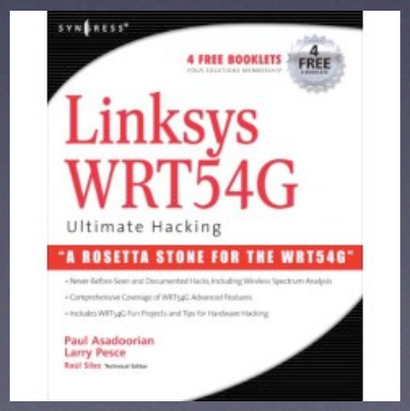
Rogue APs for "Penetration Testers"

A ~~tongue-in-cheek~~ soldering iron-in-hand look at hiding rogues

Introduction

- Penetration tester for a Rhode Island based consulting company
- Security in Healthcare
- PaulDotCom Security Weekly - http://pauldotcom.com
- Co-Author of Linksys WRT54G Ultimate Hacking from Syngress Publishing



!= 0-day

- Rogue APs are not new!
- Just a different way to think about it

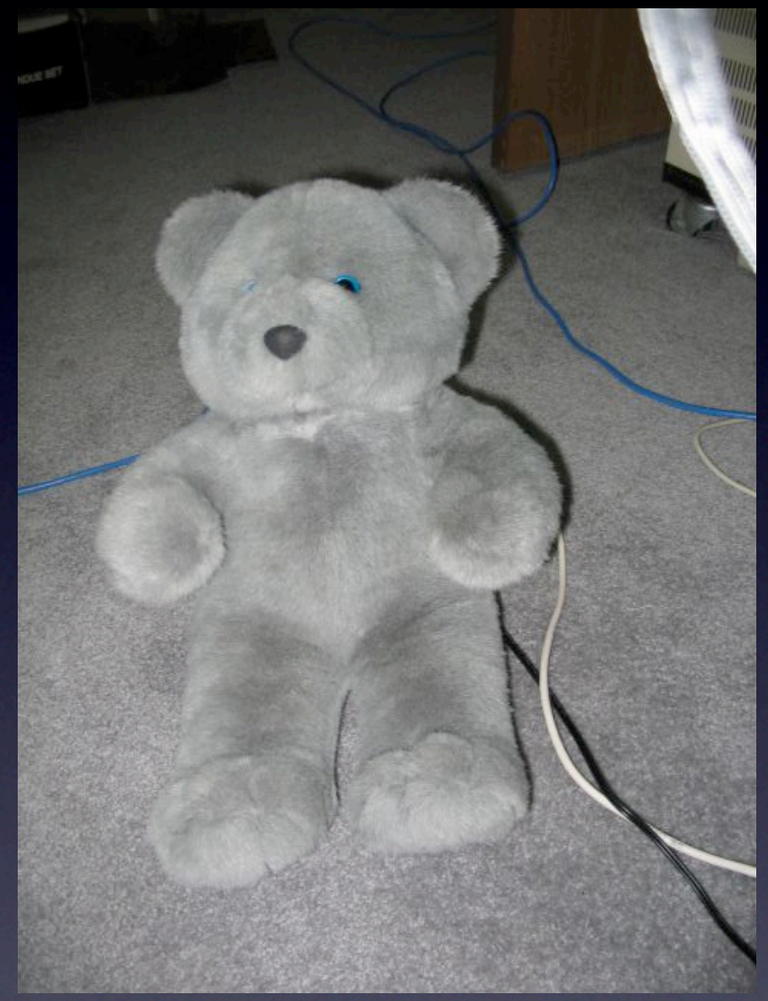
Inspiration

- A man who stuffs stuff inside of other stuff: (and no, not like that)

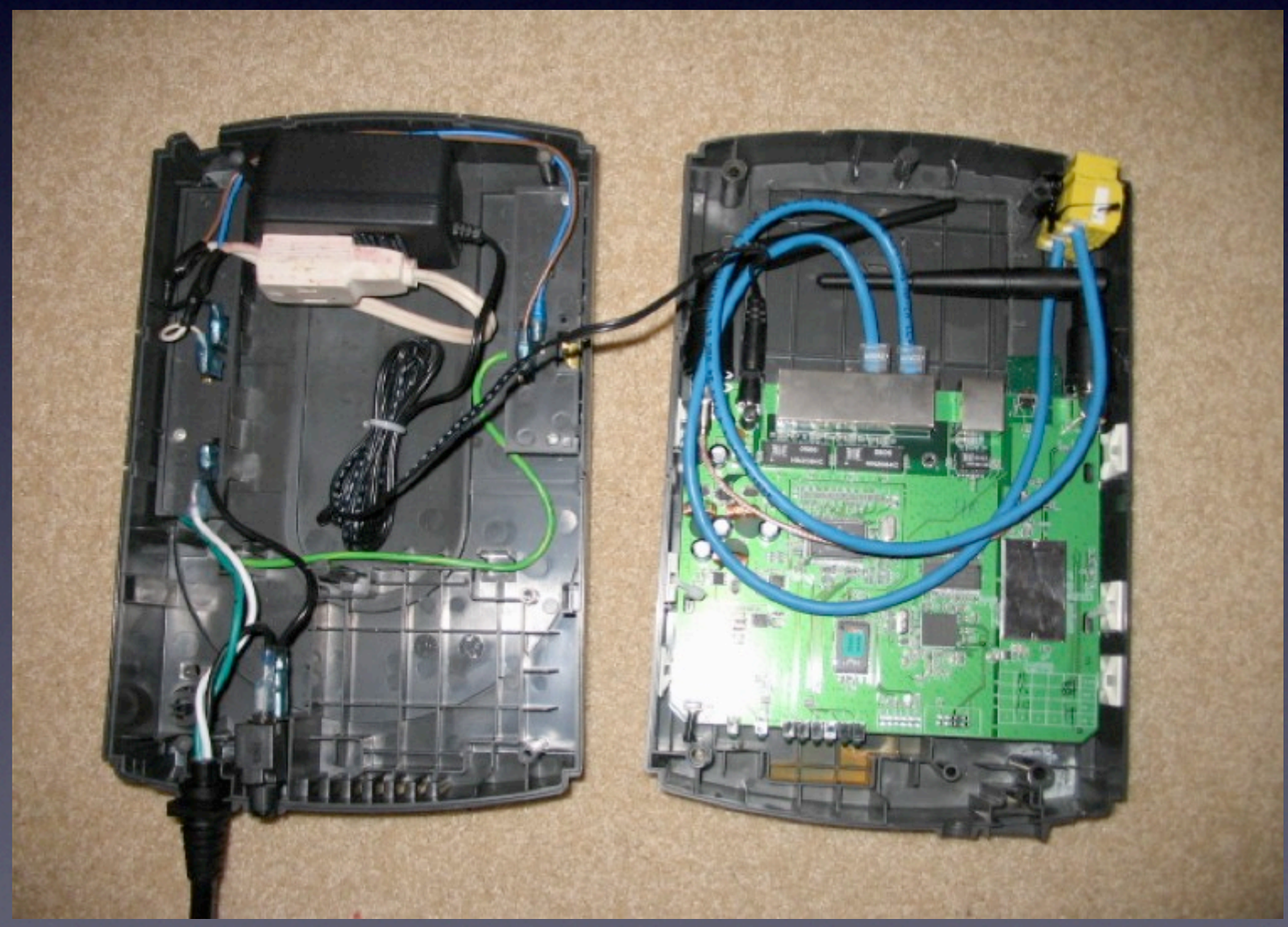

RenderMan

The first hack

- Not something found in an office environment

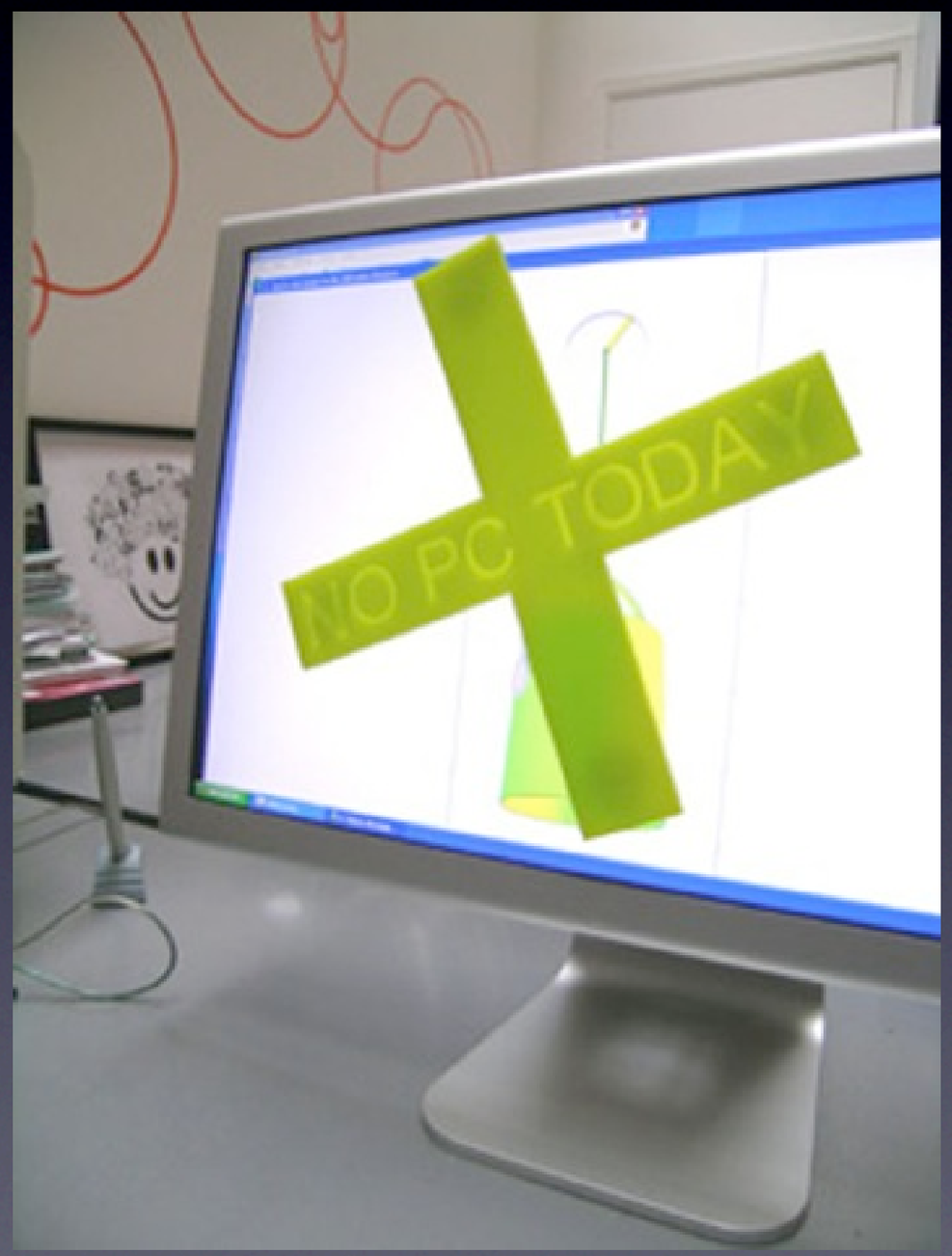


Now that's better...



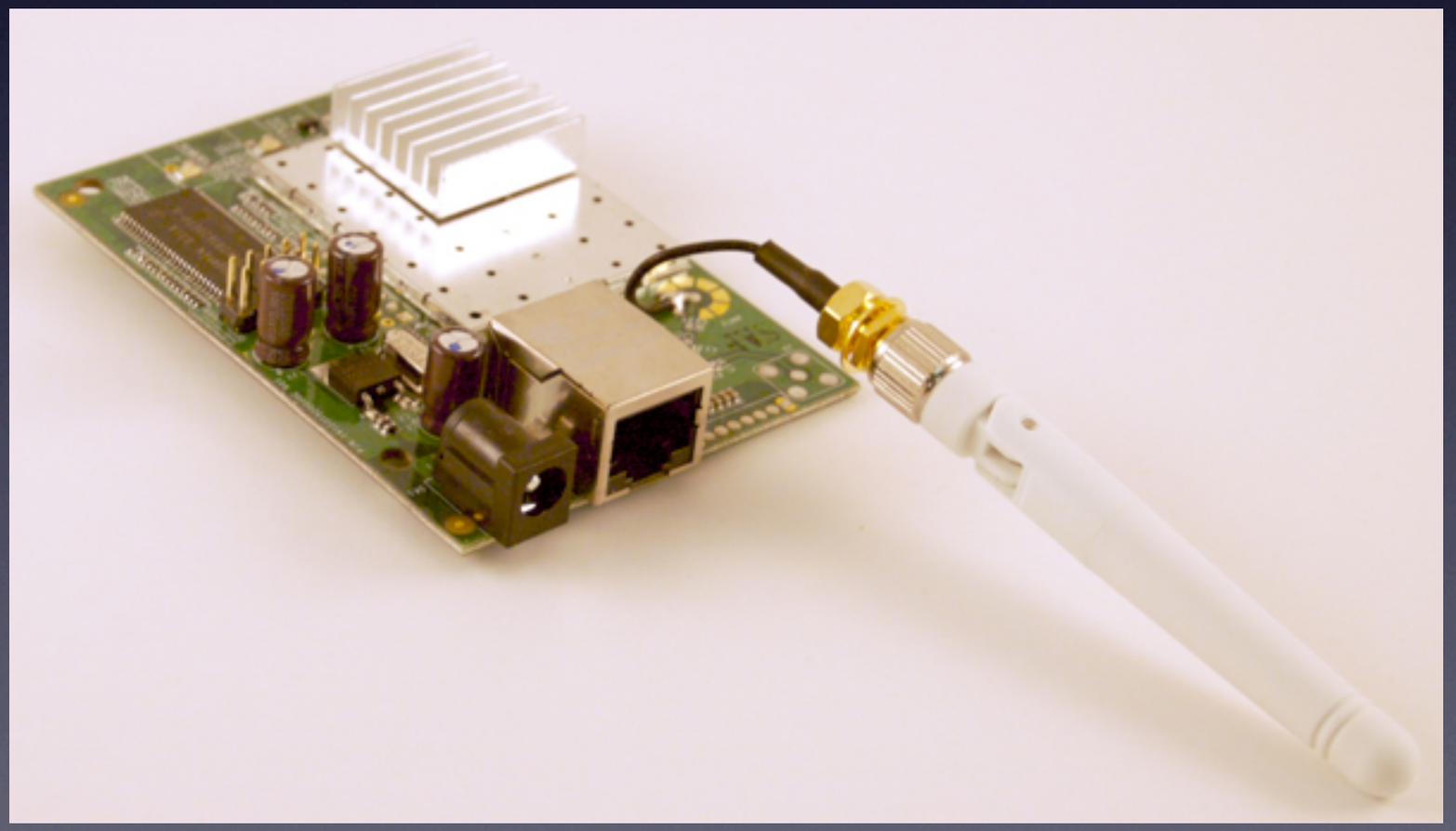
So, what else?

- What else is in a typical office environment that should be connected to a network
- Leave out the obvious - PCs and Laptops
- Now with more evil, more bastard!



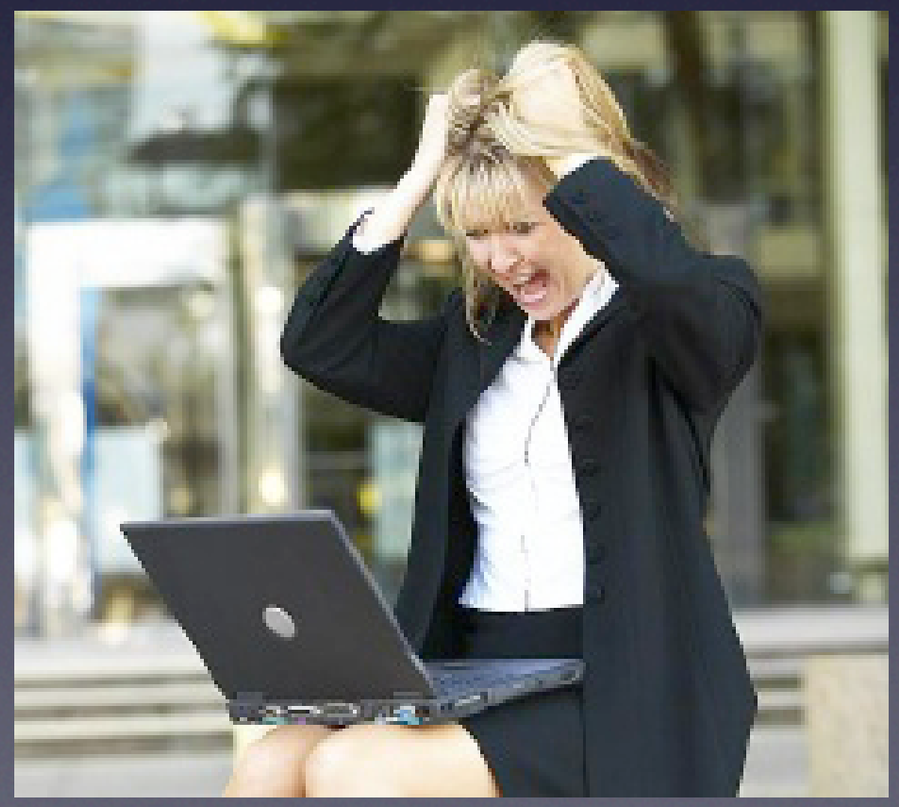
First, the AP

- LaFonera - FON
- Supports OpenWRT



One ethernet?

- Help desk, my device is not functioning
- How do we make the AP and device function?
- We need more ports!



Insert one hub...

- Netgear EN104

More Challenges?

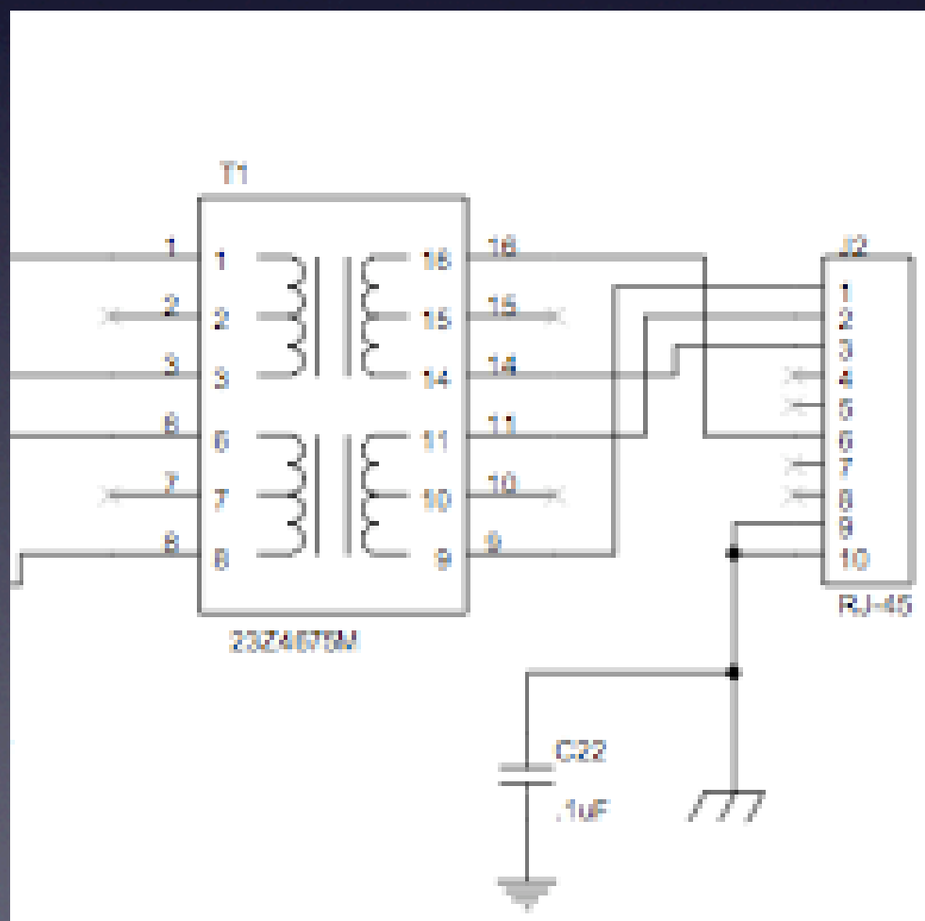
- Keep host device functional
- Size
- NAC
- Sacrificial Device
- And more...

Creative soldering...

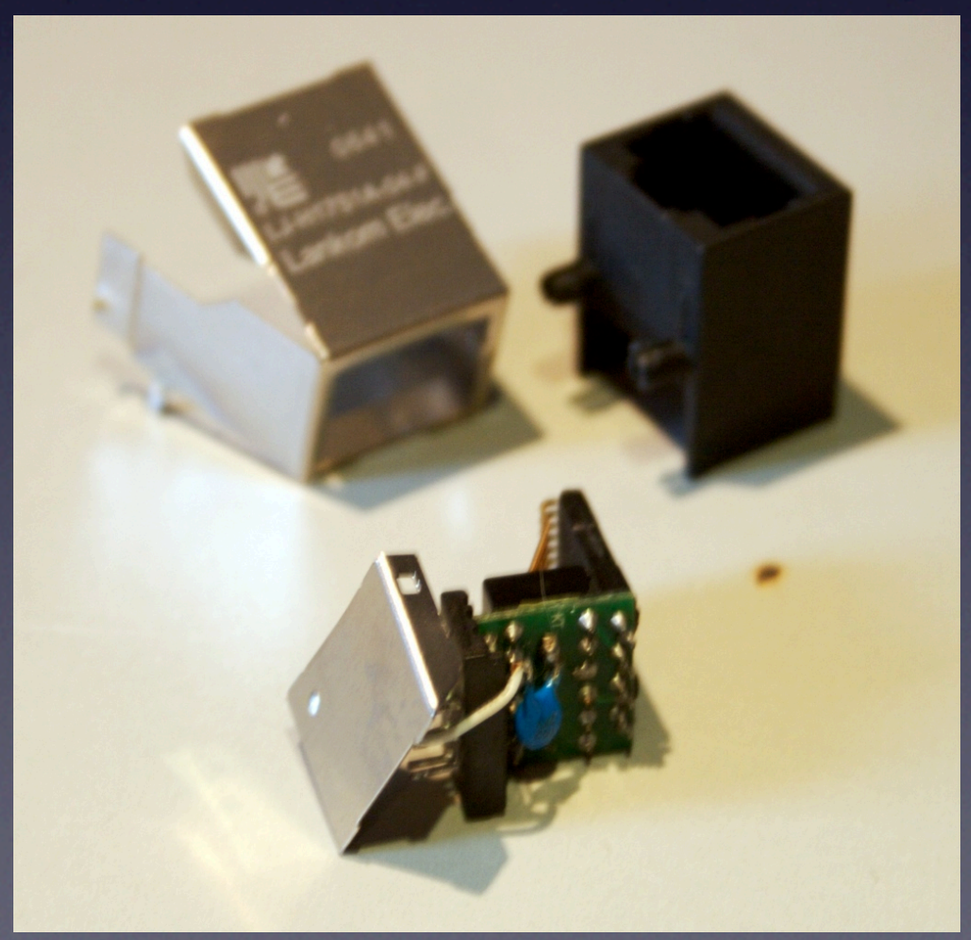
- To make our device small, we need to have some fun
- Move/remove all ethernet ports and power connectors (too big!). Lay down capacitors where needed.
- Trim boards, and jumper the bits we remove
- Ethernet for La Fonera, and for host!

Ethernet ports

- One of the most difficult portions
- Electrically isolated
- Port removal and disassembly!



RJ-45 10BASE-T



You look like a Dork!

Power

- Fon needs 5v DC, Hub need 5v DC
- Don’t want extra cables
- Find “vampire power” internally
- Matching voltage?

Even easier?

- The NEW La Fonera! - The FON+

Gaining access via Wireless

- Our own config, high risk
- Similar to corporate config, moderate risk
- Identical to corporate config, low risk
- Timed config change, moderate/low risk

Let's start talking "hosts"

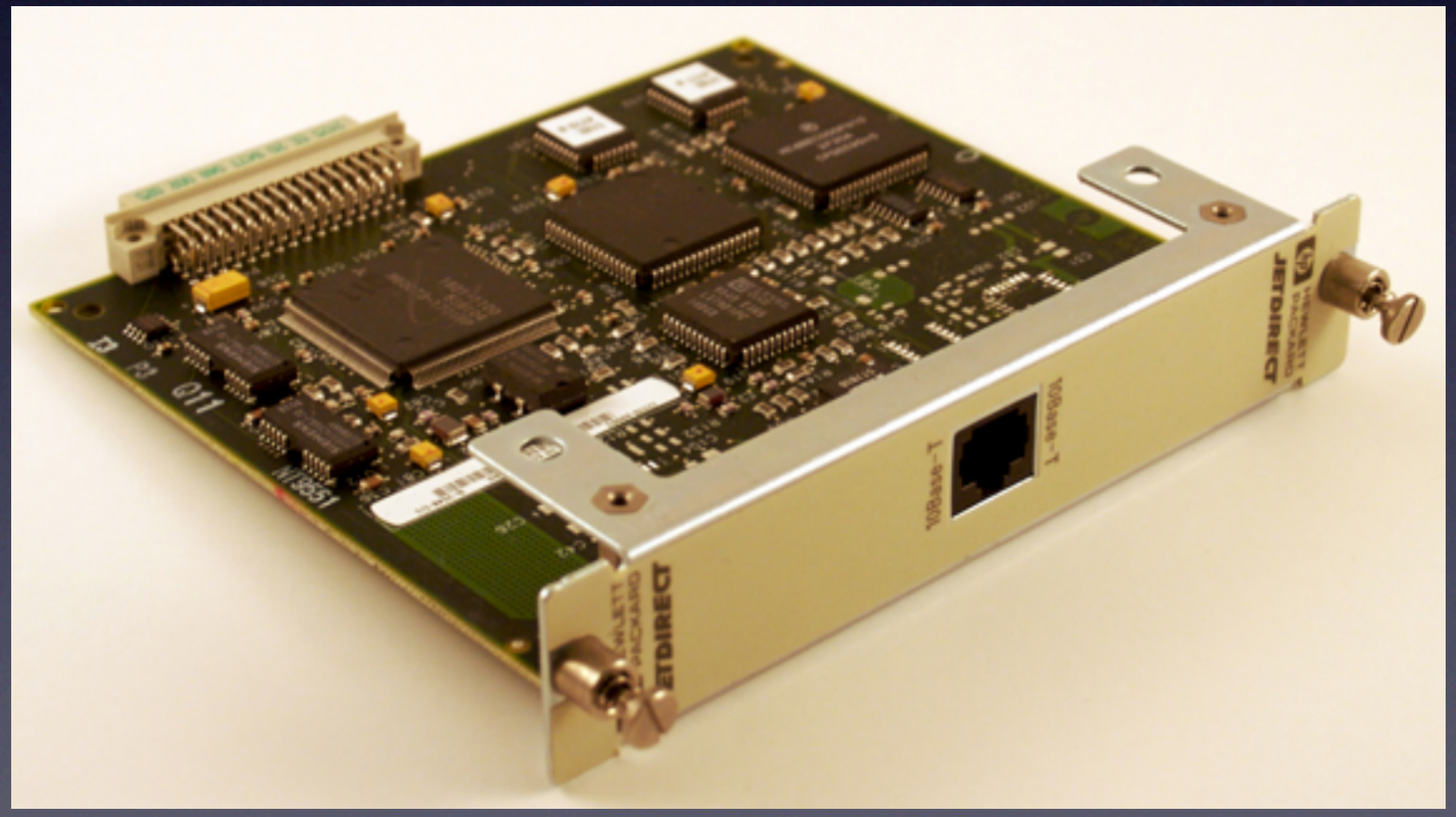
- Now that we have our requirements...
- What can we find in an office environment?
- Time to add the more evil and more bastard!

Printers!

- One of the most ubiquitous pieces of tech in most offices

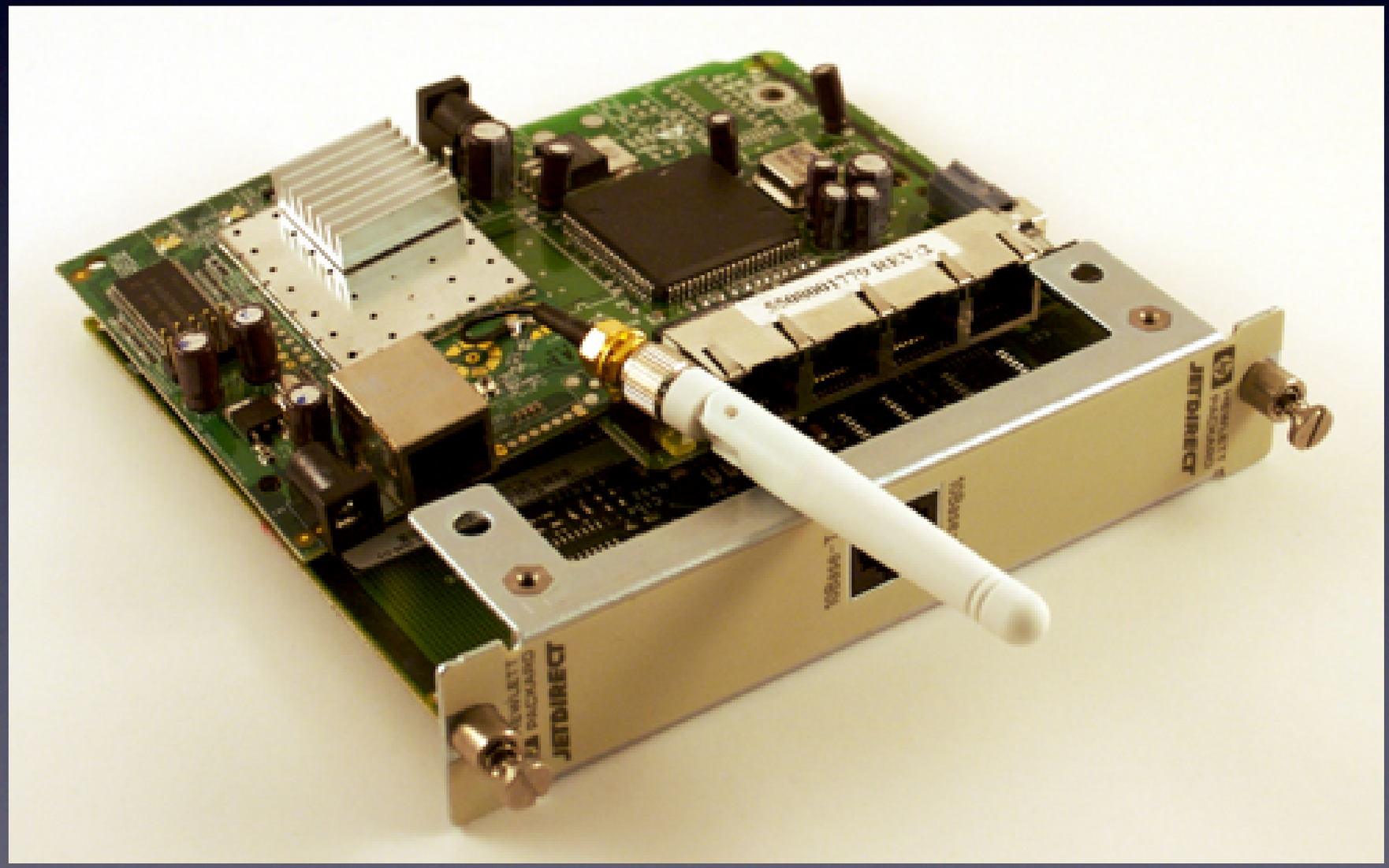
Mmmm, ethernet

- Let's start with the beginning: the HP MIO



This should be easy..

- Look ma, plenty of room!

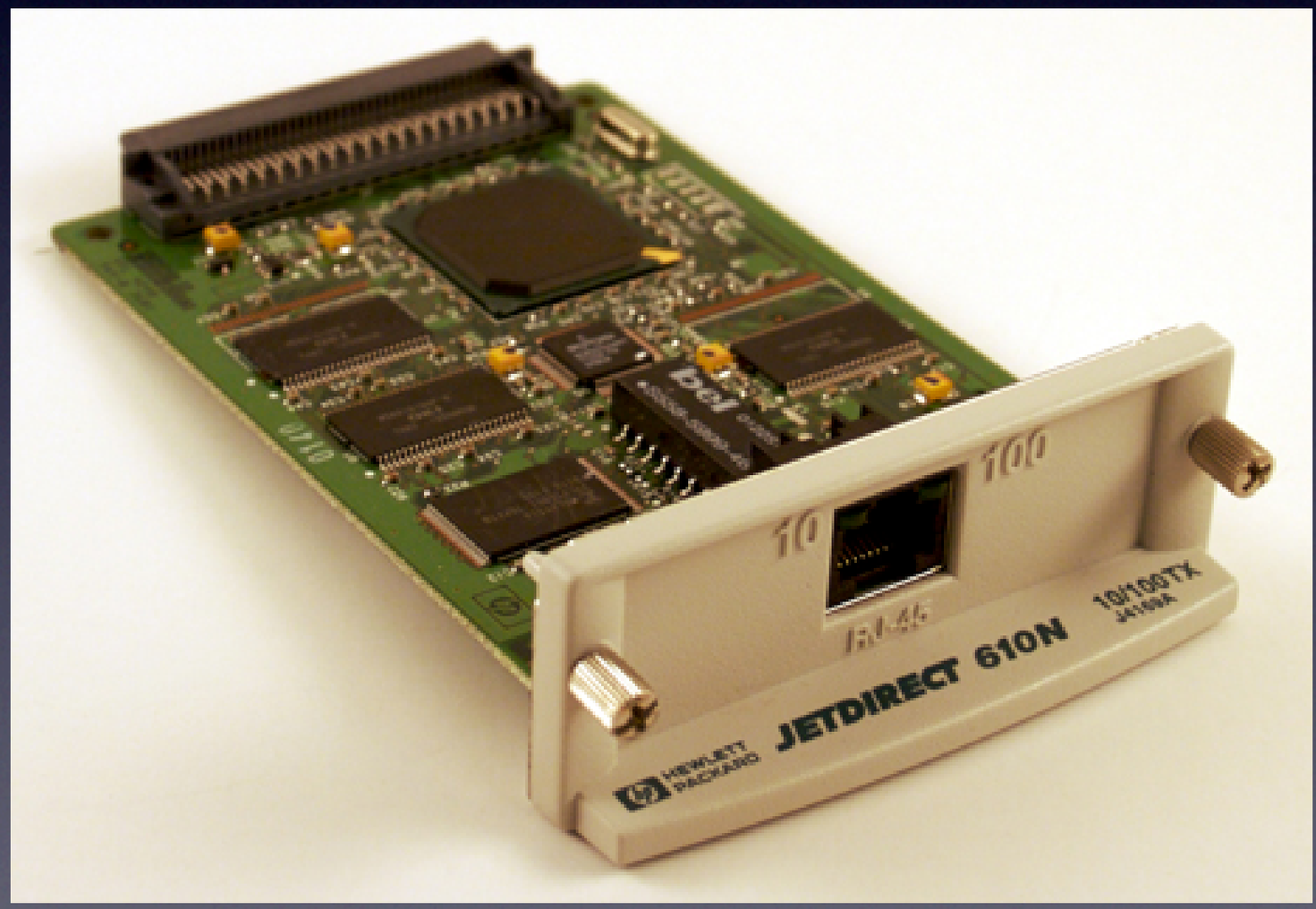


Old tech

Dead Printer Storage!

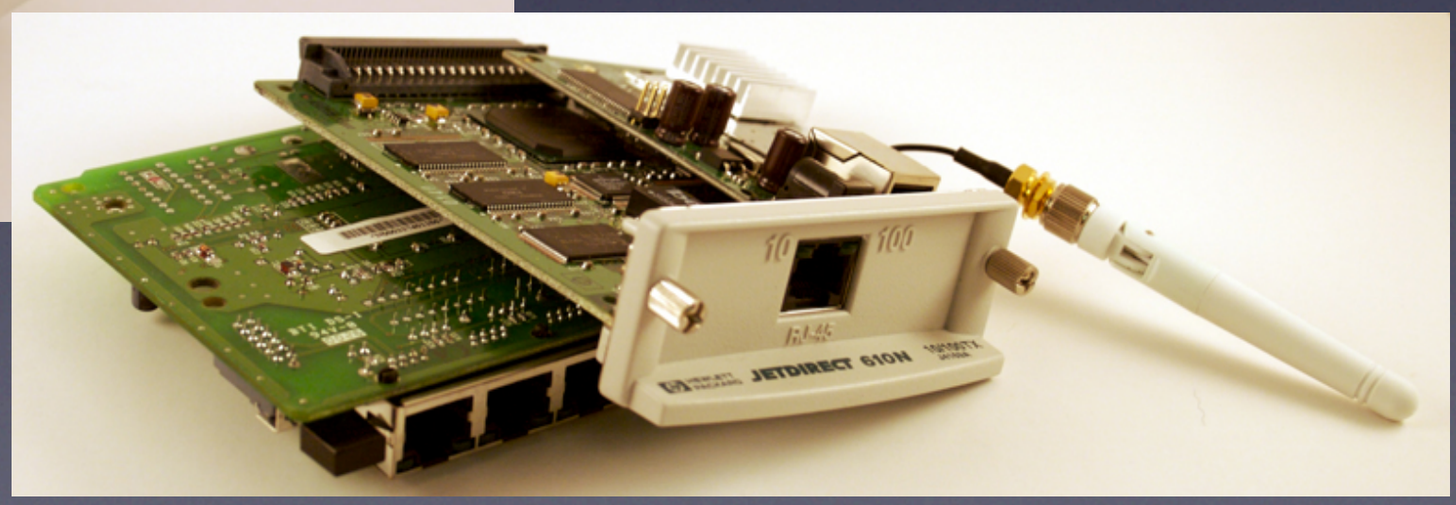
E-I-E-I-O?

- HP's upgrade to MIO - EIO!

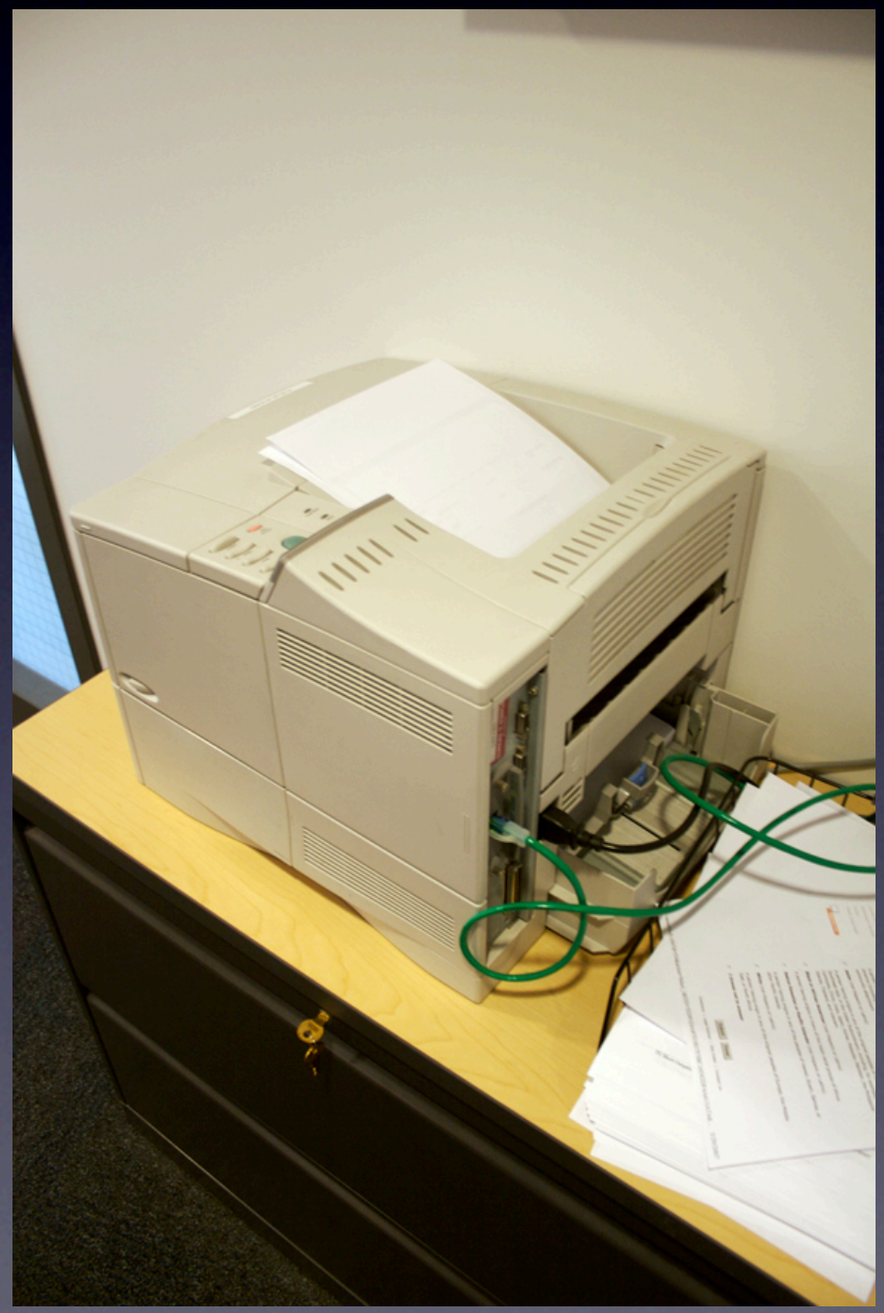


Tight fit...

- This is where the real creative soldering/ cutting comes in...



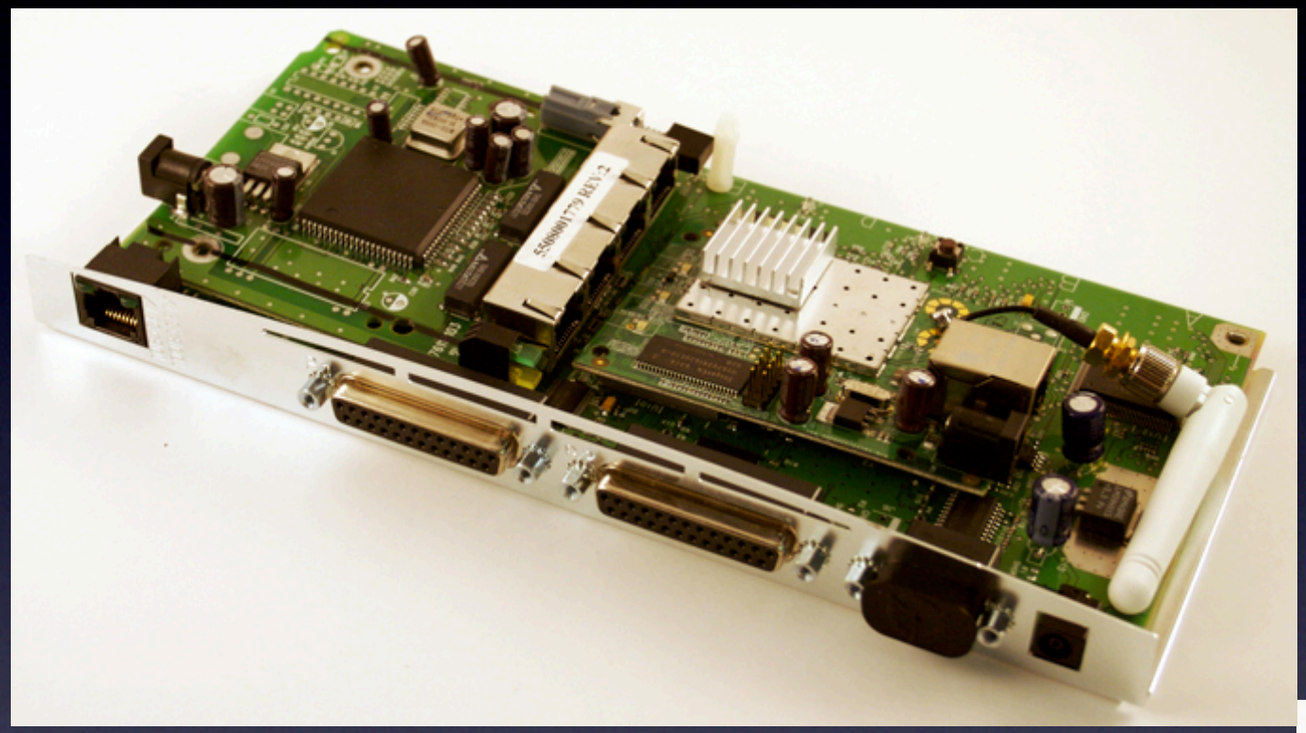
The fun we could have had...

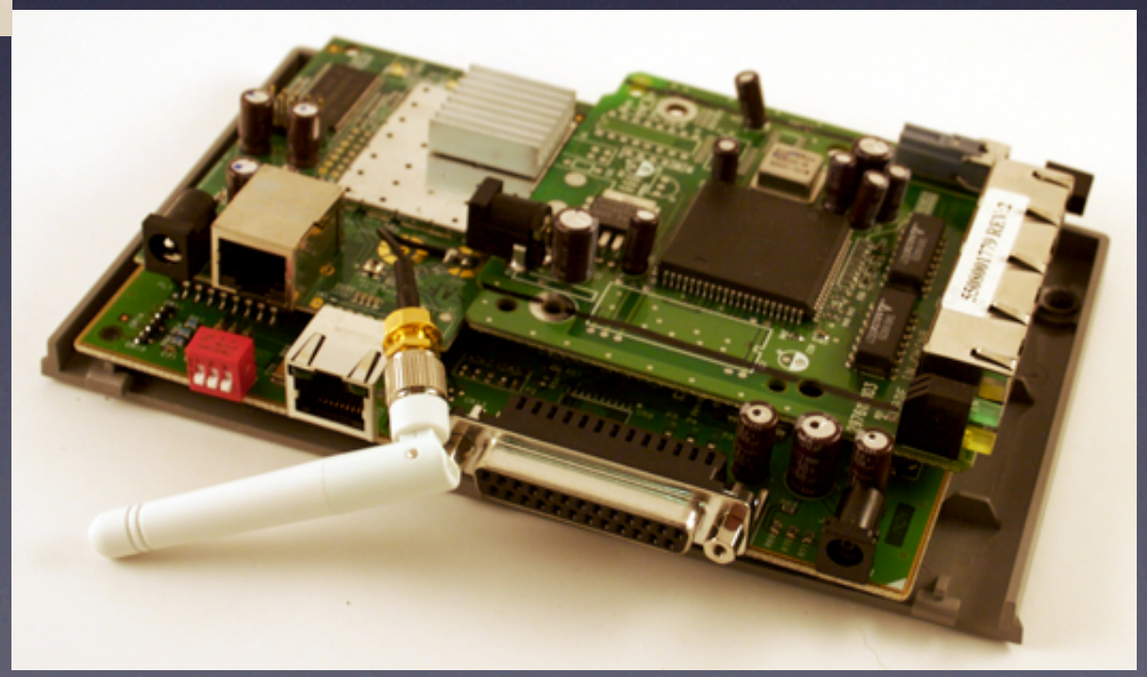


...if only it would work

But wait, there's more!

Will it ~~blend~~ fit?





Old tech?

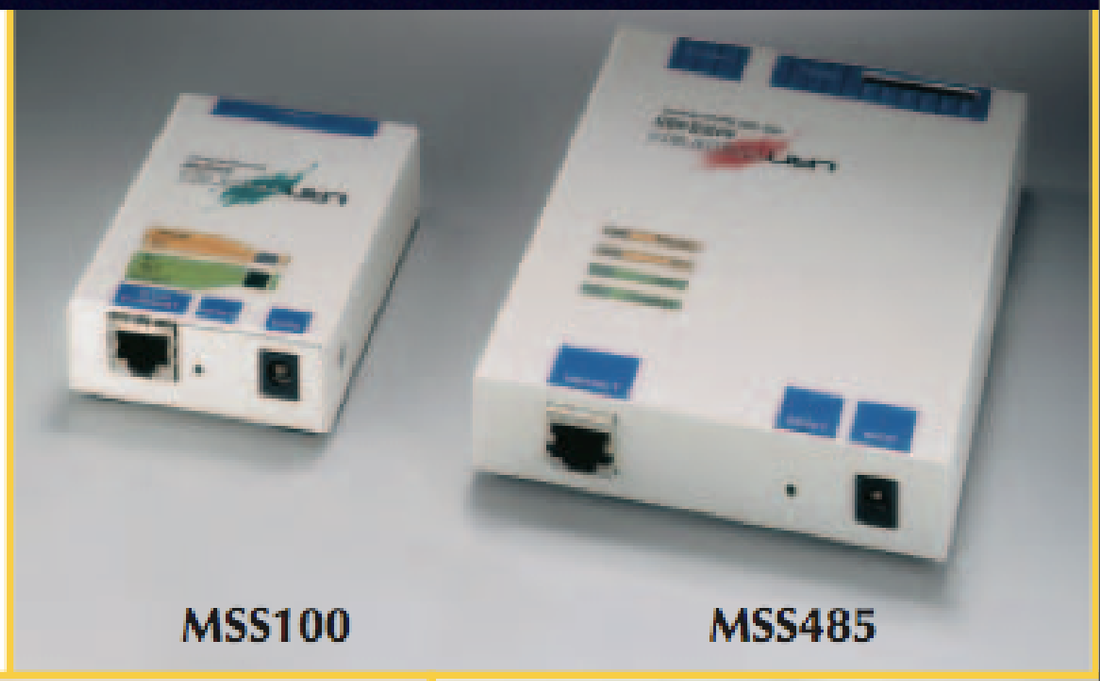
Ok, what next?

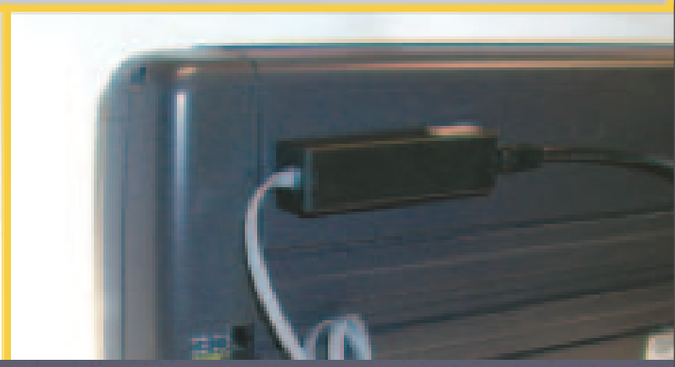
Multifunction devices!

- More ethernet!
- About EIO form factor
- Canon, amongst others
- Print, Copy
- Network Scan and Fax!

What about here?

All signs point to yes!





Or here?

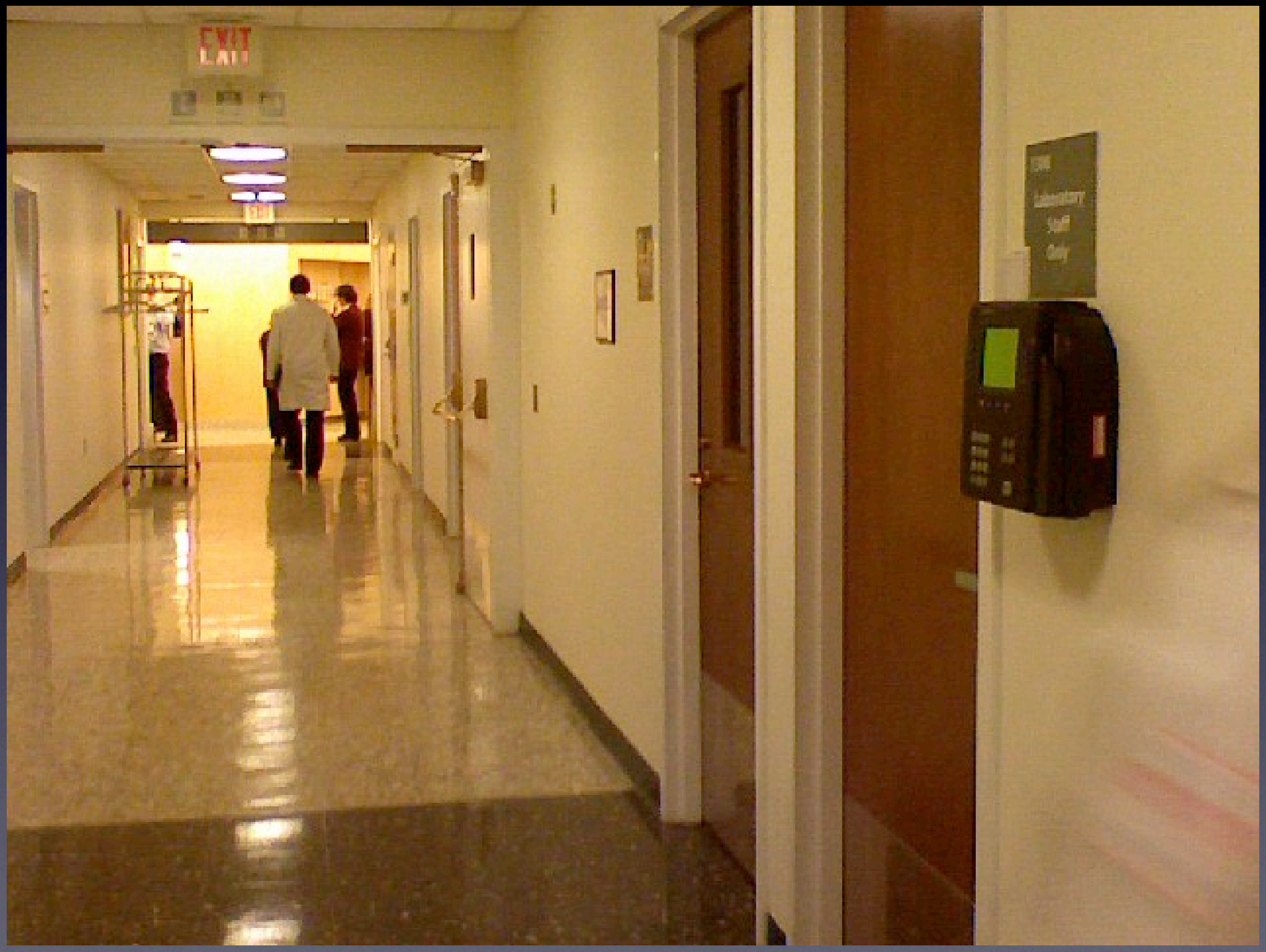
Alarm Panel

- UL 508 Listed, Industrial Control Equipment
- C-UL Listed, CSA 22.2 No. 14-M91, Industrial Control Equipment
- UL 1604 Listed, CSA Standard C22.2 No. 213-M1987, Non-Incentive Electrical Equipment for use in Class I, Division 2, Hazardous Locations (Groups A, B, C, D)
- UL 864 Recognized Component Control Units for Fire-Protective Signalling Systems (EIS8-100T and EIS6-100T/FT only)

Or here?

Climate Control

Or here?



Timeclock?


KRONOS
KRONOS
F1 F2 F3 1 2 3
F4 F5 F6 4 5 6
F7 F8 F9 7 8 9
F10 F11 F12 * 0 #
+ AM − PM NEXT PREV. CLEAR ENTER
KRONOS


ADP
3:00 PM
Maintenance Mode
Clock Setting
Display Setting
Audio Setting
Date/Time Setting
More...
ESC

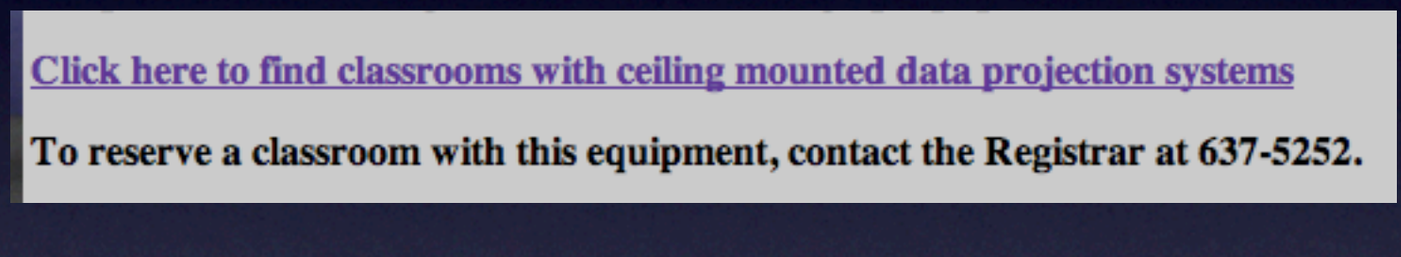
You can count on it

Meetings...

I can see the light!

Where can in find one?

- Search Google:


Click here to find classrooms with ceiling mounted data projection systems

To reserve a classroom with this equipment, contact the Registrar at 637-5252.

- Take a trip:


NORTH CENTRAL COLLEGE *Naperville, IL*

Or here?


Proud Member
HACK NAKED
WILL STOP FOR WIFI
31337
I your wireless network.
Your RF is showing
FAIR USE HAS A POSSE
DEF CON
pskl
MP3 is Not a Crime

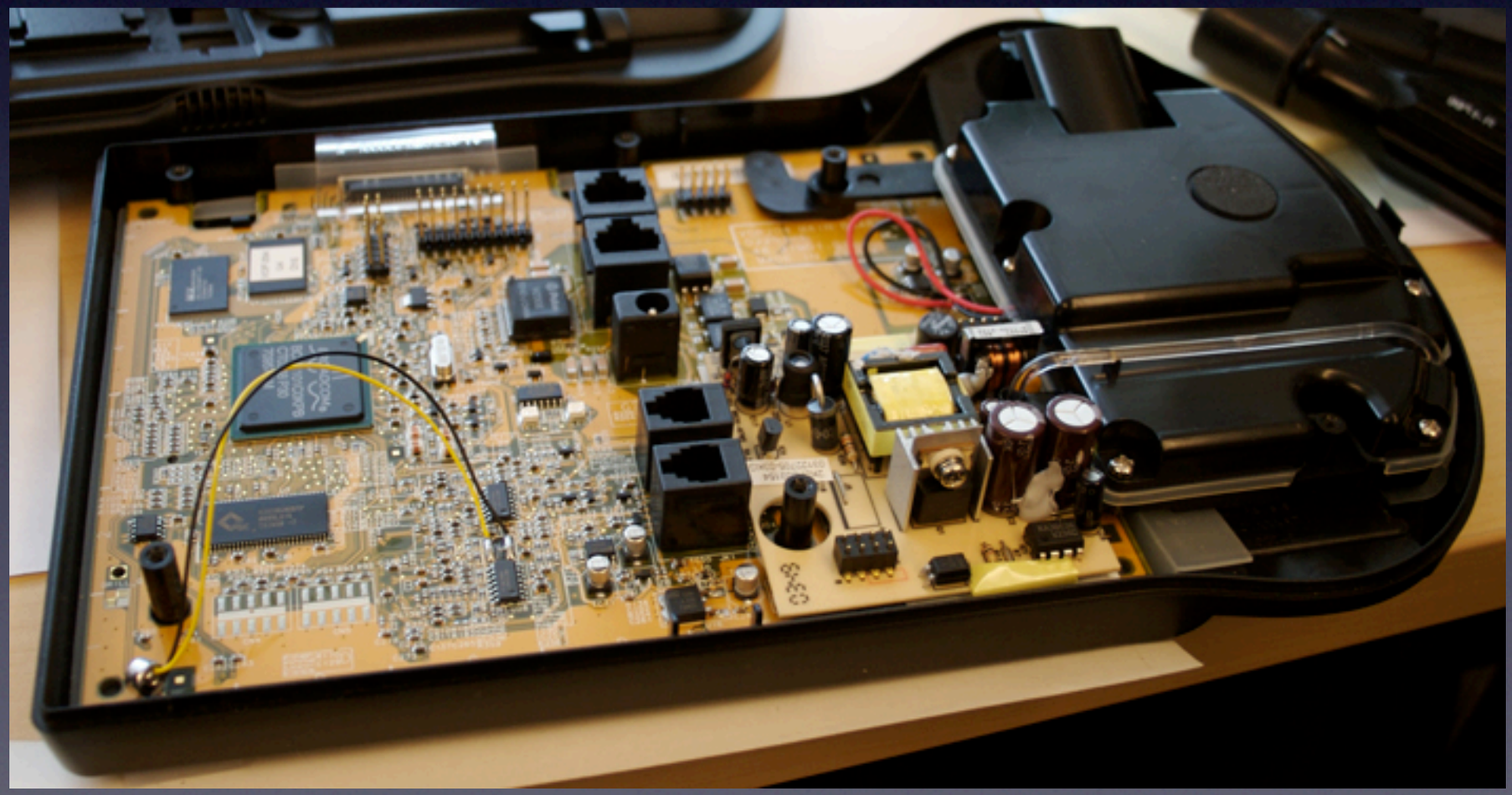
Hmmm...

Or here?

VOIP!

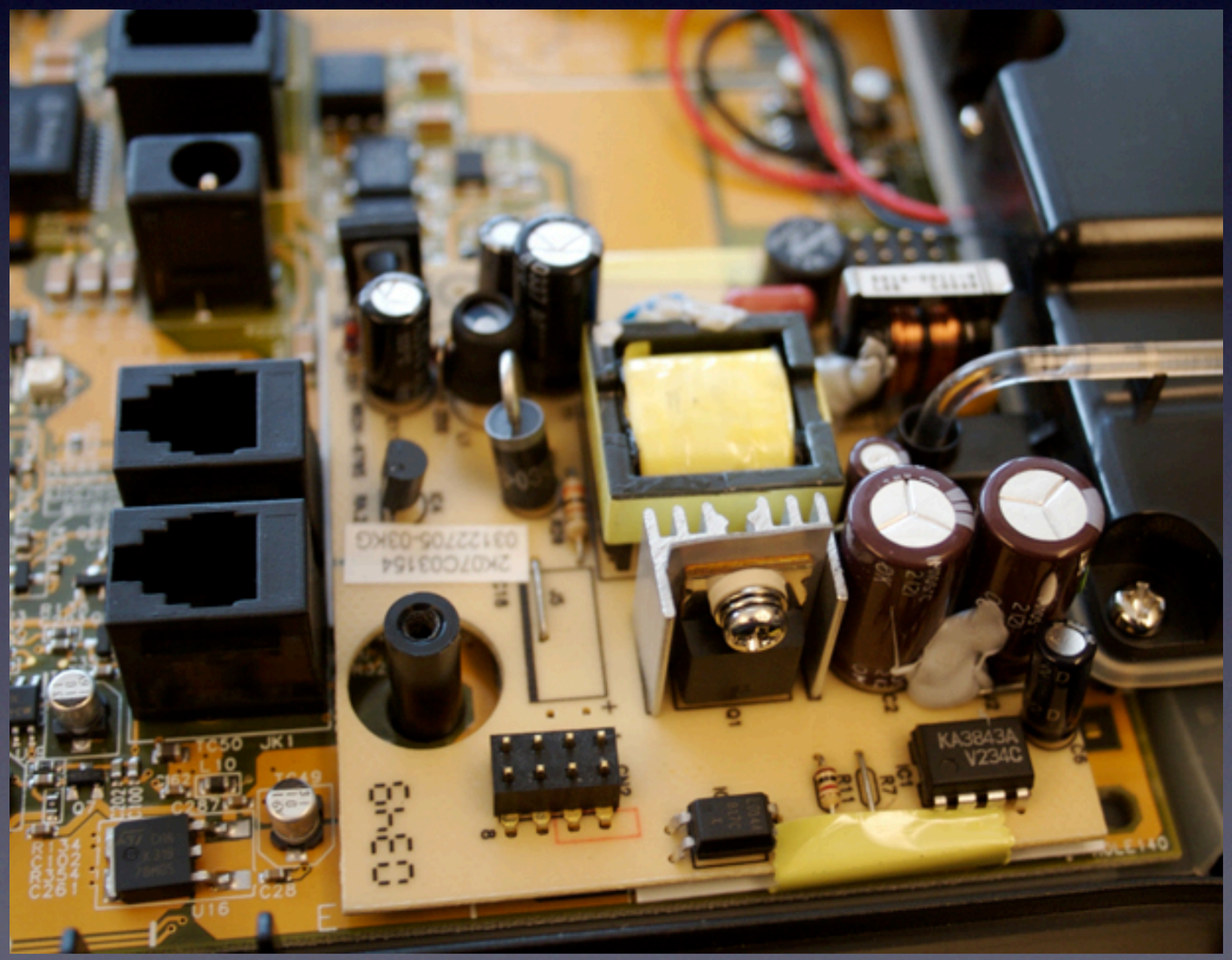
The insides..

- 2 Ethernet ports
- Power via POE

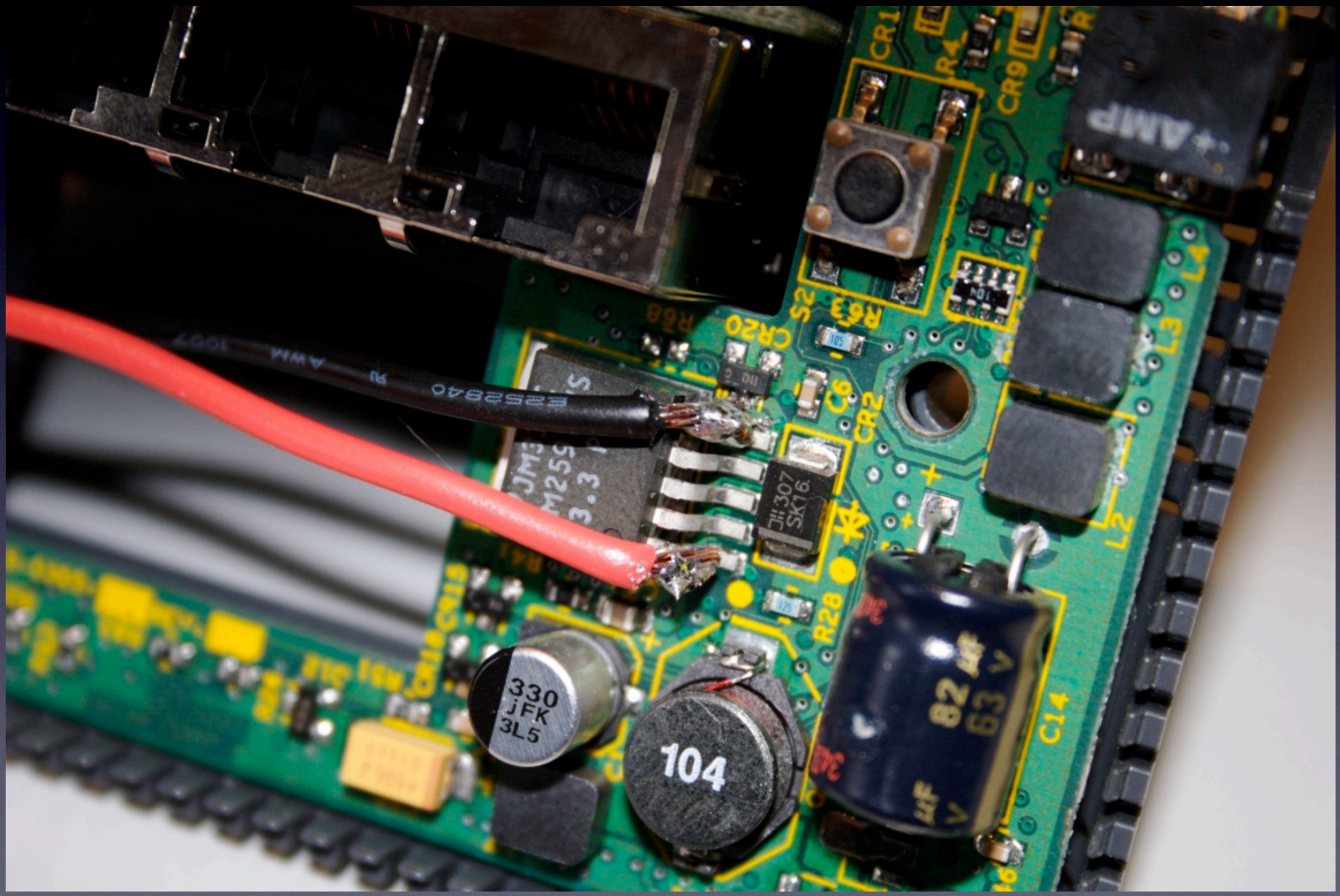


But...POE

- 802.3af requires special signaling
- What about down stream after all that has been done for us?



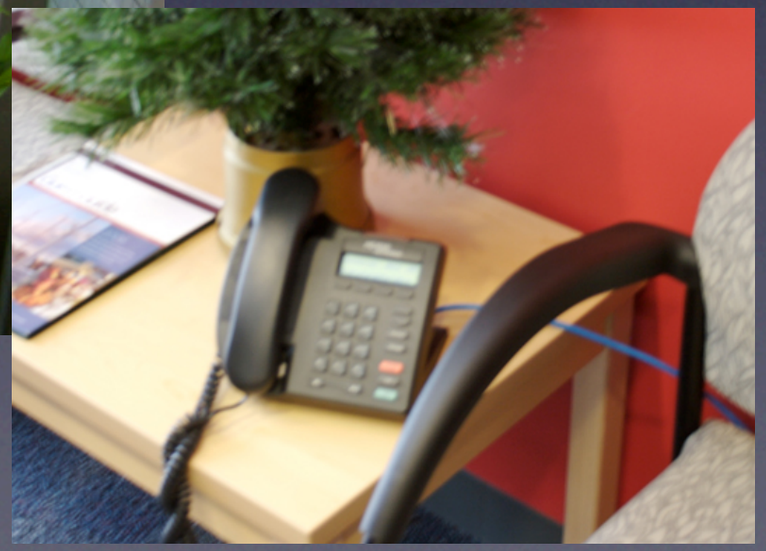
Tapped in the head



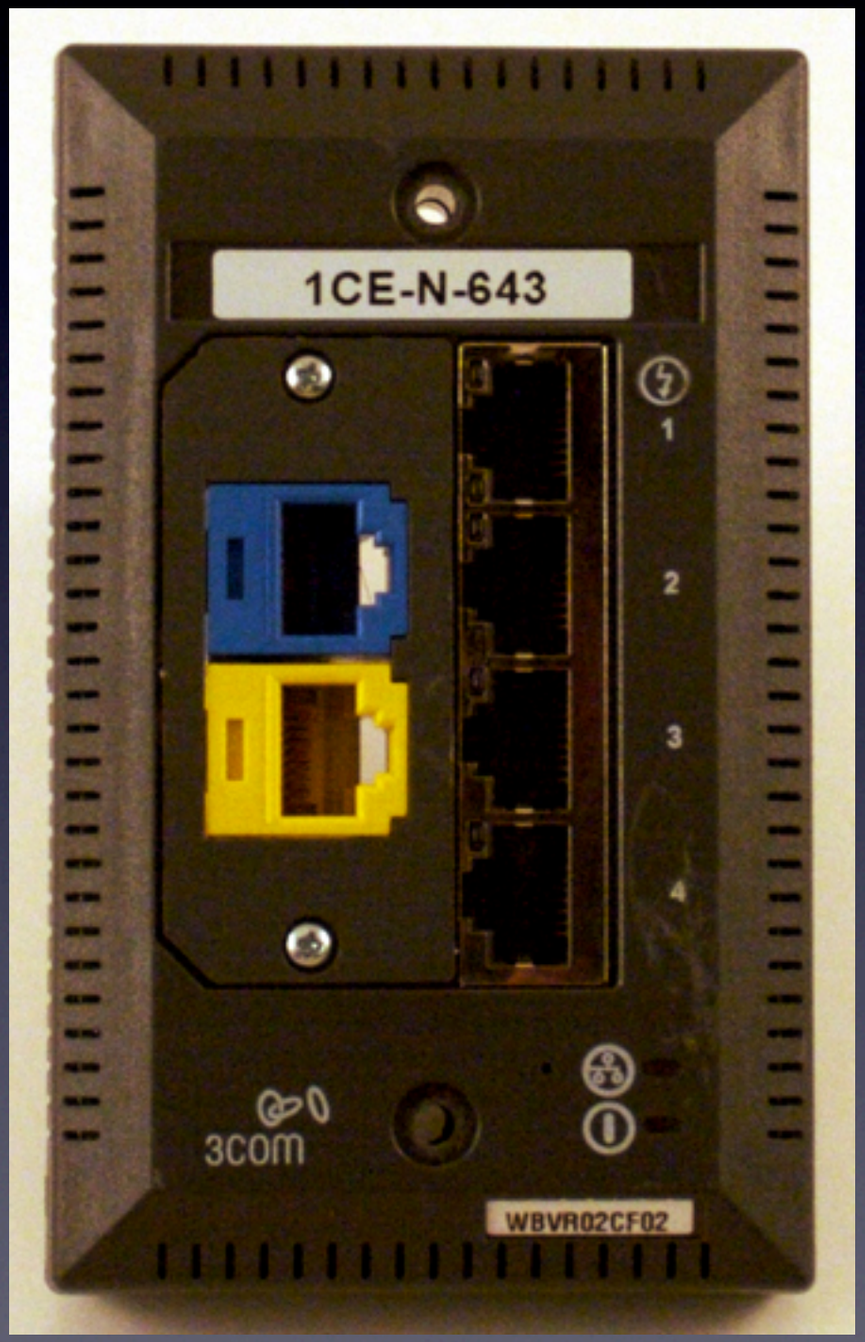
Secure area?

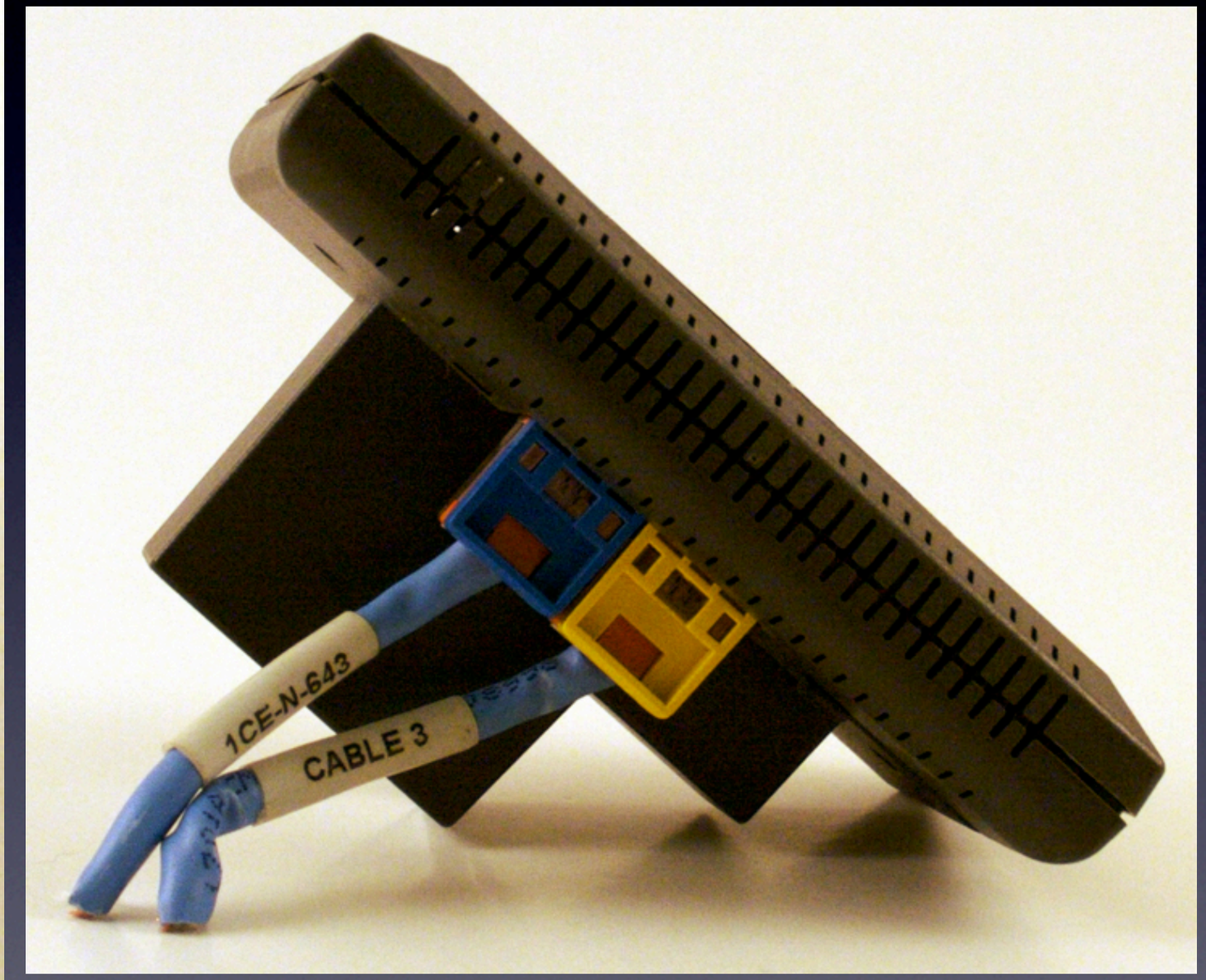
- But Larry, those phones are in a “secure” area!
- Locked door, restricted, supervised access.

Keep guests happy...

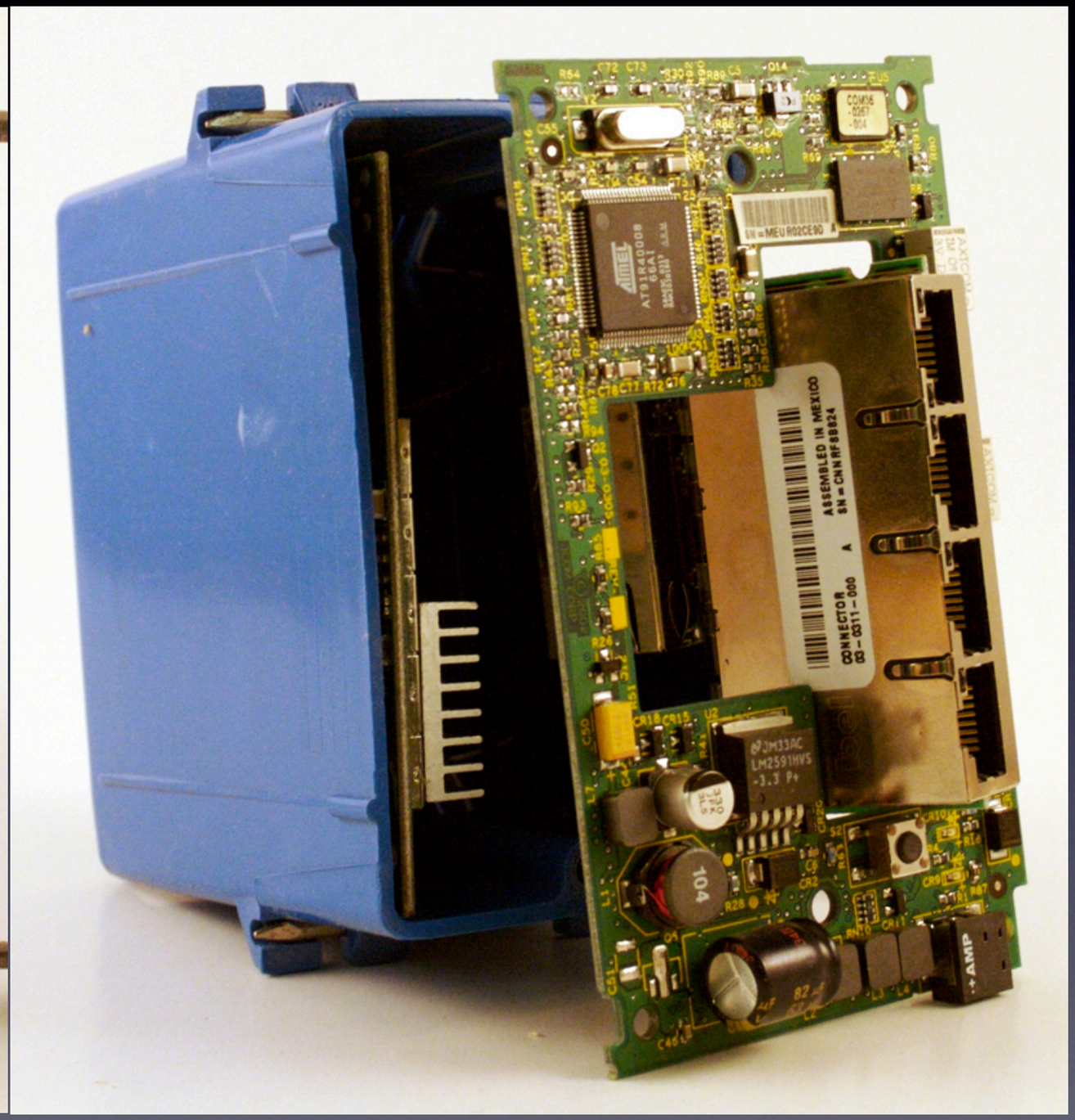


...even this...





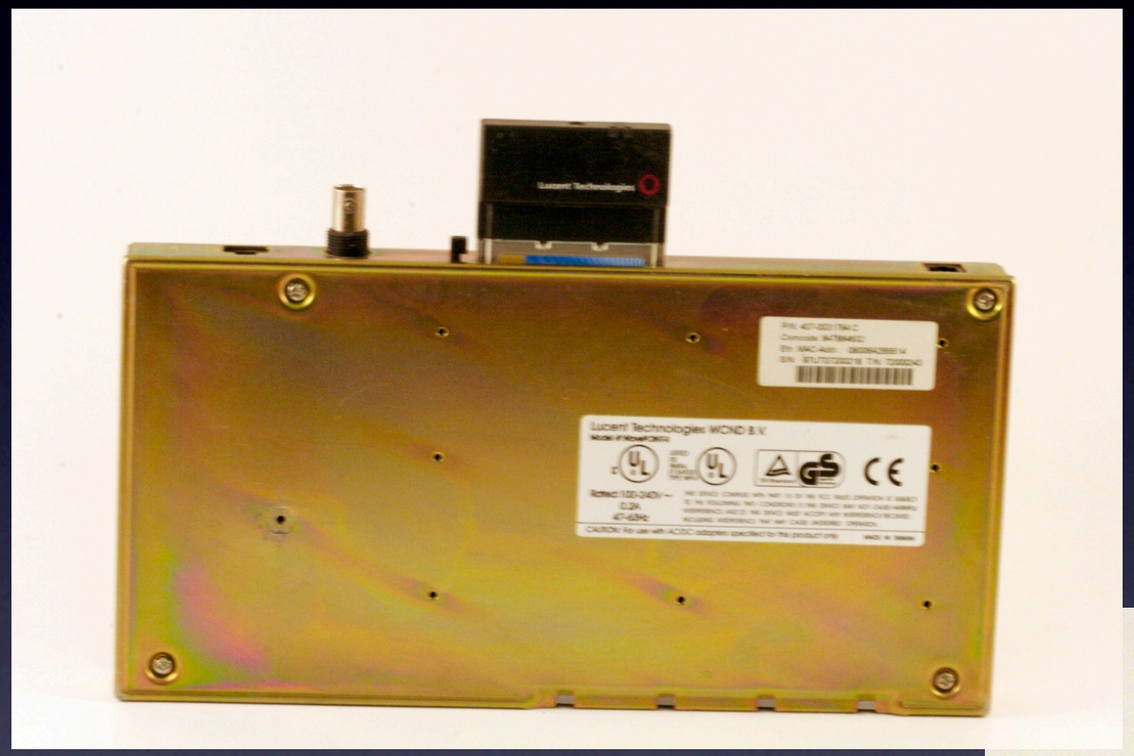
...can turn into this



But what about...

- We've covered a bunch of office technology.
- But what about wireless APs!?

This looks fun!



Just a few examples

- Loads of APs available
- Too many to discuss
- A few I’ve seen recently

Conclusion?

- Plenty of items in an office environment to deconstruct
- Often great places for APs
- How many will find a device that looks and acts just like it is supposed to, but with a surprise?

A little different

- Use OpenWRT to create a WDS (or WET)
- Bridge AP to wireless, connect via same/ times wireless
- Hide it
- ?????
- Profit!?

Endless possibilities

- If it has power, we can tap it
- There's always a battery!

Just for fun...

- These do rely on WDS or bridging wireless
- Small battery? In some cases yes.

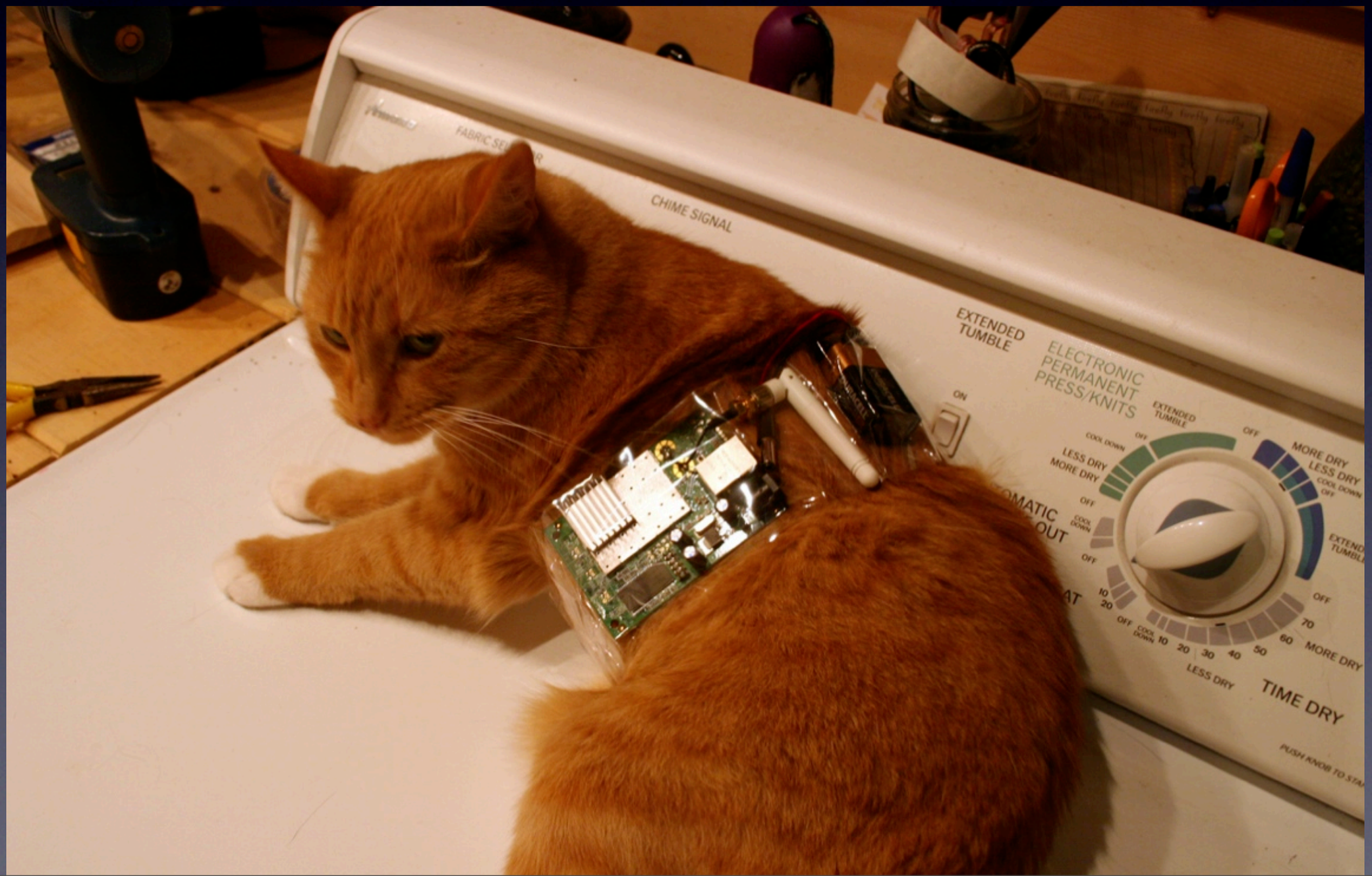
Goatse AP?

Acoustic Kitty

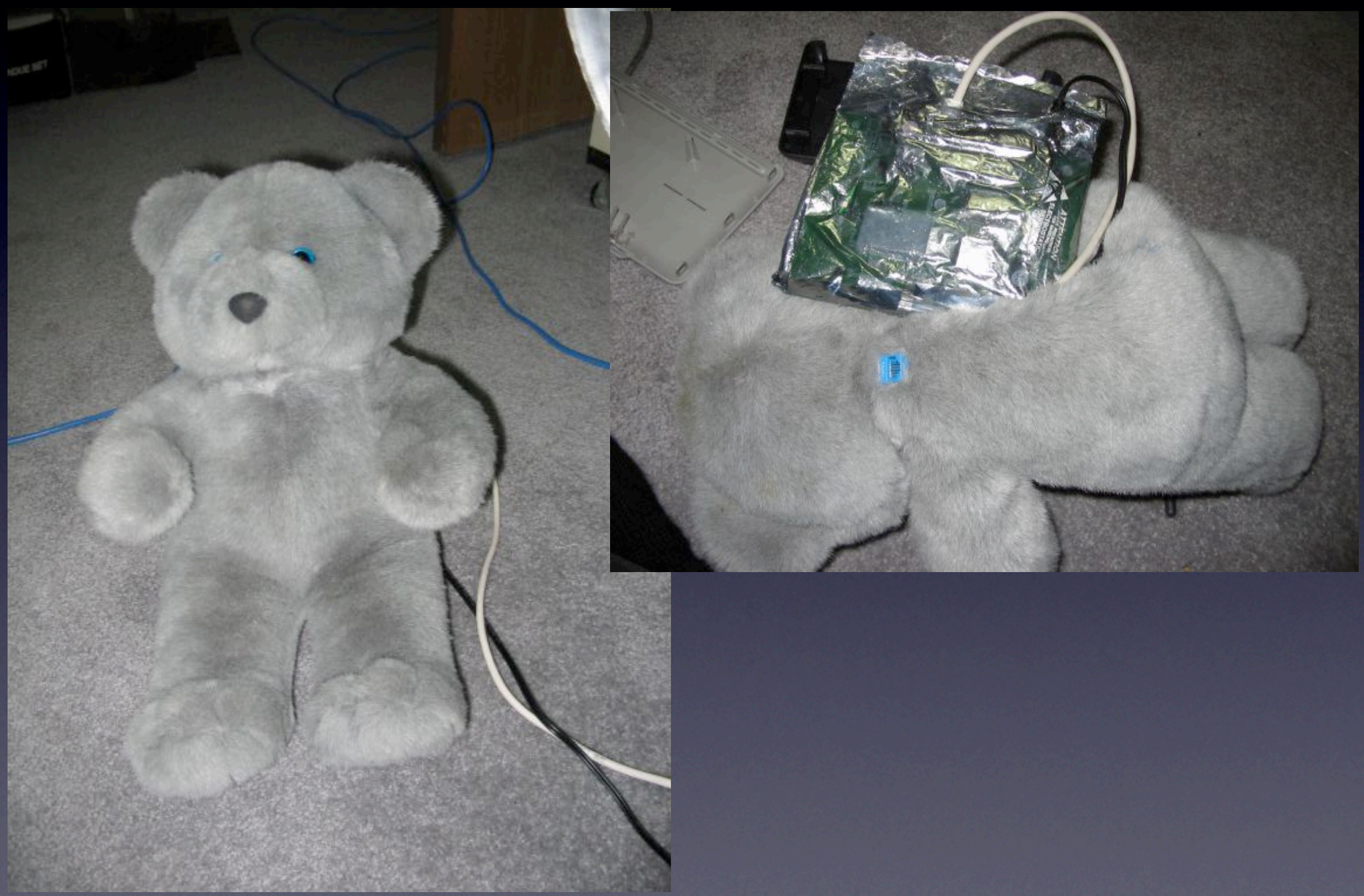
- 1960's CIA project
- *"They slit the cat open, put batteries in him, wired him up. The tail was used as an antenna. They made a monstrosity. They tested him and tested him. They found he would walk off the job when he got hungry, so they put another wire in to override that. Finally, they're ready. They took it out to a park bench and said "Listen to those two guys. Don't listen to anything else – not the birds, no cat or dog – just those two guys!" ... They put him out of the van, and a taxi comes and runs him over. There they were, sitting in the van with all those dials, and the cat was dead!"* - Victor Marchetti

WiFi Kitty

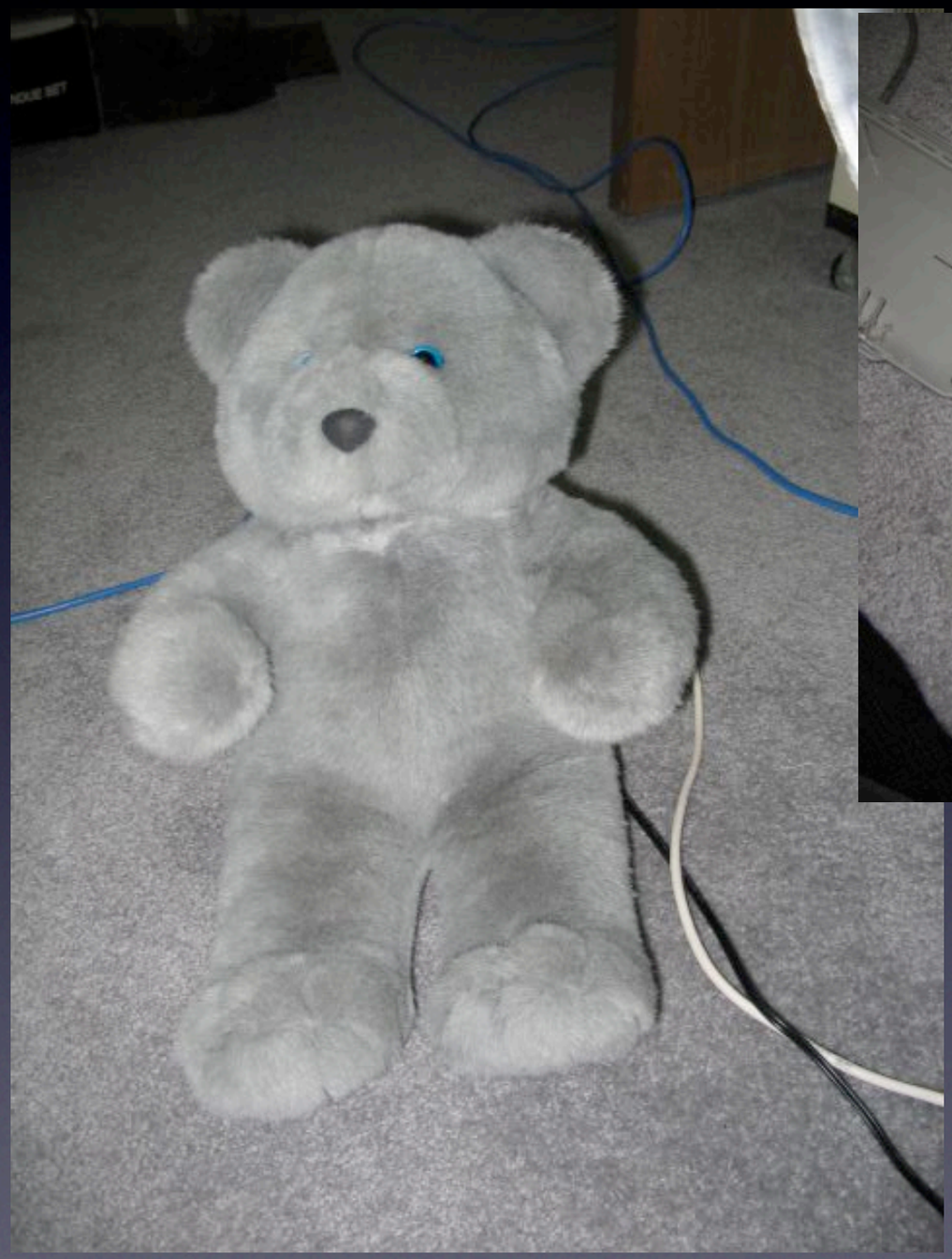
- Early field trials:

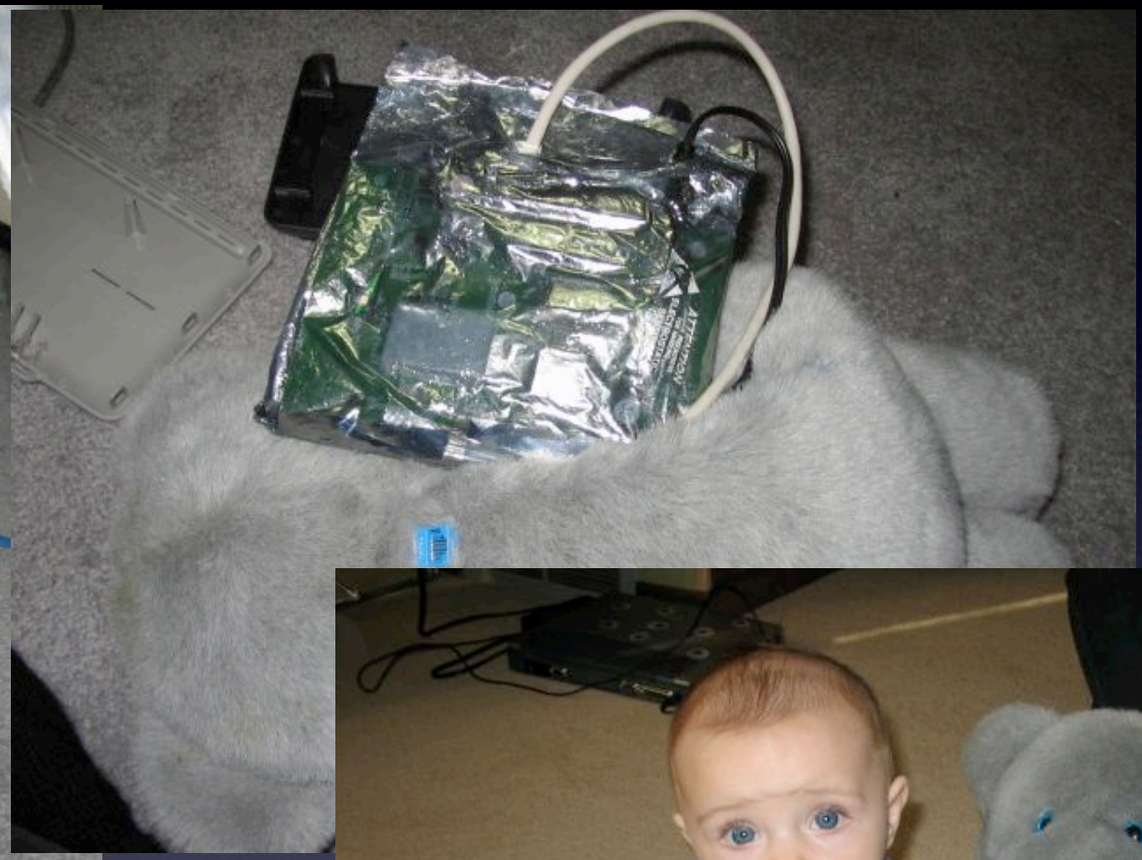


Let's bring it full circle...



Let's bring it full circle...





Baby. Check.

Diaper + AP + Power. Check.

DiAPer + Baby.

Priceless.

Defenses

- Regular scanning - Kismet & laptop
- Fixed scanning - Kismet & WRT54G
- Wired side scanning - RogueScanner, nessus
- Distributed scanning - Thin APs (Cisco, Aruba, Trapeze)
- Combine that with Inventory Management and Corporate Policy

Thanks!

- Any Questions?
- larry@pauldotcom.com
- http://www.haxorthematrix.com