802.11 "Decrypted"

Adrian Stephens
Intel Corporation
15 JJ Thompson Ave
Cambridge CB3 0FD, UK
+44 1223 763457

ABSTRACT
This short paper introduces wireless IEEE 802 standards and activities with a focus on explaining the purpose of the many 802.11 amendments.

Categories and Subject Descriptors
A.1 [**INTRODUCTORY AND SURVEY]**

C.2.5 [**Local and Wide-Area Networks**]

General Terms
Standardization

Keywords
TBD

1. INTRODUCTION
As wireless technology increasingly pervades our lives, the decisions made in wireless standards bodies such as the IEEE 802.11 have the potential to impact our lives. From the user viewpoint, emerging standards will support new applications, higher throughput and increasing mobility. From the implementer viewpoint, the increasing complexity must be hidden from the user. New standards create new challenges and emergent behaviors that call for academic scrutiny.

The question addressed here is: what are 802 and 802.11, and what do the various letters after ".11" signify?

2. IEEE 802
IEEE 802 is a project of the Institute of Electrical and Electronic Engineers (IEEE) LAN/MAN Standards Committee (LMSC). It was created in February 1980 – hence the name 802.

The LMSC is a committee of the IEEE Standards Association (IEEE-SA), which is the body that publishes completed standards and their amendments.

Within project 802, are various *working groups* – each of which defines one or more standards or recommended practices.

The currently active working groups are listed in Table 1.

Table 1 - IEEE 802 Working Groups

Working Group	Name
802.1	Higher Layer LAN protocols
802.3	Ethernet
802.11	Wireless LAN
802.15	Wireless PAN
802.16	Broadband Wireless Access
802.17	Resilient Packet Ring
802.18	Radio Regulatory technical advisory group
802.19	Coexistence technical advisory group
802.20	Mobile Broadband Wireless Access
802.21	Media Independent Handoff
802.22	Wireless Regional Area Networks

3. 802.11
The 802.11 working group working held its first meeting in September 1990 and issued the first draft of the 802.11 standard in early 1995, completed in late 1997. This document included a medium access controller (MAC) and physical layer (PHY) definitions for three media:

- Infrared
- Frequency Hopping Spread Spectrum (FHSS) in the 2.4GHz ISM band (1, 2 Mbps)
- Direct Sequence Spread Spectrum (DSSS) in the 2.4 GHz ISM band (1, 2 Mbps)

Originally the FHSS PHY was the most popular because of its lower cost and robustness. The author is not aware of any commercial products using the Infrared PHY. The DSSS PHY did not become popular until 802.11b increased the PHY rates to 5.5 and 11 Mbps. 802.11b is the version that has made wireless networking a popular commercial product.

Since the original version, 802.11 spawned *task groups* to produce amendments to the 802.11 standard. The first task group (TG) is called "TGa", and its amendment is called 802.11a, and so on. Each TG is authorized by the IEEE-SA and has a well-defined scope defined in its Project Authorization Request (PAR) document. The 802.11 task groups are described in Table 2. Those task groups that are currently active are indicated as such.

Table 2 - IEEE 802.11 Task Groups

Task Group	Description
TGa	This group developed a higher speed PHY based on orthogonal frequency division multiplexing (OFDM) in the 5GHz bands. The group cooperated with the European ETSI BRAN project and the two produced very similar

DELL-1032
9,614,566

	PHY specifications. 802.11a has the advantage of several hundred of MHz of spectrum in the 5GHz band. However, it did not have the popular impact that 802.11b had due to the increased cost of operating at these frequencies. 802.11g made 802.11a speeds available in the 2.4GHz band. As the costs of 5GHz components has fallen, 802.11a looks increasingly attractive, and 802.11 a/b/g combination products are commonly available.
TGb	802.11b extended the DSSS PHY to support 5.5 and 11 Mbps. It has been the most successful version of 802.11 to date, and is now being replaced by 802.11g.
TGc	This defines 802.11 MAC procedures to support bridge operation. It is a supplement to 802.1D developed in cooperation with the 802.1 working group.
TGd	This extends support to additional regulatory domains and provides on-the-air signaling and control of parameters affected by the regulatory domain (such as channelization and hopping patterns).
TGe	TGe is still active, although it has nearly completed the standards process. It defines support for QoS for both distributed (EDCA) and centralized (HCCA) mechanisms. It supports QoS flows based on a user priority, suitable for connectionless data. Although the 802.1 MAC interface does not support connection-oriented data transfer, the 802.11e traffic specification (TSPEC) comes close to defining a connection – describing a flow in terms of size, rate, period and many other parameters. This makes 802.11e also suitable for periodic data such as VoIP. Additional improvements include power-saving (APSD) and additional efficiency gains through a selective acknowledgement (Block Ack).
TGf	This group developed recommended practices for an Inter-Access Point Protocol (IAPP) intended to provide interoperable management of the distribution system between APs from different manufacturers. It is uncertain what impact this recommended practice has had.
TGg	The 802.11g amendment essentially allows operation of the 802.11a OFDM modulation in the 2.4 GHz band. It provides 802.11a throughput at close to 802.11b prices. The challenge for 802.11g devices is to coexist with the installed base of 802.11b devices. This is achieved through various protection mechanisms, although there is some penalty in performance for operating in such an environment.
TGh	802.11h defined enhancements to 802.11a to support operation in the license exempt bands in Europe. It supports measurement and reporting of channel energy in order to provide dynamic frequency selection (DFS). It also provides control of transmit power (TPC).
TGi	This group was created to address issues and concerns with the original 802.11 WEP security mechanism. 802.11i defines two new mechanisms. TKIP is a medium strength mechanism designed for compatibility with hardware implementing the original 802.11 WEP security mechanism. WEP has proven to be susceptible to various types of attack, and TKIP provides a stopgap solution to these. AES provides the much stronger 128-bit block encryption, which is supported by newer hardware.
TGj	802.11j supports operation in Japan in the 4.9 and 5GHz bands. It extends the operation of the 802.11a PHY to operate in a 10MHz channel (half the channel width of 802.11a), and also allows longer range communication by increasing the turnaround interval to allow for longer propagation delays.
TGk Active	802.11k defines measurement of the radio channel that allows a device (a client device or an access point, or management software above) to make informed decisions relating to selecting an access point and selecting an operating channel. TGk is currently active.
TGma	This group provides maintenance changes (editorial and technical corrections) to 802.11-1999, 2003 edition (incorporating 802.11a-1999, 802.11b-1999, 802.11b-1999 corrigendum 1-2001, and 802.11d-2001).
TGn Active	802.11n will define modifications to both PHY and MAC layers to provide substantially higher throughput than 802.11 a/g. The project requires 100Mbps of useful throughput (at the top of the MAC interface), which requires about 200Mbps at the PHY. TGn is currently in its down-selection process to select between proposed solutions. Current proposals use multiple antenna technology and increased channel width to achieve significantly higher than the target. A maximum throughput of ~600Mbps at the PHY has been described, although first generation products are unlikely to support the optional features that achieve this figure. The PHY fixed overheads are not reduced, and aggregation and other enhancements are necessary in the MAC to restore an acceptable level of efficiency (~70%).
TGp Active	The TGp amendment will support communication between vehicles and the roadside and between vehicles while operating at speeds up to a minimum of 200 km/h for communication ranges up to 1000 meters. It will use the 5.850-5.925 GHz band within North

	America defined for this purpose.
TGr Active	TGr is chartered with developing a secure, fast BSS transition solution, when a Station (STA) roams from one Access Point (AP) to another AP, within an Extended Service Set (ESS). High BSS transition latencies using existing 802.11 mechanisms (including 802.11i Security addendum), along with a lack of inter-operability between STA and AP vendors in harmoniously executing these procedures in performing this transition, are technical hurdles for widespread deployment of Voice over Internet Protocol (VoIP) over 802.11 LANs. Delay and jitter sensitive applications like multimedia, video, and voice, which have to co-exist with traditional, intermittent data traffic, demand a flexible and scalable solution, which maintains the security guarantees provided by IEEE 802.11i. It is a market-driven requirement that the BSS transitions be executed with minimal latencies, while maintaining the same Quality of Service (QoS), and confidentiality and integrity protection, that the STA was being afforded at the existing AP, when the STA moves to the next AP. By some estimates, the procedures recommended by TGr should take less than 50 milliseconds, in order to be effective for the voice/video class of applications. TGr is progressing the merger of two proposals that were voted in at the January 2005 meeting, through a down-select process, from an initial pool of eight.
TGs Active	TGs is considering how to create a Mesh of APs to provide a Wireless Distribution System (WDS) using the existing IEEE 802.11 MAC/PHY layers. The mesh needs to support broadcast and directed transmissions over potentially multiple "hops" between APs. It has to be self-configuring. TGs are executing their selection process. They have a call for proposals out that will results in proposals being heard in July 2005.
TGu Active	TGu will define an amendment to IEEE 802.11 to support interworking with external networks. The group is currently working on its functional requirements.
TGv Active	This group will provide Wireless Network Management enhancements to the 802.11 MAC, and PHY, to extend prior work in radio measurement to effect a complete and coherent upper layer interface for managing 802.11 devices in wireless networks.
TGw	802.11 and later 802.11i established mechanisms to protect data frames, but does nothing to protect control frames internal to 802.11. For example, it is possible to forge disassociation requests. 802.11w is being chartered to extend the 802.11i protections to data frames. It is expected that 802.11w will begin its work in May 2005.

4. References

The most accessible source of information are the IEEE web-sites.

The IEEE 802 LMSC home page is: http://grouper.ieee.org/groups/802/

The IEEE 802.11 WG home page is: http://www.ieee802.org/11/. This contains more detailed description of the scope and status of the individual task groups.

The IEEE 802.11 WG working documents are available (after free registration) from: http://802wirelessworld.com.

Approved amendments are available for download here: http://standards.ieee.org/getieee802/.

The author speaks for himself. Views expressed by the author are not necessarily endorsed by his employer.