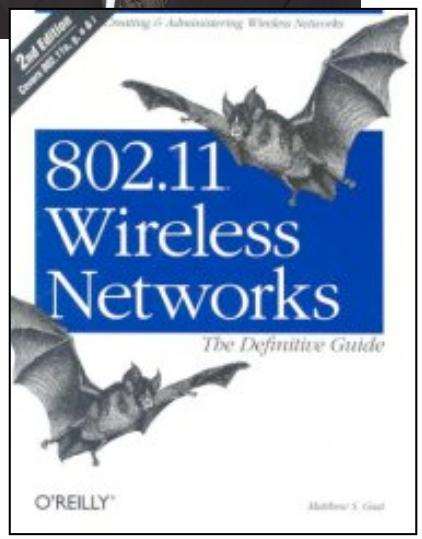
Wireless Standards Update

Matthew Gast

Director, Product Management

Networkshop 38 (March 2010), Manchester, UK

About Me



- **Director, PM at Aerohive**
- **IEEE 802.11 Voting Member; Chair of Task Group M (802.11 revision)**
- **Have held multiple leadership positions at Wi-Fi Alliance**
  - Chair, Security Technical TG
  - Vice Chair, Security Marketing TG
  - Chair, Wireless Network Management TG
- **Author of** *802.11 Wireless Networks: The Definitive Guide* **(O'Reilly)**
- **Founder/board member, OpenSEA Alliance**

Where Standards Come From

- **IEEE 802.11**
  - Current timeline for activities, updated after every meeting: http://www.ieee802.org/11/Reports/802.11_Timelines.htm
- **Wi-Fi Alliance**
  - Best known for certification programs
  - Some “packages” of multiple standards: WPA, Voice, network management
  - Wi-Fi Direct is a new WFA-developed standard

Emerging IEEE Standards 1: 802.11n-2009

- **Fully ratified September 2009**
  - Cool mousepads March 2010
- **Continuing roll-out**
  - Up to 4 spatial streams
  - Chips go up to 3 today
  - New optional Wi-Fi certifications for improved speed (3 stream operation), improved efficiency, and better range (STBC)
- **Important bridge to future gigabit PHYs**
  - My crystal ball is cloudy: maybe 5-7 years for the chips?

Emerging IEEE Standards 2: 802.11r-2008

- **802.11r-2008: "Fast BSS transition"**
- **Extend keying so that a network holds a key across multiple devices**
  - Client devices can move between APs in "mobility domain" by using the key before association
  - Re-uses 802.11 Authentication frames for, well, authentication!
- **Key technology in future Wi-Fi Alliance Voice-Enterprise certification**

Emerging IEEE Standards 3: 802.11w-2009

- **Non-real-time 802.11 management protocols are carried in Management frames**
  - Unprotected by WPA security, but will be protected by 802.11w
  - Broadcast messages are signed for integrity, so clients can validate Beacon contents after association is complete
- **"Get off my network" frames (Deauthenticate and Disassociate messages) are easily forged**
  - The only dependence is on easily observed and duplicated AP MAC address
  - Many attacks uses these frames to force reassociation to observe new exchanges, such as PSK recovery attacks
- **Need to protect Action frames to secure future management traffic**
- **Wi-Fi Alliance certification effort expected this year (successful test event last week)**

The next tranche of IEEE standards

- **802.11z: Direct Link Setup**
  - Allow APs to mediate direct connections between devices
- **802.11v: Network Management**
- **802.11u: Interworking**
  - Allow networks to self-describe their services
- **802.11s: Mesh**
  - Likely after 802.11-2011 revision

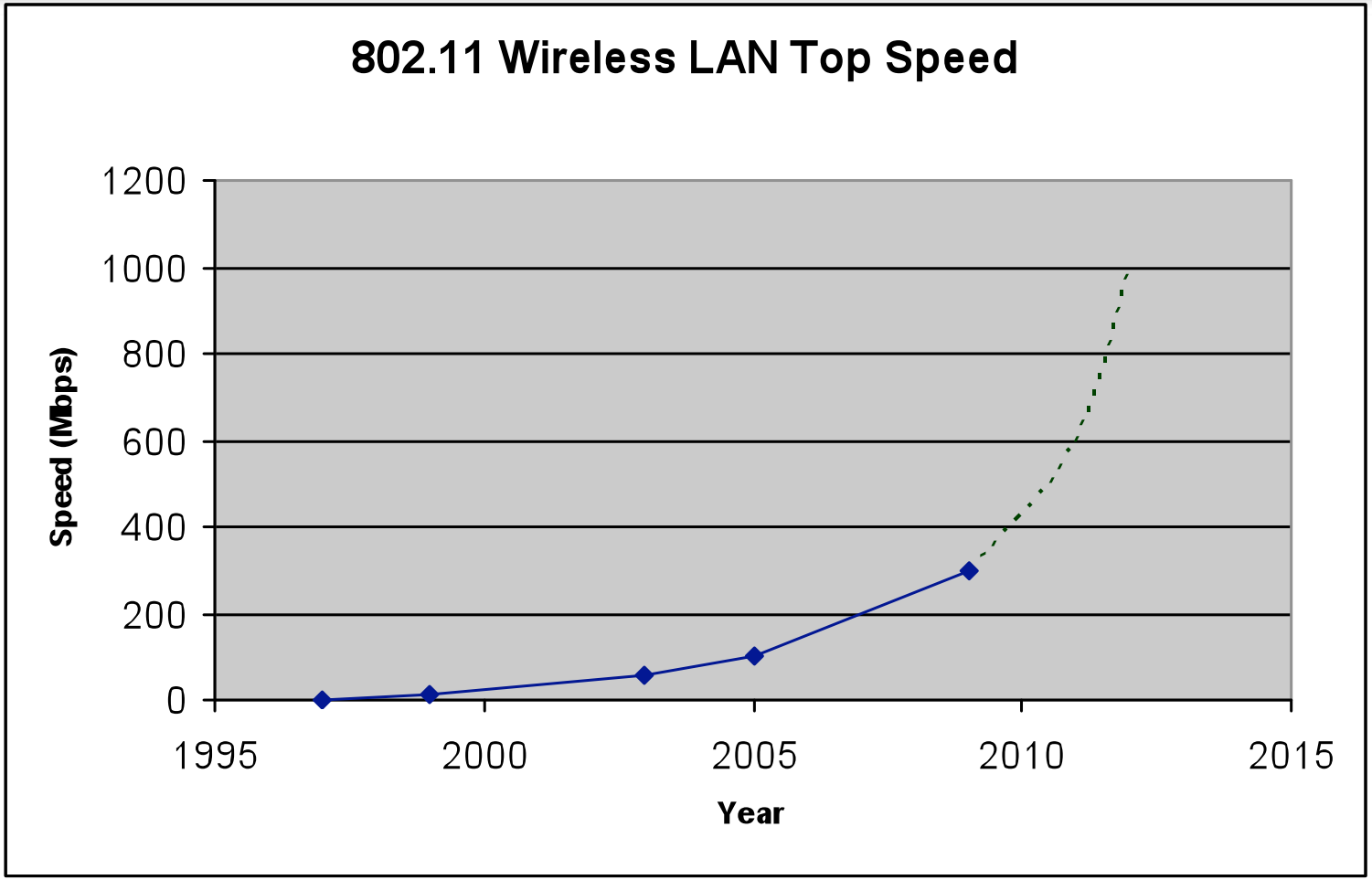
802.11v & Wi-Fi Network Management

- **802.11v has ~50 features to consider**
  - Wi-Fi Alliance effort underway to study certification requirements
- **Improved power saving**
  - Enable deeper sleep periods for devices to preserve precious electrons
  - Manage traffic which wakes up a device – network only transmits SIP control frames to a sleeping telephony device
  - Handheld/battery operated devices (phones & RFID)
- **Better statistical & event reporting/influence**
  - Collect information on network operation to spot problems
  - Manage client transitions between networks
- **Location & timing management for networks**

Bring on the PHYs

- **VHT (Very High Throughput) study group came up with two task groups**
  - Future 802.11ac: Gigabit @ < 6 GHz
  - Future 802.11ad: Gigabit @ 60 GHz
  - Like 11n in 2003-4: excitement without hardware
- **Future 802.11af: (USA) TV white space: sub-1 GHz (~ 700 MHz)**
- **Sub 1 GHz study group**
  - Standardize 900 MHz ISM band for 802.11
  - Main initial target is USA smart grid applications

Getting PHYsical with IEEE 802.11?



- **"Top speed" of widely available equipment shows repeated efforts by IEEE 802.11 WG to design new physical layers**

Thank you for listening!

mgast (at) aerohive (dot) com