



# Wi-Fi® Technology presentation



# Topics

- **Background**
- **Benefits**
- **802.11 Architecture**
- **Wi-Fi Future**
- **Wi-Fi® Alliance**
- **Certification**
- **More Information**



The IEEE 802.11 specification is an international standard describing the characteristics of a wireless Local Area Network



The term *Wi-Fi* suggests *Wireless Fidelity*, resembling the long-established audio-equipment classification term *high fidelity*

# Background

## Background

- **1990 : 802.11 development started by IEEE**  
The aim was to develop a standards for medium access control (MAC) and physical layer (PHY)
- **1997 : First version of 802.11 standard was ratified**  
First version delivered 1Mb/s and 2Mb/s data rates
- **1999 : 802.11a and 802.11b amendments were released**  
Data rates improved to 5.5Mb/s and 11Mb/s at 2.4GHz (802.11)  
Wired Equivalent Privace (WEP) introduced  
5GHz operation with OFDM modulation at 54Mb/s (802.11a)
- **2001 : FCC approved the use of OFDM at 2.4GHz**
- **2003 : OFDM modulation at 54Mb/s at 2.4GHz (802.11g)**

## Background

- **2009 : 801.11n amendment were ratified**  
PHY relies heavily on multiple-input multiple-output (MIMO) technology  
Can use both 2.4Ghz and 5Ghz at the same time  
Throughput increased even up to 600Mbps
- **2009 : Bluetooth 3.0 + HS**  
802.11 selected as the Bluetooth high speed channel
- **2009 : Wi-Fi direct specification introduced**
- **2011 : 802.11ac under development**  
More throughput with wider bandwidth, more MIMO streams and wider 256-QAM modulation. Provides 500-1000Mbps throughput



# Benefits

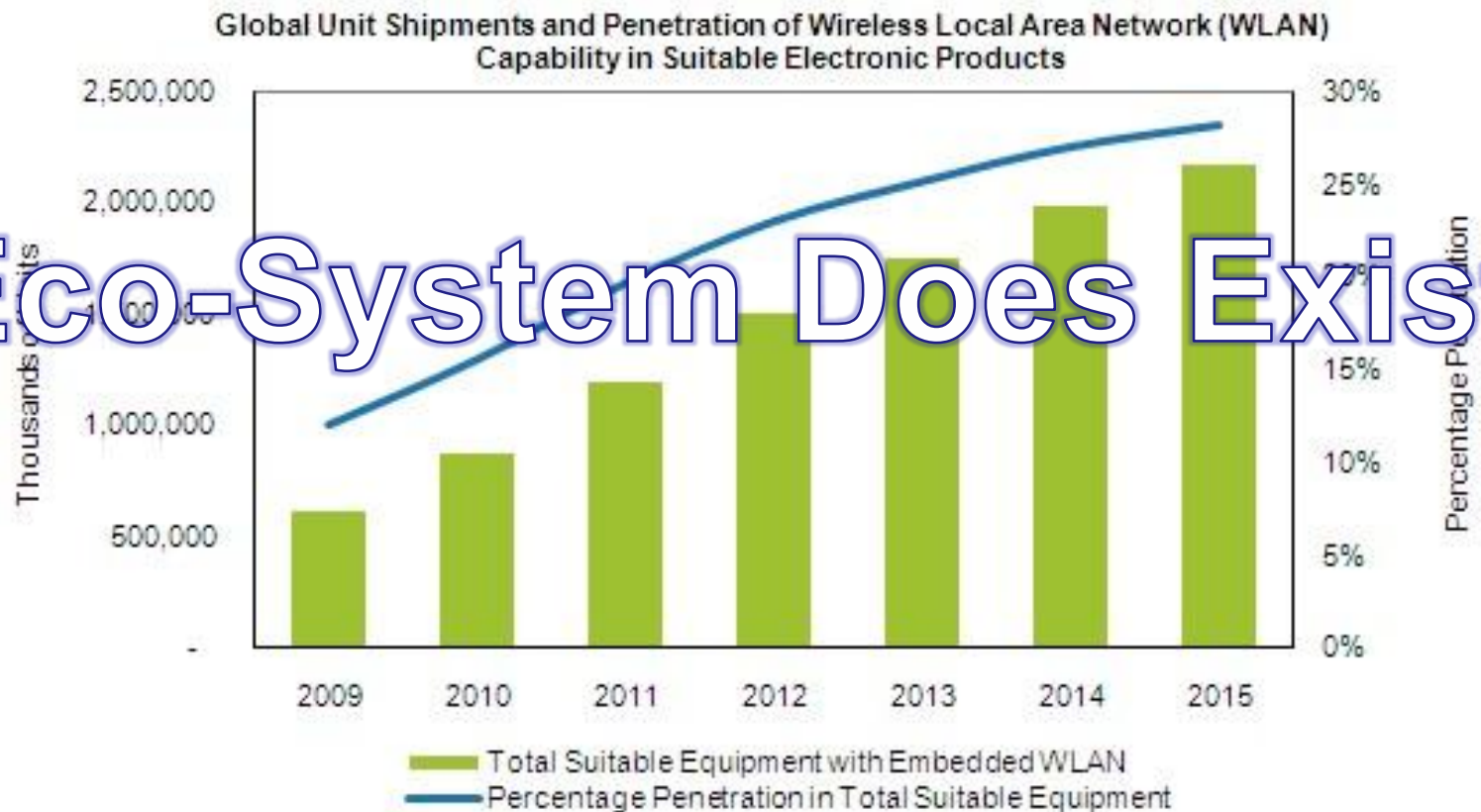
## **Benefits of Wi-Fi**

- **Mobility**
- **Compatibility with IP networks**
- **High speed data**
- **Unlicenced frequencies**
- **Security**
- **Easy and fast installation**
- **Scalability**
- **Installed infrastucture**
- **Low cost**



## Eco-System Growth

- The number of Wi-Fi products is growing steadily.

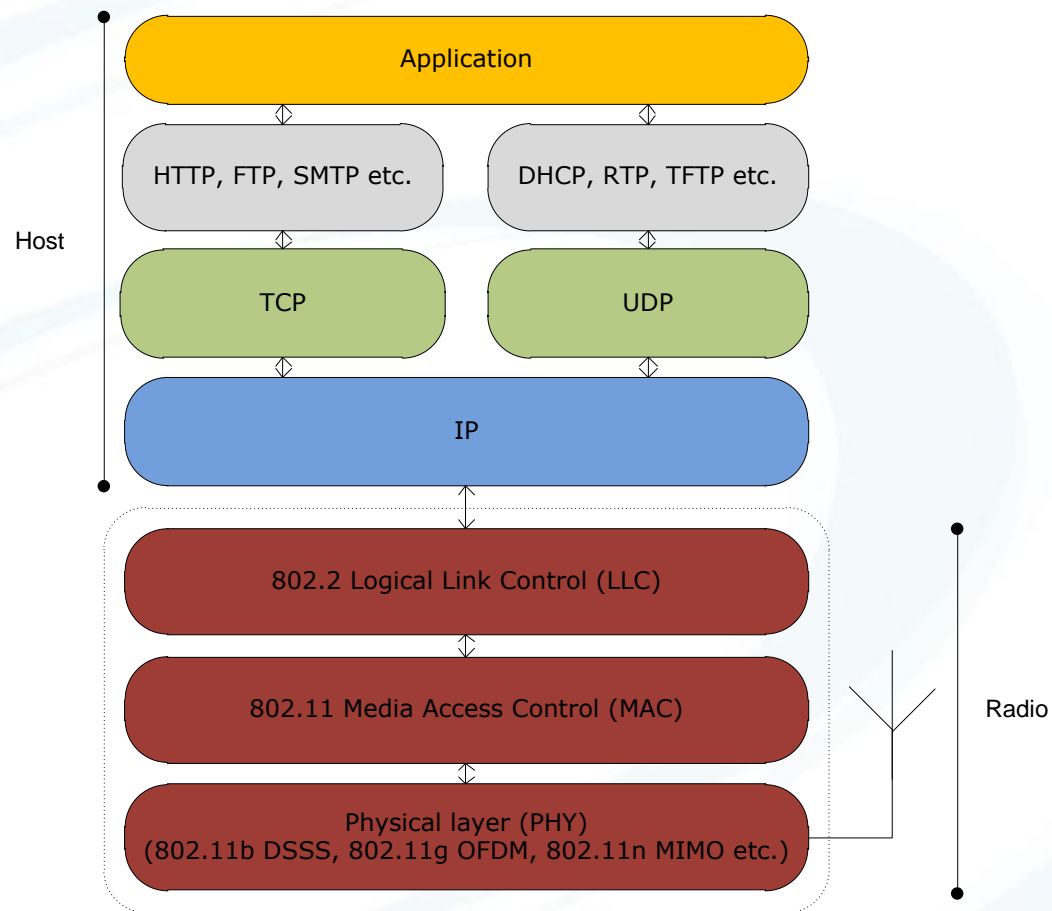


Eco-System Does Exist!



# **802.11 Architecture**

# 802.11 Architecture



# Physical layer

## 2.4 GHz and/or 5GHz transceiver

- Industrial Scientific Medical (ISM) band
- License free

## Spread spectrum technology

- FHSS, DSSS and OFDM modulations

### FHSS (Frequency Hopping Spread Spectrum)

- Bandwidth divided into 75 1MHz channels
- Data throughput limited to 2Mbps because of hopping overhead and FCC regulations (1 Mhz channel bandwidth)
- Obsolete

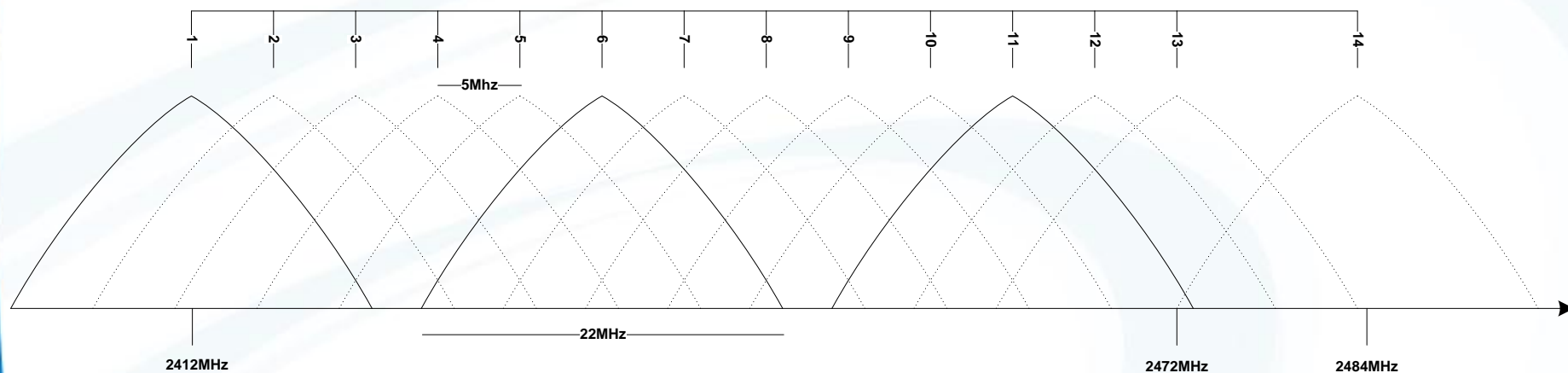
### DSSS (Direct Sequence Spread Spectrum)

- Bandwidth divided into 14 22MHz channels
- Channels overlap partially

### OFDM (Orthogonal Frequency-Division Multiplexing)

- 20 or 40MHz bandwidth
- Uses several non-overlapping channels
- Channels overlap partially

# Physical layer



**Europe : channels 1-13**

**USA : channels 1-11**

**Japan : channels 1-14**

# Physical layer

Standard	Frequency	Bandwidth	Symbol rate (Mb/s)	MIMO streams	Modulation
802.11	2.4GHz	20	1, 2	1	DSSS, FHSS
802.11a	5Ghz	20	6, 9, 12, 18, 24, 36, 48, 54	1	OFDM
802.11b	2.4GHz	20	5.5,11	1	DSSS
802.11g	2.4GHz	20	6, 9, 12, 18, 24, 36, 48, 54	1	OFDM, DSSS
802.11n	2.4/5GHz	20	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2	4	OFDM
		40	15, 30, 34, 60, 90, 120, 135, 150		

## 802.11 Media Access Control (MAC)

- **Manages and maintains communications between 802.11 stations and clients**
- **Coordinates access to shared radio channels**
- **Uses CSMA/CA algorithm to access the media (Carrier Sense Multiple Access / Collision Avoidance)**
- **Similar to *Bluetooth* Link Layer**

# 802.11 Media Access Control (MAC)

Function	Explanation
<b>Scanning</b>	Scanning of access points. Both active (probe) and passive (beacon) scanning are provided by the standard.
<b>Authentication</b>	Authentication is the process of proving identity between the client and the access point.
<b>Association</b>	Once authenticated, the client must associate with the access point before sending data frames.
<b>Encryption</b>	Encryption of payload
<b>RTS/CTS</b>	The optional request-to send and clear-to-send (RTS/CTS) function allows the access point to control use of the medium for stations activating RTS/CTS.
<b>Power Save Mode</b>	The power save mode enables the user to turn on or off enables the radio.
<b>Fragmentation</b>	The fragmentation function enables an 802.11 station to divide data packets into smaller frames.



# Logical Link Control (LLC)

- The LLC provides end-to-end link control over 802.11-based wireless LAN

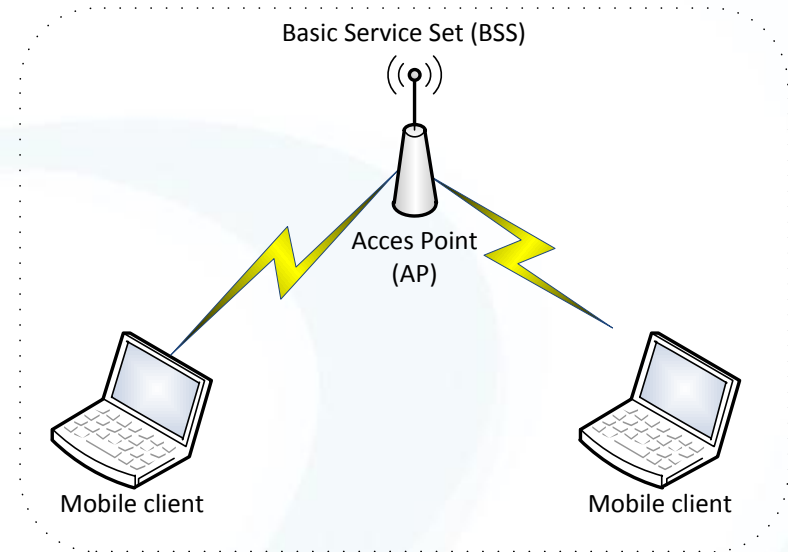
## LLC services:

- **Unacknowledged connectionless service**  
Higher layers must take care of error and flow control mechanisms  
Peer-to-peer, multicast and broadcast communication
- **Connection-oriented service**  
Error and flow control  
Peer-to-peer communication
- **Acknowledged connectionless service**  
Flow and error control with stop-and wait ARQ  
Peer-to-peer, multicast and broadcast communication

# Infrastructure

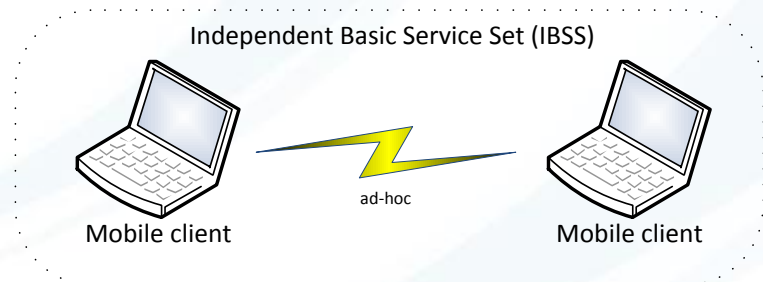
## Basic Service Set (BSS)

- A set of stations controlled by a single “Coordination Function”
- Typically uses an Access Point (AP)
- All mobile stations must be accessible by the access point of the infrastructure BSS
- In the infrastructure network, stations must associate with the access point in order to get access to network services



## Independent Basic Service Set (IBSS)

- A BSS without an Access-Point
- ad-hoc networking



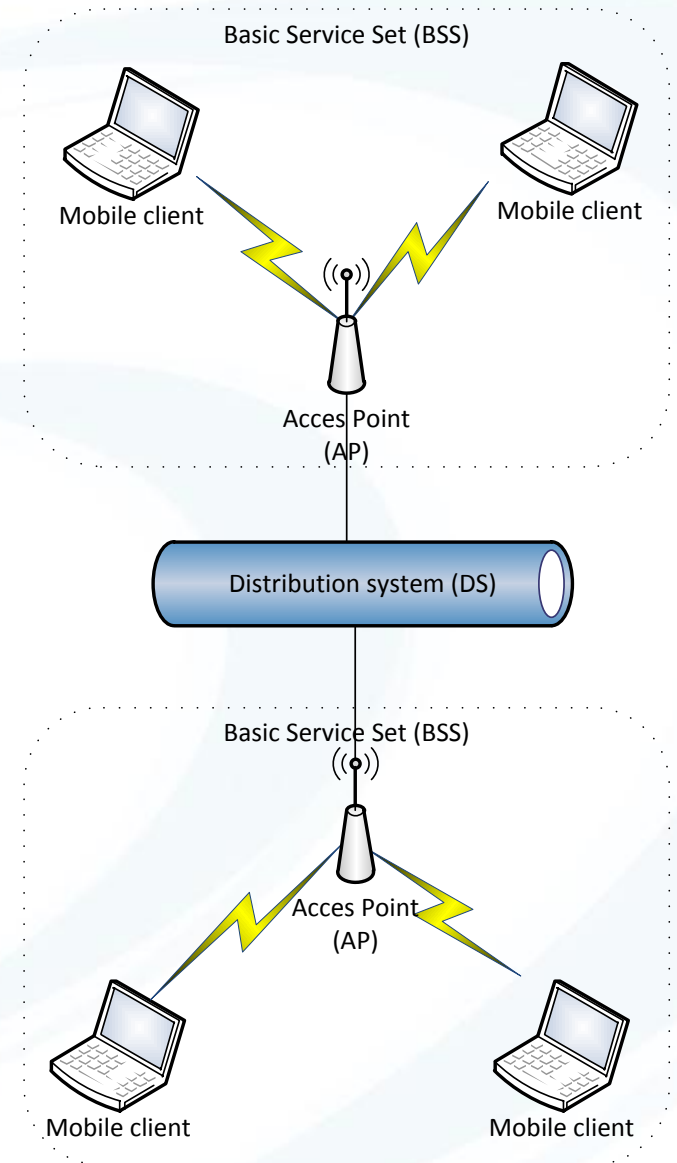
# Infrastructure

## Extended Service Set (ESS)

- A set of one or more Basic Service Sets interconnected by a Distribution System (DS)
- Traffic always flows via Access-Point

## Distribution System (DS):

- A system to interconnect two or more BSS
- Typically wired Ethernet
- Could be also wireless like 802.11, WiMax, 3G/4G etc.



# Infrastructure

## **AP – client services:**

- Authentication : open, shared key or WPS
- De-authentication
- Privacy : WEP, WPA or WPA2

## **Distribution System services:**

- Association : maps the client into the distribution system via access point
- Disassociation : release of association
- Distribution : used to deliver MAC frames across the distribution system
- Integration : enables delivery of MAC frames between DS and non 802.11
- Re-association : transition of association from one access point to an other

# Security

# Security

The 802.11 provides the following security features

- **Association**  
Client needs to associate with the Access Point
- **Authentication**  
Authentication is either open, shared key or WPS
- **Access control**  
Access Point can decide which clients are allowed to associate based on MAC address

Trivial to spoof MAC address

# Security

- **Encryption**

Wired Equivalent Privacy (WEP)	(insecure)
Wireless Protected Access (WPA)	(insecure)
Wireless Protected Access 2 (WPA2)	(recommended)
WAPI	(for China)

- **Data integrity**

Data can not be modified on-the-fly. Quaranteed by encryption.

- **Data confidentiality**

No eavesdropping with decryption of data. Quaranteed by encryption.

# Security

- **Wired Equivalent Privacy (WEP)**

Wired Equivalent Privacy. This encryption standard was the original encryption standard for wireless.

Security issues known since 2001, can be cracked in <1minute

- **Wirelsss Protected Access (WPA)**

A software/firmware improvement over WEP. WPA is a trimmed-down version of the 802.11i security standard that was developed by the IEEE 802.11 to replace WEP.

WPA uses TKIP for encryption, some routers also support AES.

Security issues known since 2008 in TKIP, considered unsecure

- **WLAN Authentication and Privacy Infrastructure (WAPI)**

A wireless security standard defined by the Chinese government.

Must be supported by cell phones sold in China.



# Security

## Wireless Protected Access 2 (WPA2)

- WPA2 is a Wi-Fi Alliance branded version of the final 802.11i standard.
- The primary enhancement over WPA is the inclusion of the AES-CCMP algorithm as a mandatory feature.
- The CCMP/AES algorithm is considered secure, given a good enough password
- WPA2 Personal (WPA2-PSK): Uses a password, common.
- WPA2 Enterprise (WPA2-RADIUS): Certificates on server

**Note: Wi-Fi Alliance will mandate Wi-Fi CERTIFIED products only to support WPA2 CCMP/AES**

# Wi-Fi Protected Setup

The standard for easy and secure establishment of a wireless home network, created by the Wi-Fi Alliance. It is not a security scheme but just a way to configure one.

The protocol is meant to allow home users who know little of wireless security.

- **PIN entry (mandatory)**  
Commonly a numeric code printed on the AP needs to be fed to STA
- **Push button configuration (optional for STA)**  
Configured by pressing physical button on both device and AP
- **A security problem with WPS devices was identified in 2011 allowing brute force attacks on the PIN**  
It is expected that future AP will prevent brute force attacks  
In the meanwhile, security researchers recommend turning disabling WPS
- **AOSS is Buffalo's proprietary equivalent to WPS**

**Note: A major security flaw was revealed in December 2011**



# Upcoming technology

## Wi-Fi Direct

- Allows Wi-Fi devices to talk to each other without the need for wireless access points
- Wi-Fi Direct essentially embeds a software access point, or "soft AP", into any device that wishes to support Direct.
- Requires support for Wi-Fi Protected Setup with its push-button or PIN-based setup.
- When a device enters the range of the Wi-Fi Direct host, it can connect to it

### **Primary use cases:**

- Point-to-point file sharing (phones, picture frames, HDDs)
- Synchronization
- Wi-Fi tethering

## Wi-Fi Multimedia - WMM

- Quality of Service (QoS) targeting multimedia applications
- Implemented on MAC layer as amendment (IEEE 802.11e)
- For queues or categories: **voice, video, best effort** and **background**. No guaranteed throughput.

### WMM power save:

- Requires AP to buffer each queue
- Allows STA to request data from the queue or schedule delivery
- Power saving comes from sleeping while AP is buffering

## IEEE 802.11ac

- **The next generation after IEEE 802.11n**  
433Mbit/s - 1Gbit/s datarates (not throughput)
- **Working in the 5GHz band**
- **Currently being drafted**  
Working group approval expected late 2013  
Demonstrations done, products released 2012-2013
- **Througput through wider channels**  
80MHz and 160MHz
- **More dense modulation**  
256-QAM

# **Wi-Fi Alliance**

## Wi-Fi Alliance

- An open, non-profit organization responsible of : Wi-Fi standards development, marketing, Wi-Fi certification etc.
- Wi-Fi Alliance developed standards: WPA, WPA2, WMM, Wi-Fi Direct etc.
- Formed originally to resolve the interoperability issues between different manufacturers' 802.11 devices.
- Similar organization to Bluetooth SIG



# **Certification**

# Certification

- **Typical two step process:**  
Wi-Fi certification (optional)  
Regulatory testing (FCC, CE, IC, Telec etc.)
- **Consists of mandatory and optional certifications**
- **Mandatory**  
IEEE 802.11 based radio standards  
WPA and WPA2  
EAP
- **Optional**  
Wi-Fi Direct  
Wi-Fi Protected Setup  
WMM  
WMM Power save
- **Wi-Fi Alliance membership required to make the certification**
- **Gives right to use Wi-Fi logo on the product and marketing material**

**More information**

## More information

- Bluegiga Technologies  
[www.bluegiga.com](http://www.bluegiga.com)
- IEEE 801.11  
[www.ieee802.org/11](http://www.ieee802.org/11)  
[www.en.wikipedia.org/wiki/IEEE\\_802.11](http://www.en.wikipedia.org/wiki/IEEE_802.11)
- Wi-Fi Alliance  
[www.wi-fi.org](http://www.wi-fi.org)  
[www.wi-fi.org/knowledge\\_center\\_overview.php](http://www.wi-fi.org/knowledge_center_overview.php)



**blue giga**

**Thank you**

**[www.bluegiga.com](http://www.bluegiga.com)**