我想看得更远

XFocus Team

www.xfocus.org

www.xfocus.net

X'con 2005

工欲善其事

- 合适的设备
  - 无线网卡
  - 蓝牙适配器
- 合适的天线
  - 定向天线
  - 全向天线
- 把它们连起来

挑选合适的无线网卡

- 芯片组和兼容性
  - 是否支持**Monitor**模式和**Master**模式？
  - 是否支持**Packet Injection**？
  - 是否能在**Linux**下良好工作**?**
    - **Ndiswapper**是一个很棒的项目，但是对我们没用
  - 是否支持**Wireless Extensions**？

挑选合适的无线网卡

```
[root@TOMB tk]# iwlist wifi0 scanning
wifi0     Scan completed :
          Cell 01 - Address: 00:11:22:33:44:55
                    ESSID:"research"
                    Mode:Master
                    Frequency:2.462 GHz (Channel 11)
                    Quality:0/70  Signal level:-53 dBm  Noise level:-86 dBm
                    ……
[root@TOMB tk]# iwlist eth1 scanning
eth1      Interface doesn't support scanning : Operation not supported
```

挑选合适的无线网卡

- 最大发射功率
- 接收灵敏度
- 有没有天线接口？
  - 如果没有，
    是否方便自己安装？

挑选合适的无线网卡

- 802.11b
  - Prism Chipset
    - Senao SL-2511CD PLUS EXT2
    - ASUS WL100
  - Realtek RT8180 Chipset
- 802.11g
  - Atheros Chipset
  - Ralink RT2500 Chipset

挑选合适的无线网卡

- **Lucent Family**
  - **Agere(ORiNICO) & Avaya**
  - **OEMs**
- **Cisco Air-LMC350 Series**
  - **Air-LMC352**
- 软件支持不好的芯片
  - **Broadcom & TI Chipset**

陷阱

- 一定要注意硬件版本号！
  - **eg: D-Link DWL-650**
    - **DWL-650(A1-J3)**
    - **DWL-650(K1)**
    - **DWL-650(L1/L2/M1/P1)**

- **LinkSys WPC11、SMC 2632W……**

挑选合适的蓝牙适配器

- 是否便于安装天线接口
- 发射功率
  - **Class I　　100mW(+20dBm)　　100m**
  - **Class II　　2.5mW(+4dBm)　　10m**
  - **Class III　　1mW(+0dBm)　　1m**
- 接收灵敏度

发射功率	型号	生产厂商	接收灵敏度
Class I	MS-6967	MSI	-90 dBm
Class I	BT3030	TECOM	-76 dBm
Class I	F8T001	Belkin	-80 dBm
Class I	BT-700	Acer	-70 dBm
Class I	USBBT100	LinkSys	-80 dBm
Class I	USBBTC1A	Billionton	-80 dBm

蓝牙适配器

- 兼容性
  - **CSR/BroadCom**
- 芯片型号决定了支持的功能

```
[tk@TOMB ~]$ sudo hciconfig hci0 features
hci0:   Type: USB
        BD Address: 00:11:12:33:44:55 ACL MTU: 128:8 SCO MTU: 64:8
        Features: 0xff 0xff 0x05 0x00 0x00 0x00 0x00 0x00
                <3-slot packets> <5-slot packets> <encryption> <slot offset>
                <timing accuracy> <role switch> <hold mode> <sniff mode>
                <park state> <RSSI> <channel quality> <SCO link> <HV2 packets>
                <HV3 packets> <u-law log> <A-law log> <CVSD> <power control>
```

挑选合适的天线

- 足够的增益

Gain (Sender)	Gain (Receiver)				
	18dBi	14dBi	8dBi	6dBi	5dBi
18dBi	3.4 miles	2.5 miles	1 mile	1100 yards	656 yards
14dBi	1.5 miles	1.5 miles	1 mile	874yards	656 yards
8dBi	1100 yards	1100 yards	1100 yards	874 yards	656 yards
6dBi	874 yards	874 yards	874 yards	874 yards	656 yards
5dBi	656 yards	656 yards	656 yards	656 yards	656 yards

挑选合适的天线

- 在体积和增益之间取得平衡
- 容易获得价格合适

Arecibo, 305m

挑选合适的天线

- 赫兹天线
  - 半波长偶极振子
- 马可尼天线
  - 四分之一波长单极振子

几个选择

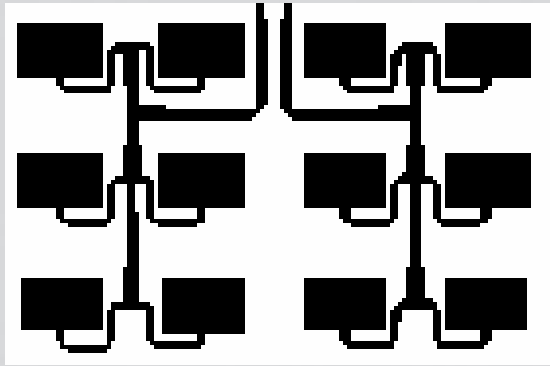
- 八木天线
  - 通常制作为中等增益
- “平板天线”
  - 可以有比较高的增益
- 自制天线
  - 一种不错的消遣
  - 增益也不错

八木天线

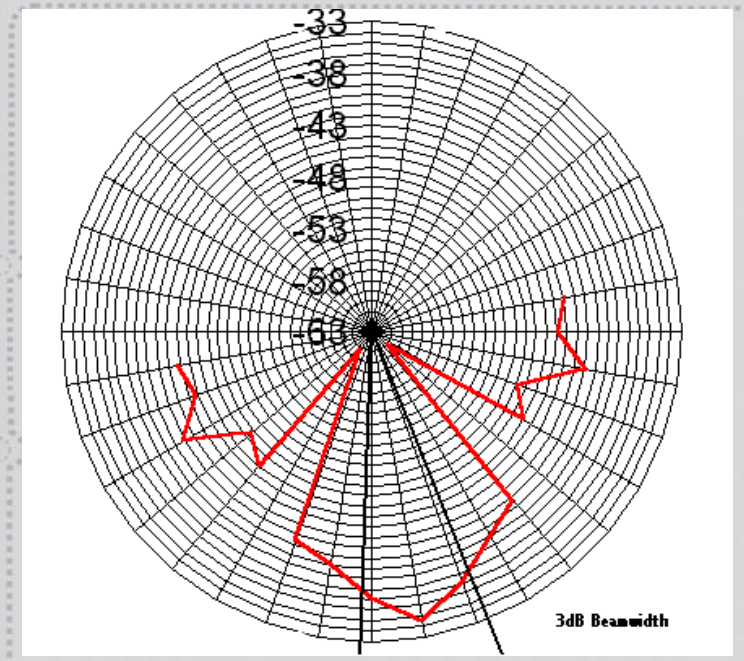
- 八木秀次&宇田太郎
- 价钱便宜，尺寸可以接受
- 中等大小的增益

“平板天线”

- 增益可以超过**20dBi**
- 便于携带
- 价格较贵



比较严肃的自制天线


-33
-38
-43
-48
-53
-58
-63
3dB Beamwidth

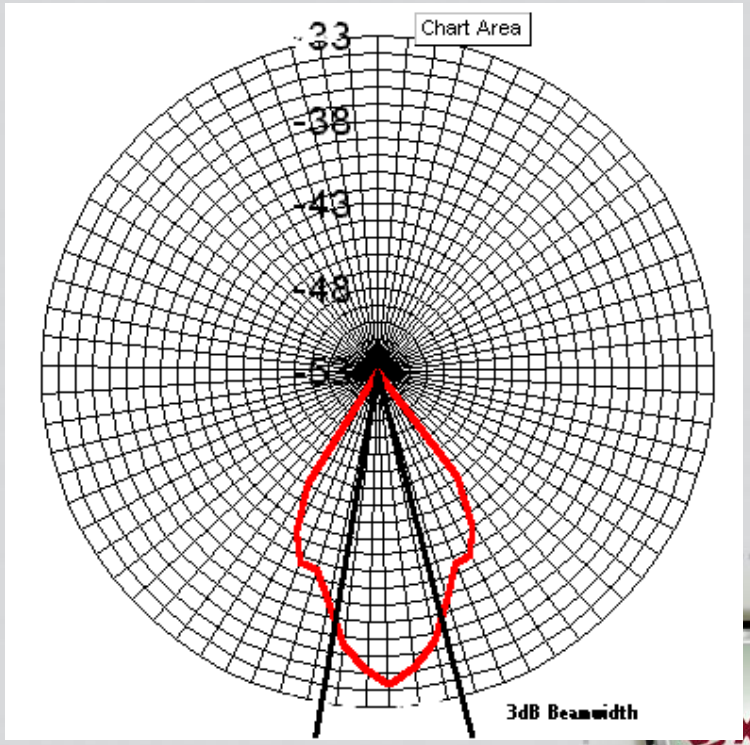
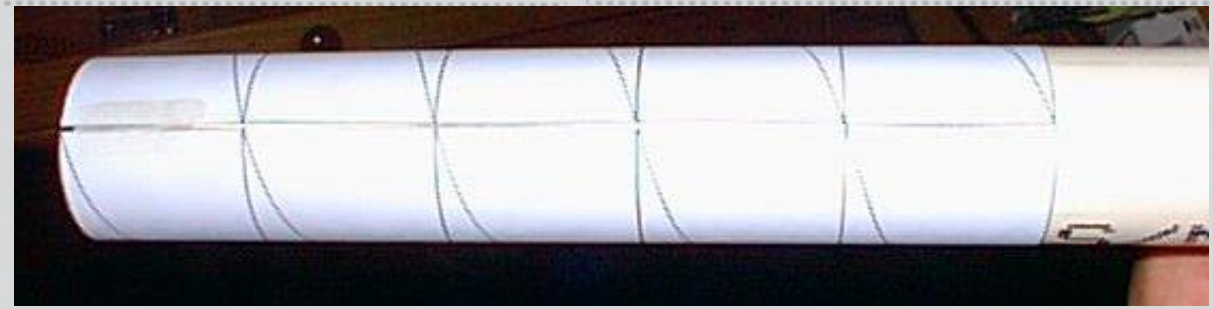
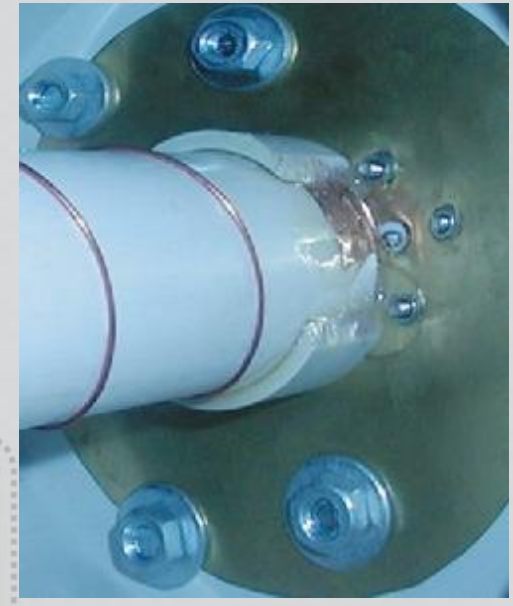


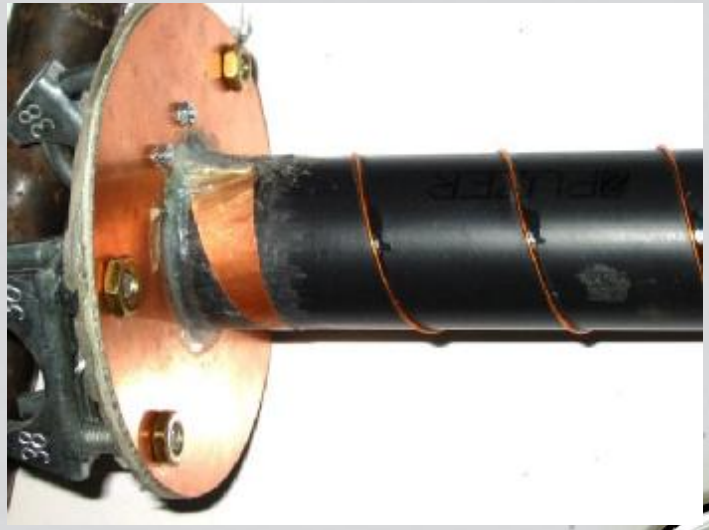
Chart Area
-33
-38
-43
-48
3dB Beamwidth

比较严肃的自制天线

比较严肃的自制天线







比较严肃的自制天线

比较严肃的自制天线

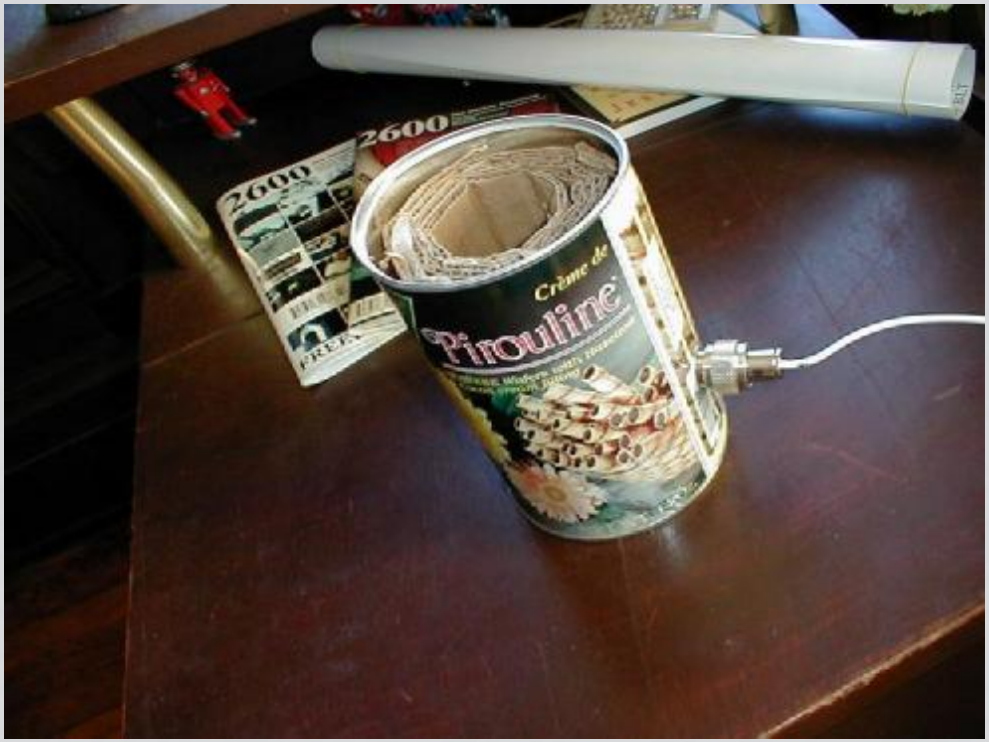
比较严肃的自制天线

比较幽默的自制天线

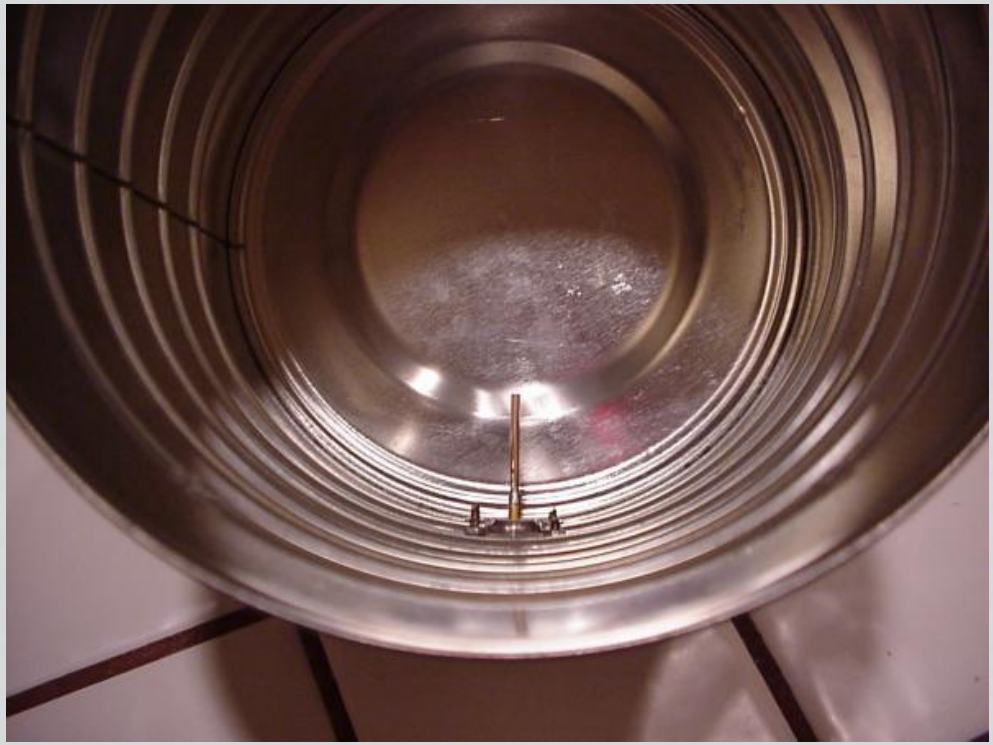
比较幽默的自制天线

比较幽默的自制天线

比较幽默的自制天线



比较幽默的自制天线



比较幽默的天线


Mmm- certainly cost effective- NZ$8 ! A 300mm diam (12") Chinese cooking vat scoop that closely approximates a shallow parabola. It's mesh holes (~5mm) are well under the min. .1 wavelength at 2.4GHz (1 wave= 125mm) & it gives little wind resistance & rust.
Diam = 300 mm, with 60mm depth (D) (c) to centre
$f = \frac{D^2}{16c}$
$= \frac{300 \times 300}{16 \times 60}$
$= \frac{1500}{16}$
So focus ~94mm out
which is beyond screen rim & may give weak signal pickup from sources not being looked at
f / D ratio desirably 0.25-0.55 for such 2.4GHz parabolas
Here = 94/300 = 0.31
Experiences show mesh equiv. to "0.8" of a dish of similar size. Hence this equates to a solid dish 0.8 x 300 ~240mm & is likely to have gain ~15dB
(A trial verified >12dB !)
With one at each end of a link,the 30dB system gain could give >10km LOS
Focal point ~94mm out
Other simple DIY reflectors abound - with "BBQ grill" style likely better gain. Doubling dish diam gives 6dB gain & doubles range
This setup could look very professional spray painted black & maybe mounted on a simple photographic tripod
Suitable support for the USB WiFi adaptor (here a ~US$40 "ZyDAS ZD 1201" sold in NZ by DSE) will of course be needed, maybe fed thru' the mesh from the back ? USB dongle then can be removed until needed
POOR MANS WIFI ?
Cheap & "lossless" long run (5m+) USB cables mean reception "sweet spots" more easily exploited than normal costly microwave cable & connectors can justify. Cost !
Parabolic reflective performance of similar "appropriate technology" dishes can be quickly verified by Al foil curved around the mesh to direct the sun, or a bright light, to a focus
Stan. Swan. -MU@W - 2nd May 2004
== s.t.swan@massey.ac.nz

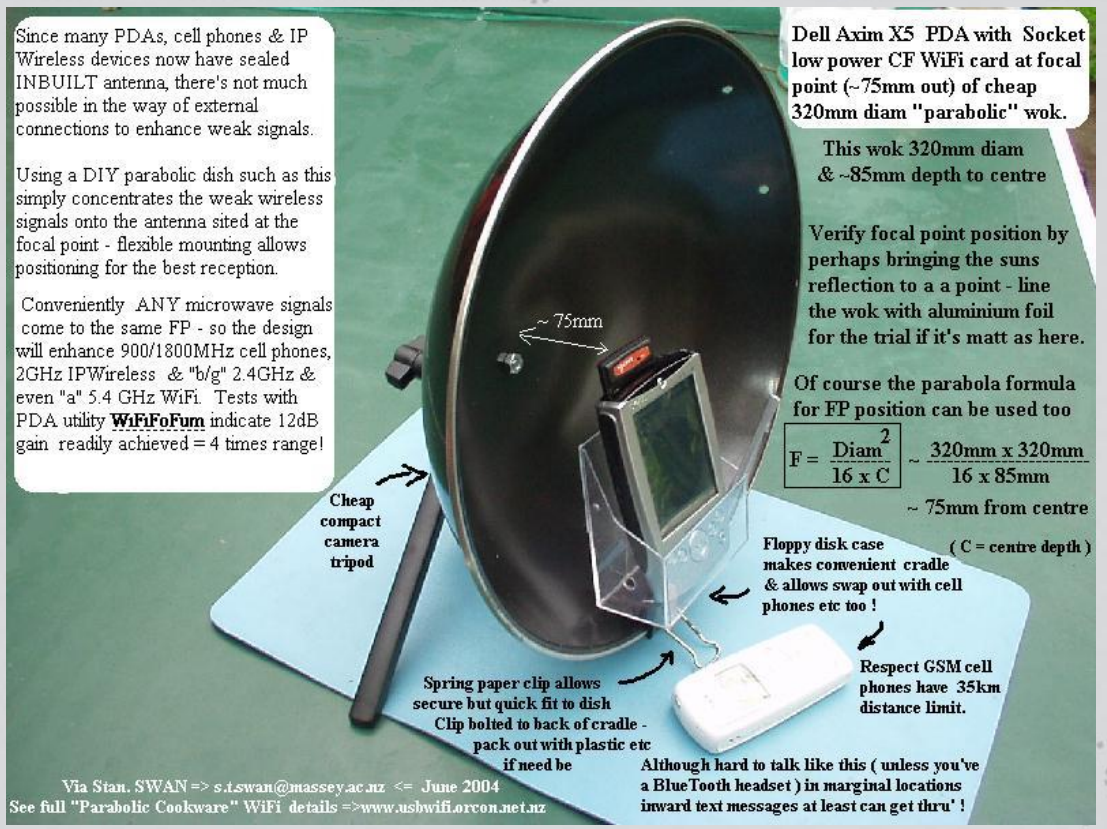
比较幽默的天线


Park bench WiFi - "Scoop" antenna here has not yet had the cable feed & hose mender adaptor mount fitted. To avoid curious stares it's suggested a plastic bag be placed over the entire unit - people won't bother you with just a laptop PC !

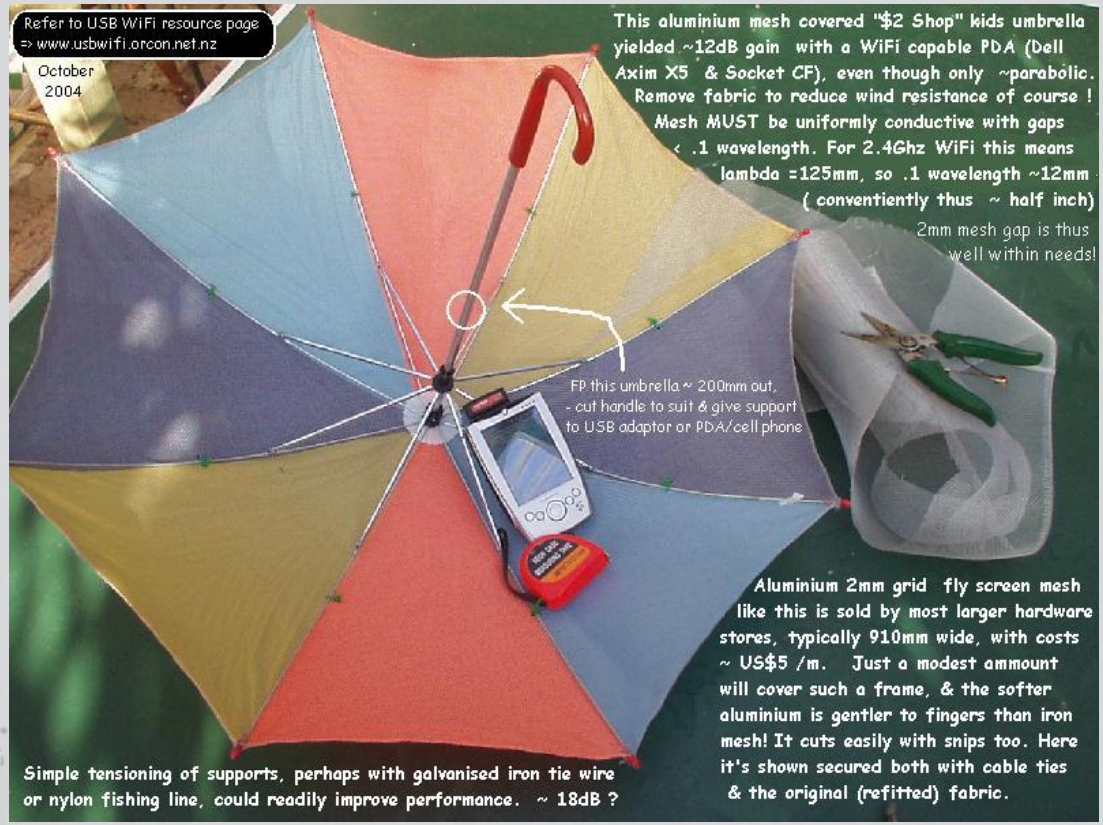
比较幽默的天线


Not your usual stir fry ! Here's a cheap wok from NZ's celebrated Warehouse, that's ~parabolic !
With diam. 330mm & depth ~90mm it has a verified focal point ~75mm out. Being inside the rim this should gather signals well, & indeed performance looked superior (~17dB ?) beside the Scoop's ~15dB.
A hose mender again provides both USB cable protection & (when internally trimmed to suit) good support & standoff for the USB WiFi adaptor.
Handles will drill out if desired
A vitamin pill holder neatly fits over the USB adaptor if weather proofing needed
The chassis nibbler eases drilling out of the 25mm(1") mount hole. Recommended !

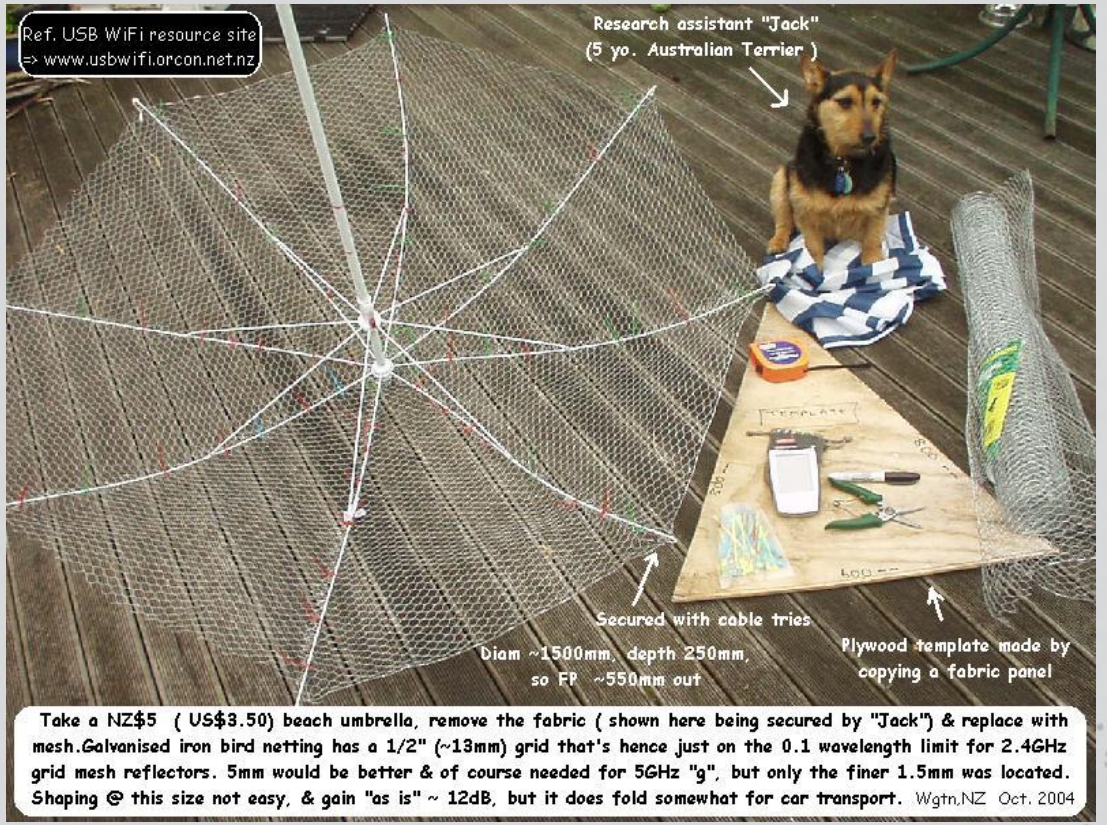
比较幽默的天线


Since many PDAs, cell phones & IP Wireless devices now have sealed INBUILT antenna, there's not much possible in the way of external connections to enhance weak signals.
Using a DIY parabolic dish such as this simply concentrates the weak wireless signals onto the antenna sited at the focal point - flexible mounting allows positioning for the best reception.
Conveniently ANY microwave signals come to the same FP - so the design will enhance 900/1800MHz cell phones, 2GHz IPWireless & "b/g" 2.4GHz & even "a" 5.4 GHz WiFi. Tests with PDA utility WiFiFoFum indicate 12dB gain readily achieved = 4 times range!
Dell Axim X5 PDA with Socket low power CF WiFi card at focal point (~75mm out) of cheap 320mm diam "parabolic" wok.
This wok 320mm diam & ~85mm depth to centre
Verify focal point position by perhaps bringing the suns reflection to a a point - line the wok with aluminium foil for the trial if it's matt as here.
Of course the parabola formula for FP position can be used too
F = Diam² / 16 x C ~ 320mm x 320mm / 16 x 85mm
~ 75mm from centre
(C = centre depth)
~ 75mm
Cheap compact camera tripod
Floppy disk case makes convenient cradle & allows swap out with cell phones etc too !
Respect GSM cell phones have 35km distance limit.
Spring paper clip allows secure but quick fit to dish
Clip bolted to back of cradle - pack out with plastic etc if need be
Although hard to talk like this (unless you've a BlueTooth headset) in marginal locations inward text messages at least can get thru' !
Via Stan. SWAN => s.t.swan@massey.ac.nz <= June 2004
See full "Parabolic Cookware" WiFi details =>www.usbwifi.orcon.net.nz

比较幽默的天线


Refer to USB WiFi resource page
=> www.usbwifi.orcon.net.nz
October 2004
This aluminium mesh covered "$2 Shop" kids umbrella yielded ~12dB gain with a WiFi capable PDA (Dell Axim X5 & Socket CF), even though only ~parabolic. Remove fabric to reduce wind resistance of course ! Mesh MUST be uniformly conductive with gaps < .1 wavelength. For 2.4Ghz WiFi this means lambda =125mm, so .1 wavelength ~12mm (conventiently thus ~ half inch)
2mm mesh gap is thus well within needs!
FP this umbrella ~ 200mm out, - cut handle to suit & give support to USB adaptor or PDA/cell phone
Aluminium 2mm grid fly screen mesh like this is sold by most larger hardware stores, typically 910mm wide, with costs ~ US$5 /m. Just a modest ammount will cover such a frame, & the softer aluminium is gentler to fingers than iron mesh! It cuts easily with snips too. Here it's shown secured both with cable ties & the original (refitted) fabric.
Simple tensioning of supports, perhaps with galvanised iron tie wire or nylon fishing line, could readily improve performance. ~ 18dB ?

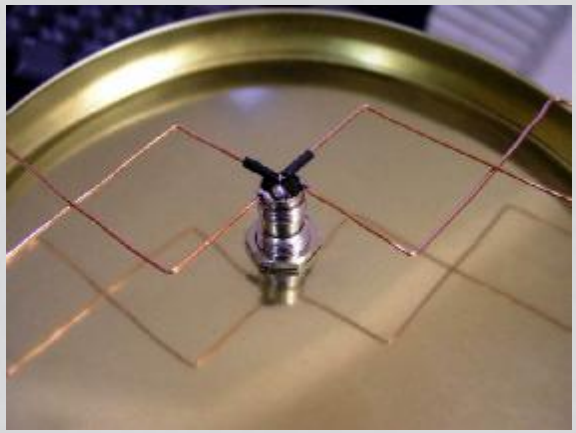
比较幽默的天线



Take a NZ$5 (US$3.50) beach umbrella, remove the fabric (shown here being secured by "Jack") & replace with mesh.Galvanised iron bird netting has a 1/2" (~13mm) grid that's hence just on the 0.1 wavelength limit for 2.4GHz grid mesh reflectors. 5mm would be better & of course needed for 5GHz "g", but only the finer 1.5mm was located. Shaping @ this size not easy, & gain "as is" ~ 12dB, but it does fold somewhat for car transport. Wgtn,NZ Oct. 2004

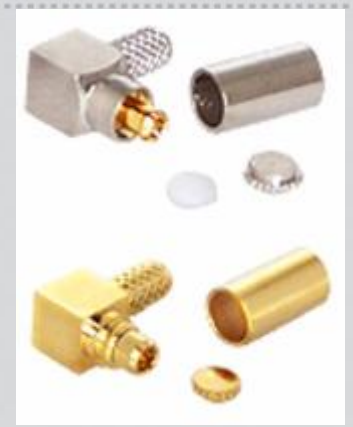
推荐的自制天线方案

- 卫星电视天线的抛物面
  +赫兹天线
- 菱形振子
  +反射面
- **USB**无线网卡
  +弧形反射面
- 螺旋天线



把它们连接起来

- 设备端接口
  - **MC-CARD(Lucent Family)**
  - **MMCX(Others)**



- 天线端接口
  - **TNC**
  - **SMA**
  - **……**

把它们连起来

- 已经有合适接口的设备
  - 找一条合适的转接线（**Pigtail**）
- 没有接口的设备
  - 改造
    - 安装插座
      - 更完美的外形
    - 直接焊接
      - 更低的信号损失

预留了插座位置的设备

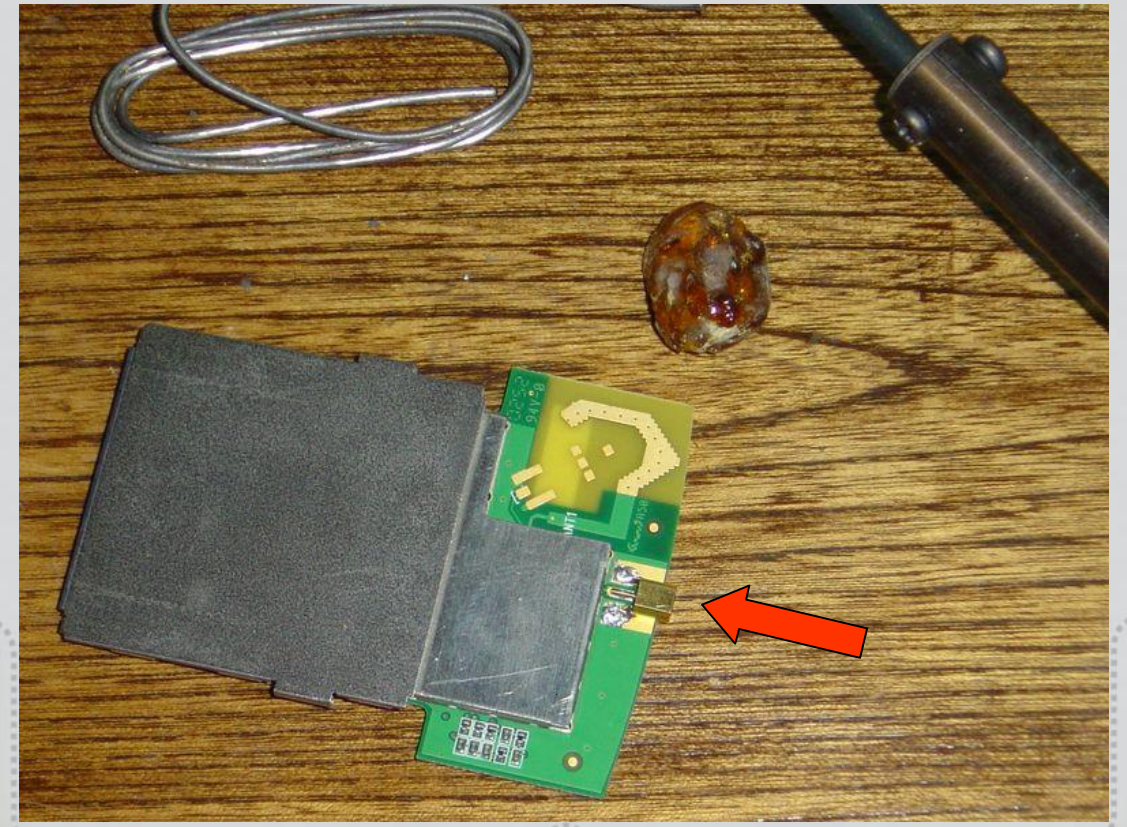
- 西门子 **SS2521**

预留了插座位置的设备

- 拆开

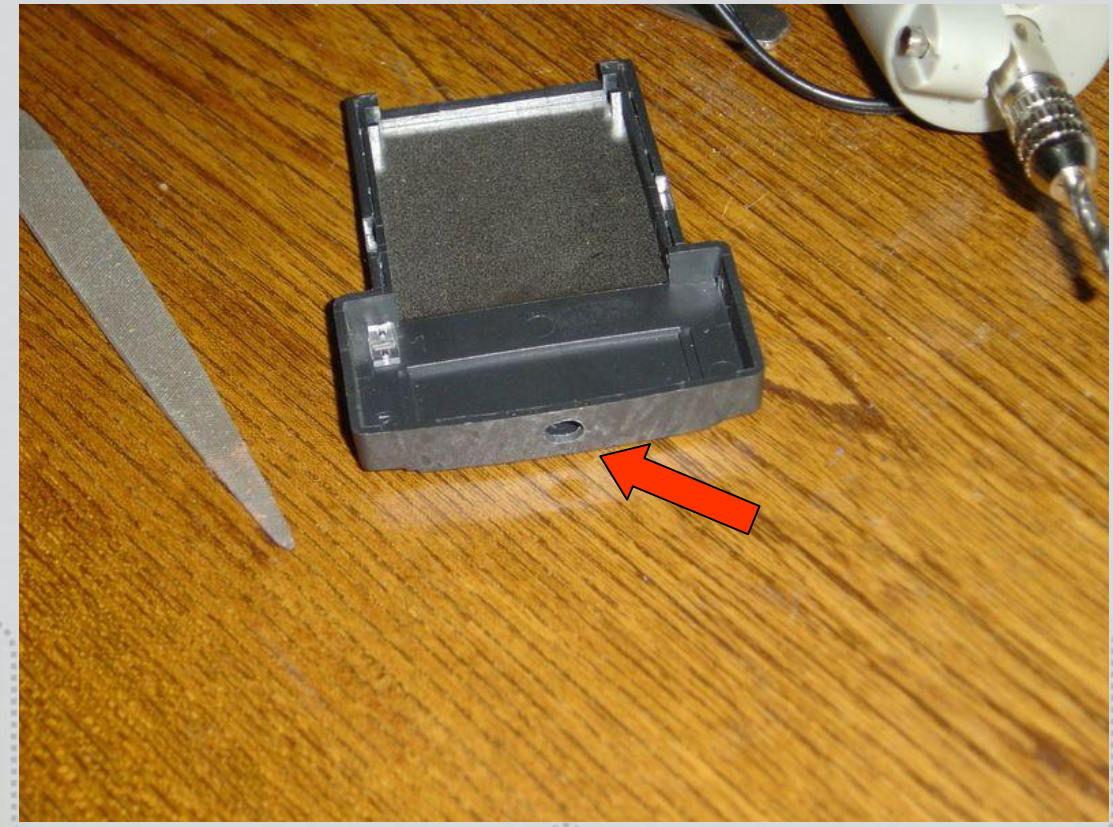
预留了插座位置的设备

- 将**MMCX**插座焊接到线路板上



预留了插座位置的设备

- 在外壳上钻孔



预留了插座位置的设备

- 网卡+PDA+八木天线

预留了插座位置的设备

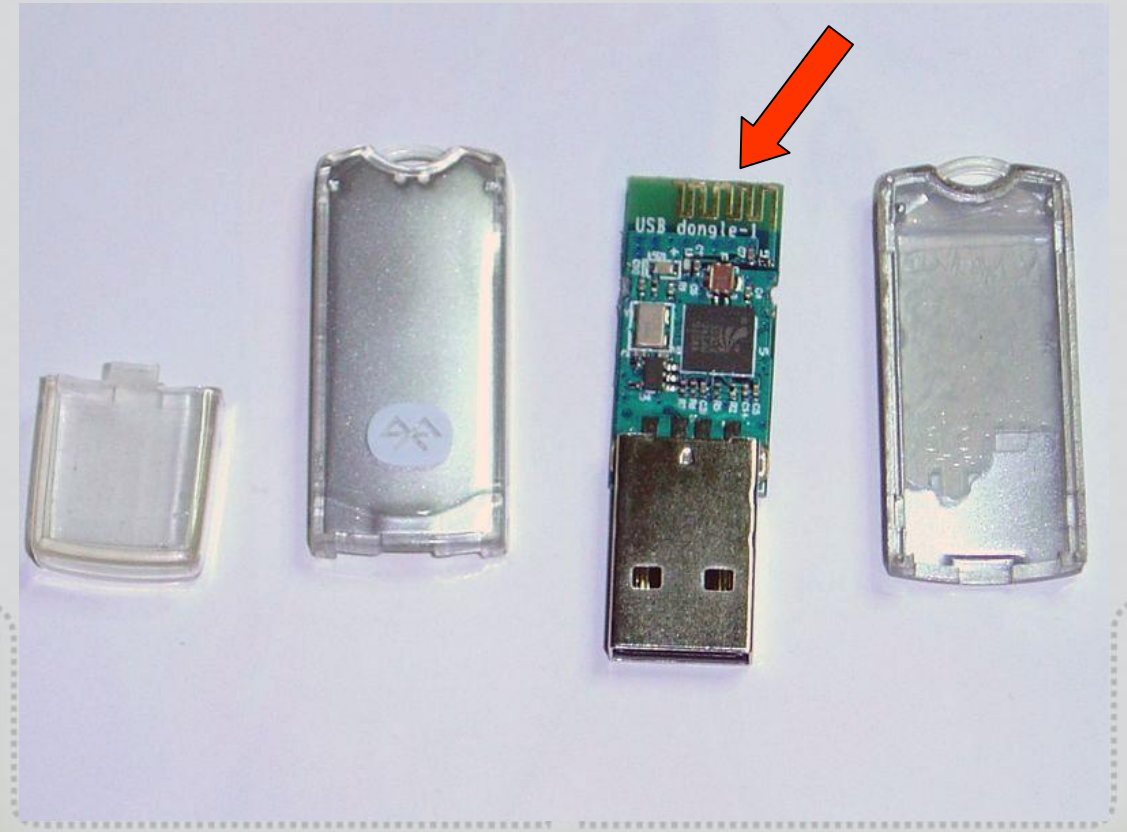
- 开始工作

没有预留插座位置的设备

- 一个廉价的三无产品，**Class 2**的蓝牙

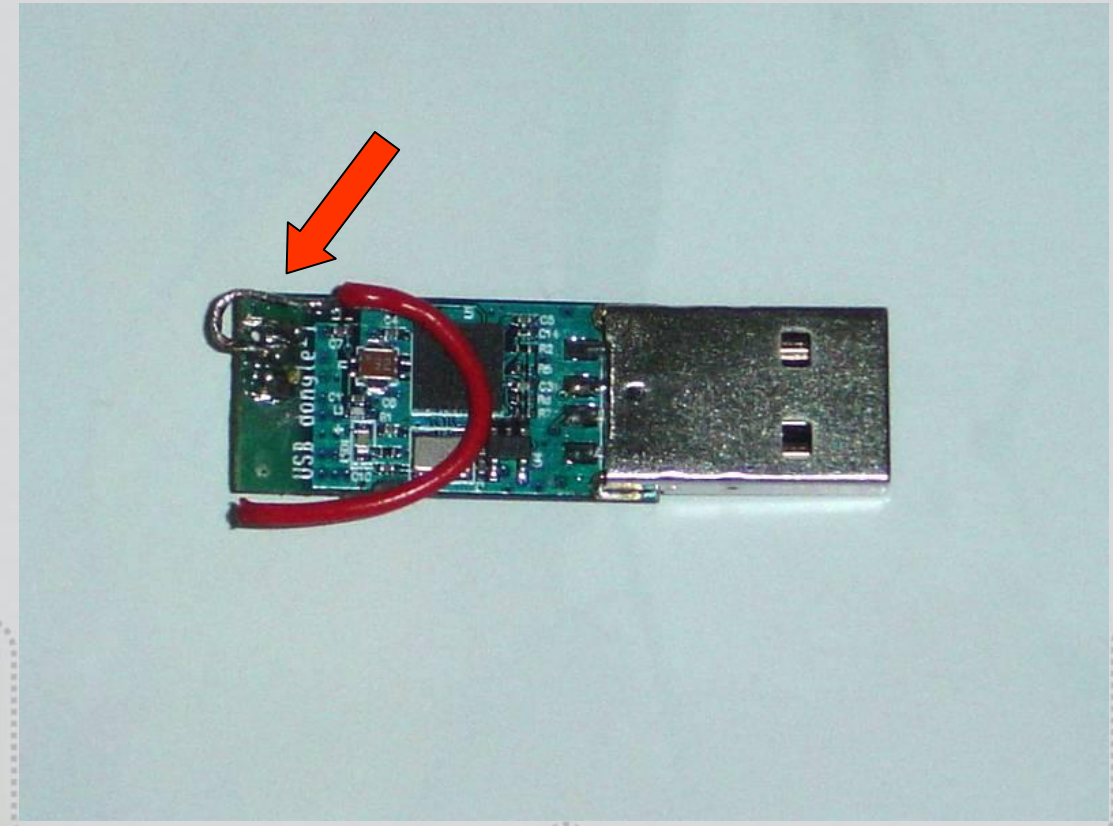
没有预留插座位置的设备

- 用吹风机使热熔胶软化，然后拆开



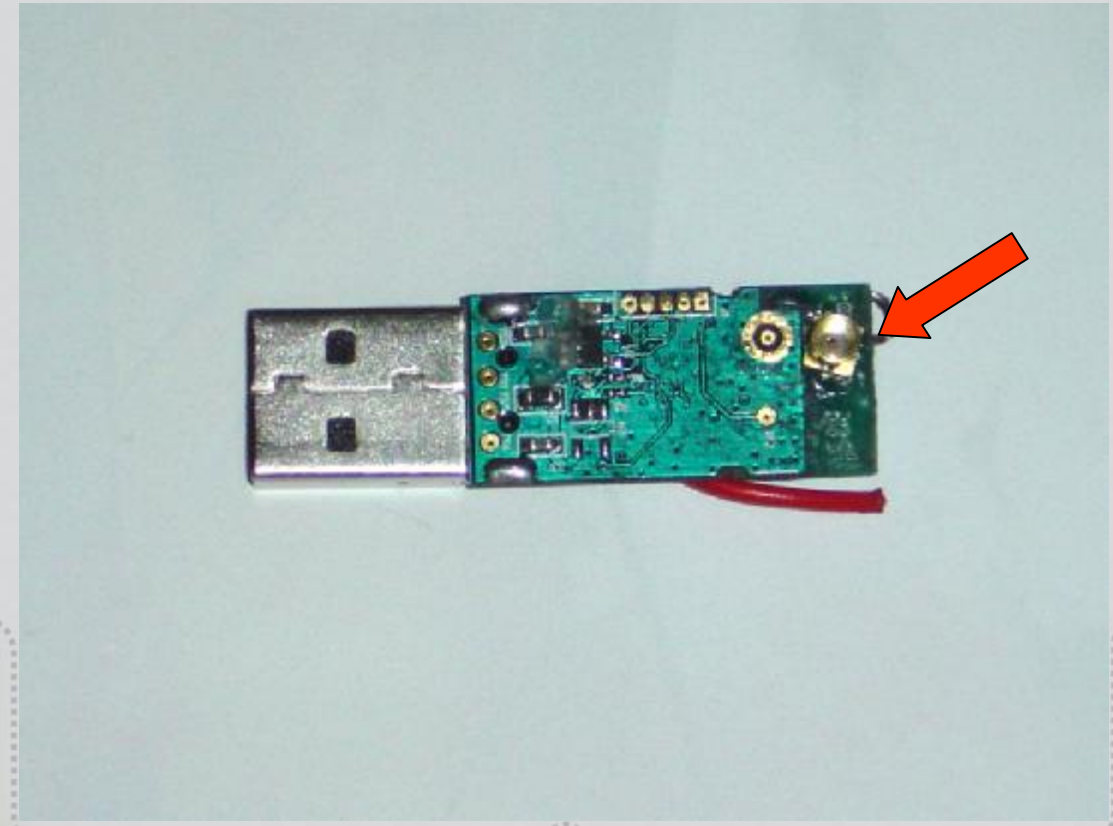
没有预留插座位置的设备

- 刮掉原来的印刷天线，焊接上替代的导线



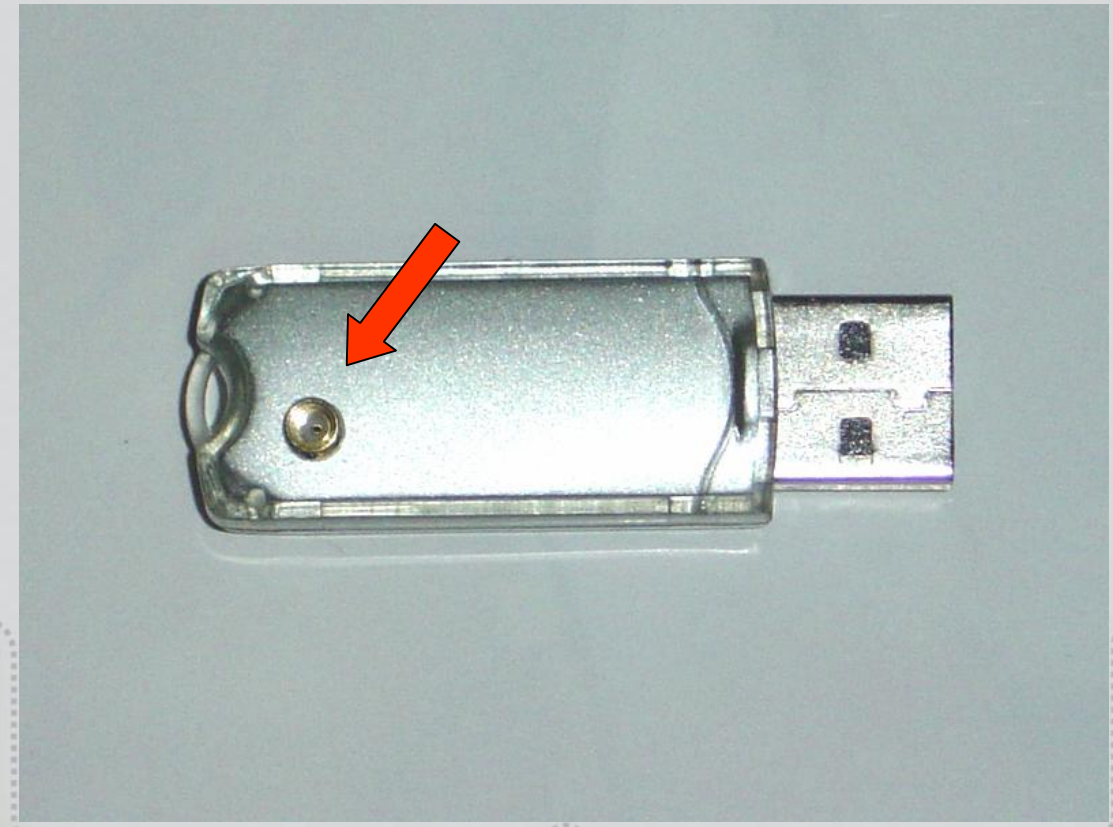
没有预留插座位置的设备

- 在线路板上钻**1mm**的孔，焊接**MMCX**插座



没有预留插座位置的设备

- 在外壳上钻**3.5mm**的孔，按照原样装回去

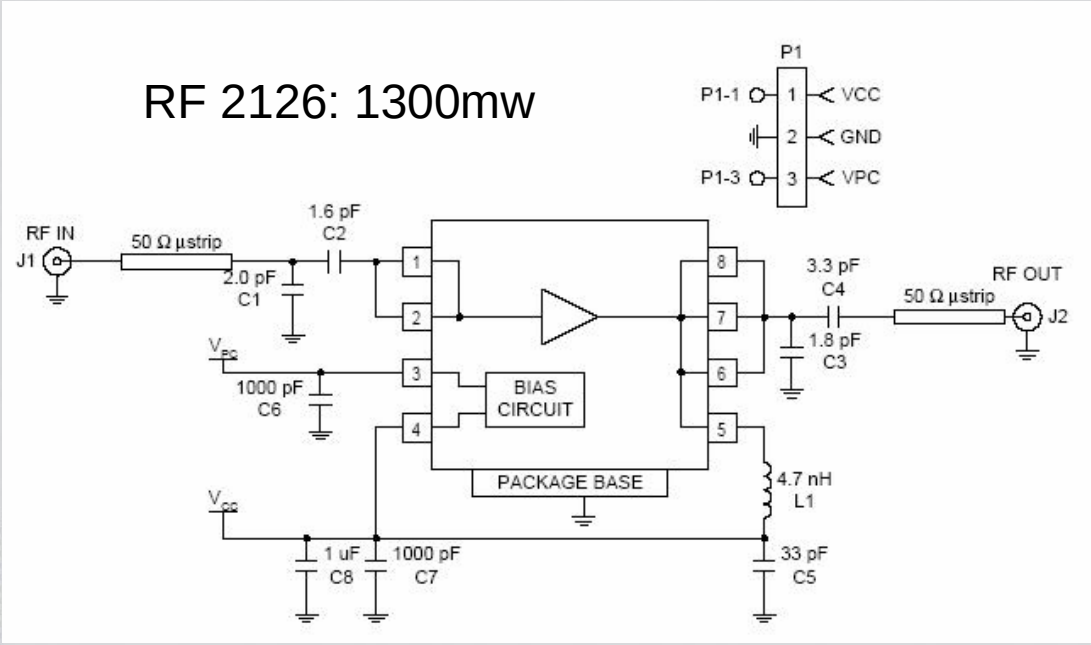


没有预留插座位置的设备

- 现在可以连接天线了

还有什么可以做的？

- 用射频芯片制作微波功放
  - 得到超过**1000mw**的输出功率



DEFCON Wifi Shootout

X'con 2005

- 2004
  - 55.1 miles
- 2005
  - 125 miles
- 2006
  - ?

XCon 2006 再见！

- **tombkeeper[0x40]xfocus.org**