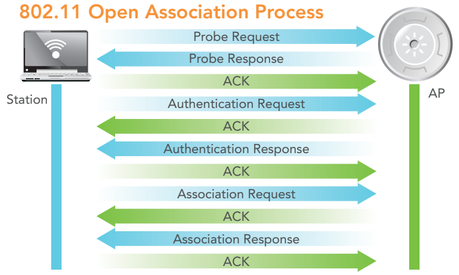
Wi-Fi™ REFERENCE SERIES

XIRRUS®

802.11a/b/g DEMYSTIFIED

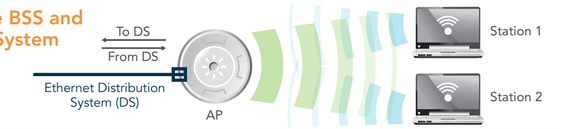
802.11 ACCESS POINT & CLIENT INTERACTION

802.11 Open Association Process

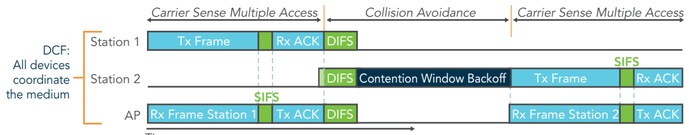


BSS: **B**asic **S**ervice **S**et is a group of stations communicating through an Access Point (AP)
Probe Request: Packet requesting Information about available APs in range
Probe Response: Packet from APs responding to a Probe Request w/BSS information
ACK: Packet sent to acknowledge a received packet

Infrastructure BSS and Distribution System



Wireless Medium Access via Distributed Coordination



SIFS: **S**hort **I**nterframe **S**pace
DIFS: **D**CF **I**nterframe **S**pace
DCF: **D**istributed **C**oordination **F**unction
CSMA/CA: **C**arrier **S**ense **M**ultiple **A**ccess/**C**ollision **A**voidance

DATA RATE/MODULATION

Spreading Method	DSSS		CCK		OFDM								
Modulation	DBPSK	DQPSK	DQPSK		BPSK		QPSK		16-QAM		64-QAM		
Data Rate (Mbps)	1	2	5.5	11	6	9	12	18	24	36	48	54	
802.11a					●	●	●	●	●	●	●	●	5GHz
802.11b	●	●	●	●									2.4GHz
802.11g	●	●	●	●	●	●	●	●	●	●	●	●	

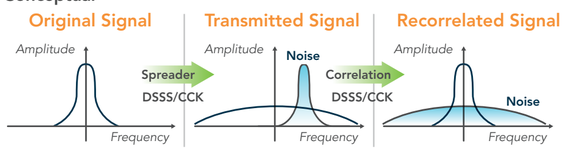
To maintain 802.11 operation in the presence of both 11b and 11g clients, Request-to-Send/ Clear-to-Send (RTS/CTS) frames are sent by 11g devices at CCK rates prior to sending OFDM data.

DSSS: **D**irect **S**equence **S**pread **S**pectrum (Barker Code)
CCK: **C**omplementary **C**ode **K**eying
OFDM: **O**rthogonal **F**requency **D**ivision **M**ultiplexing
DBPSK: **D**ifferential **B**inary **P**hase **S**hift **K**eying
DQPSK: **D**ifferential **Q**uadrature **P**hase **S**hift **K**eying
BPSK: **B**inary **P**hase **S**hift **K**eying
QPSK: **Q**uadrature **P**hase **S**hift **K**eying
16-QAM: 16 Point **Q**uadrature **A**mplitude **M**odulation
64-QAM: 64 Point **Q**uadrature **A**mplitude **M**odulation

SPREAD SPECTRUM TECHINQUES

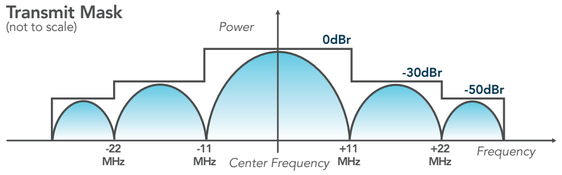
DSSS/CCK Conceptual

Original signal is spread with code words to create a wider band signal, then recovered at the receiver with a correlation process.



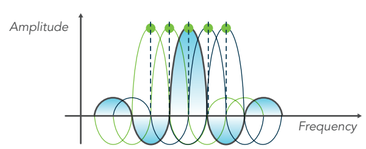
Transmit Mask

(not to scale)



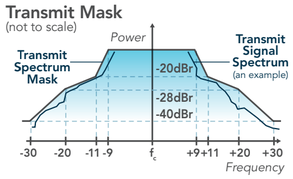
OFDM Conceptual

Transmission data is spread across 52 concurrent subcarriers within the channel. Subcarrier signal peaks occur at neighboring subcarrier nulls, providing orthogonality.

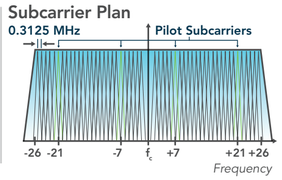


Transmit Mask

(not to scale)



Subcarrier Plan



CHANNEL ALLOCATION

2.4GHz Channel Allocation

Channel	Frequency f_c (MHz)	U.S.	EU	Japan
1	2412	X	X	X
2	2417	X	X	X
3	2422	X	X	X
4	2427	X	X	X
5	2432	X	X	X
6	2437	X	X	X
7	2442	X	X	X
8	2447	X	X	X
9	2452	X	X	X
10	2457	X	X	X
11	2462	X	X	X
12	2467		X	X
13	2472		X	X
14	2484			X

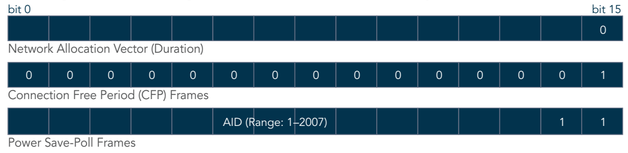
5GHz Channel Allocation

Channel	Frequency f_c (MHz)	U.S.	EU	Japan
184	4920			X
188	4940			X
192	4960			X
196	4980			X
208	5040			X
212	5060			X
216	5080			X
36	5180	X	X	X
40	5200	X	X	X
44	5220	X	X	X
48	5240	X	X	X
52	5260	X	X	X
56	5280	X	X	X
60	5300	X	X	X
64	5320	X	X	X
100	5500	X	X	
104	5520	X	X	
108	5540	X	X	
112	5560	X	X	
116	5580	X	X	
120	5600	X	X	
124	5620	X	X	
128	5640	X	X	
132	5660	X	X	
136	5680	X	X	
140	5700	X	X	
149	5745	X		
153	5765	X		
157	5785	X		
161	5805	X		

802.11 FRAME FORMAT

Duration/ID Field

Depending on bits 14-15 (most significant) this field is defined one of three ways:



Address 1 Field

Used by the receiver.

Address 2 Field

Used by the transmitter.

Address 3 Field

Used by the receiver for filtering.

Sequence Number (Seq No) Field

Address 4 Field

Additional addressing used to traverse the Distribution System.

Frame Body Field

This is also known as the data body or packet payload. Higher level protocols and/or user application data reside in this field (length can be 0–2312 bytes).

Frame Check Sequence (FCS) Field

The FCS is often referred to as the cyclic redundancy check (CRC). It allows stations and APs to check the integrity of received frames.

QoS: **Q**uality of **S**ervice
IBSS: **I**ndependent **B**asic **S**ervice **S**et
802.11h: Defines dynamic frequency selection (DFS) for spectrum management and transmit power control (TPC) for power management in the 5GHz band.

Protocol Field = 00

Type & Subtype Field

00 = Management
- 0000–Association Request
- 0001–Association Response
- 0010–Reassociation Request
- 0011–Reassociation Response
- 0100–Probe Request
- 0101–Probe Response
- 1000–Beacon
- 1001–Announcement Traffic Indication Message (ATIM)
- 1010–Disassociation
- 1011–Authentication
- 1100–Deauthentication
- 1101–Action (used for 802.11h & QoS)

01 = Control
- 1000–Block Acknowledgement Request (used for QoS)
- 1001–Block Acknowledgement (used for QoS)
- 1010–Power Save (PS) Poll
- 1011–Request to Send (RTS)
- 1100–Clear to Send (CTS)
- 1101–Acknowledgment (ACK)
- 1110–Contention Free (CF) End
- 1111–CF-end + CF-ACK

10 = Data
- 0000–Data
- 0001–Data + CF-ACK
- 0010–Data + CF-Poll
- 0011–Data + CF-ACK + CF-Poll
- 0100–Null Data
- 0101–CF-ACK
- 0110–CF-Poll*
- 0111–CF-ACK + CF-Poll*
- 1000–QoS Data
- 1001–QoS Data + CF-ACK
- 1010–QoS Data + CF-Poll
- 1011–QoS Data + CF-ACK + CF-Poll
- 1100–QoS Null*
- 1110–QoS CF-Poll*
- 1111–QoS CF-ACK + CF-Poll*

11 = Reserved

* No data transmitted.

To DS & From DS Fields

	To DS = 0	To DS = 1
From DS = 0	All Management and Control frames. Data frames within IBSS (never Infrastructure data frames).	Data frames transmitted from a wireless station in an infrastructure network to the DS.
From DS = 1	Data frames received from the DS for a wireless station in an infrastructure network.	Frames within a distribution system.

All Other Frame Control Fields

More Fragments (MF)
1 = additional fragments to follow
0 = last frame

Retry
1 = this packet is a retransmission
0 = this packet is not a retransmission

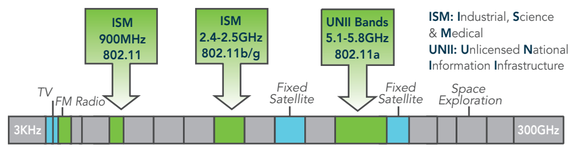
Protected Frame (Prot Frame)
1 = the frame is protected with link layer security such as WEP or WPA/2
0 = the frame is transmitted as clear text

More Data (MD)
1 = indicates to the stations the AP has at least one frame buffered for the station
0 = no buffered packets in the AP for the station

Order
1 = strict ordering supported
0 = strict ordering not supported

Power Management (Pwr Mgt)
1 = station is in power save mode
0 = station is active (out of power save mode)

802.11 FREQUENCY BANDS



ISM: **I**ndustrial, **S**cience & **M**edical
UNII: **U**nlicensed **N**ational **I**nformation **I**nfrastructure

GLOSSARY

802.11—A group of wireless networking standards set by the Institute of Electrical and Electronics Engineers (IEEE), commonly referred to as Wi-Fi, but were previously known as WLAN.

802.11a—A supplement to the IEEE 802.11 specification that describes radio transmissions at a frequency of 5GHz and data rates of up to 54Mbps.

802.11b—A supplement to the IEEE 802.11 specification that describes radio transmissions at a frequency of 2.4GHz and data rates of up to 11Mbps.

802.11g—A supplement to the IEEE 802.11 specification that describes radio transmissions at a frequency of 2.4GHz and data rates of up to 54Mbps.

802.11e—An IEEE standard that adds Quality of Service (QoS) functionality and multimedia support to existing 802.11b, 802.11g, and 802.11a.

802.11i—An IEEE standard that hardens the security mechanisms for 802.11 networks. The 802.11i standard included improvements in key management, user authentication using 802.1X, and the data integrity of headers.

802.11n—A task group of the IEEE 802.11 committee whose goal is to define a standard for high throughput speeds of at least 100Mbps on wireless networks.

802.1X—A standard for port-based authentication first used in wired networks, that has been adapted for use in Wi-Fi networks. 802.1X provides a framework for authenticating users and controlling their access to a protected network with dynamic encryption keys that protect data privacy.

Wi-Fi or WLAN AP (Access Point)—A small to medium capacity Wi-Fi device (1–3 radios) that connects wireless devices/users to another network.

Wi-Fi or WLAN Array—A medium to high capacity device (4–16 radios) that connects wireless devices/users to another network. The Wi-Fi/ WLAN Array differs from an Access Point in that it usually contains an embedded Switch, Router, and AP controller that acts as a seamless extension of the wired network over the basic connectivity provided by Access Points.

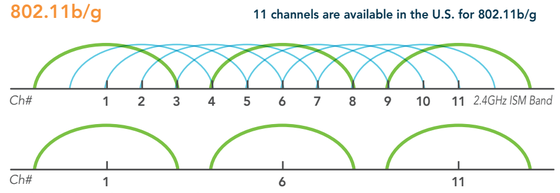
SSID (Service Set Identifier)—A unique 32-character network name, or identifier, that differentiates one wireless LAN from another. All access points and clients attempting to connect to a specific WLAN must use the same SSID. The SSID can be any alphanumeric entry up to a maximum of 32 characters.

Wi-Fi—Short for wireless fidelity. A term developed by the Wi-Fi Alliance to describe wireless local area network (WLAN) products that are based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards.

CHANNELS AND CAPACITY

802.11b/g

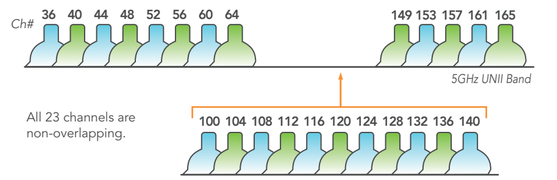
11 channels are available in the U.S. for 802.11b/g



Only 3 channels are non-overlapping.

802.11a

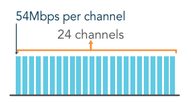
23 channels are available in the U.S. for 802.11a



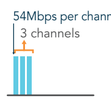
All 23 channels are non-overlapping.

Wireless Capacity Comparison

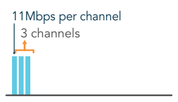
802.11a Capacity
24 channels x 54Mbps = 1,296Mbps of RF capacity



802.11g Capacity
3 channels x 54Mbps = 162Mbps of RF capacity



802.11b Capacity
3 channels x 11Mbps = 33Mbps of RF capacity



+805.262.1600 • 800.947.7871 • posters@xirrus.com • www.xirrus.com