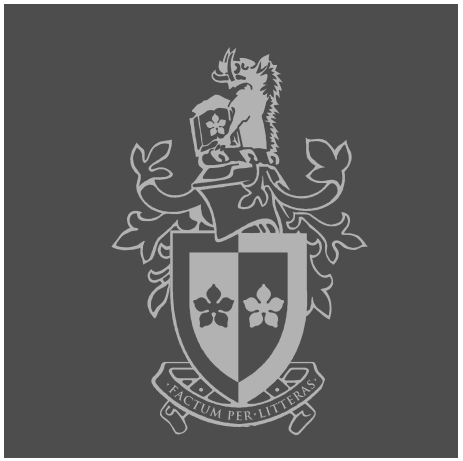
SWINBURNE

CENTRE FOR ADVANCED INTERNET ARCHITECTURES

Linux Madwifi driver debugging

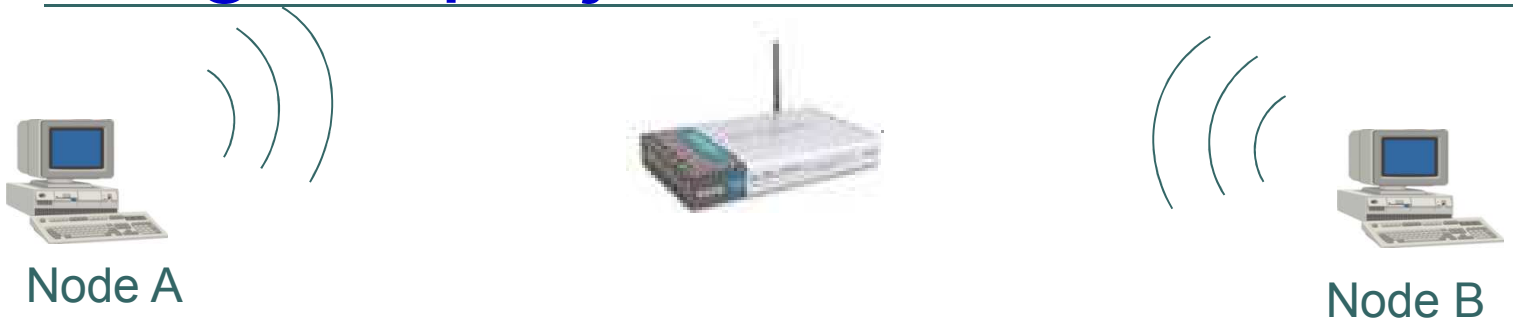
Tung Le, July 2010

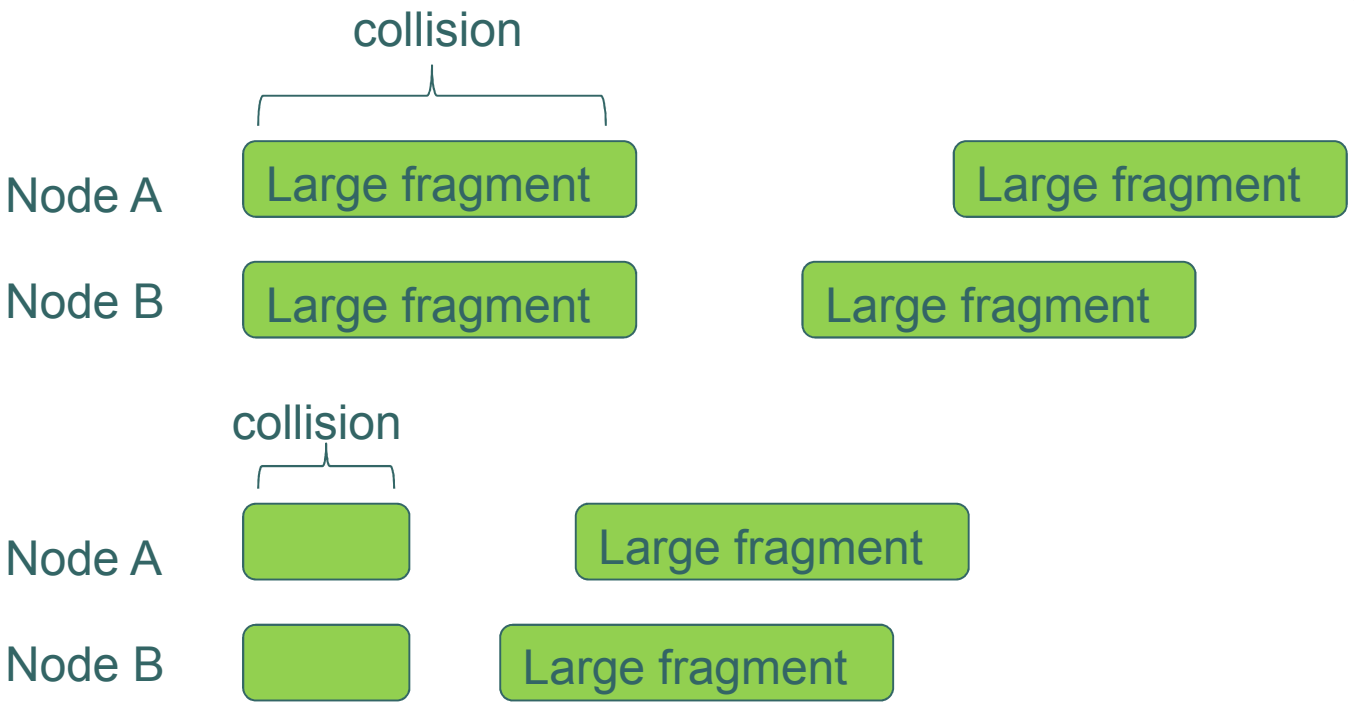


Outline

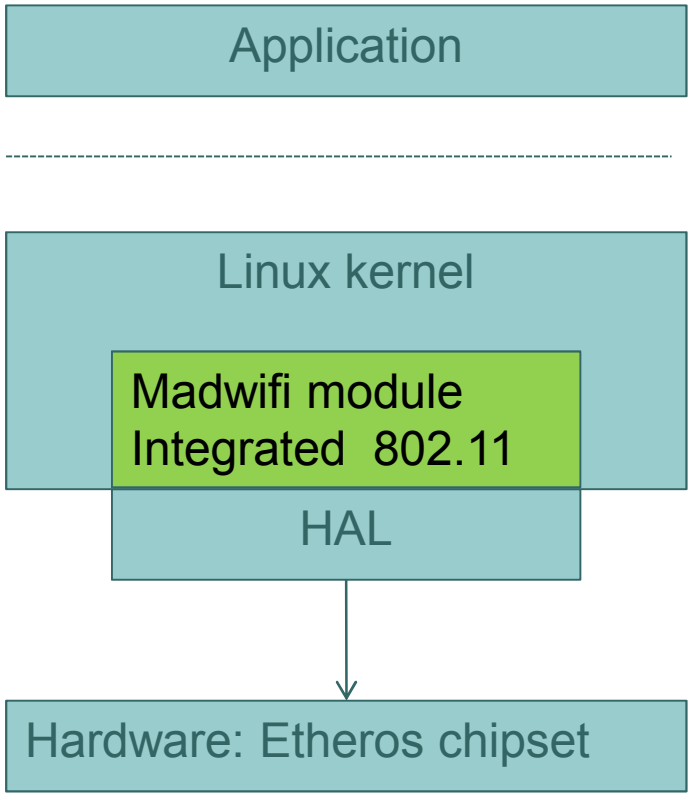
- Original project – 802.11 fragmentation
- System fails
- Collecting information
- Debugging techniques
- Result

Original project





Madwifi overview



- One of the most advanced WLAN driver
- Open source driver
- Aim to change fragmentation of 802.11

Outline

- Original project
- System fails
- Collecting information
- Debugging techniques
- Result

Oops… System crashed !!!

Hey, send this packet

A ping packet

No problem

A ping packet

Hey, fragment then send this packet

A ping packet

System crashed !

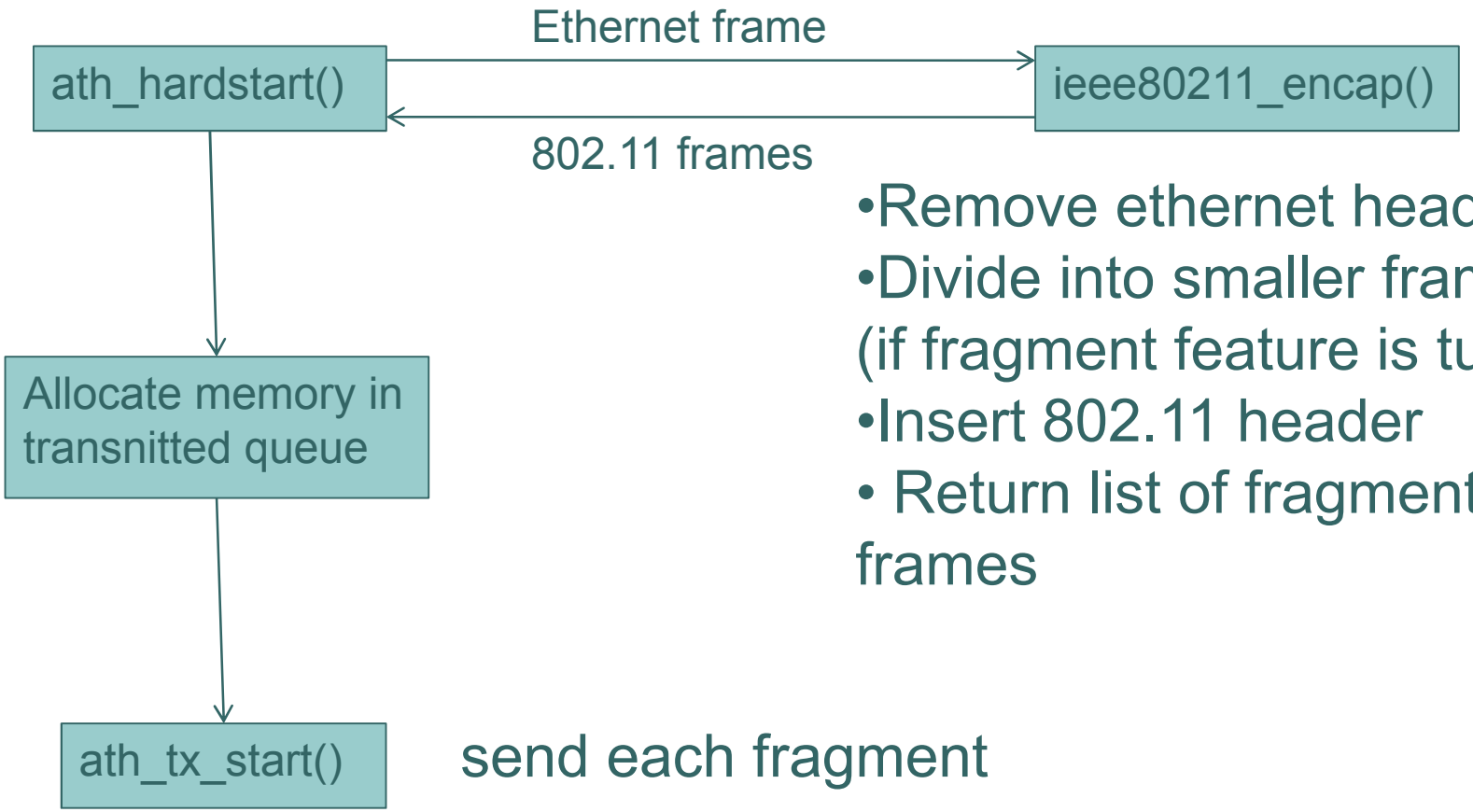
Outline

- Original project
- System fails
- Collecting information
- Debugging techniques
- Result

Possible error source

- Improper Madwifi installation
- Hardware incompatibility
- Kernel bug
- Madwifi bug

Madwifi transmission process



- Remove ethernet header
- Divide into smaller frame (if fragment feature is turned on)
- Insert 802.11 header
- Return list of fragmented frames

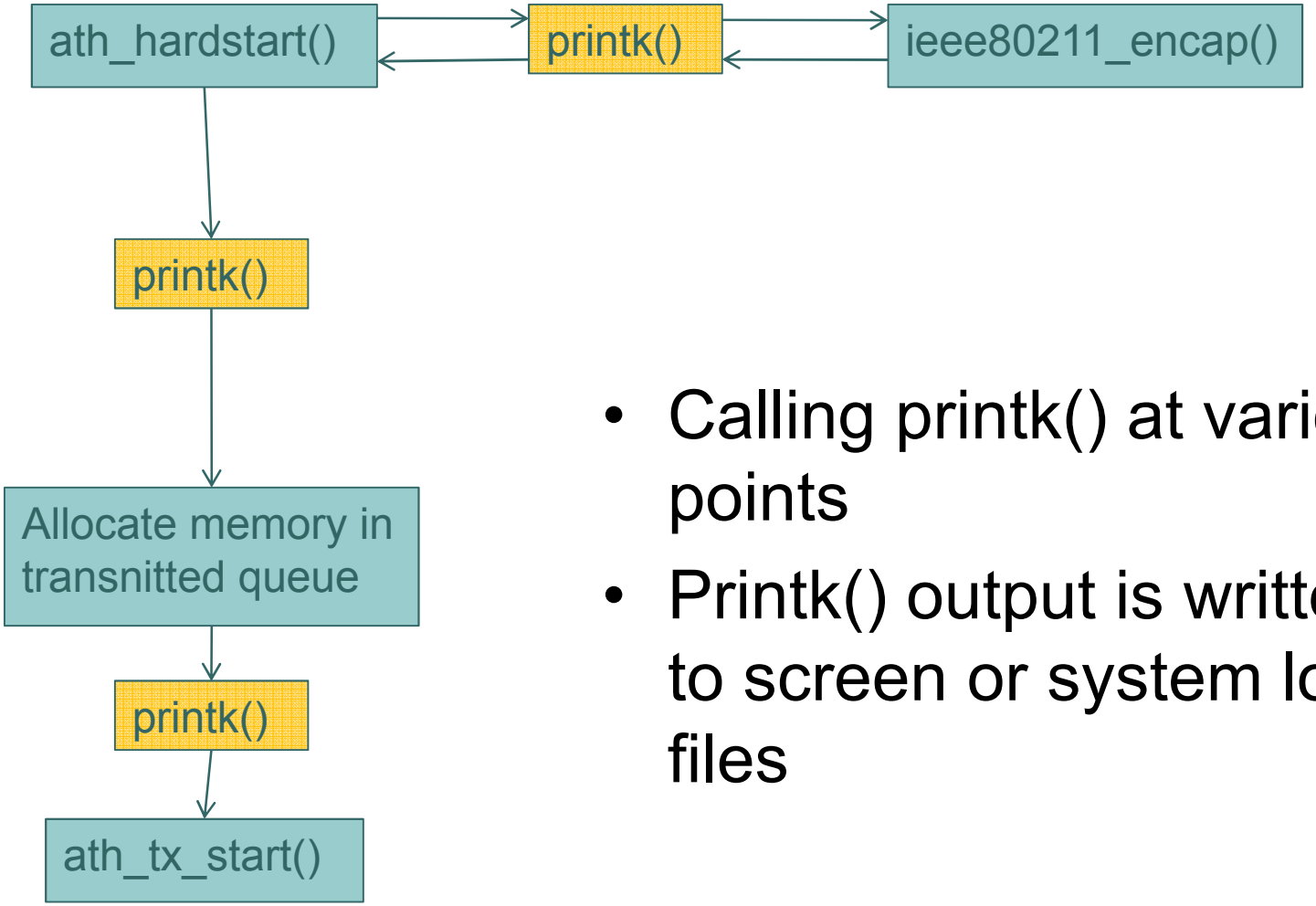
Opps messages

```
[ 4656.967047]  [<c0167740>] ? autoremove_wake_function+0x0/0x50
[ 4656.967047]  [<f85751c9>] ? soft_cursor+0x1c9/0x230 [softcursor]
[ 4656.967047]  [<c03532bd>] ? copy_from_user+0x3d/0x130
[ 4656.967047]  [<c04bc8da>] ? verify_iovec+0x5a/0xa0
[ 4656.967047]  [<c04b41fd>] sys_sendmsg+0x15d/0x290
[ 4656.967047]  [<c058a479>] ? mutex_lock+0x19/0x40
[ 4656.967047]  [<c0353189>] ? copy_to_user+0x39/0x130
[ 4656.967047]  [<c03b87f5>] ? copy_termios+0x35/0x50
[ 4656.967047]  [<c01c9ca2>] ? find_get_page+0x22/0xa0
[ 4656.967047]  [<c01304cc>] ? kmap_atomic_prot+0x4c/0xf0
[ 4656.967047]  [<c01ca036>] ? unlock_page+0x46/0x50
[ 4656.967047]  [<c01e49b8>] ? __do_fault+0x3a8/0x490
[ 4656.967047]  [<c01e6259>] ? handle_mm_fault+0x139/0x390
[ 4656.967047]  [<c04b481c>] sys_socketcall+0xcc/0x280
[ 4656.967047]  [<c058db30>] ? do_page_fault+0x160/0x3a0
[ 4656.967047]  [<c01033ec>] syscall_call+0x7/0xb
[ 4656.967047] NOHZ: local_softirq_pending 2c2
```

Outline

- Original project
- System fails
- Collecting information
- Debugging techniques
- Result

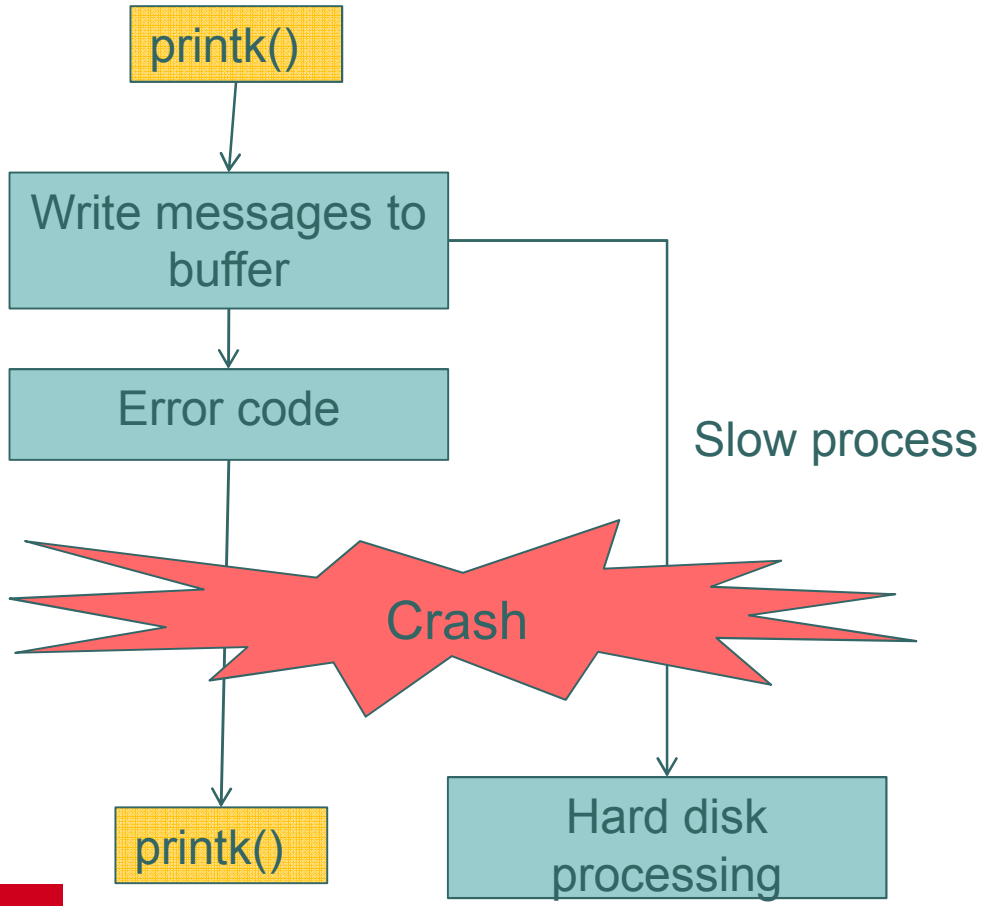
Diagnostic output



- Calling printk() at various points
- Printk() output is written to screen or system log files

Diagnostic output

- But... Printk does not help much !



Diagnostic output

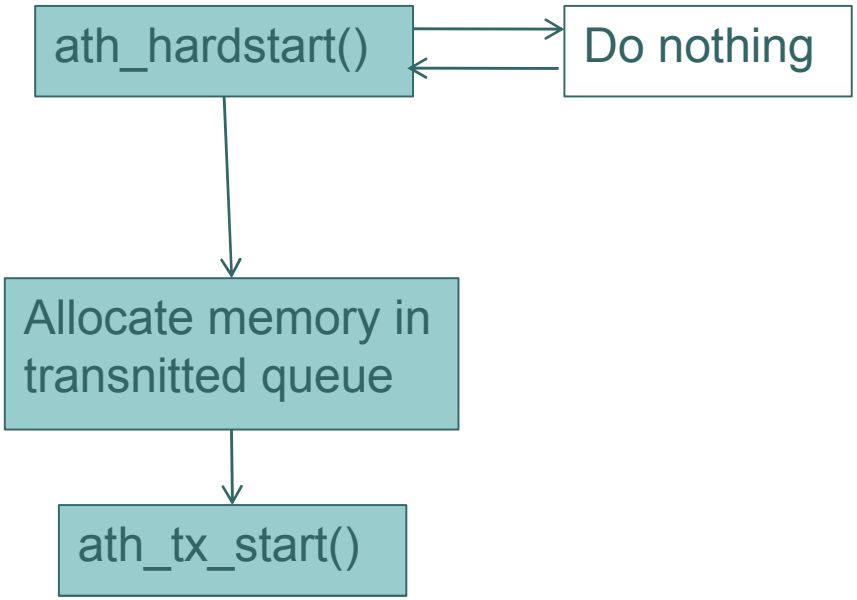
- Debug without printk()

```
int main()
{
```

```
return 0;
```

```
return 0;
```

```
return 0;
}
```



Debugging technique: watching

- Sometime, the problem can be tracked down by ... watching error messages

modprobe netconsole
netconsole=@/eth0,12345@10.0.0.1/00:E0:81:2B:0C:C1

nc -dul 12345

Wired connection

Bug

Print oops messages

Send oops messages to remote host

Stop working

Debugging technique: watching

- What I got by watching

```
root@wlan-proj-6:~# nc -dul 12345
[ 4656.358987] ------------[ cut here ]------------
[ 4656.359188] kernel BUG at /home/tung/madwifi/ath/if_ath.c:3345!
[ 4656.359438] invalid opcode: 0000 [#1] SMP
[ 4656.359649] last sysfs file: /sys/devices/virtual/sound/timer/u
[ 4656.359896] Modules linked in: netconsole configfs wlan_wep wla
[ 4656.360022]
[ 4656.360022] Pid: 4815, comm: ping Not tainted (2.6.32-22-generi
[ 4656.360022] EIP: 0060:[<fa0cb3ba>] EFLAGS: 00010286 CPU: 0
[ 4656.360022] EIP is at _take_txbuf_locked+0x10a/0x1d0 [ath_pci]
[ 4656.360022] EAX: 00000001 EBX: e97a43a0 ECX: fffffdc EDX: 0000
[ 4656.360022] ESI: e97bf638 EDI: 00000000 EBP: d8809a6c ESP: d880
[ 4656.360022]  DS: 007b ES: 007b FS: 00d8 GS: 00e0 SS: 0068
[ 4656.360022] Process ping (pid: 4815, ti=d8808000 task=f021e680
[ 4656.360022] Stack:
[ 4656.360022]  fa0eb4f4 fa0cb4c9 00000000 f03e80c0 f03e8000 00000
[ 4656.360022] <0> d8809b08 fa0d36d9 fa06554c 00000000 00000005 00
```

Outline

- Original project
- System fails
- Collecting information
- Debugging techniques
- Result

Found bug

```
ATH_TXBUF_LOCK_IRQ(sc);
for (bfcnt = 1; bfcnt < framecnt; ++bfcnt) {
    tbf = ath_take_txbuf_locked(sc); //Bug here
    if (tbf == NULL)
    break;
    STAILQ_INSERT_TAIL(&bf_head, tbf,
    bf_list);
        }
ATH_TXBUF_UNLOCK_IRQ(sc);
```

Working system

No. .	Time	packet size	Source	Destination	Protocol
2191	16.107483	368	BelkinIn_ed:a8:af	IPv4mcast_7f:ff:fa	IEEE 802
2192	16.110967	423	BelkinIn_ed:a8:af	IPv4mcast_7f:ff:fa	IEEE 802
2239	16.531173	71	HonHaiPr_85:16:c1	Cisco-Li_90:ad:0b	IEEE 802
2240	16.534913	323	HonHaiPr_85:16:c1	Cisco-Li_90:ad:0b	IEEE 802
2241	16.534921	323	HonHaiPr_85:16:c1	Cisco-Li_90:ad:0b	IEEE 802
2242	16.534930	323	HonHaiPr_85:16:c1	Cisco-Li_90:ad:0b	IEEE 802
2244	16.536302	251	HonHaiPr_85:16:c1	Cisco-Li_90:ad:0b	IEEE 802
2246	16.537887	1098	Cisco-Li_90:ad:0b	HonHaiPr_85:16:c1	IEEE 802
2349	17.532236	71	HonHaiPr_85:16:c1	Cisco-Li_90:ad:0b	IEEE 802
2350	17.535038	323	HonHaiPr_85:16:c1	Cisco-Li_90:ad:0b	IEEE 802
2351	17.535050	323	HonHaiPr_85:16:c1	Cisco-Li_90:ad:0b	IEEE 802
2352	17.535063	323	HonHaiPr_85:16:c1	Cisco-Li_90:ad:0b	IEEE 802
2354	17.536422	251	HonHaiPr_85:16:c1	Cisco-Li_90:ad:0b	IEEE 802
2355	17.537992	1098	Cisco-Li_90:ad:0b	HonHaiPr_85:16:c1	IEEE 802

Conclusion

- Listen to the kernel
- Bugs can happen anywhere
- Bug fixing is fun (if you can fix it)

Thanks to

- Grenville
- Lachlan
- Hai
- Kewin
- Jason
- David