transmissions on this channel are received by all stations within range. Each station is constantly tuned in on the radio frequency communication channel to pick up available transmissions.

A Wi-Fi-enabled device can connect to the Internet when within range of a wireless network which is configured to permit this. The coverage of one or more (interconnected) access points can extend from an area as small as a few rooms to as large as many square miles. Coverage in a larger area may require a group of access points with overlapping coverage.

A group of wireless stations (STA) that form an association is called a Basic Service Set or BSS. There are two types of BSS – Ad hoc and Infrastructure. The Ad hoc BSS offers direct communication between STAs, but does not include central control. With the Infrastructure BSS, STAs associate with an Access Point (AP), which may also be connected to a network (Figure 16).

This section provides an overview of the WLAN operational process for establishing communication links and transferring data between 802.11 devices.

Anatomy of a WLAN Device

In the early days of 802.11 dedicated PC cards were commonly inserted into desktop and laptop computers. Today, embedded WLAN modules are designed into all mobile computers and the majority of cellular phones as well. In addition, these embedded modules are becoming available in a wide variety of appliances and non-traditional computing devices. These real-time operating systems provide a simple means of wirelessly enabling any device which has and communicates via a serial port. This allows the design of simple monitoring devices. An example is a portable ECG device monitoring a patient at home. This Wi-Fi-enabled device can communicate via the Internet.

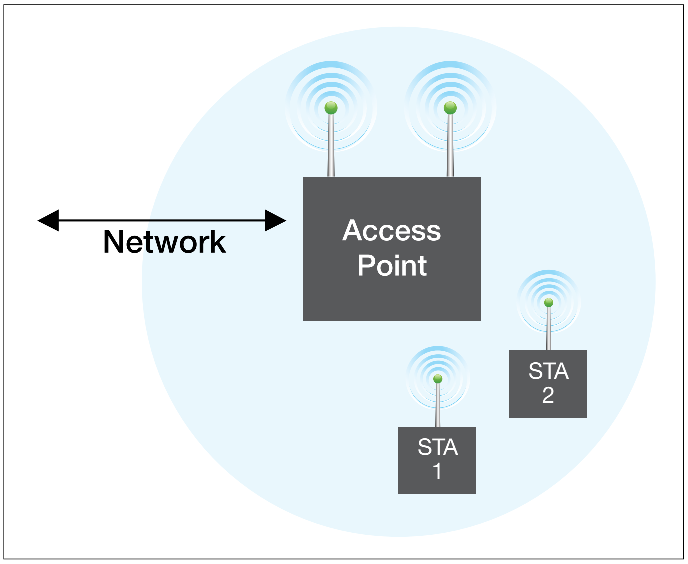


Figure 16. The Basic Service Set (BSS) is a group of wireless stations (STA) that form an association.

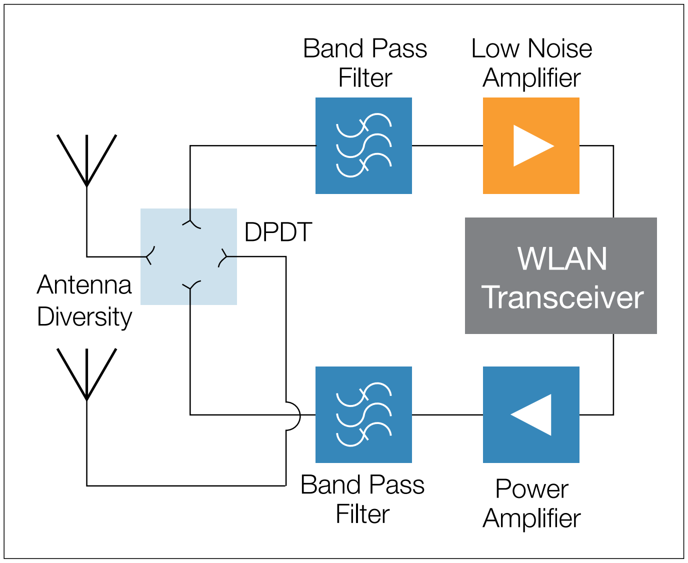


Figure 17. Simple example of a WLAN design.

Figure 17 is a simple block diagram of a WLAN radio system. As with most electronic systems, newer radio designs have higher levels of integration, although performance trade-offs must be made.

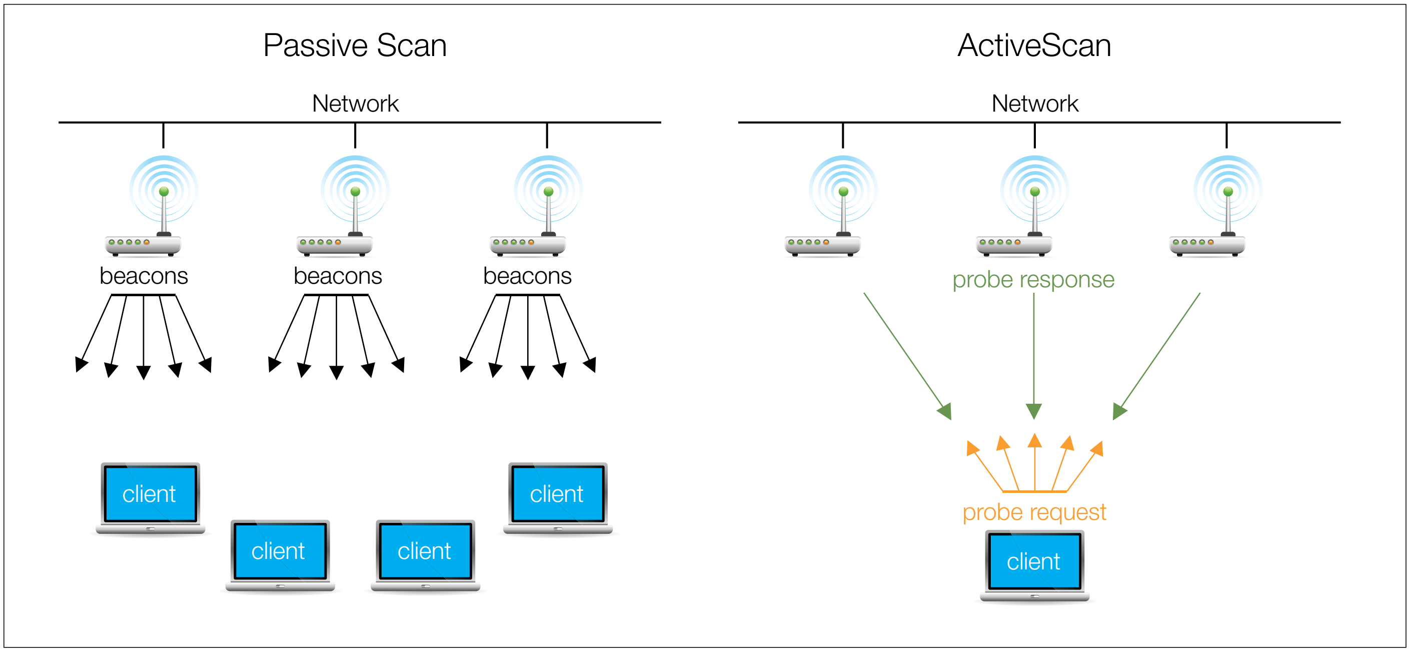


Figure 18. 802.11 devices may establish contact with either passive or active scanning.

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 with other users. In a real-world environment, interference suppression and linearity will directly affect the performance of the radio. A Receive Signal Strength Indication (RSSI) test, made during the short training sequence, determines which path is switched in for a particular burst.

On the transmit side, it is often necessary to include an external power amplifier (PA). Cost, current consumption, and linearity demand careful consideration. Although the analog hardware can be tested in isolation, it needs to be combined with the DSP (Digital Signal Processing) of the Baseband circuit in order to comprise a complete transceiver.

Establishing Contact

When a device is first powered up, the software above the MAC layer stimulates the device to establish contact. The device will use either active or passive scanning. The IEEE specification allows for different implementations, so characteristics may differ between devices.

Passive Scanning uses Beacons and Probe Requests. After selecting a channel, the scanning device listens for Beacons or Probe Requests from other devices. In the case of passive scanning the client just waits to receive a Beacon Frame from the AP. A Beacon is transmitted from an AP and contains information about the AP along with a timing reference. Like other transmissions, they are subject to a clear channel test and so may be delayed. The device searches for a network by just listening for beacons until it finds a suitable network to join.

With Active Scanning the device tries to locate an AP by transmitting Probe Request Frames, and waits for a Probe Response from the AP. Listening for a clear channel, the device which seeks to establish contact sends a Probe Request. The probe request frame can be a directed or a broadcast probe request. The probe response frame from the AP is similar to the beacon frame. Based on the response from the AP, the client makes a decision about connecting to the AP. While active scanning is a faster way to establish contact, it consumes more battery power.

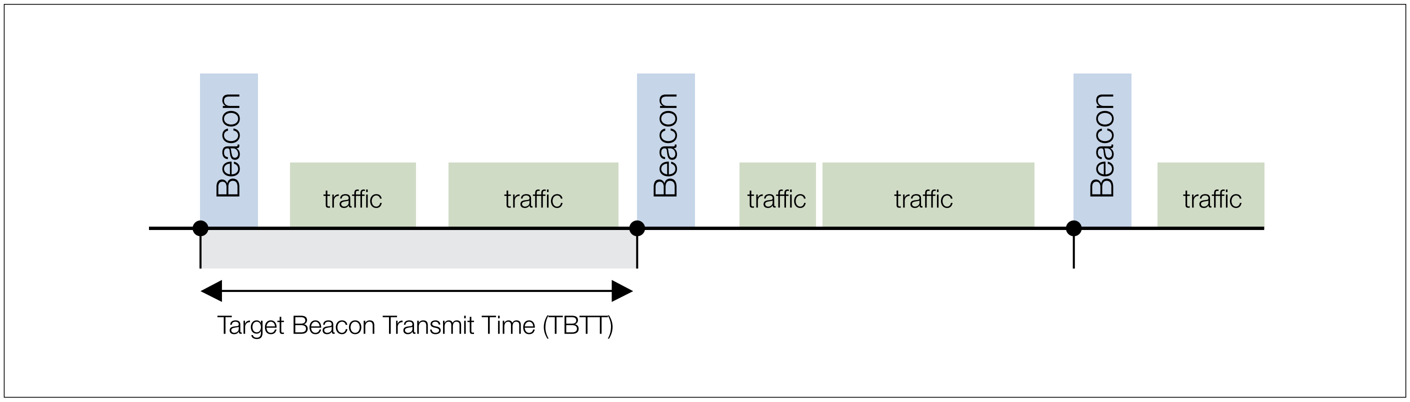


Figure 19. The AP periodically broadcasts a Beacon frame or packet at regular intervals to advertise its capabilities.

Synchronization

The AP periodically broadcasts a Beacon frame (packet) at regular intervals, typically every 100 msec. This is called the Target Beacon Transmit Time or TBTT. The beacon carries regulatory, capability, and BSS management information, including:

- Supported Data Rates
- SSID – Service Set ID (AP's nickname)
- Timestamp (synchronization)

The AP also uses the beacon to advertise its capabilities and this information is used by the passively scanning clients to make a decision to connect to the AP. This is necessary to keep all the clients synchronized with the AP in order for the clients to perform functions like power save.

Authentication

Next, the station needs to be authenticated by the AP in order to join the APs network. With an open network, a device sends an authentication request and the AP sends the result back. For a secure network there is a more formal authentication process. 802.1X authentication involves three parties: the access point, device, and the authentication server which is typically a host running software supporting the required protocols. The access point provides the security to protect the network. The device is not allowed access through the AP to the protected side of the network until the device's identity has been validated and authorized. If the authentication server determines the credentials are valid, the supplicant (client device) is allowed to access resources located on the protected side of the network.

Association

Association is the next step after authentication and it enables data transfer between the device and the AP. The device sends an association request frame to the AP who replies to the client with an association response frame either allowing or disallowing the association. Once the association is successful, the AP issues an Association ID to the client and adds the client to its database of connected clients.

Exchanging Data

Data transfer is allowed only after authentication and association. Attempting to send data to an AP without proper authentication and association causes the AP to respond with a de-authentication frame. Data frames are always acknowledged. If a device sends a data frame to an AP, the AP must send an acknowledgement. If the AP sends a data frame to a device, the device must send an acknowledgement. The AP will forward data frames received from the client to the required destination on the wired network. It will also forward data directed to the client from the wired network. APs can also forward traffic between two clients, but this is not common.

Making Transmitter Measurements

Transmitter impairments can reduce the performance of WLAN systems, or even prevent RF devices from working together. Transmitter tests are significant because some transceiver problems can be found quickly by analyzing transmitted output first. Since the local oscillator(s) (LO) are shared between the transmit and receive side, any problems with the LO which would affect the receiver, will be seen during transmitter testing.

This section highlights the tests that have been specified to ensure a device's compliance and performance for the 802.11 standards.

Transmitter Test Conditions

The IEEE 802.11 standard defines the conditions for transmitter testing, however it does not include any over-the-air control of test mode functions. Testing must be performed via test ports accessible on the WLAN device or module.

When testing a device one wants to be sure that it is not interacting with other WLAN devices. In addition the particular standard being tested (a,b,g,..) needs to be controlled. Device-specific or proprietary software is often needed to control the device through specific test modes. The standard specifies various test modes which control the operational state of the radio and the transmitter parameters. The use of independent test equipment and software to control the device requires that test engineers pay special attention to the triggering and timing of their measurements.

Transmitter Tests

Transmitter Power

The nominal transmit power of a frame is defined as part of the PMD Transmit specifications for the Frequency-Hopping Spread Spectrum (FHSS) PHY (14.7.14.2). Maximum allowable output power is measured in accordance with practices specified by the regional regulatory bodies. Otherwise, the measurement is done as an average power over the entire packet, regardless of signal type.

Transmit Spectrum Mask

The Transmit Spectrum Mask is defined for each variant of the standard. This mask provides the limit under which the signal power is allowed to distribute over the channel. For DSSS PHY, the transmitted spectral products shall be less than –30 dBr (decibel relative to the SINx/x peak) for fc – 22 MHz < f < fc –11 MHz, and fc +11 MHz < f < fc + 22 MHz, –50 dBr for f < fc –22 MHz, and f > fc + 22 MHz, where fc is the channel center frequency. The transmit spectral mask is shown in Figure 7. The measurements shall be made using 100 kHz resolution bandwidth and a 30 kHz video bandwidth. For OFDM PHY, the transmit spectrum mask may also be defined by regulatory restrictions. In the presence of additional regulatory restrictions, the device needs to meet both the regulatory requirements and the mask defined by the IEEE standard, and its emissions need to be no higher at any frequency offset than the minimum of the values specified in the regulatory and default masks. The transmitted spectral density of the transmitted signal shall fall within the spectral mask, as shown in Figure 8. The Spectral Mask can be used to diagnose distortions present in the signal (such as compression), or any leakage into adjacent channels that may compromise the signal quality in the adjacent channels.

Spectral Flatness

Spectral flatness is a measurement of the power variations for the sub-carriers in an OFDM signal. It should be used to ensure that power is spread out evenly over the channel and detect issues with the output filter performance. Spectral flatness is defined as follows in the standard for 802.11n (HT PHY): In a 20 MHz channel and in corresponding 20 MHz transmission in a 40 MHz channel, the average energy of the constellations in each of the subcarriers with indices –16 to –1 and +1 to +16 shall deviate no more than ± 4 dB from their average energy. The average energy of the constellations in each of the subcarriers with indices –28 to –17 and +17 to +28 shall deviate no more than +4/–6 dB from the average energy of subcarriers with indices –16 to –1 and +1 to +16.

In a 40 MHz transmission (excluding MCS 32 format and non-HT duplicate format), the average energy of the constellations in each of the subcarriers with indices –42 to –2 and +2 to +42 shall deviate no more than ± 4 dB from their average energy. The average energy of the constellations in each of the subcarriers with indices –43 to –58 and +43 to +58 shall deviate no more than +4/–6 dB from the average energy of subcarriers with indices –42 to –2 and +2 to +42.

In MCS 32 format and non-HT duplicate format, the average energy of the constellations in each of the subcarriers with indices –42 to –33, –31 to –6, +6 to +31, and +33 to +42 shall deviate no more than ± 4 dB from their average energy. The average energy of the constellations in each of the subcarriers with indices –43 to –58 and +43 to +58 shall deviate no more than +4/–6 dB from the average energy of subcarriers with indices –42 to –33, –31 to –6, +6 to +31, and +33 to +42. The tests for the spectral flatness requirements may be performed with spatial mapping.

Transmit Center Frequency Tolerance

The transmitter center frequency tolerance shall be ± 20 ppm maximum for the 5 GHz band and ± 25 ppm maximum for the 2.4 GHz band. The different transmit chain center frequencies (LO) and each transmit chain symbol clock frequency shall all be derived from the same reference oscillator.

Transmit Center Frequency Leakage

Certain transmitter implementations may cause leakage of the center frequency component. Such carrier leakage can occur in some transmitter because of DC offset. This issue is seen on the receiver side as energy in the transmit center frequency. Often OFDM-based receiver systems utilize some way to remove the carrier leakage. IEEE mandates that the transmitter center frequency leakage does not exceed –15 dB relative to overall transmitted power or equivalently, +2 dB relative to the average energy of the rest of the subcarriers) for transmission in a 20 MHz channel width. For transmissions in a 40 MHz channel width, the center frequency leakage shall not exceed –20 dB relative to overall transmitted power, or, equivalently, 0 dB relative to the average energy of the rest of the subcarriers. For upper or lower 20 MHz transmissions in a 40 MHz channel, the center frequency leakage (center of a 40 MHz channel) shall not exceed –17 dB relative to overall transmitted power, or, equivalently, 0 dB relative to the average energy of the rest of the subcarriers. For 802.11ac, all formats and bandwidths except non-contiguous 80+80 MHz where the RF LO falls outside both frequency segments shall meet the following requirements:

- When the RF LO is in the center of the transmitted bandwidth, the power measured at the center of transmission bandwidth using a resolution of 312.5 kHz shall not exceed the average power per-subcarrier of the transmitted burst.
- When the RF LO is not at the center of the transmitted bandwidth, the power measured at the location of the RF LO using a resolution of 312.5 kHz shall not exceed the maximum of -32 dB relative to the total transmit power and -20 dBm.

For an 80+80 MHz transmission where the RF LO falls outside both frequency segments, the RF LO shall follow the spectral mask requirements as defined in the standard. The transmit center frequency leakage is specified per antenna.

Transmitter Constellation Error

Transmit Modulation tests include a verification of the Constellation Diagram and a measurement of the Error Vector Magnitude (EVM). These tests provide critical information on the types of distortion in the entire transmit chain that can affect the signal quality.

The Transmit Constellation Error, also known as EVM RMS is the RMS averaged deviation of the actual constellation points from the ideal error-free locations in the constellation diagram (in % RMS or dB). The RMS error is averaged over subcarriers, OFDM frames, and packets. This measurement allows for the detection of imperfections such as compression, dynamic range, I/Q errors, interference and phase noise. IEEE mandates that the test is performed over at least 20 frames (Nf), each frame being at least 16 OFDM symbols long. Random data is to be used for the symbols.

Transmitter Modulation Accuracy (EVM) Test

This test is essentially a repeat of the Transmitter Constellation Error.

Symbol Clock Frequency Tolerance

The symbol clock frequency tolerance shall be ± 20 ppm maximum for 5 GHz bands and ± 25 ppm for 2.4 GHz bands. The transmit center frequency and the symbol clock frequency for all transmit antennas shall be derived from the same reference oscillator.

802.11 and 802.11b Transmitter Requirements

802.11 and 802.11b Transmit Requirements[1]			
DSSS (802.11-2012, Section 16)			
Spurious Display	16.4.6.6 17.4.6.9	Tx & Rx Inband & OOB Spurious EM	No specification ("...shall conform to in-band and out-of-band spurious emissions as set by regulatory bodies.")
Channel Power Display	16.4.7.2 17.4.7.2	Transmit Power Levels	No specification ("...measured in accordance with practices specified by the appropriate regulatory bodies.")
Spectral Emission Mask (SEM)	16.4.7.5 17.4.7.4	Transmit Spectrum Mask	dBr Spectrum Mask
Summary Display Carrier Frequency Error	16.4.7.6 17.4.7.5	Transmit Center Frequency Tolerance	+/-25 ppm
Summary Display Symbol Clock Error	16.4.7.7 17.4.7.6	Chip Clock Frequency Tolerance	+/-25 ppm
Power On / Power Off	16.4.7.8 17.4.7.7	Transmit Power On / Power Off	10%- 90% in < = 2 usec
Summary Display IQ Origin Offset	16.4.7.9 17.4.7.8	RF Carrier Suppression	-15 dB w.r.t. sin(x)/x shape
Summary Display - EVM	16.4.7.10 17.4.7.9	Transmit Modulation Accuracy	Peak EVM (1000 samples) <0.35

[1] Defined by the IEEE 802.11- 2012 revision of the standard.

802.11a Transmitter Requirements

<table>
<tr><th colspan="6">802.11a Transmit Requirements[1]</th></tr>
<tr><td colspan="6">OFDM ("a") (802.11-2012, Section 18)</td></tr>
<tr><td>Spurious Display</td><td>18.3.8.5</td><td>Tx & Rx Inband & OOB Spurious EM</td><td colspan="3">No specification ("...shall conform to in-band and out-of-band spurious emissions as set by regulatory bodies.")</td></tr>
<tr><td>Channel Power Display</td><td>18.3.9.2</td><td>Transmit Power Levels</td><td colspan="3">No specification ("...measured in accordance with practices specified by the appropriate regulatory bodies.")</td></tr>
<tr><td>Spectral Emission Mask (SEM)</td><td>18.3.9.3</td><td>Transmit Spectrum Mask</td><td colspan="3">dBr Spectrum Mask</td></tr>
<tr><td>Spurious Display</td><td>18.3.9.4</td><td>Transmit Spurious</td><td colspan="3">No specification ("...shall conform to regulations.")</td></tr>
<tr><td>Summary Display Carrier Frequency Error</td><td>18.3.9.5</td><td>Transmit Center Frequency Tolerance</td><td colspan="3">+/-20 ppm (20 MHz and 10 MHz), +/-10 (5MHz)</td></tr>
<tr><td>Summary Display Symbol Clock Error</td><td>18.3.9.6</td><td>Symbol Clock Frequency Tolerance</td><td colspan="3">+/-20 ppm (20 MHz and 10 MHz), +/-10 (5MHz)</td></tr>
<tr><td>Summary Display IQ Origin Offset</td><td>18.3.9.7.2</td><td>Transmitter Center Frequency Leakage</td><td colspan="3">-15 dBc or +2 dB w.r.t. average subcarrier power</td></tr>
<tr><td>Spectral Flatness</td><td>18.3.9.7.3</td><td>Transmitter Spectral Flatness</td><td colspan="3">+/- 4 dB (SC=-16...16), +4/-6 dB (other)</td></tr>
<tr><td rowspan="10">Summary Display - EVM</td><td rowspan="10">18.3.9.7.4</td><td rowspan="10">Transmit Constellation Error</td><td colspan="3"><b>Allowed Relative Constellation Error Versus Data Rate</b></td></tr>
<tr><td><b>Modulation</b></td><td>Coding Rate (R)</td><td>Relative Constellation Error (dB)</td></tr>
<tr><td>BPSK</td><td>1/2</td><td>-5</td></tr>
<tr><td>BPSK</td><td>3/4</td><td>-8</td></tr>
<tr><td>QPSK</td><td>1/2</td><td>-10</td></tr>
<tr><td>QPSK</td><td>3/4</td><td>-13</td></tr>
<tr><td>16-QAM</td><td>1/2</td><td>-16</td></tr>
<tr><td>16-QAM</td><td>3/4</td><td>-19</td></tr>
<tr><td>64-QAM</td><td>2/3</td><td>-22</td></tr>
<tr><td>64-QAM</td><td>3/4</td><td>-25</td></tr>
</table>

[1] Defined by the IEEE 802.11- 2012 revision of the standard.

802.11g and 802.11n Transmitter Requirements

<table>
<tr><th colspan="6">802.11g and 802.11n Transmit Requirements[1]</th></tr>
<tr><td colspan="6">ERP (802.11-2012, Section 19)</td></tr>
<tr><td>Spurious Display</td><td>19.4.4</td><td>Tx & Rx Inband & OOB Spurious EM</td><td colspan="3">No specification ("...shall conform to in-band and out-of-band spurious emissions as set by regulatory bodies.")</td></tr>
<tr><td>Channel Power Display</td><td>19.4.8.2</td><td>Transmit Power Levels</td><td colspan="3">No specification ("...measured in accordance with practices specified by the appropriate regulatory bodies.")</td></tr>
<tr><td>Summary Display Carrier Frequency Error</td><td>19.4.8.3</td><td>Transmit Center Frequency Tolerance</td><td colspan="3">+/-25 ppm</td></tr>
<tr><td>Summary Display Symbol Clock Error</td><td>19.4.8.4</td><td>Symbol Clock Frequency Tolerance</td><td colspan="3">+/-25 ppm</td></tr>
<tr><td>Spectral Emission Mask (SEM)</td><td>19.5.5</td><td>Transmit Spectrum Mask
ERP-OFDM
ERP-DSSS</td><td colspan="3">
follow 18.3.9.3
follow 17.4.7.4</td></tr>
<tr><td colspan="6"></td></tr>
<tr><td colspan="6">OFDM/HT ("n") (802.11-2012, Section 20)</td></tr>
<tr><td>Spectral Emission Mask (SEM)</td><td>17.4.7.4</td><td>Transmit Spectrum Mask</td><td colspan="3">dBr Spectrum Mask</td></tr>
<tr><td>Spectral Flatness</td><td>20.3.20.2</td><td>Spectral Flatness</td><td colspan="3">+/-4 dB, +4/-6 dB</td></tr>
<tr><td>Channel Power Display</td><td>20.3.20.3</td><td>Transmit Power</td><td colspan="3">No specification ("...measured in accordance with practices specified by the appropriate regulatory bodies.")</td></tr>
<tr><td>Summary Display Carrier Frequency Error</td><td>20.3.20.4</td><td>Transmit Center Frequency Tolerance</td><td colspan="3">+/-20 ppm (5GHz band), +/-25 ppm (2.4 GHz band)</td></tr>
<tr><td>Summary Display Symbol Clock Error</td><td>20.3.20.6</td><td>Symbol Clock Frequency Tolerance</td><td colspan="3">+/-20 ppm (5GHz band), +/-25 ppm (2.4 GHz band)</td></tr>
<tr><td>Summary Display IQ Origin Offset</td><td>20.3.20.7.2</td><td>Transmitter Center Frequency Leakage</td><td colspan="3">20 MHz: follow 18.3.9.7.2
40 MHz: -20 dBc or 0 dB w.r.t average subcarrier power</td></tr>
<tr><td rowspan="10">Summary Display - EVM</td><td rowspan="10">20.3.20.7.3</td><td rowspan="10">Transmit Constellation Error</td><th colspan="3">Allowed Relative Constellation Error Versus Data Rate</th></tr>
<tr><th>Modulation</th><th>Coding Rate (R)</th><th>Relative Constellation Error (dB)</th></tr>
<tr><td>BPSK</td><td>1/2</td><td>-5</td></tr>
<tr><td>QPSK</td><td>1/2</td><td>-10</td></tr>
<tr><td>QPSK</td><td>3/4</td><td>-13</td></tr>
<tr><td>16-QAM</td><td>1/2</td><td>-16</td></tr>
<tr><td>16-QAM</td><td>3/4</td><td>-19</td></tr>
<tr><td>64-QAM</td><td>2/3</td><td>-22</td></tr>
<tr><td>64-QAM</td><td>3/4</td><td>-25</td></tr>
<tr><td>64-QAM</td><td>5/6</td><td>-27</td></tr>
</table>

[1] Defined by the IEEE 802.11- 2012 revision of the standard.

802.11ac Transmitter Requirements

<table>
<tr><th colspan="6">802.11ac Transmit Requirements[1]</th></tr>
<tr><td colspan="6">OFDM/VHT ("ac") (802.11-2012, Section 22)</td></tr>
<tr><td>Spectral Emission Mask (SEM)</td><td>22.3.18.15</td><td>Transmit Spectrum Mask</td><td colspan="3">dBr Spectrum Mask</td></tr>
<tr><td>Spectral Flatness</td><td>22.3.18.2</td><td>Spectral Flatness</td><td colspan="3">+/-4 dB, +4/-6 dB (various BWs, 20-160 MHz)</td></tr>
<tr><td>Summary Display Carrier Frequency Error</td><td>22.3.18.3</td><td>Transmit Center Frequency Tolerance</td><td colspan="3">+/-20 ppm</td></tr>
<tr><td>Summary Display Symbol Clock Error</td><td></td><td>Symbol Clock Frequency Tolerance</td><td colspan="3">+/-20 ppm</td></tr>
<tr><td>Summary Display IQ Origin Offset</td><td>22.3.18.4.2</td><td>Transmitter Center Frequency Leakage</td><td colspan="3">For 20, 40, 80 and 160 MHz, and CF is in the center:
< average power per-subcarrier
For 20,40, 80 and 160 MHz and CF not in center:
<max (total power - 32dB, -20 dBm
For 80+80 MHz:
meet spectral mask</td></tr>
<tr><td rowspan="12">Summary Display - EVM</td><td rowspan="12">22.3.18.4.3</td><td rowspan="12">Transmit Constellation Error</td><th colspan="3">Allowed Relative Constellation Error Versus Data Rate</th></tr>
<tr><th>Modulation</th><th>Coding Rate (R)</th><th>Relative Constellation Error (dB)</th></tr>
<tr><td>BPSK</td><td>1/2</td><td>-5</td></tr>
<tr><td>QPSK</td><td>1/2</td><td>-10</td></tr>
<tr><td>QPSK</td><td>3/4</td><td>-13</td></tr>
<tr><td>16-QAM</td><td>1/2</td><td>-16</td></tr>
<tr><td>16-QAM</td><td>3/4</td><td>-19</td></tr>
<tr><td>64-QAM</td><td>2/3</td><td>-22</td></tr>
<tr><td>64-QAM</td><td>3/4</td><td>-25</td></tr>
<tr><td>64-QAM</td><td>5/6</td><td>-27</td></tr>
<tr><td>256-QAM</td><td>3/4</td><td>-30</td></tr>
<tr><td>256-QAM</td><td>5/6</td><td>-32</td></tr>
</table>

[1] Defined by the IEEE 802.11- 2012 revision of the standard.

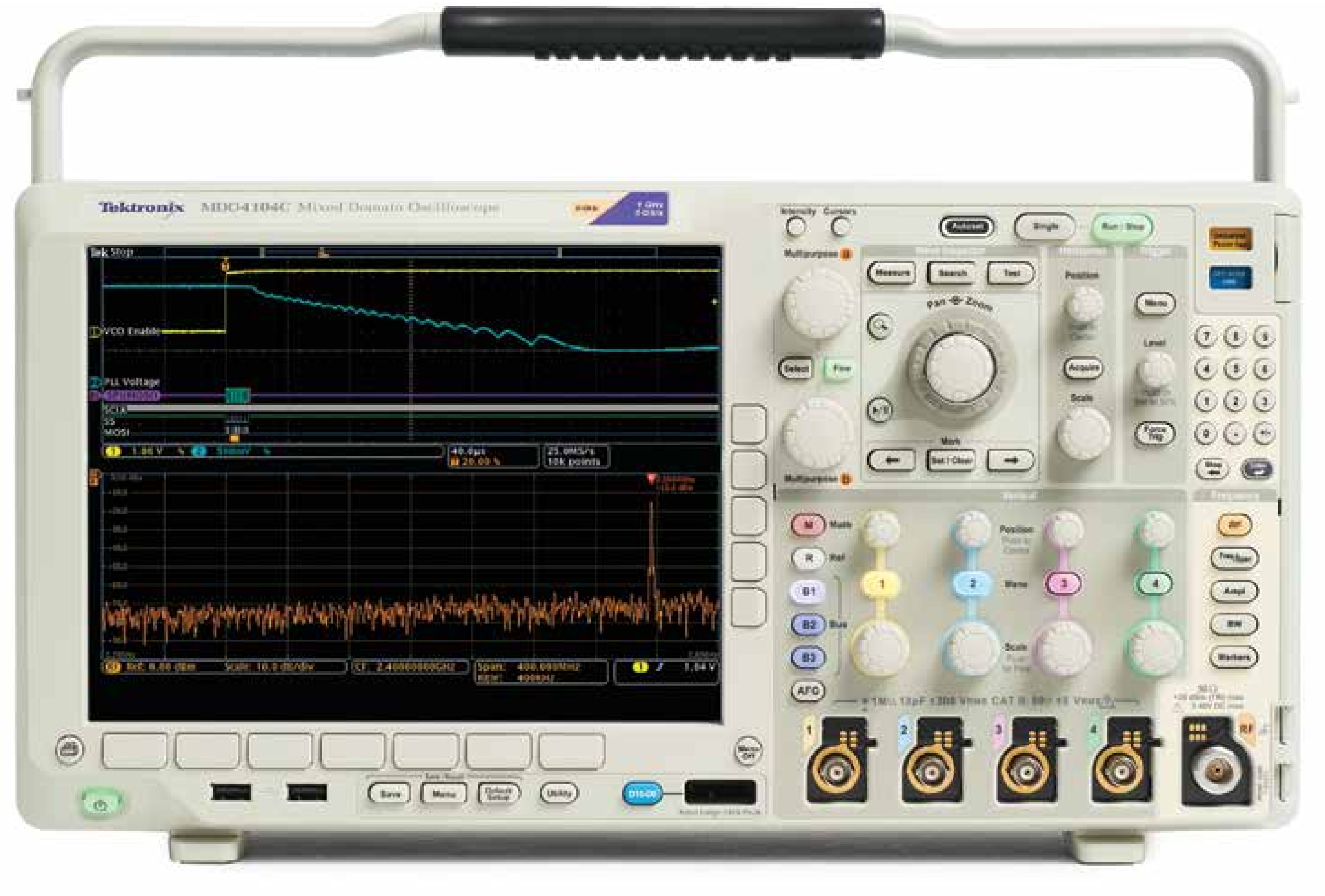


Figure 20. The MDO4000 Series allows you to capture time-correlated analog, digital and RF signals for a complete system view of your device.

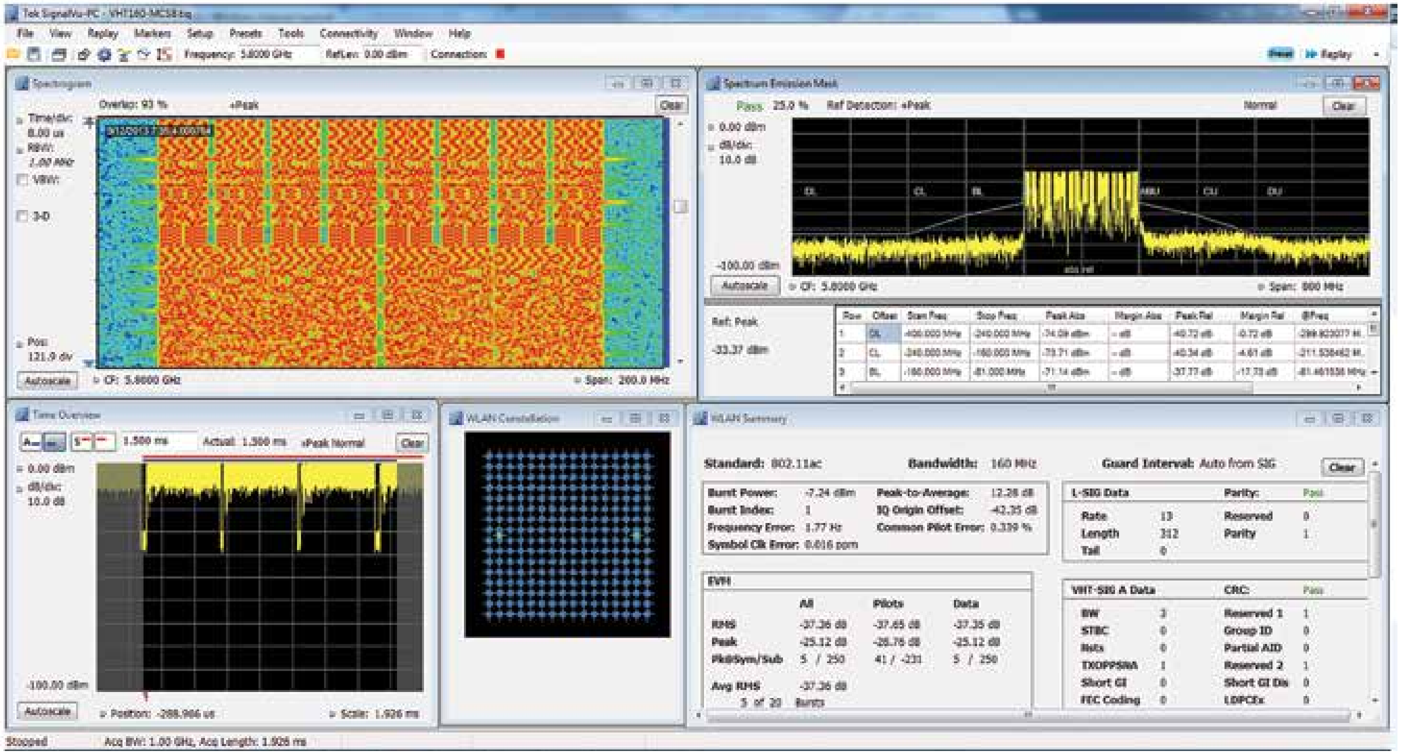
Testing Solutions

In order to meet your test needs for both today and tomorrow's 802.11 specifications, Tektronix offers a suite of tools to meet your particular needs.

With RSA5000 Real-Time Spectrum Analyzers, you can quickly detect, capture and analyze RF signals such as 802.11ac signals. Tektronix invented Real-Time Spectrum Analysis over two decades ago with this in mind. No other spectrum analyzer family provides more confidence in testing wireless signals. You get wideband signal search with highest probability of detection.

The RSA306 USB Spectrum Analyzer takes many of the capabilities of the larger benchtop RSA5000, but puts them into a much smaller form factor. About the size of the paperback book, the form factor of the RSA306 breaks the mold for use cases of a spectrum analyzer. The RSA306 can be used for quick checks of WLAN device functionality and pre-compliance for both EMI and WLAN standards. The RSA306 takes advantage of SignalVu-PC software, which is the same user interface and programmatic interface as the larger spectrum analyzer.

Further information on EMI Pre Compliance testing is available in the application note "Low Cost EMI Pre-compliance Testing using a Spectrum Analyzer", 37A-60141-0.



Ref: Peak

-33.37 dBm

Row	Offset	Start Freq	Stop Freq	Peak Abs	Margin Abs	Peak Rel	Margin Rel	@Freq
1	DL	-400.000 MHz	-240.000 MHz	-74.09 dBm	-- dB	-40.72 dB	-0.72 dB	-299.803077 M..
2	CL	-240.000 MHz	-160.000 MHz	-73.71 dBm	-- dB	-40.34 dB	-4.61 dB	-211.538462 M..
3	BL	-160.000 MHz	-81.000 MHz	-71.14 dBm	-- dB	-37.77 dB	-17.73 dB	-81.461538 MHz

Standard: 802.11ac **Bandwidth:** 160 MHz **Guard Interval:** Auto from SIG

Burst Power:	-7.24 dBm	**Peak-to-Average:**	12.28 dB
Burst Index:	1	**IQ Origin Offset:**	-42.35 dB
Frequency Error:	1.77 Hz	**Common Pilot Error:**	0.339 %
Symbol Clk Error:	0.016 ppm		

EVM

	All	Pilots	Data
RMS	-37.36 dB	-37.65 dB	-37.35 dB
Peak	-25.12 dB	-28.76 dB	-25.12 dB
Pk@Sym/Sub	5 / 250	41 / -231	5 / 250
Avg RMS	-37.36 dB		
5 of 20	Bursts		

L-SIG Data		Parity:	Pass
Rate	13	Reserved	0
Length	312	Parity	1
Tail	0		

VHT-SIG A Data		CRC:	Pass
BW	3	Reserved 1	1
STBC	0	Group ID	0
Nsts	0	Partial AID	0
TXOPPSNA	1	Reserved 2	1
Short GI	0	Short GI Dis	0
FEC Coding	0	LDPCEx	0

Figure 21. SignalVu-PC gives you all the measurements for 802.11ac in one acquisition.

With the MDO4000 Series, the world's first oscilloscope with a built in spectrum analyzer, and capture time-correlated analog, digital and RF signals for a complete system view of your device. You see both the time and frequency domain in a single glance and view the RF spectrum at any point in time to see how it changes with time or device state, to solve the most complicated design issues, quickly and efficiently.

When both the spectrum analyzer and any analog or digital channels are on, the oscilloscope display is split into two views. The upper half of the display is a traditional oscilloscope view of the Time Domain. The lower half of the display is a Frequency Domain view of the spectrum analyzer input.

Note that the Frequency Domain view is not simply an FFT of the analog or digital channels in the instrument, but is the spectrum acquired from the spectrum analyzer input.

Another key difference is that with traditional oscilloscope FFTs, you typically get either the desired view of the FFT display, or the desired view of your other time domain signals of interest, but never both at the same time. With the MDO4000 Series, the spectrum analyzer has its own acquisition system that is independent, but time-correlated to the analog and digital channel acquisition systems. This allows each domain to be configured optimally, providing a complete time-correlated system view of all analog, digital, and RF signals of interest.

And now, with a live link the between MDO4000 and SignalVu-PC, you can analyze the RF signal phase and amplitude in time and frequency as well as demodulate it. Plus, qualify the RF signal quality as well as extract the symbol information. There are also dedicated options to analyze Wi-Fi signals and in particular the wide bandwidth IEEE 802.11ac signals. And because the MDO4000 Series is able to acquire 1 GHz in one shot, all spectral, time-domain and modulation measurements can be done simultaneously. Other narrower bandwidth signal analyzers need to sweep to capture the Spectral Emission Mask for example, as more than 160 MHz of bandwidth is required for this measurement.

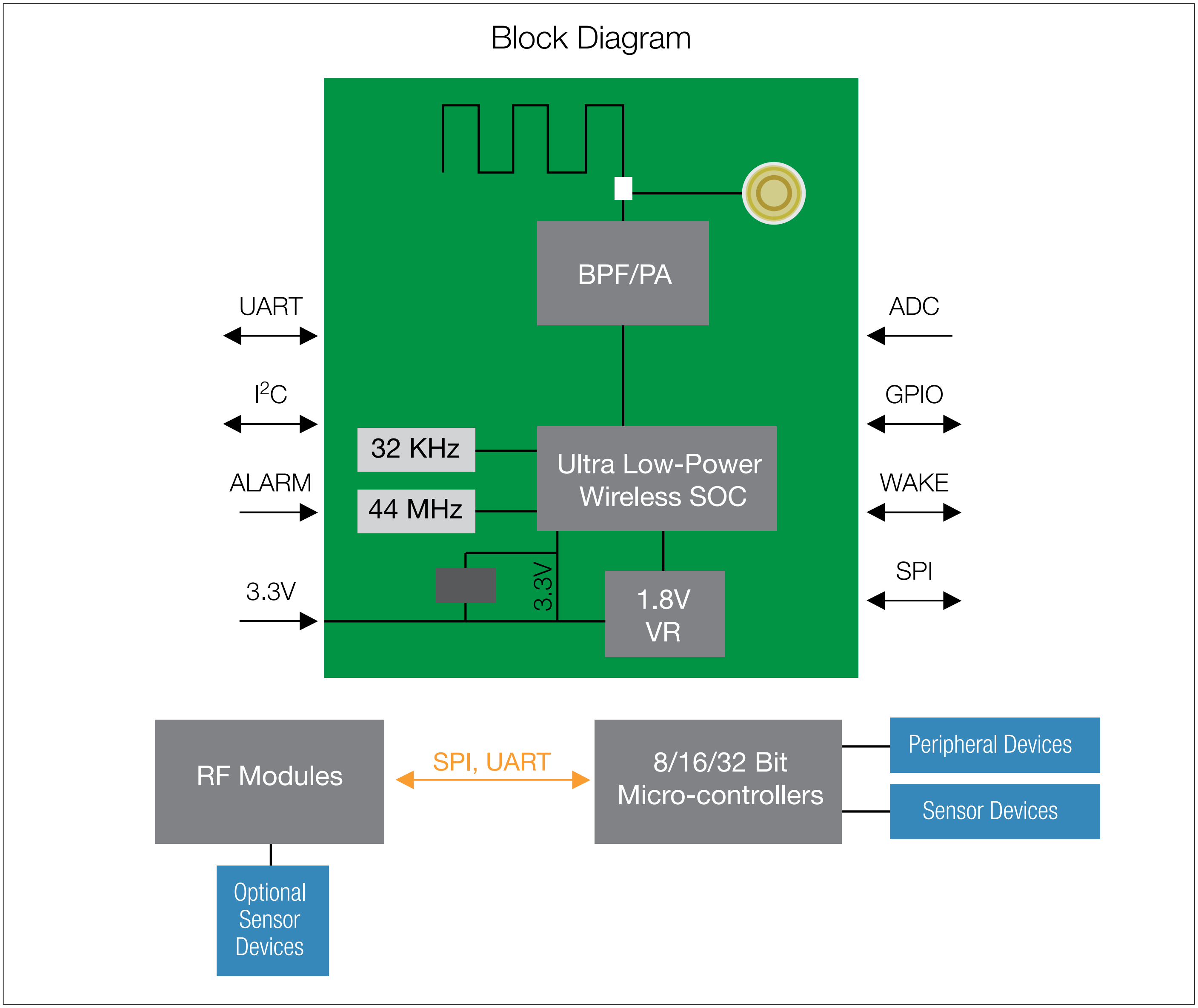


Figure 22. High level block diagram of an RF module and its usage.

Most RF modules used in embedded applications are controlled by a microcontroller via a serial data bus type of interface. Spectrum analyzers cannot help with the debug of the interface between the RF module and the microcontroller; a new type of test equipment is needed, a tool that can visualize the control signals going on the SPI or UART buses and at the same time provide the effects on the RF radio transmission. Only the MDO4000 Series, coupled with SignalVu-PC, provides this system level debug functionality as one affordable tool.

The MDO4000 is the only instrument that allows you to see the controlling signals going to the RF module and the RF output as one instrument.

For more information, please check our website:
www.tektronix.com/mdo4000

Contact Tektronix:

ASEAN / Australasia	(65) 6356 3900
Austria*	00800 2255 4835
Balkans, Israel, South Africa and other ISE Countries	+41 52 675 3777
Belgium*	00800 2255 4835
Brazil	+55 (11) 3759 7627
Canada	1 (800) 833-9200
Central East Europe and the Baltics	+41 52 675 3777
Central Europe & Greece	+41 52 675 3777
Denmark	+45 80 88 1401
Finland	+41 52 675 3777
France*	00800 2255 4835
Germany*	00800 2255 4835
Hong Kong	400-820-5835
India	+91-80-30792600
Italy*	00800 2255 4835
Japan	0120-441-046
Luxembourg	+41 52 675 3777
Macau	400-820-5835
Mongolia	400-820-5835
Mexico, Central/South America & Caribbean	52 (55) 56 04 50 90
Middle East, Asia and North Africa	+41 52 675 3777
The Netherlands*	00800 2255 4835
Norway	800 16098
People's Republic of China	400-820-5835
Poland	+41 52 675 3777
Portugal	80 08 12370
Puerto Rico	1 (800) 833-9200
Republic of Korea	+822-6917-5000
Russia	+7 (495) 7484900
Singapore	+65 6356-3900
South Africa	+27 11 206 8360
Spain*	00800 2255 4835
Sweden*	00800 2255 4835
Switzerland*	00800 2255 4835
Taiwan	886-2-2656-6688
United Kingdom & Ireland*	00800 2255 4835
USA	1 (800) 833-9200

*** If the European phone number above is not accessible, please call +41 52 675 3777**

Contact List Updated March 2013

For Further Information
Tektronix maintains a comprehensive, constantly expanding collection of application notes, technical briefs and other resources to help engineers working on the cutting edge of technology. Please visit **www.tektronix.com**

11/16 SMD/WWW 37W-29447-2