Broadcom 802.11g Chipset Reverse Engineered

December 2005. For Immediate Release.

Over two years ago a group was founded to reverse engineer the Broadcom Wireless LAN chipsets to provide Linux drivers. This chipset is used by many OEMs, for example in Apple's AirPort Extreme in Power- and iBooks, Linksys' WAP and WRT series of consumer grade wireless routers, various laptops from Acer, Dell, Gateway, HP and others and many more external and internal devices, including CardBus cards.

That work has now come to a first milestone as there now is a free (GPL2 or later) Linux driver for a variety of these chipsets. Currently, only infrastructure and monitor modes are supported, but the chipset has advanced functionality for access point and ad-hoc modes which will be supported in the future, along with encryption and powersave features. A lot of work remains to be done for robust handling of all cases even in infrastructure mode.

Work is also being done to support plain 802.11b and also 802.11a chipsets, but is stalled because no such product is available to the developers.

Nonetheless, this development marks a breakthrough in Linux wireless capability as this chipset is used in many systems and was previously unusable with Linux systems.

This driver was made possible through the work by Johannes Berg, Jason Bouzane, Steve Cheng, Matthew Clark, Sven Henkel, Joseph Jezak, Asheesh Laroia, Andrew Miklas, Mattias Nissler, Florian Schirmer, Gary Simmons, Matthew Whitworth (in alphabetical order) and others who contributed to the reverse engineering effort, as well as Stefano Brivio, Michael Buesch, Danny van Dyk, Martin Langer and others who implemented the free driver. This driver was written based on specifications written by Johannes Berg, Sven Henkel, Joseph Jezak and Matthew Whitworth who joined the reverse engineering effort only this year.

The chip specifications are available at `http://bcm-specs.sipsolutions.net/`, the driver at `http://bcm43xx.berlios.de/` and the reverse engineering group has some information on its homepage at `http://linux-bcom4301.sourceforge.net/`. The so-called SoftMAC, a software implementation of management functions of the 802.11 protocol, can be found on `http://softmac.sipsolutions.net`.

For more information contact Johannes Berg at `johannes@sipsolutions.net`.