Wireless Fidelity with bwfm(4)

Patrick Wildt

September 22, 2019

Patrick Wildt Wireless Fidelity with bwfm(4)

э

AP ► < E ►

Personally Hardware Milestones

Who am I?

- OpenBSD developer
- ARM64-subtree maintainer
- LLVM-subtree updater
- SBC hoarder



Þ

Personally Hardware Milestones

Collection of devices

- Cubox-i
- Macbook
- Raspberry Pi 3
- Z83 Mini-PC



・ロト ・日下・ ・ ヨト

< ∃ →

Why?	Personally
How?	
What now?	Milestones

Milestones



2

Study

Find documentation

- Search the web for datasheets (by chip name)
- git grep in various OS (chip name, vendor/product ID)
- Neither code nor datasheet? Quit now.
- Alternative: reverse engineering
- Study code and/or documentation to grasp concepts
 - Attention: license concerns!
- Sealize it's going to be a long project

Start Details Tricky bits

Full vs Soft (simplified)



Patrick Wildt Wireless Fidelity with bwfm(4)

2

Why?	Start
How?	Details
What now?	



ISC-licensed brcm80211 drivers (Linux):

brcmfmac	brcmsmac
FullMAC	SoftMAC
35 496 LoC	75177 LoC

brcmsmac/phy/phy n.c: 28624 Lines Of Magic

御 🕨 🖌 🖉 🕨 🗸 🖻 🕨

What do we not have to do?

- No beacons
- No frequency changes
- No MCS handling

What do we have to do?

- Initiate scan
- Configure SSID
- Configure keys
- Handle events
- Handle network packets

Why?	Start
How?	Details
What now?	

Skeleton



Dongle

- Started with SDIO
 - But realized testing kernels will take too long
 - Unsure if SDIO layer actually worked
- 2 Bought a USB device
- Started with the lower layers
- Added PCIe/SDIO backend later



Start Details Tricky bits

Write code that compiles

- Skeleton-driver
- Initialize bus access
- Try to figure out whether the device is alive
 - read chip id
 - read MAC address
 - receive an interrupt

Why?	
How?	Details
What now?	

USB







Data+Events



2

Configuration

Initiate Scan:

Connect to SSID:

イロト イポト イヨト イヨト

Why?	
How?	Details
Vhat now?	Tricky bi

Connect to SSID

cm	d len	flags	status	variable + params
----	-------	-------	--------	-------------------

j	о	i	n	0	3	0	0	0	В	S	D	
	јо	in				SS Le	SID en			SSID		

・ロト ・日 ・ ・ ヨ ・ ・

문 🕨 🗄 문

Why?	
How?	Details
What now?	

BCDC Packets

Data	flags	prio	flags2	data offset	firmware signals	Ethernet Destination Mac	Ethernet Source Mac	Ethertype	Data Payload
Events	flags	prio	flags2	data offset	firmware signals	Ethernet Destination Mac	Ethernet Source Mac	Ethertype 0x886c	Event

 type	status	reason	 event-specific payload

э

ъ.

・日・ ・ ヨ・・

	Why? How? What now?	Start Details Tricky bits		
SDIO				



2

- 세 문 ► - 세 문 ►

SDIO Interrupt

- Shared pin: DAT[1]/IRQ
- Sampled as IRQ during Interrupt Period
- Some host controllers have troubles
- Workaround: externally routed GPIO



- Packet-based
- Multiple Ringbuffers
 - TX Control Ring
 - TX RX-Post Ring
 - (Control, TX, RX) Complete Rings
 - *n* Flowrings



▲ 同 ▶ → ● 三



- Read/write access to backplane
- Write Firmware & NVRAM
- Turn on/off ARM core
- Read dmesg



(日)

э

hndarm armr addr: 0x18002000. cr4 idx: 0 000000.001 RTE (SDIO-MSG BUF) 7.35.180.119 (r594535) on BCM4350 r8 @ 37.4/240.8/240.8MHz 000000.001 allocating a max of 255 rxcplid buffers 000000.002 pciemsgbuf0: Broadcom PCIE MSGBUF driver 000000.003 reclaim section 0: Returned 59036 bytes to the heap 000000.131 enable 1: a0 frmcnt 0. wrdcnt 0. a1 frmcnt 0. wrdcnt 0 000000.131 enable 1: g0 frmcnt 0, wrdcnt 0, g1 frmcnt 0, wrdcnt 0 000000.175 wl0: Broadcom BCM4350 802.11 Wireless Controller 7.35.180.119 (r594535) 000000 175 TCAM: 256 used: 255 exceed:0 000000.176 reclaim section 1: Returned 147512 bytes to the heap 000005.375 wl0: wlc enable probe req: state down, deferring setting of host flags 000005.413 wlc bmac_switch_macfreq: 4350 need fix for 37.4Mhz 000005.421 wlo: wlc_enable_probe_req: state down, deferring setting of host flags 000005.421 enable 1: g0 frmcnt 0, wrdcnt 0, g1 frmcnt 0, wrdcnt 0

イロト イヨト イヨト イヨト

3

Firmware Features

4356a2-roml/**pcie**-ag-msgbuf-splitrx-**p2p**-pno-aoe-pktfilterkeepalive-**sr-mchan**-pktctx-proptxstatus-ampduhostreorder-lpcpwropt-txbf-wl11u-mfp-tdls-amsdutx-sarctrl-proxd-hs20sta-rccwepso-ndoe-linkstat-gscan-hchk-logtrace-roamexp-rmon

Version: 7.35.101.6 (r702795) CRC: 4f3f65c5 Date: Sun 2017-06-04 16:51:38 PDT Ucode Ver: 963.316 FWID: 01-5e8eb735

Why?	
How?	Details
What now?	Tricky bits

Tricky bits

- Flow-control
- Asynchronous control messages
- Asynchronous creation of flowrings
- net80211 Integration





- Remote Control Message Injection (CVE-2016-0801): Updated firmware in November 2017
- KRACK (October 2017): Updated firmware in June 2018



(based on linux-firmware.git)

Why?	Issues
How?	
What now?	Future



```
/*
 * The firmware supplicant can handle the WPA
 * handshake for us, but we honestly want to
 * do this ourselves, so disable the firmware
 * supplicant and let our stack handle it.
 */
bwfm_fwvar_var_set_int(sc, "sup_wpa", 0);
```



NVRAM

Purpose:

- Provides configuration for the specific package
- Sets up antenna configuration, max dB, etc.

Needed on:

- PCle (sometimes)
- SDIO (always)
- USB (not yet?)

Provided by:

- Hardware designer (in their git repo)
- EFI BIOS (in an EFI variable)

Why?	
How?	Status
What now?	Future

Current Status

methook 140				feggy 377/920	ac/160% wed jan 10 12:13
JosBmuchbookino egres 'OpenSSD MacBook Dafe8 [1.0003] OpenSSD 5.2-current (CEENSIC.W) [1.0003] Isafes Apple Tre. Meshoolia,1 [1.0003] Nefe8 at pci2 dev 0 function 0 JosBmuchbookino	at' /vær/run/dmesg.boot) 80: Wed Jan 18 11:30:40 CST 28: "Broadcom BCM4350" rev 8x05: mxi	18			
 (?) Speedtest by Ookla - The X + (← → ○) ① www.speedtest.net 		e > (a 🖉 🖉 🗗 🖓 🐽	Edaily Ej Ework Eperm Etodo	○ ❷ 🖬 🗷 🕫 ≫ 🚍
	Go to the © PING © DOWN 3 19/ ms Mbps	Legacy site (Requires Flash) LOAD (© UPLOAD 1.53 91.64 Mbps	SHARE Ø @ @ @ @ Result ID 6953813481	Results History Settings Help	Login
-	AT&T Internet 99104.71220 *****	2 60 ⊕	ATÀT Cicero, IL Change Server		
Сомрану	PRODUCTS	ACCOUNT	ZIFF DAVIS	ooit	
		MacBook			

Patrick Wildt Wireless Fidelity with bwfm(4)



Current Status

- Works as client
- Properly fast 802.11ac (Wi-Fi 5)
- Implemented on recent Macbooks
- Implemented on raspberry Pis
- Available as *official raspberry Pi USB Dongle* (while supplies last)
- Works as access point often enough

Why?	lssues
How?	Status
What now?	Future

Future

- Better AP support
- Multi-AP support
- Suspend/Resume
- Firmware Signals
- Support for more devices

Why?	Issues
How?	Status
What now?	Future

Questions?



・四・・モ・・モ・

2