Receiving 900 MHz Band Cordless Phones

This is a overview of a really nice 900 MHz Yagi antenna, band pass filter, and receive pre–amplifer one can use to greatly enhance their SIGINT reception of normal (unencrypted, non–digital), Frequency Modulated (FM), 900 MHz band cordless phones.

The 902 MHz to 928 MHz Part 15 band is an operating haven for today's cordless phones. Lots of people have been leaving their "new" 2.4 GHz and 5.8 GHz phones (which have horrible range and can disrupt wireless LAN devices) for the good ole' 900 MHz band phones. The main reason for this is simple, phones operating in the 900 MHz will have greater range due to their lower wavelength. This little fact also helps us SIGINT guys monitor our neighborhood Commies, Nazis, $2600 readers, terrorists, nutcases, etc.

The first part of this setup is the antenna. Thankfully, good high–gain antennas are available commercially for low cost. Yes, that's right. Fair Radio sells the Antenna Specialists Model #ASPJ2996, 7–element Yagi antenna for only $19.95. This antenna is meant for the 928 MHz to 960 MHz Studio–to–Transmitter Link (STL) band, but works beautifully in the 902–928 MHz band. There is a slight gain roll–off on the lower frequencies due to the SWR mismatch, but the gain will still be around 8 dBi.

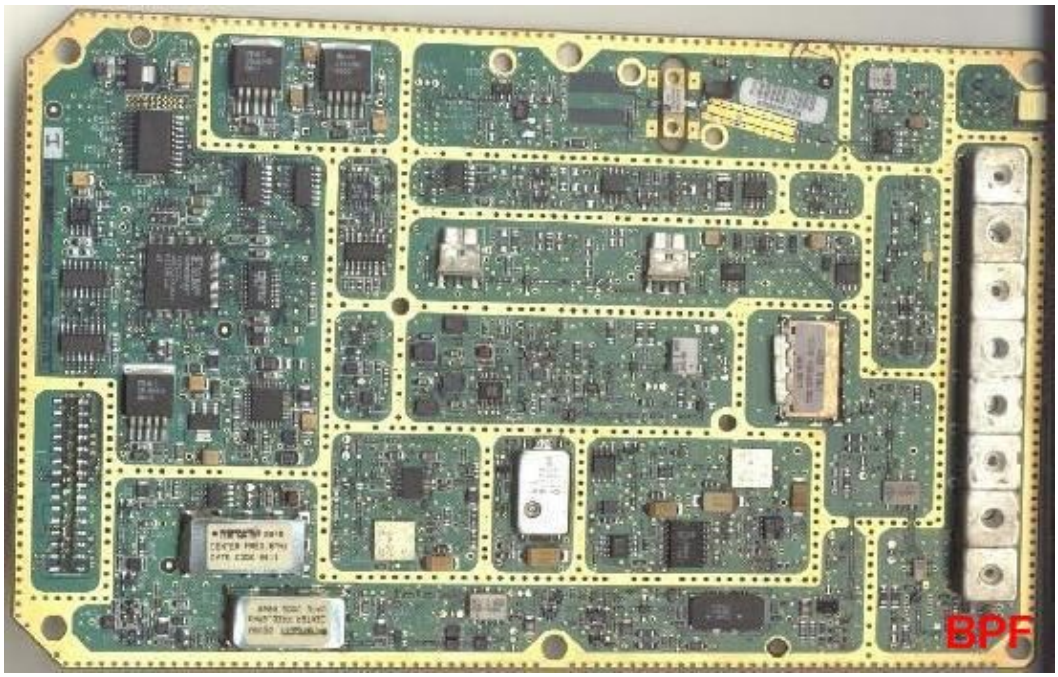
Antenna Specialists Model #ASPJ2996 Antenna

<–– Point in Direction of Receive Point Towards Interference ––>

Mount this antenna, vertically polarized (elements running up–and–down), as high as possible, away from any nearby trees or metal objects, and pointing to your target's general location. A neat trick with directional antennas of this type is that you can "null" out any interfering co–channel stations by pointing the back–end of the antenna (the part with the N–connector) at the intefering station. This is very useful for "nulling–out" those interfering 900 MHz pager stations or other in–band cordless phones. Also, those cheap Radio Shack TV antenna rotators are *very* handy for providing complete 360° rotaing antenna coverage. You'll want to use very high–quality coaxial cable for all the long antenna feedline runs. Times Microwave LMR–400, "name brand" RG–8, or Belden 9913 (all using N–connectors) is the probably the best choice right now, and easiest to obtain. Avoid RG–58 (except for short jumpers) or Radio Shack RG–8 coax, it's crap. RG–6QS (75 ohm, Quad–Shield), with adapters for the F–connectors, works surprisingly well in a pinch.

This next part of this setup is the Band Pass Filter (BPF) after the antenna and in–front of the receive pre–amplifier. This device helps to attenuate out–of–band RF interference from the 880 MHz cellular phone and 929 MHz pager bands. This will prevent signals from overloading the pre–amplifier's front–end and causing any intermodulation degradation. My favorite BPF is the ComNav Engineering 8BCR12C–915/C25–DX. This is actually the BPF used in the 900 MHz Metricom Ricochet pole–top RF modems, which where popular in the late 1990s.

ComNav Model 8BCR12C–915/C25–DX Filter on a Ricochet RF Modem



The above picture is a 900 MHz Metricom Ricochet RF modem PC board showing the ComNav Model 8BCR12C–915/C25–DX filter (the long silver rectangle on the right). To remove it, heat the underside of the PC board with a slowly rotating hot–air gun. The filter will fall right out when the heated board is turned upside down. The RF input to the filter is the end nearest the PC board's RF connector. You'll need to make some small coax jumpers to connect to the antenna's feedline and the receive pre–amplifier. The performance specifications for this ComNav filter are:

```
    Center Frequency : 913.5 MHz
         2.5 dB Loss : 906 - 921.5 MHz
         4.0 dB Loss : 902 - 925.5 MHz
      30 dB Rejection : 895 & 929 MHz  (pagers at 929 MHz)
      50 dB Rejection : 880 & 945 MHz  (cellular phones at 880 MHz)
        Passband VSWR : 1.7:1
     Passband Ripple  : < 0.25 dB
RF In/Out Impedance   : 50 ohms
```

This particular filter is optional, but highly recommended. Digi–Key carries the Toko 4DFB–915E–10 3–pole BPF equivalent, Part No. TKS2617CT–ND, but its passband isn't nearly as sharp.

The two "prongs" on the filter's ends are the input/output connections. Solder your coax's center conductor to the "prong" and the shield of coax to one of the filter's ground tabs.

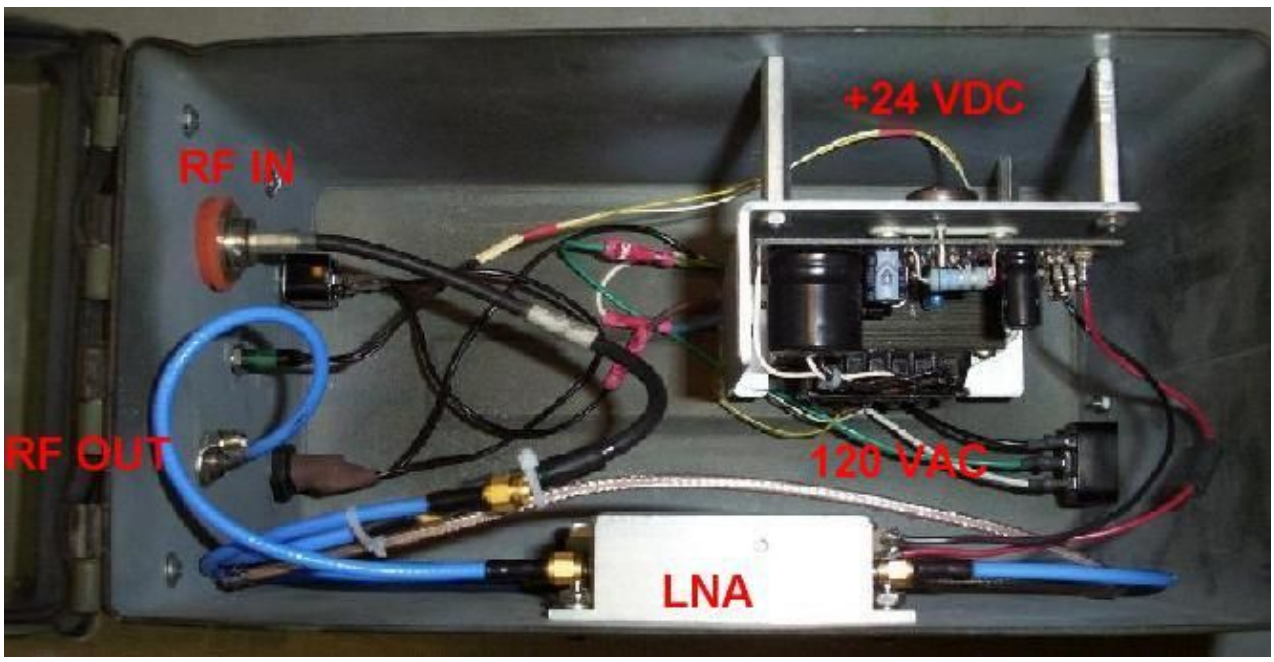
The most important part of this setup is the actual receive Low Noise Amplifier (LNA). Thankfully, these are also cheap and easy to obtain. We will be using surplus M/A-Com AM-1383A 821 – 851 MHz LNA from Surplus Sales of Nebraska, Part No. (RF) KS21583L9, for $65. These where originally designed as receive pre–amplifiers for the 800 MHz cellular site uplink (receive) frequency band. They will also work beautifully in the 902 – 928 MHz band.

M/A–Com AM–1383A Low Noise Amplifier

A drawback to these amplifiers is that they require a clean +24 VDC supply (at around 200 mA). Voltages down to +18 VDC will work fine as the LNA has an internal regulator. The LNA uses SMA connectors for the RF input and output, so small jumper cables should be made to connect it to the antenna/filter and the communications receiver. Performance specifications for this LNA are:

```
          Gain : 44 dB  (821 - 851 MHz)
Noise Figure : 0.8 dB
  Output IP3 : +38 dBm
```

On certain communications receivers, usually Radio Shack scanners, this LNA will provide *too much* gain, and can overload the receiver's front–end. Too prevent this, add about a 10 dB resistive attenuation pad to the output of the LNA, or flip the "10 dB ATT" switch on the back of some Radio Shack scanner models.



Example of my 900 MHz LNA setup.

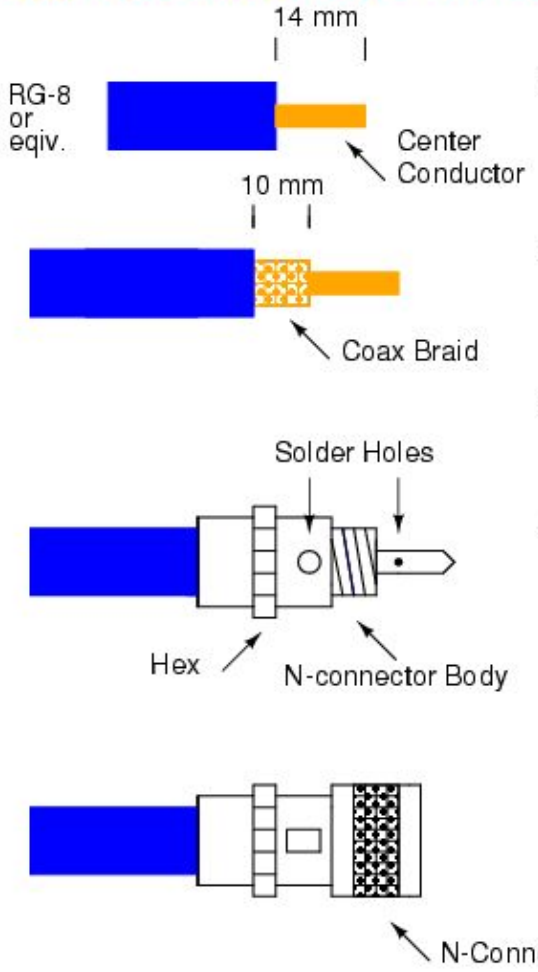
RF INPUT (from the antenna) is the upper−left N−connector, this feeds the BPF INPUT (the BPF is hidden), the BPF OUTPUT goes to the LNA RF INPUT, the LNA RF OUTPUT goes to the bottom−left N−connector, then to a Radio Shack PRO−2042 scanner. This is all powered from a linear +24 VDC power supply (RED wire positive).

Here is the outside case overview of the complete amplifier assembly. It is housed in an old ammo box, with all the holes sealed with rubber washers or sealant to make it somewhat water resistant. The RF input is on the left, the RF output is on the right. The switch, 1 Amp fuse, and green neon light control the power supply. The protection bars are brass drawer handles. A plug for the 120 VAC power cord is provided on the rear of the ammo box.

To use the new amplifier assembly, connect it between your directional antenna and your communications receiver capable of tuning between 902 MHz and 928 MHz in 5 kHz steps (narrowband & wideband FM). There really is no bandplan to the 900 MHz band, but you'll usually find the cordless phone's HANDSET transmitting around 924 – 928 MHz and the BASE transmitting between 902 – 908 MHz. Scanning the BASE frequencies will allow you to hear both sides of the conversation (in analog hybrid systems) and will usually also have a higher output RF power. Use both 5 kHz and 12.5 kHz steps to scan the band and use the narrow or wide FM selection mode to maintain the highest receivability.

The Radio Shack PRO–2035/2042 line of scanners is ideal for monitoring the 900 MHz cordless phone band. The picture on the left is of a PRO–2042 scanner with its stock BNC connector replaced with a N–connector. This allows the use of high–quality connecting coaxial cables. The IC picture on the right is of a 8,000 channel modification to the PRO–2042. Both of these modifications are also highly recommended. The 8,000 channel modification is covered in detail here: http://www.dafh.org/gbppr/mil/rsscanner.

Installing a 2-Piece N-Connector on RG-8-type Coax



1. Strip cable as shown. Be careful not to nick the center conductor.
2. Remove jacket as shown. Be careful not to nick the braid.
3. Screw body onto cable as far as it will go.
4. Solder braid through the two holes in the body. Solder the center through the hole in the pin. The solder must seal the holes for the connector to be waterproof.
5. When the connector cools, screw the shell assembly onto the body. Wrench tighten until the shell assembly bottoms on the hex.