Have a Software Defined Radio? Design and make your own antennas

Demystifying the dark arts of antenna design

Erwin Karincic
Cyber Security Researcher

Problem Statement

Many researchers indicated that having a better antenna would make their discoveries work at a better range

higher antenna gain

environment. A more sophisticated attacker, could use better equipment with a lower noise floor and higher antenna gain to undertake such an attack from an even further distance. This should open the discussion about what

Even though the units have the intended functionality, there are still some improvement to be done concerning the range of the units. Here, a further investigation regarding a better antenna is something we would recommend. Another area that we would

better antenna

better antenna

for R and determine that he can only be at 35.48 cm away. Thus for practical attacks, he will have to get a better antenna or significantly increase his transmit power. In

10 cm is not a sufficient defense against eavesdropping attacks. While neither experiment achieved the predicted eavesdropping range of 10 meters, better antenna design increases the maximum eavesdropping range significantly. In [72], Hancke was able to eavesdrop at

better antenna design

I do not think this would be a factor at all if I had better antenna directional gain capability, but I do not and for now am looking forward to any improvements to a selectivity that is already the best that I have ever used in a radio's receiver.

better antenna directional gain

Software Defined Radio (SDR)

A radio communication system which uses software for the modulation and demodulation of radio signals

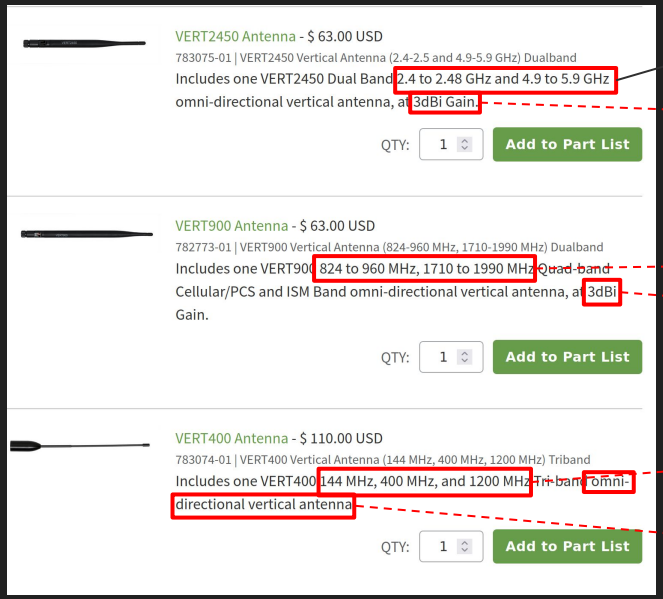
The goal of this design is to produce a radio that can receive and transmit a new form of radio protocol just by running new software configuration

SDR	Frequency
Ettus B210	70 MHz - 6 GHz
HackRF One	1 MHz - 6 GHz
BladeRF x40	300 MHz - 3.8 GHz
RTL-SDR	22 MHz - 2.2 GHz

Commonly Included Antennas

ANTST500 from Great Scott Gadgets is a telescopic antenna designed for operation from 75 MHz to 1 GHz. Its total length is configurable from 20 cm to 88 cm. ANT500 is constructed of stainless steel and features an SMA male connector, rotating shaft, and adjustable elbow.

75 MHz to 1 GHz.



2.4 to 2.48 GHz and 4.9 to 5.9 GHz

3dBi Gain.

824 to 960 MHz, 1710 to 1990 MHz

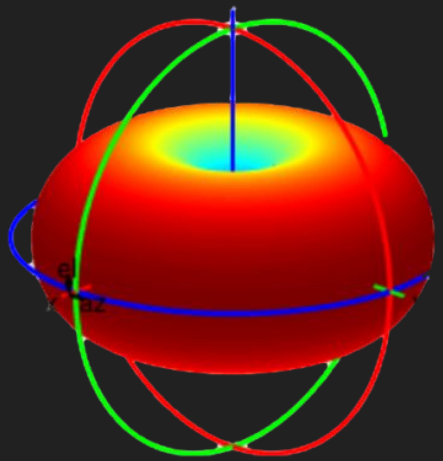
3dBi

144 MHz, 400 MHz, and 1200 MHz

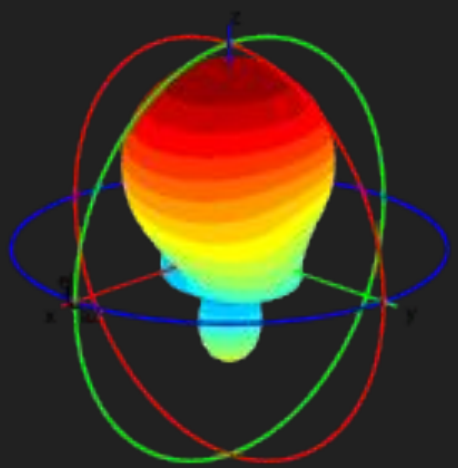
omni-directional vertical antenna

Directivity

Directivity is a ratio between antenna's radiation intensity in a given direction and the radiation intensity averaged over all directions



Omni-Directional

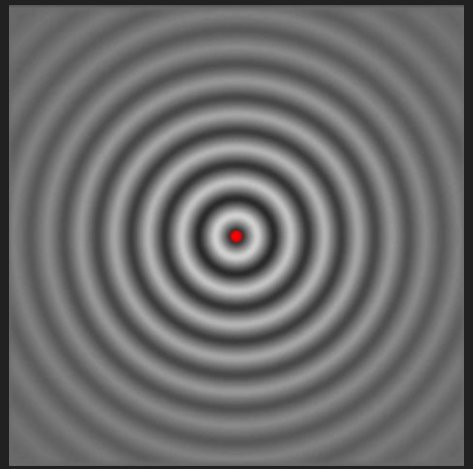


Directional

Antenna Gain

Antenna Gain is a measure of power radiated in a particular direction

Antenna	Gain
Loops Dipoles Monopoles	5 dBi or less
Microstrip Patches	5 dBi to 8 dBi
Yagi-Uda Log Periodic	8 dBi to 15 dBi
Horns Reflectors	15 dBi and more

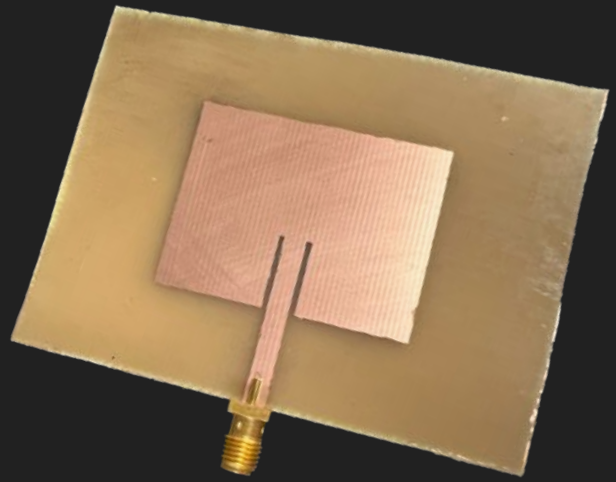


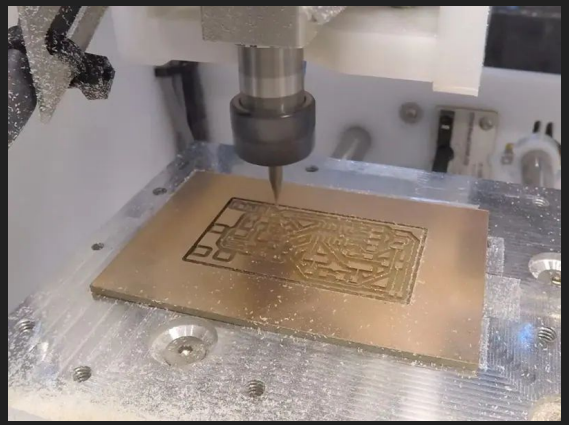
Solution

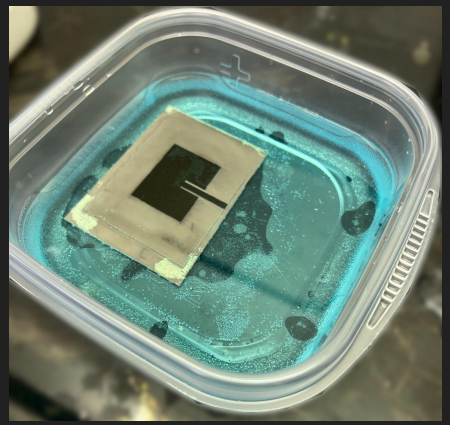
Design your own rectangular patch antenna

Use the tool from this presentation for measurements

Manufacture it using outlined methods







#whoami

Senior Security Consulting Engineer - Cisco Systems

PhD student - Virginia Commonwealth University

Experience with Reverse Engineering, Exploit Development, Pentesting, TCP/IP Networking, and Software Defined Radios

Certifications: OSCP/OSCE/OSWP/OSWE/OSEE/CCIE EI (#64597)

Part of WhatTheFreq! CTF team

Acknowledgments

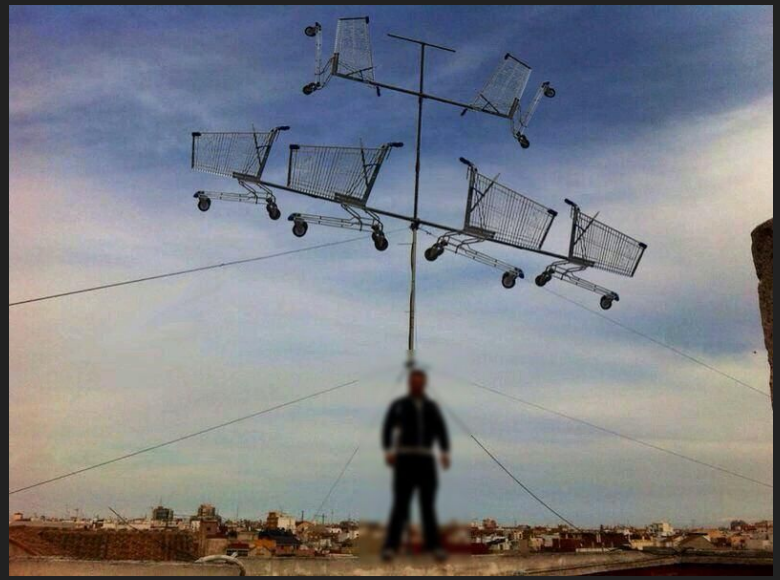
Jonathan Lundquist - PhD student (Virginia Commonwealth University)

Lauren Linkous - PhD student (Virginia Commonwealth University)

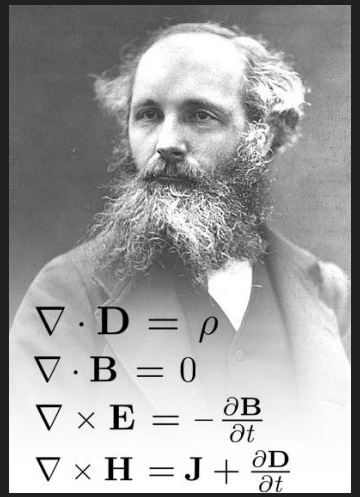
Dr. Erdem Topsakal - PhD advisor (Virginia Commonwealth University)

What’s an Antenna?

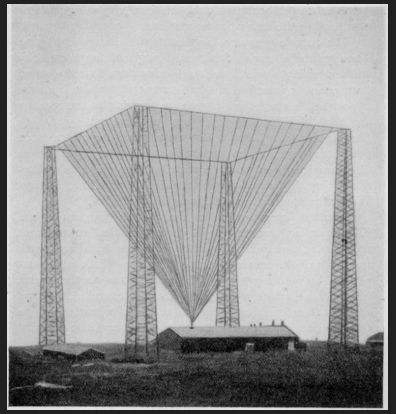
An antenna is a device that is used to efficiently transmit and receive electromagnetic waves.



History of Antennas

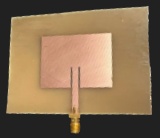


1864

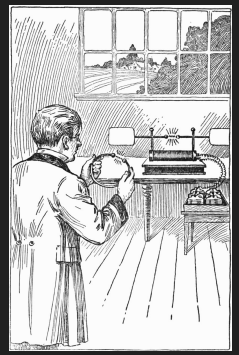


1901

1960s



1970s



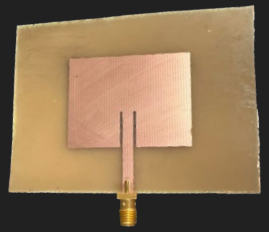
1886

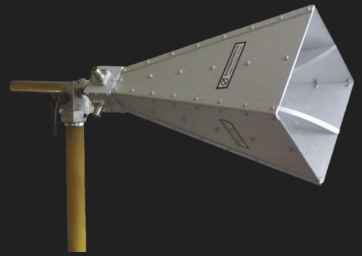
1935

1980s

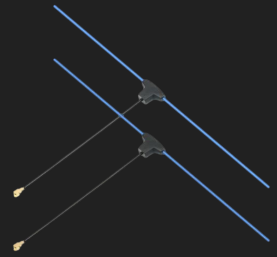
Common Antenna Types

- Wire antennas
- Microstrip antennas
- Antenna arrays
- Aperture antennas
- Reflector antennas



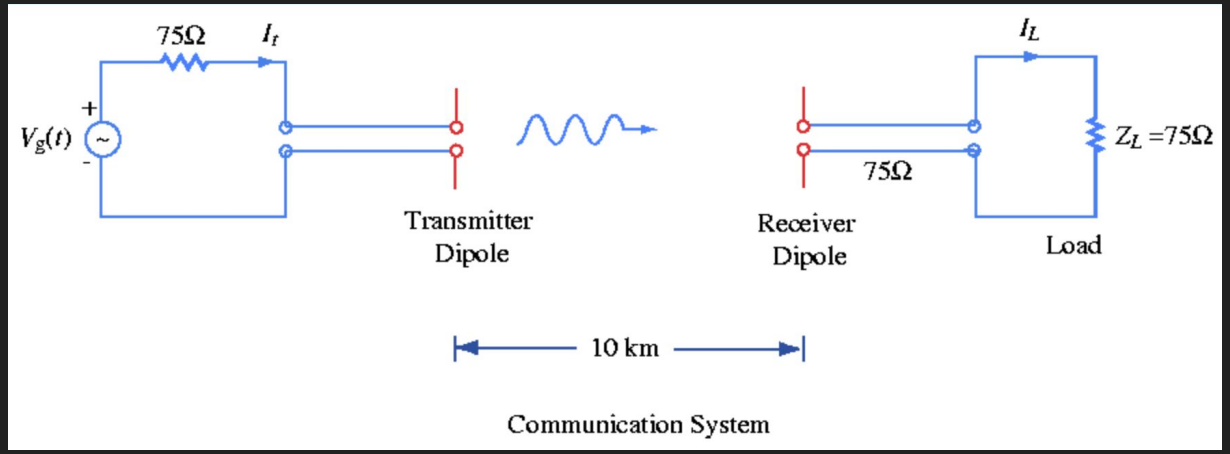


Dipole Antenna Example



Dipoles consist of two equal length conductors fed by a transmission line

The half wave dipole is named such because it is half a wavelength long



$$\lambda = \frac{v}{f}$$

λ = wavelength

v = velocity

f = frequency

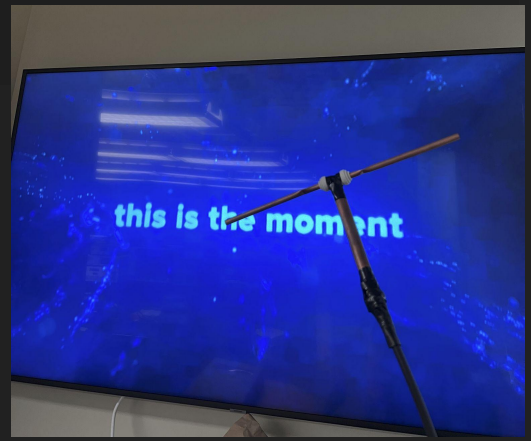
Dipole Antenna Example

Designing a Dipole Antenna for local TV

● WCVW + 1 subchannel	PBS RICHMOND, VA	57	W (15 miles)	UHF 560 Mhz

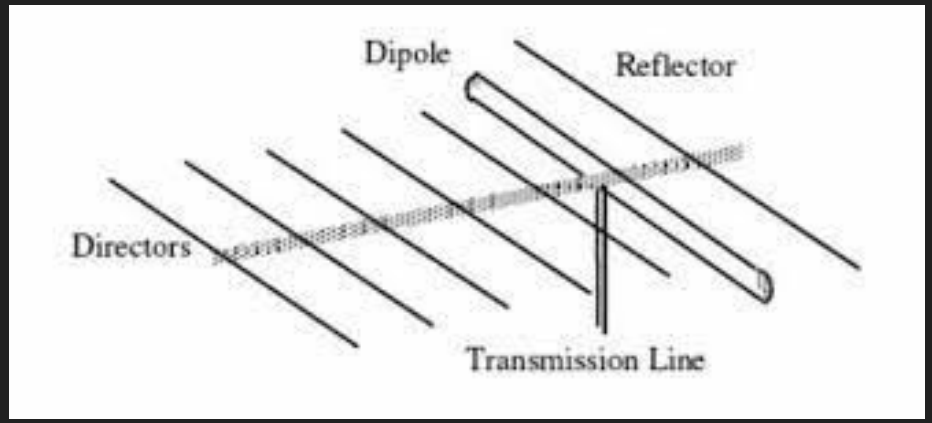
```
dollarhyde@ops:~/VCU/AntennaCalculator$ python3 antenna_calculator.py half_wave_dipole --frequency
560e6 --unit centimeter
[*] Total Dipole Length = 26.79 centimeter
[*] Each Dipole Element Length = 13.39 centimeter
```

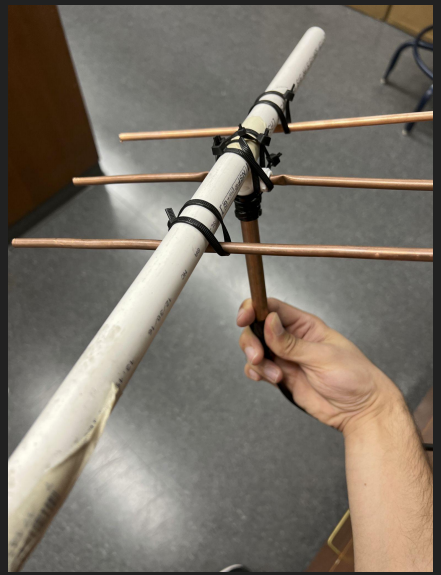
```
usage: antenna_calculator.py half_wave_dipole [--help] [--verbose] -f FREQUENCY
                                              [-u {meter,centimeter,millimeter,inch}]

optional arguments:
  --help                Show this help message and exit
  --verbose
  -f FREQUENCY, --frequency FREQUENCY
                        Frequency in Hz
  -u {meter,centimeter,millimeter,inch}, --unit {meter,centimeter,millimeter,inch}
                        Unit of measurement
```



Yagi-Uda Example

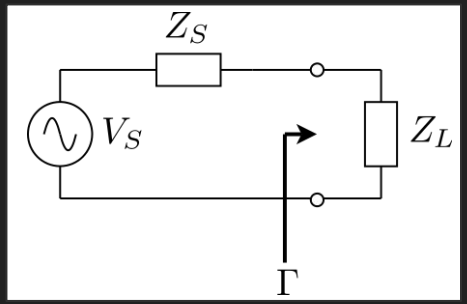
Yagi-Uda Antennas are commonly used TV antennas





Reflection Issues

Using Yagi-Uda antenna with SDRs will usually not result in advertised gain



$$\Gamma = \frac{Z_L - Z_0}{Z_L + Z_0}$$

Receive crystal clear digital 4K 1080p, 1080i HD broadcast local channel over the air. Built-in upgraded smart chip provides advanced VHF/UHF HD channels. Extended length and multi-element design allows stronger reception. Long range reach up to 200 mile (based on how far away from your local broadcast tower). Superior and durable construction to withstand tough outdoor weather conditions. Can be mounted in attic, roof, chimney, eave, mast or higher place to receive better signal. Easily Assemble required: antenna comes pre-assembled for some parts, fully assemble needed

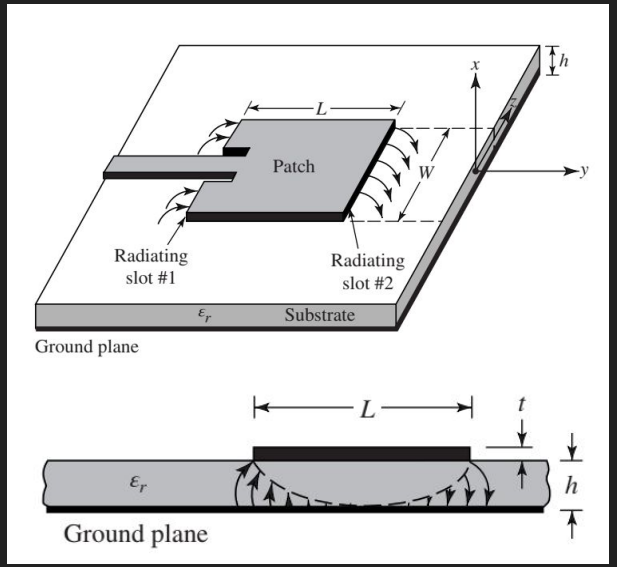
- Specification
  Frequency: VHF:45~230MHz UHF:470~860MHz
  Actual Gain: VHF:8dB UHF:12dB
  VSWR: VHF:<3dB UHF:<2.5dB
  Output Impedance: 75Ω
  Transmission Distance: 200+ Miles
- Package Included:
  one Antenna
  one 40ft cable
  one 4-way splitter
  one J-pole

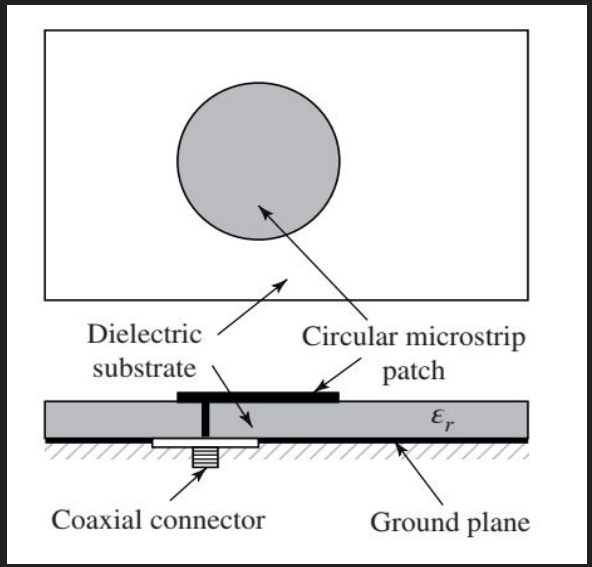
Actual Gain: VHF:8dB UHF:12dB

Output Impedance: 75Ω

Patch Antennas

- High directivity
- High gain
- Low power
- Low profile
- Easy to manufacture





Patch Antenna Math

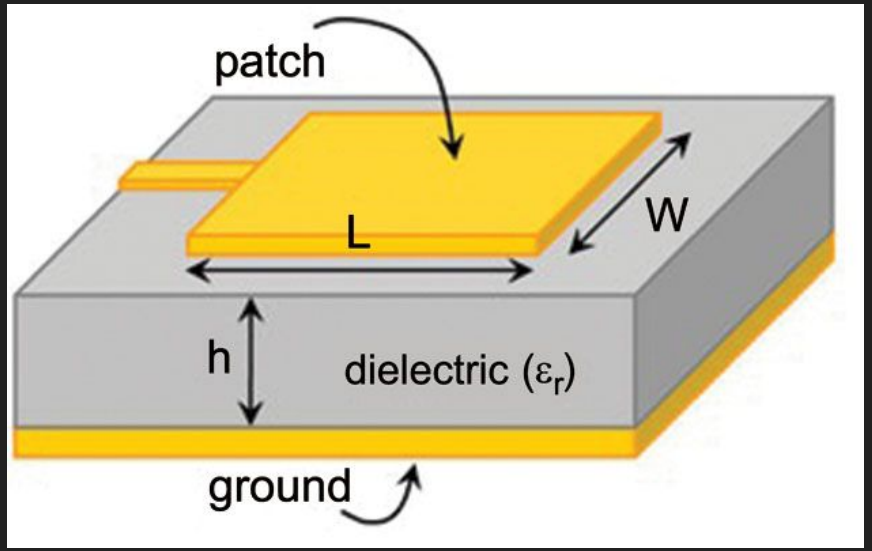
Transmission-Line Model

Given the following:

- Frequency
- Dielectric constant of the substrate
- Height of the substrate

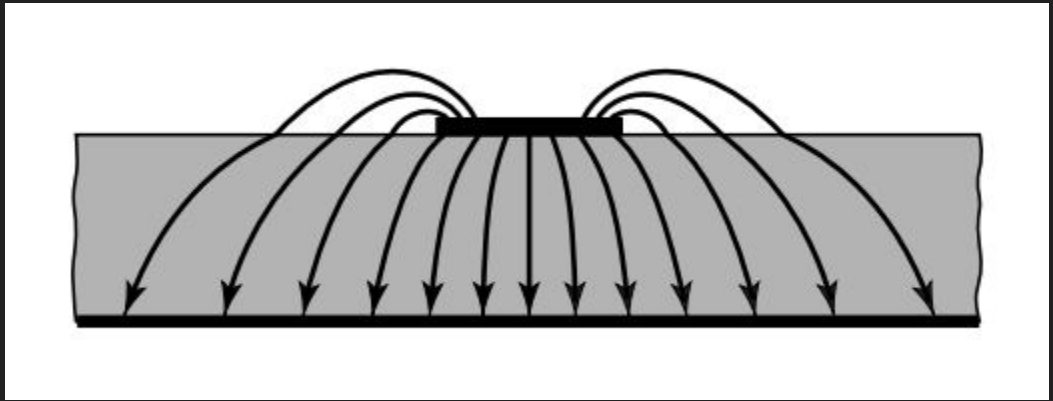
Most commonly used substrate is FR4:

- Dielectric constant of 4.4
- Height of 1.6 mm



Patch Antenna Math

The fields at the edge of the patch undergo fringing



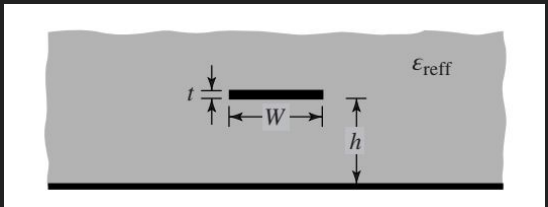
Patch Antenna Math

Width of the patch can be find with following formula

$$W = \frac{1}{2f_r\sqrt{\mu_0\varepsilon_0}}\sqrt{\frac{2}{\varepsilon_r + 1}} = \frac{v_0}{2f_r}\sqrt{\frac{2}{\varepsilon_r + 1}}$$

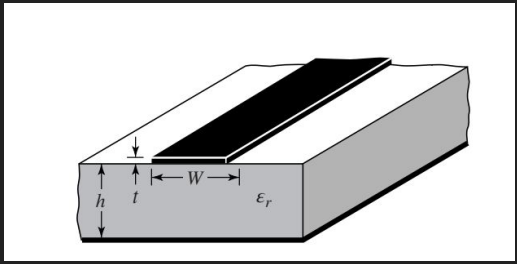
Patch Antenna Math

Effective Dielectric Constant Ereff is the dielectric constant of the uniform dielectric material so that following figure has identical electrical characteristics as actual line



Effective Dielectric Constant

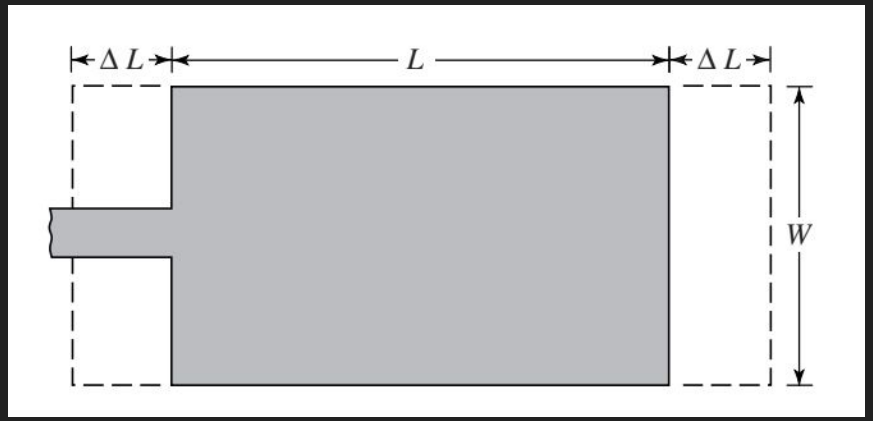
$$\varepsilon_{reff} = \frac{\varepsilon_r + 1}{2} + \frac{\varepsilon_r - 1}{2}\left[1 + 12\frac{h}{W}\right]^{-1/2}$$

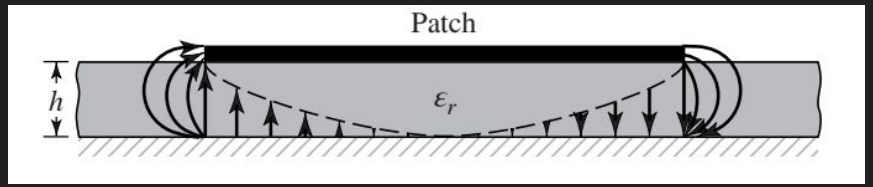


Actual microstrip line

Patch Antenna Math

Due to fringing effects, electrically the patch looks greater than physical dimensions





$$\frac{\Delta L}{h} = 0.412 \frac{(\varepsilon_{\text{reff}} + 0.3)\left(\frac{W}{h} + 0.264\right)}{(\varepsilon_{\text{reff}} - 0.258)\left(\frac{W}{h} + 0.8\right)}$$

$$L = \frac{1}{2f_r\sqrt{\varepsilon_{\text{reff}}}\sqrt{\mu_0\varepsilon_0}} - 2\Delta L$$

Patch Antenna Math

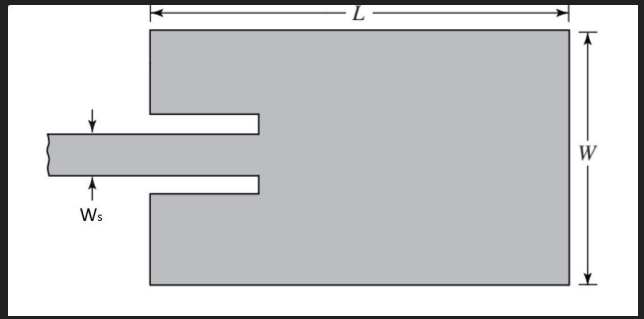
Stripline calculation

If following is satisfied then use that strip width

$$A = \frac{Z_0}{60}\sqrt{\frac{\epsilon_r + 1}{2}} + \frac{\epsilon_r - 1}{\epsilon_r + 1}\left(0.23 + \frac{0.11}{\epsilon_r}\right) \qquad \frac{W_s}{d} = \frac{8e^A}{e^{2A} - 2} \quad if \quad \frac{W_s}{d} < 2$$

Else use following

$$B = \frac{377\pi}{2Z_0\sqrt{\epsilon_r}} \qquad \frac{W_s}{d} = \frac{2}{\pi}\left[B - 1 - ln(2B - 1) + \frac{\epsilon_r - 1}{2\epsilon_r}\left\{ln(B - 1) + 0.39 - \frac{0.61}{\epsilon_r}\right\}\right] \quad if \quad \frac{W_s}{d} > 2$$



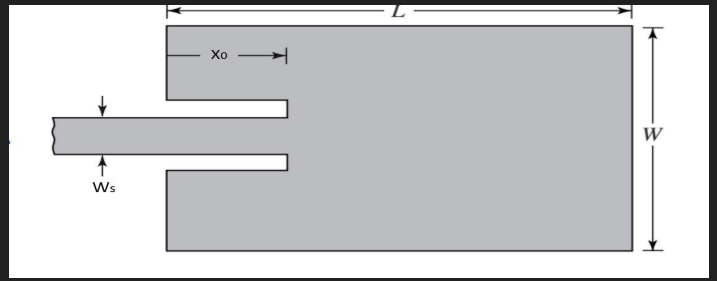
Patch Antenna Math

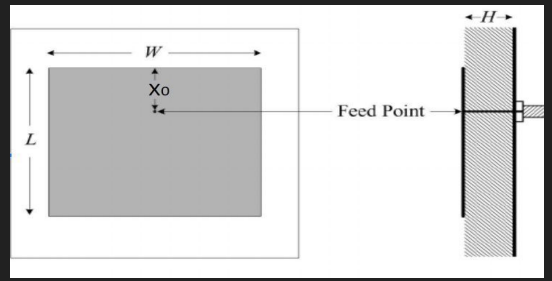
Inset calculation for both microstrip and probe fed patch antennas

$$Z_{in}(x=0) = 90\frac{\epsilon_r^2}{\epsilon_r - 1}\left(\frac{L}{W}\right)^2$$

$$Z_{in}(x=x_0) = Z_{in}(x=0)cos^2\left(\frac{\pi}{L}x_0\right)$$

$$y_0 = \frac{1}{2}W$$





Automating Patch Antenna Math

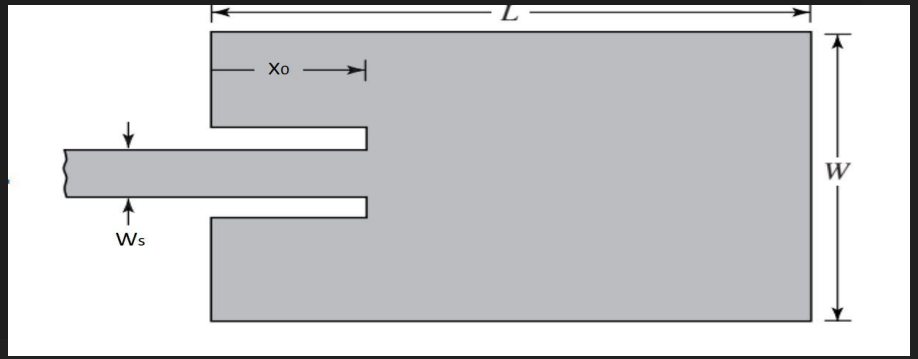
```
dollarhyde@ops:~/VCU/AntennaCalculator$ python3 antenna_calculator.py rectangular_patch --help
usage: antenna_calculator.py rectangular_patch [--help] [--verbose] [--type {microstrip,probe}] -f FREQUENCY -er RELATIVE_PERMITTIVITY -h HEIGHT
                                               [-u {meter,centimeter,millimeter,inch}] [-du {meter,centimeter,millimeter,inch}] [--dxfoutput DXFOUTPUT]
                                               [--pngoutput PNGOUTPUT]

optional arguments:
  --help                Show this help message and exit
  --verbose
  --type {microstrip,probe}
                        Type of patch
  -f FREQUENCY, --frequency FREQUENCY
                        Frequency in Hz
  -er RELATIVE_PERMITTIVITY, --relative_permittivity RELATIVE_PERMITTIVITY
                        Relative permittivity
  -h HEIGHT, --height HEIGHT
                        Substrate height in meters
  -u {meter,centimeter,millimeter,inch}, --unit {meter,centimeter,millimeter,inch}
                        Unit of measurement
  -du {meter,centimeter,millimeter,inch}, --dxfunit {meter,centimeter,millimeter,inch}
                        DXF Unit of measurement
  --dxfoutput DXFOUTPUT
                        Name of DXF file
  --pngoutput PNGOUTPUT
                        Name of PNG image for printing
```

Automating Patch Antenna Math

Example 2.4 GHz antenna with FR4

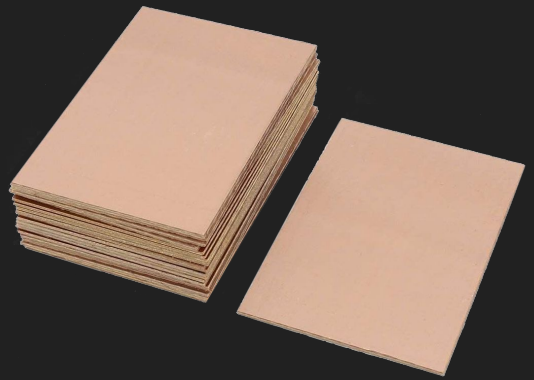
```
dollarhyde@ops:~/VCU/AntennaCalculator$ python3 antenna_calculator.py rectangular_patch --type microstrip -f 2.4e9 -er 4.4 -h 1.6e-3
[*] W = 38.04 millimeter
[*] L = 29.44 millimeter
[*] Ws = 3.06 millimeter
[*] y0 = 19.02 millimeter
[*] x0 = 11.32 millimeter
```

```
dollarhyde@ops:~/VCU/AntennaCalculator$ python3 antenna_calculator.py rectangular_patch --type microstrip -f 2.4e9 -er 4.4 -h 1.6e-3 --verbose
{'subparser_name': 'rectangular_patch', 'verbose': True, 'type': 'microstrip', 'frequency': 2400000000.0, 'relative_permittivity': 4.4, 'height': 0.0016,
 'unit': None, 'dxfunit': None, 'dxfoutput': 'patch.dxf', 'pngoutput': 'patch.png'}
[*] W = 38.04 millimeter
[*] Ereff = 4.09
[*] dL = 738.82 micrometer
[*] Leff = 30.92 millimeter
[*] L = 29.44 millimeter
[*] A = 1.529861949318471
[*] A Ws/d = 1.9118593643297774
[*] A is valid
[*] Ws = 3.06 millimeter
[*] y0 = 0.01901814435781827
[*] y0 = 19.02 millimeter
[*] Zin_0 = 396.6828700137873
[*] Zin_x0 = 50
[*] x0 = 0.01131973828663886
[*] x0 = 11.32 millimeter
```



Manufacturing Patch Antennas

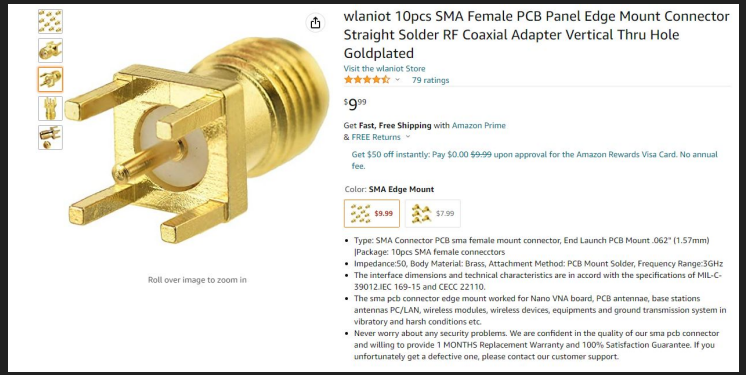
- Copper tape
- Chemical etching
- PCB milling
- Computer numerical control (CNC) method
- Professional fabrication



Copper Tape

Materials needed:

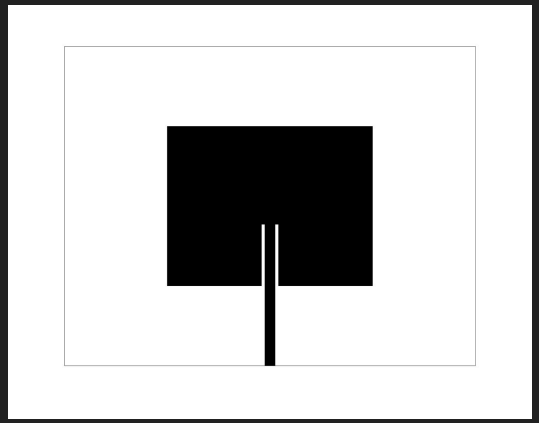
- Copper Tape
- Single Sided FR-4
- SMA Connector

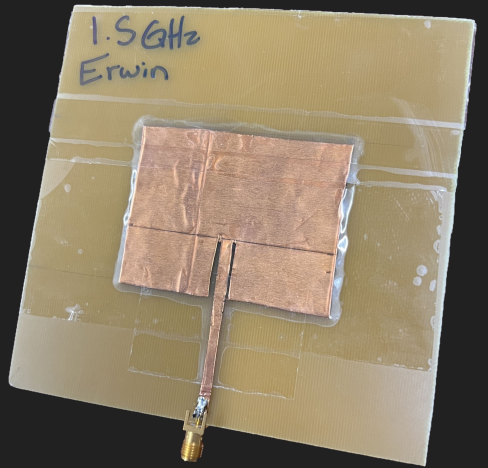


Copper Tape

Use the printout as a template to help cut the tape

```
dollarhyde@ops:~/VCU/AntennaCalculator$ python3 antenna_calculator.py rectangular_patch --type microstrip -f 1.5e9 -er 4.4 -h 1.6e-3 --pngoutput 1_5_FR4_
microstrip.png
[*] W = 60.86 millimeter
[*] L = 47.41 millimeter
[*] Ws = 3.06 millimeter
[*] y0 = 30.43 millimeter
[*] x0 = 18.25 millimeter
```

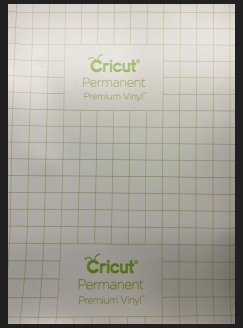


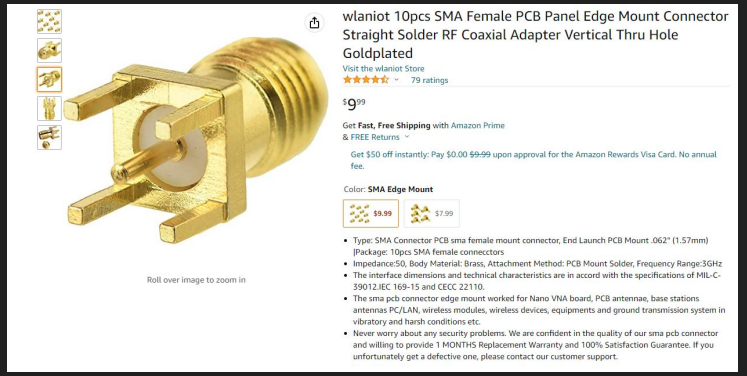


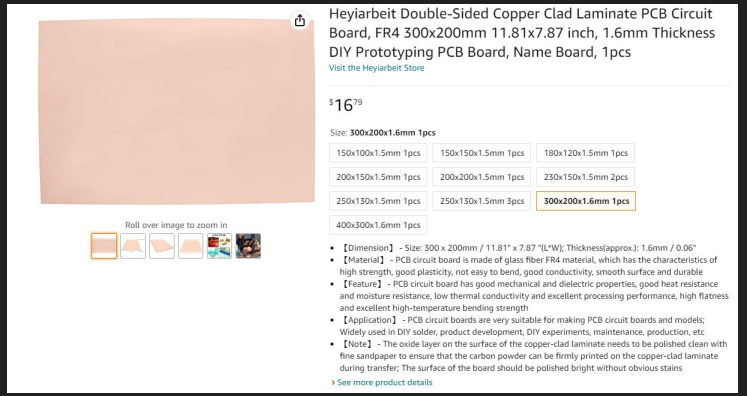
Chemical Etching

Materials needed:

- Muriatic Acid (HCl)
- Hydrogen Peroxide (H_2O_2)
- Double Sided FR-4
- SMA Connector
- Iron
- Laser Printer
- Vinyl Backing
- Nail Polish (optional)
- Thermometer/FLIR camera (optional)

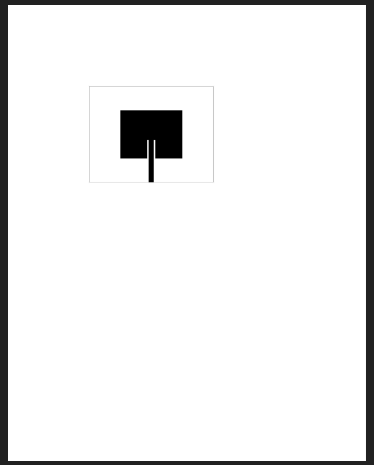


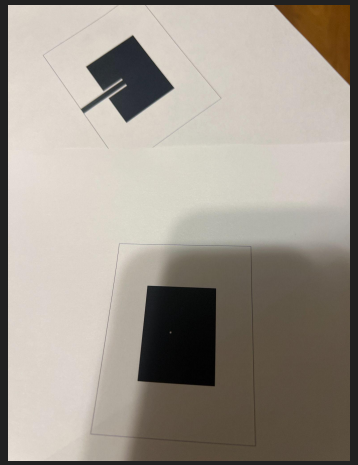


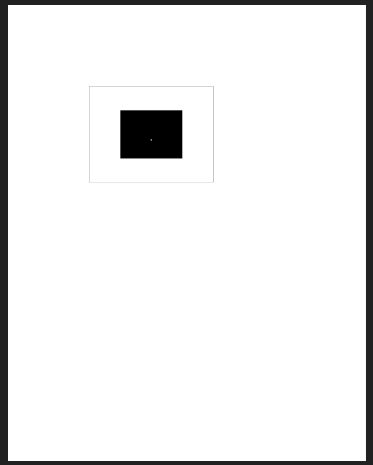


Chemical Etching

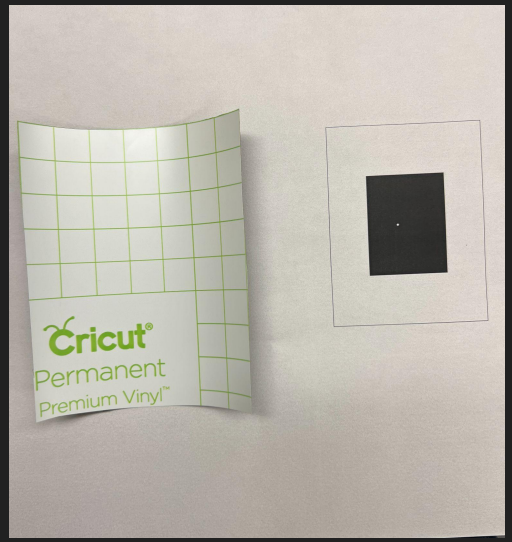
```
dollarhyde@ops:~/VCU/AntennaCalculator$ python3 antenna_calculator.py rectangular_patch --type microstrip -f 2.4e9 -er 4.4 -h 1.6e-3 --pngoutput 2_4_FR4_
microstrip.png
[*] W = 38.04 millimeter
[*] L = 29.44 millimeter
[*] Ws = 3.06 millimeter
[*] y0 = 19.02 millimeter
[*] x0 = 11.32 millimeter
dollarhyde@ops:~/VCU/AntennaCalculator$ python3 antenna_calculator.py rectangular_patch --type probe -f 2.4e9 -er 4.4 -h 1.6e-3 --pngoutput 2_4_FR4_probe
.png
[*] W = 38.04 millimeter
[*] L = 29.44 millimeter
[*] y0 = 19.02 millimeter
[*] x0 = 11.32 millimeter
```



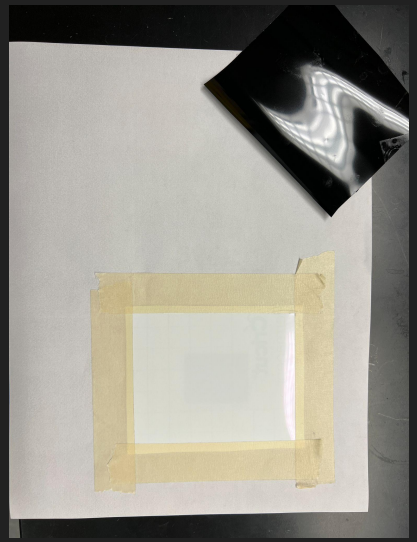




Chemical Etching

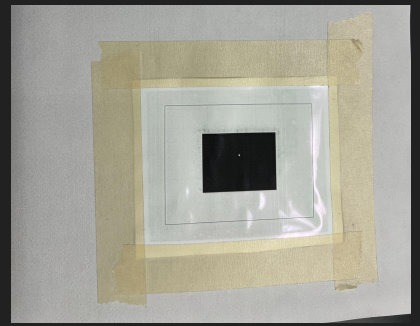


Print on regular paper

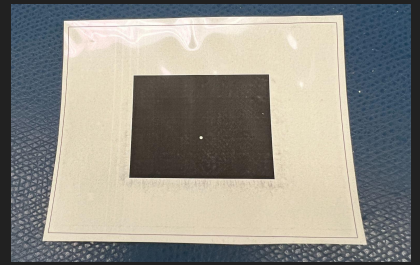


Attach vinyl backing glossy side up

Place paper back in the printer's input tray



Print again

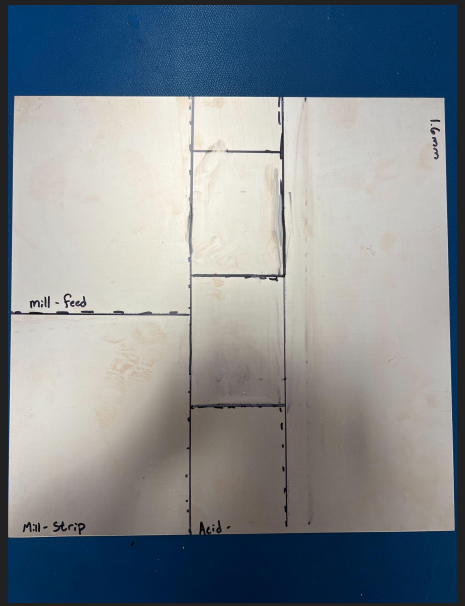


Trim excess backing

Chemical Etching

Double-sided FR-4

Measure the thickness



Measure cuts

Cut

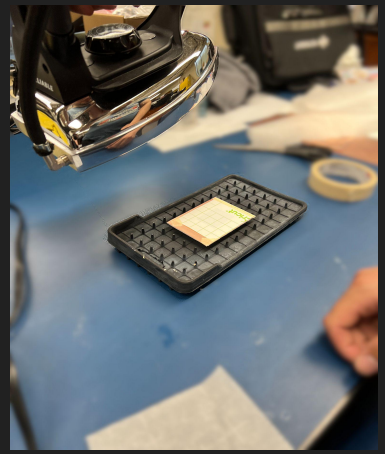
Chemical Etching

Turn on the iron

It should be between 140-158 °C

Chemical Etching

Tape the printed patch to FR-4



Place it under the iron

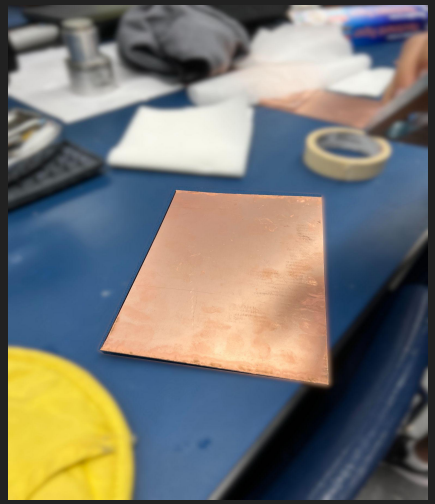
Place parchment (baking) paper on top

Iron for about 2-3 min

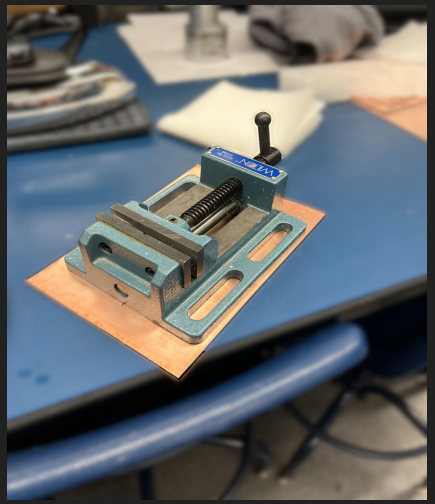
Move the iron around

Chemical Etching

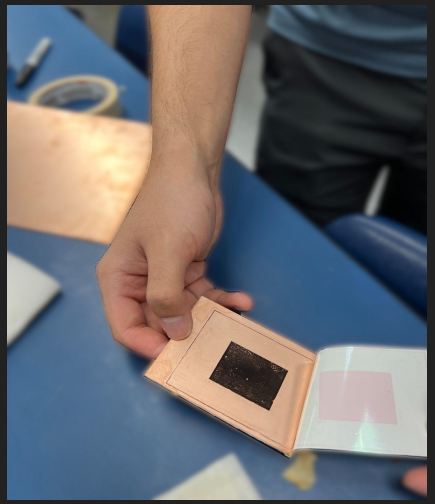
Remove the iron



Add a flat surface

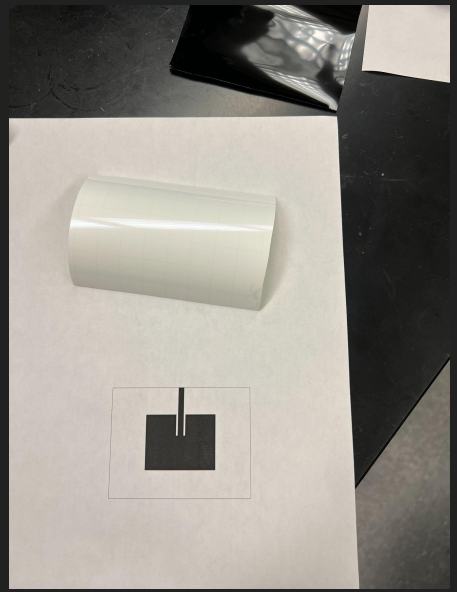


Place a heavy weight

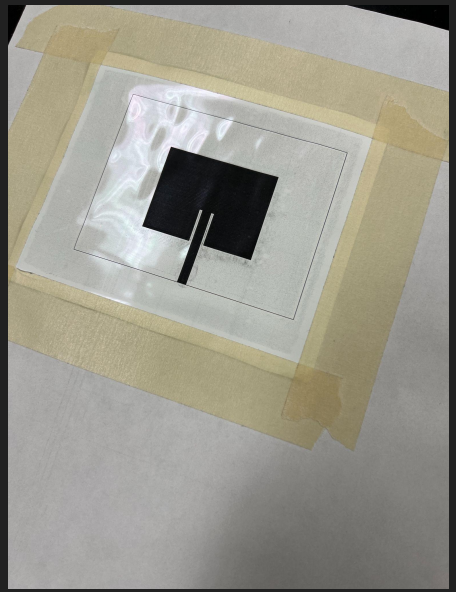


Peel the vinyl

Chemical Etching

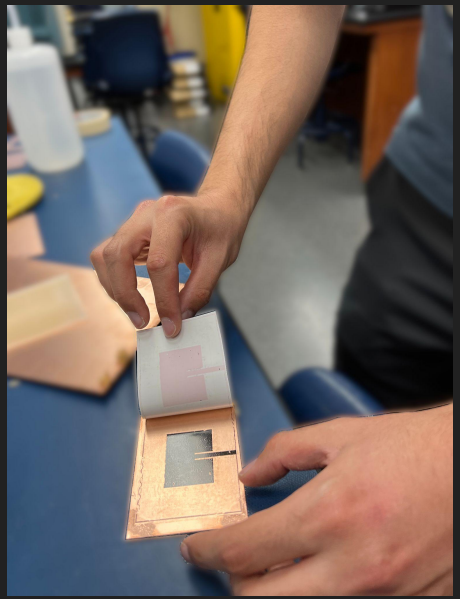


Attach vinyl backing



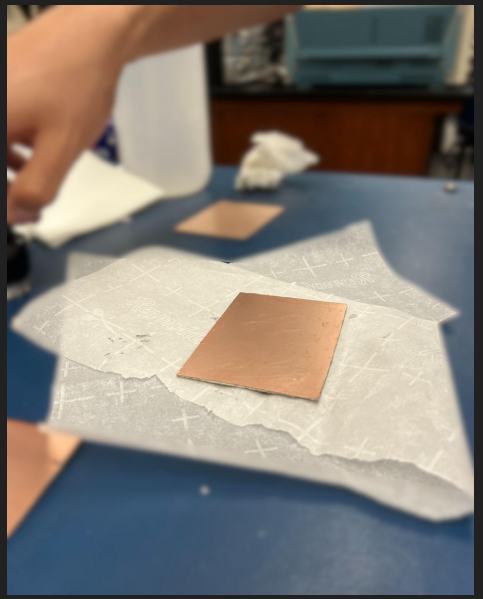
Print

Iron



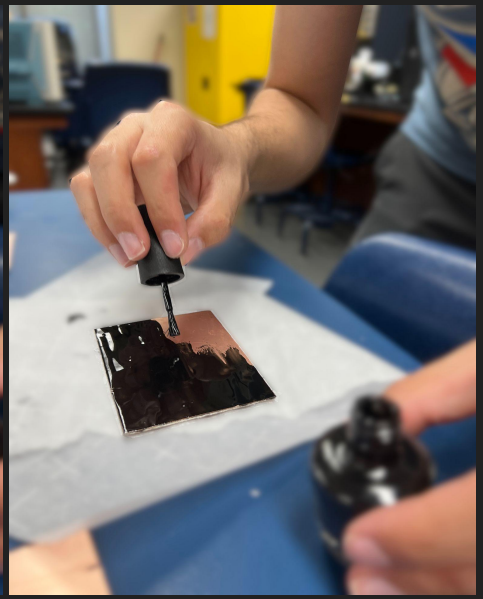
Done

Chemical Etching



Turn the patch to the other side

Apply a coating



Apply a coating

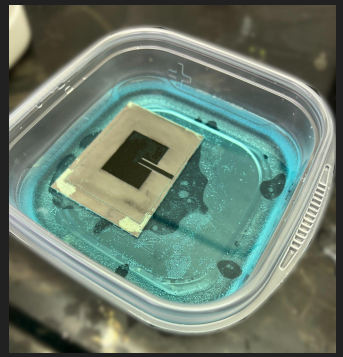
Let it dry

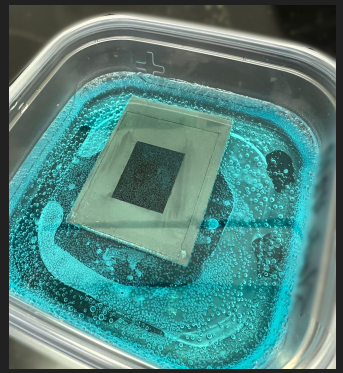
Chemical Etching

1x Muriatic Acid (HCl)

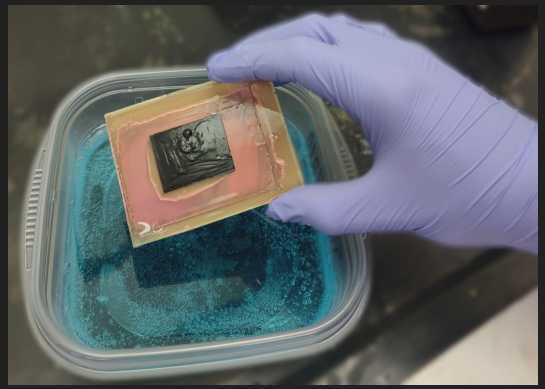
2x Hydrogen Peroxide (H2O2)

Chemical Etching

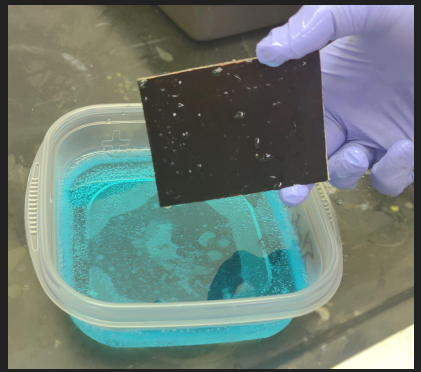


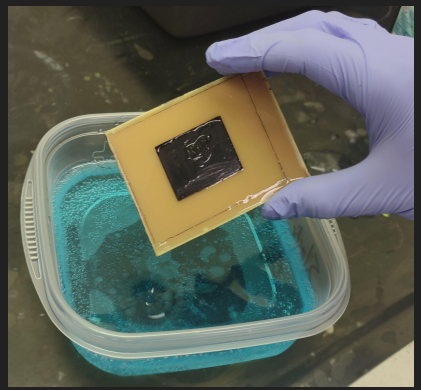


Start the process

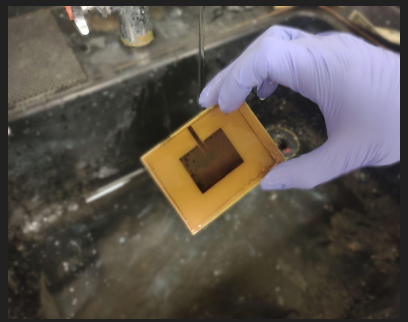


Acid removing the copper



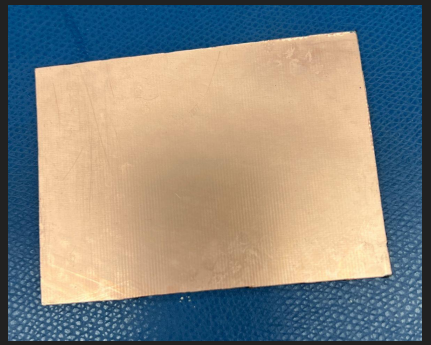


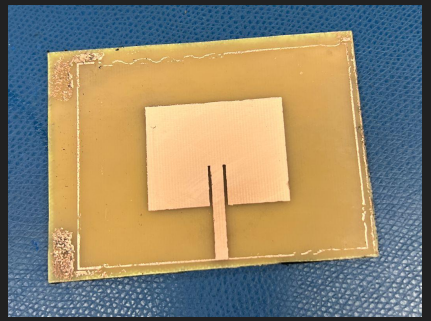
Copper removed



Rinse with water

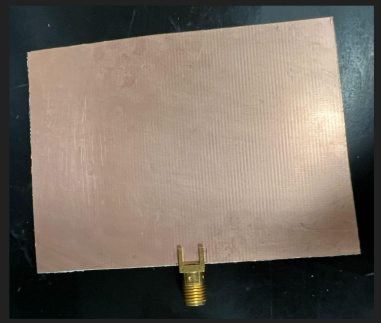
Chemical Etching

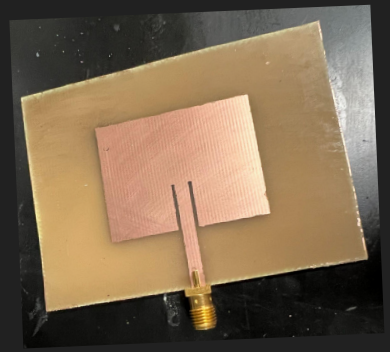




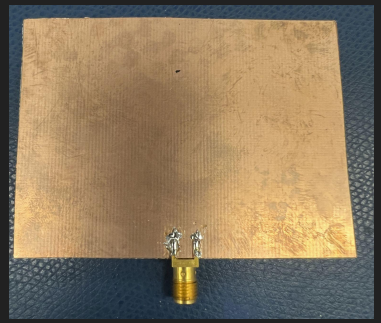
Clean using acetone

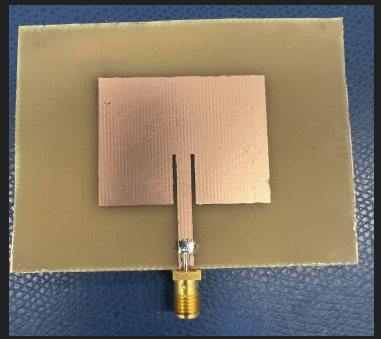
Cut SMA connector legs





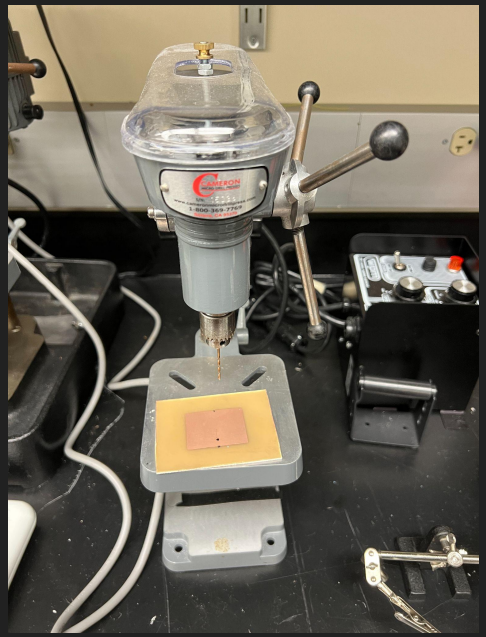
Attach SMA connector



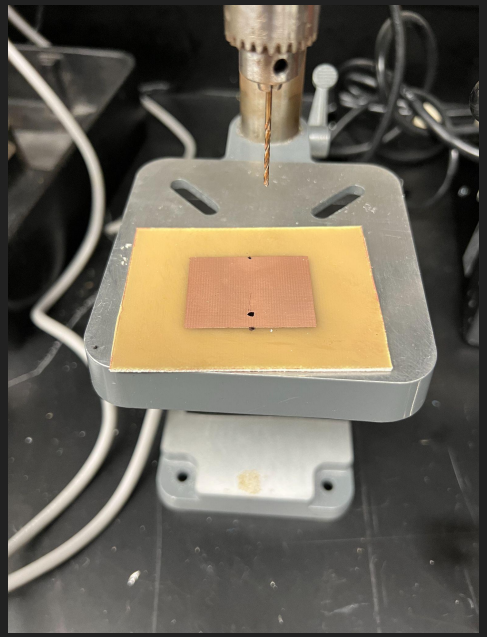


Solder the pin

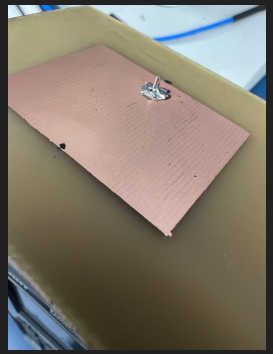
Chemical Etching



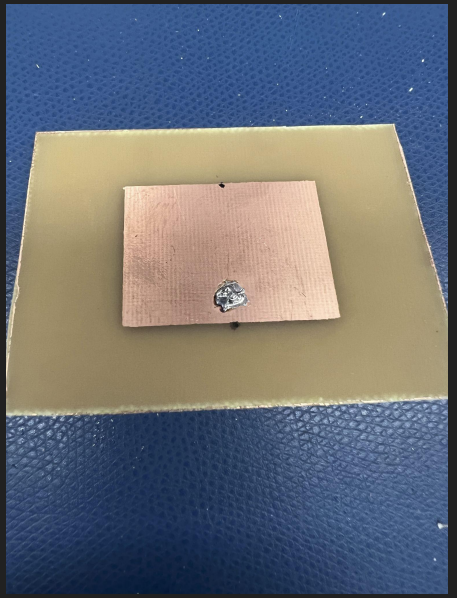
Position thin drill bit carefully



Drill the hole



Solder on both sides

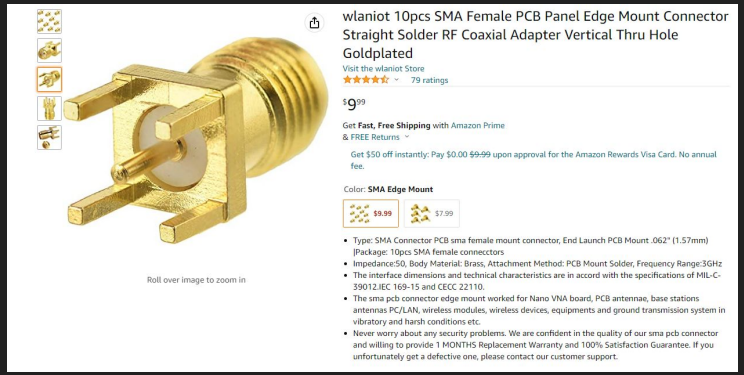


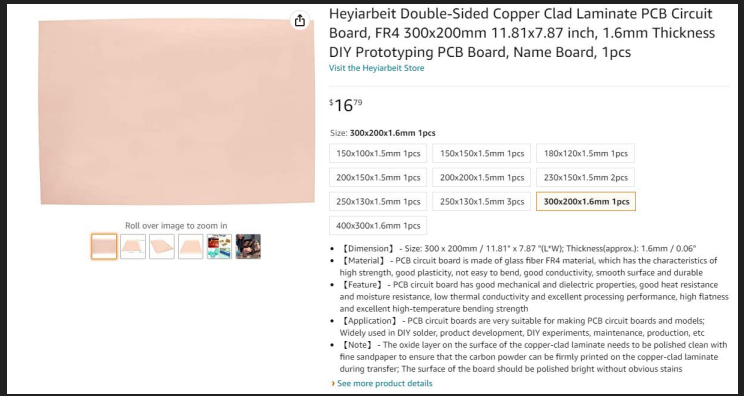
Cut the top of the pin

PCB milling

Materials needed:

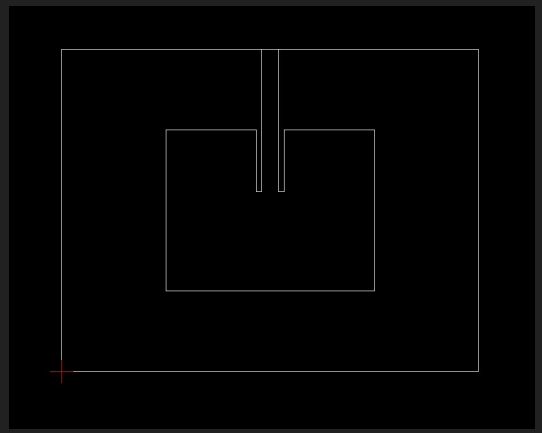
- PCB Prototyping Machine
- Double Sided FR-4
- SMA Connector

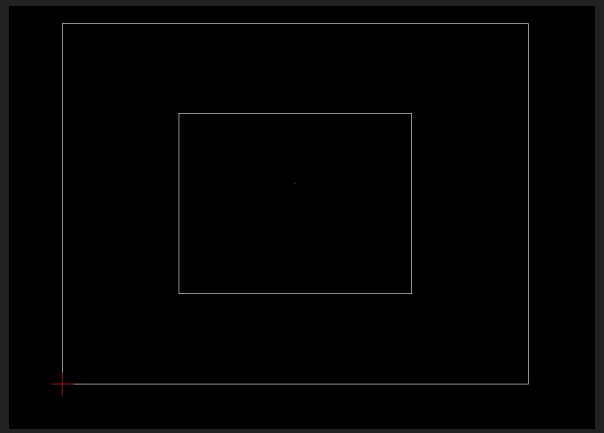




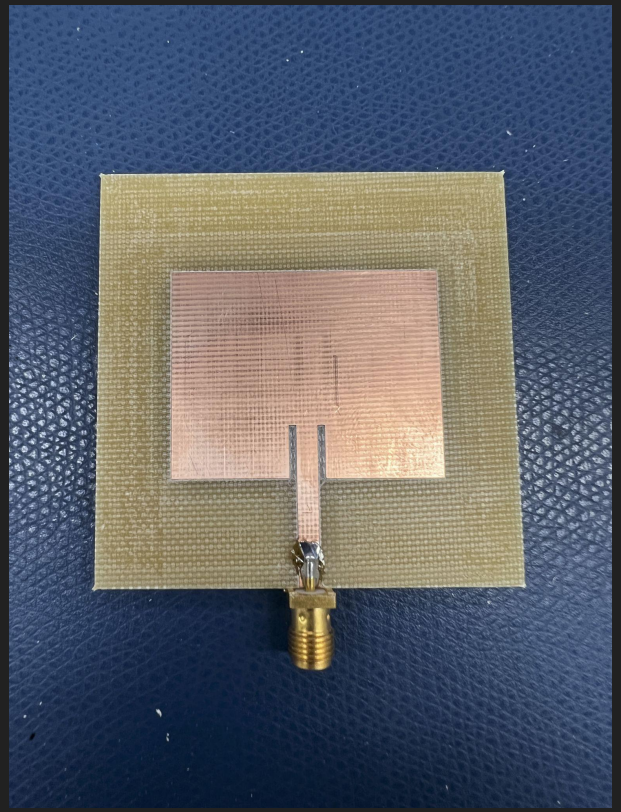
PCB milling

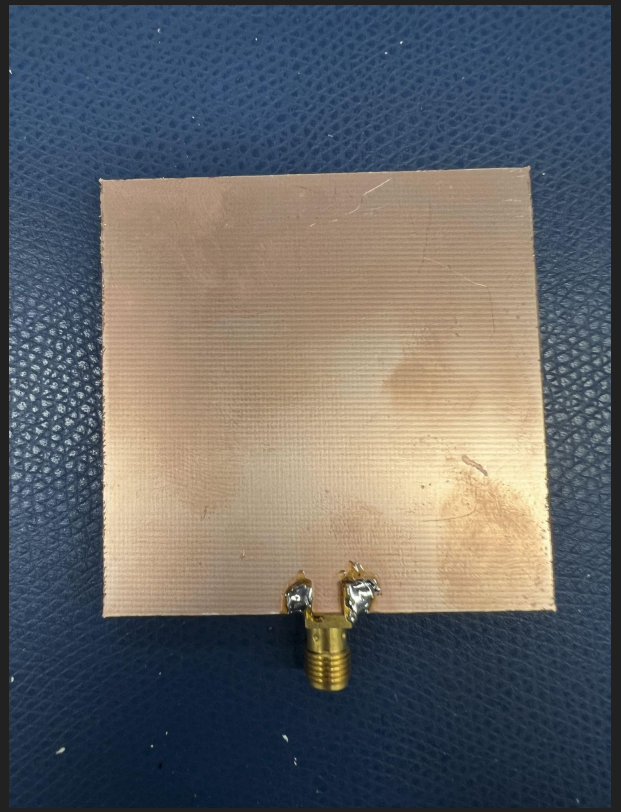
```
dollarhyde@ops:~/VCU/AntennaCalculator$ python3 antenna_calculator.py rectangular_patch --type microstrip -f 2.4e9 -er 4.4 -h 1.6e-3 --dxfunit millimeter
 --dxfoutput 2_4_FR4_microstrip_mm.dxf
[*] W = 38.04 millimeter
[*] L = 29.44 millimeter
[*] Ws = 3.06 millimeter
[*] y0 = 19.02 millimeter
[*] x0 = 11.32 millimeter
dollarhyde@ops:~/VCU/AntennaCalculator$ python3 antenna_calculator.py rectangular_patch --type probe -f 2.4e9 -er 4.4 -h 1.6e-3 --dxfunit millimeter --dx
foutput 2_4_FR4_probe_mm.dxf
[*] W = 38.04 millimeter
[*] L = 29.44 millimeter
[*] y0 = 19.02 millimeter
[*] x0 = 11.32 millimeter
```





PCB milling

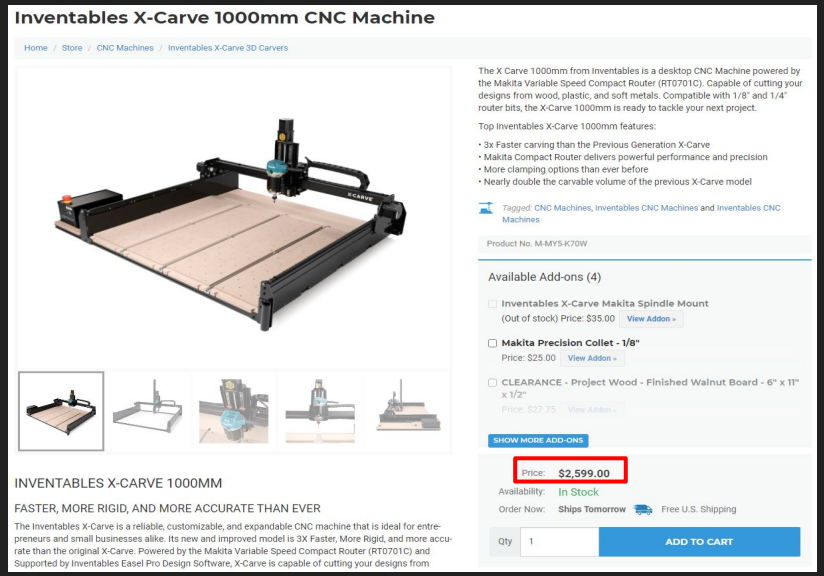




CNC Method

Materials needed:

- CNC Machine
- Double Sided FR-4
- SMA Connector



Inventables X-Carve 1000mm CNC Machine

Home / Store / CNC Machines / Inventables X-Carve 3D Carvers

The X Carve 1000mm from Inventables is a desktop CNC Machine powered by the Makita Variable Speed Compact Router (RT0701C). Capable of cutting your designs from wood, plastic, and soft metals. Compatible with 1/8" and 1/4" router bits, the X-Carve 1000mm is ready to tackle your next project.

Top Inventables X-Carve 1000mm features:

- 3x Faster carving than the Previous Generation X-Carve
- Makita Compact Router delivers powerful performance and precision
- More clamping options than ever before
- Nearly double the carvable volume of the previous X-Carve model

Tagged: CNC Machines, Inventables CNC Machines and Inventables CNC Machines

Product No. M-MYS-K70W

Available Add-ons (4)

Inventables X-Carve Makita Spindle Mount
(Out of stock) Price: $35.00 View Addon »

Makita Precision Collet - 1/8"
Price: $25.00 View Addon »

CLEARANCE - Project Wood - Finished Walnut Board - 6" x 11" x 1/2"
Price: $27.75 View Addon »

SHOW MORE ADD-ONS

Price: $2,599.00
Availability: In Stock
Order Now: Ships Tomorrow Free U.S. Shipping

Qty 1 ADD TO CART

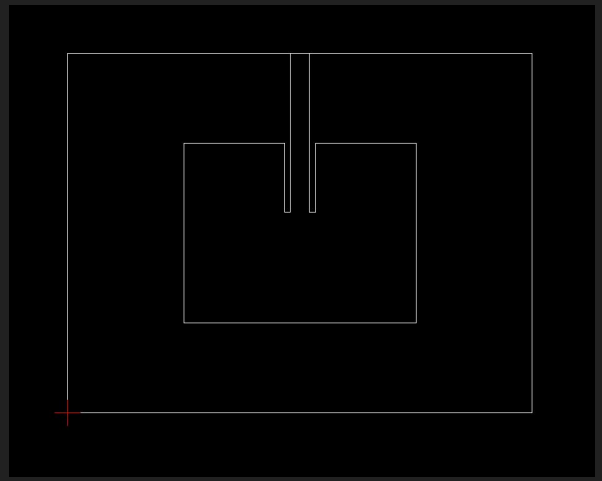
INVENTABLES X-CARVE 1000MM

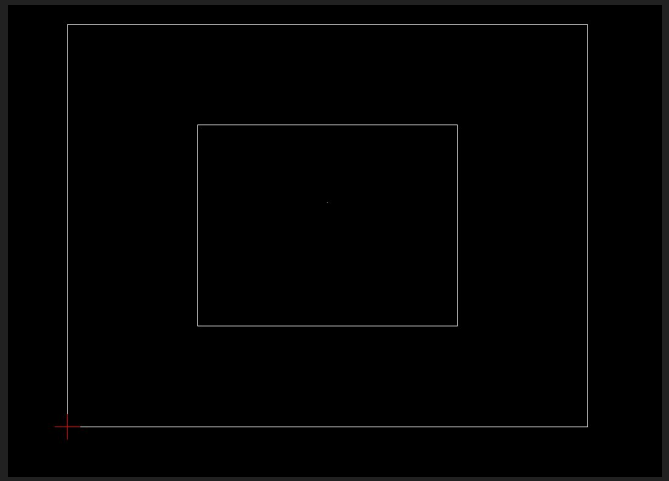
FASTER, MORE RIGID, AND MORE ACCURATE THAN EVER

The Inventables X-Carve is a reliable, customizable, and expandable CNC machine that is ideal for entrepreneurs and small businesses alike. Its new and improved model is 3X Faster, More Rigid, and more accurate than the original X-Carve. Powered by the Makita Variable Speed Compact Router (RT0701C) and Supported by Inventables Easel Pro Design Software, X-Carve is capable of cutting your designs from

CNC Method

```
dollarhyde@ops:~/VCU/AntennaCalculator$ python3 antenna_calculator.py rectangular_patch --type microstrip -f 2.4e9 -er 4.4 -h 1.6e-3 --dxfunit inch --dxf
output 2_4_FR4_microstrip_inch.dxf
[*] W = 38.04 millimeter
[*] L = 29.44 millimeter
[*] Ws = 3.06 millimeter
[*] y0 = 19.02 millimeter
[*] x0 = 11.32 millimeter
dollarhyde@ops:~/VCU/AntennaCalculator$ python3 antenna_calculator.py rectangular_patch --type probe -f 2.4e9 -er 4.4 -h 1.6e-3 --dxfunit inch --dxfoutpu
t 2_4_FR4_probe_inch.dxf
[*] W = 38.04 millimeter
[*] L = 29.44 millimeter
[*] y0 = 19.02 millimeter
[*] x0 = 11.32 millimeter
```





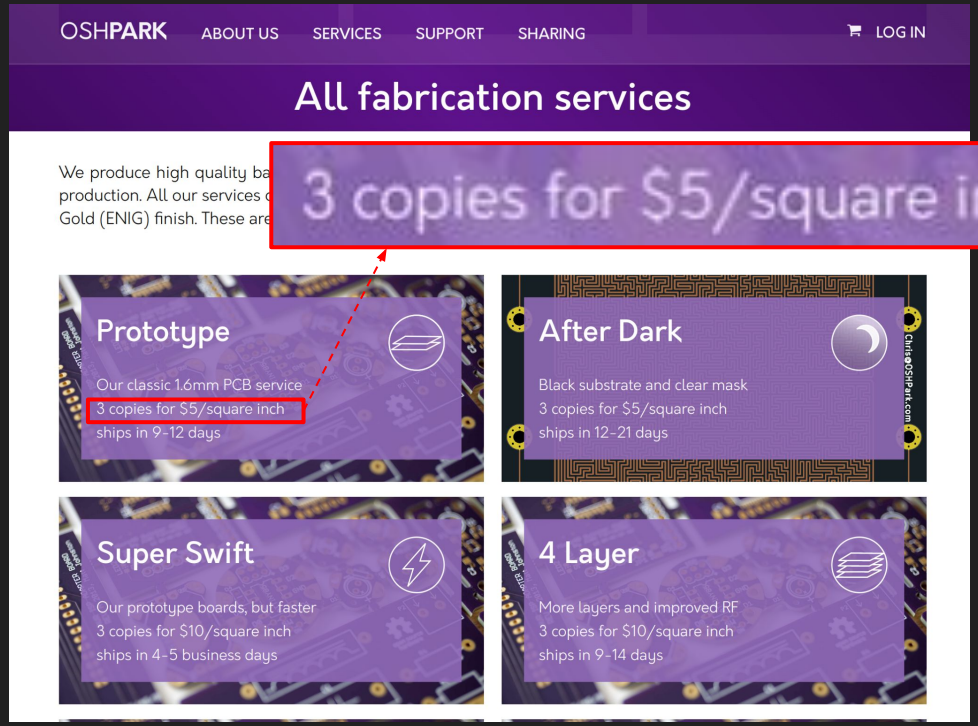
Professional Fabrication

Common file formats:

- KiCAD
- EagleCAD
- Gerber

Let's get started!

Drag and drop your KiCAD, EagleCAD, or zipped Gerber files

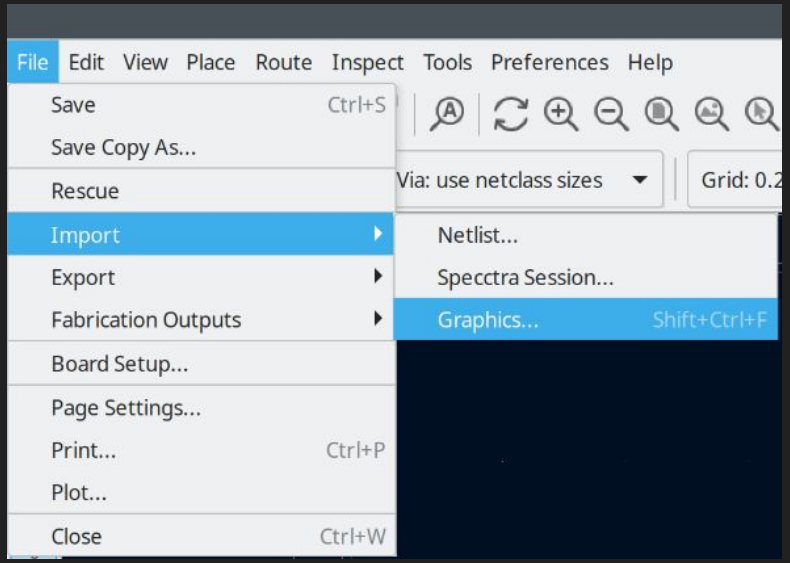


Professional Fabrication

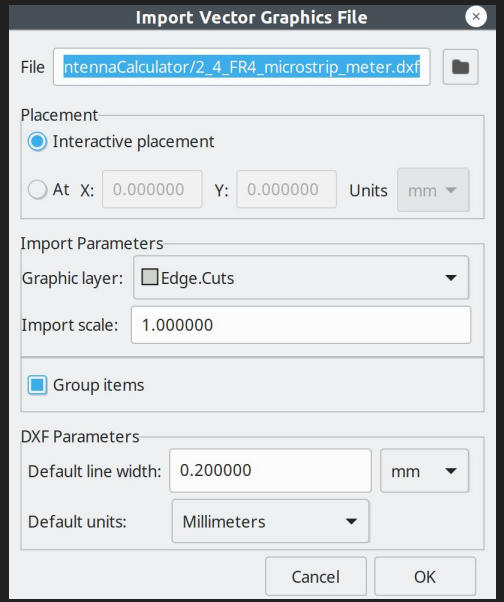
- Currently not supported direct export
- Planned in future releases
- Workaround: DXF file can be converted
  - KiCAD 6 PCB Editor allows DXF import
  - It can be exported as KiCAD file or Gerber

```
dollarhyde@ops:~/VCU/AntennaCalculator$ python3 antenna_calculator.py rectangular_patch --type microstrip -f 2.4e9 -er 4.4 -h 1.6e-3 --dxfunit meter --dx
foutput 2_4_FR4_microstrip_meter.dxf
[*] W = 38.04 millimeter
[*] L = 29.44 millimeter
[*] Ws = 3.06 millimeter
[*] y0 = 19.02 millimeter
[*] x0 = 11.32 millimeter
```

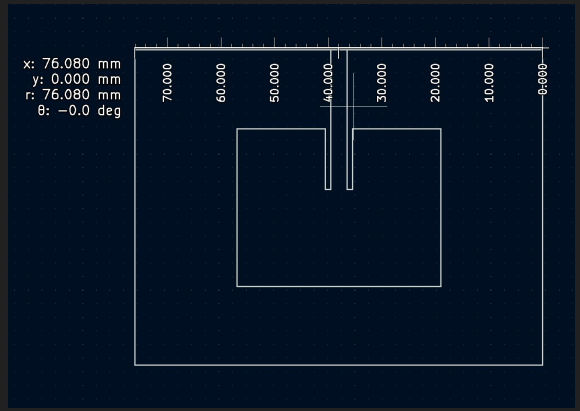
Professional Fabrication



Import Graphics

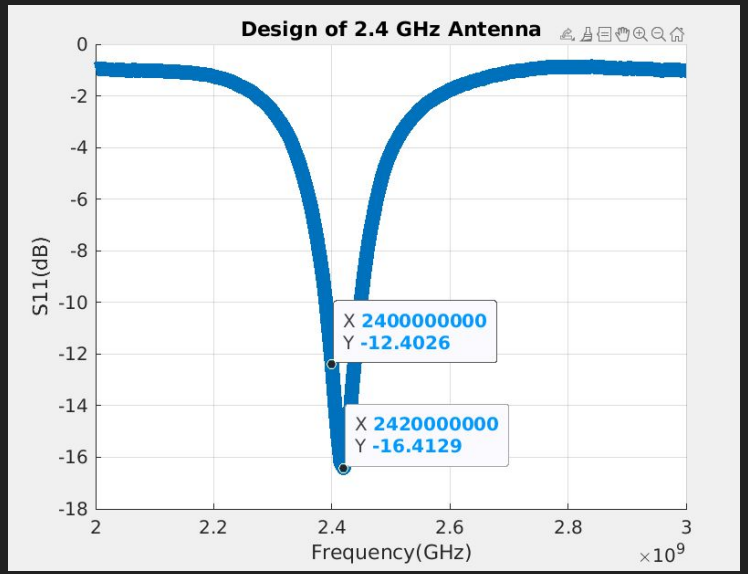


Import dxf with mm settings



Confirm the size is accurate

Measurements



S11 measured

Gain measured - 5.12 dBi

Measurements

Calculate the Power Received by the Receiver

Transmit Power (P_t)

0 dBm

Transmit Antenna Gain (G_t)

5 dBi

Receive Antenna Gain (G_r)

5 dBi

Wavelength

0.12491352 meter

Antenna Separation (R)

1 meter

Calculate Reset

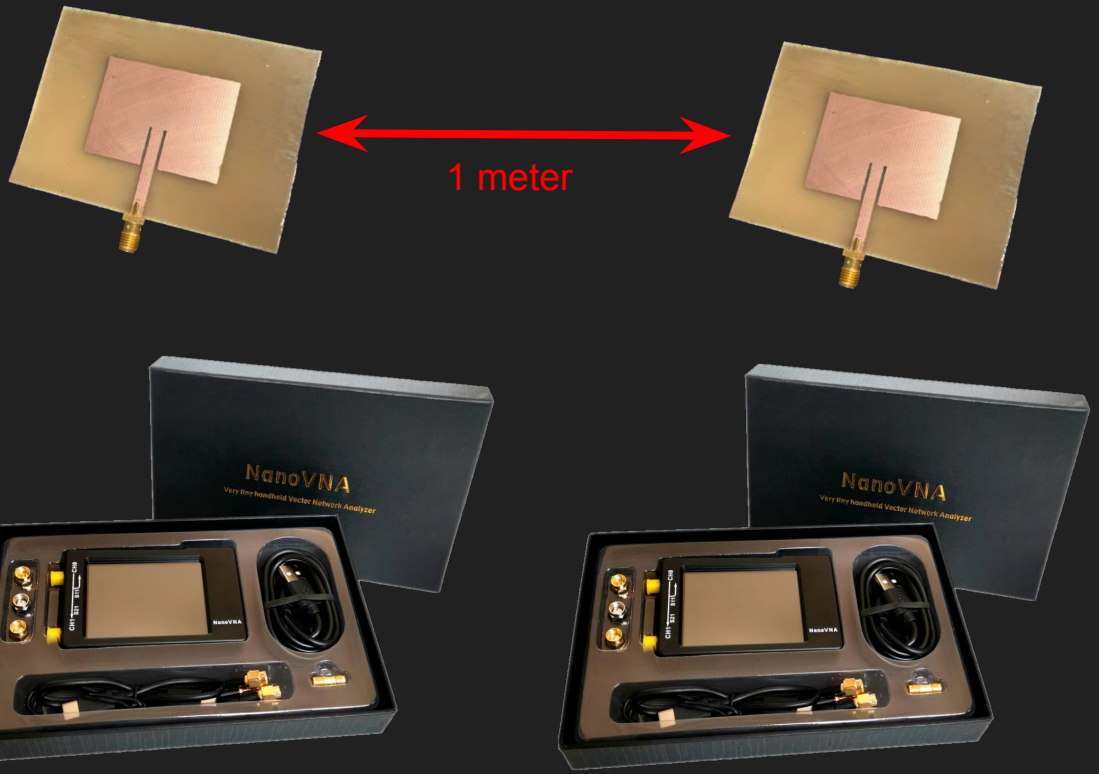
Result

Power Received (dBm):

-30.04760385

Power Received (W):

9.9E-07



Check Local Laws

ISM Frequency Range		ISM Band Type
6.765 MHz	6.795 MHz	Regional
13.553 MHz	13.567 MHz	Worldwide
26.957 MHz	27.283 MHz	Worldwide
40.66 MHz	40.7 MHz	Worldwide
433.05 MHz	434.79 MHz	Regional
902 MHz	928 MHz	Regional
2.4 GHz	2.5 GHz	Worldwide
5.725 GHz	5.875 GHz	Worldwide
24 GHz	24.25 GHz	Worldwide
61 GHz	61.5 GHz	Regional
122 GHz	123 GHz	Regional
244 GHz	246 GHz	Regional

Conclusion

Rectangular patch antennas are simple and inexpensive to manufacture

This presentation showcased a tool to help with antenna calculations:

- https://github.com/dollarhyde/AntennaCalculator

Make your own antenna and share it with the community

References

[1] C. A. Balanis, Antenna theory: Analysis and design. Hoboken, NJ: Wiley, 2016.

[2] J. D. Kraus and R. J. Marhefka, Antennas for all applications. Boston, Mass: McGraw-Hill, 2008.

[3] W. L. Stutzman and G. A. Thiele, Antenna Theory and design. Hoboken, NJ: Wiley, 2013.