So What the Heck Is This Radio Thing, Anyway?

Who am I?

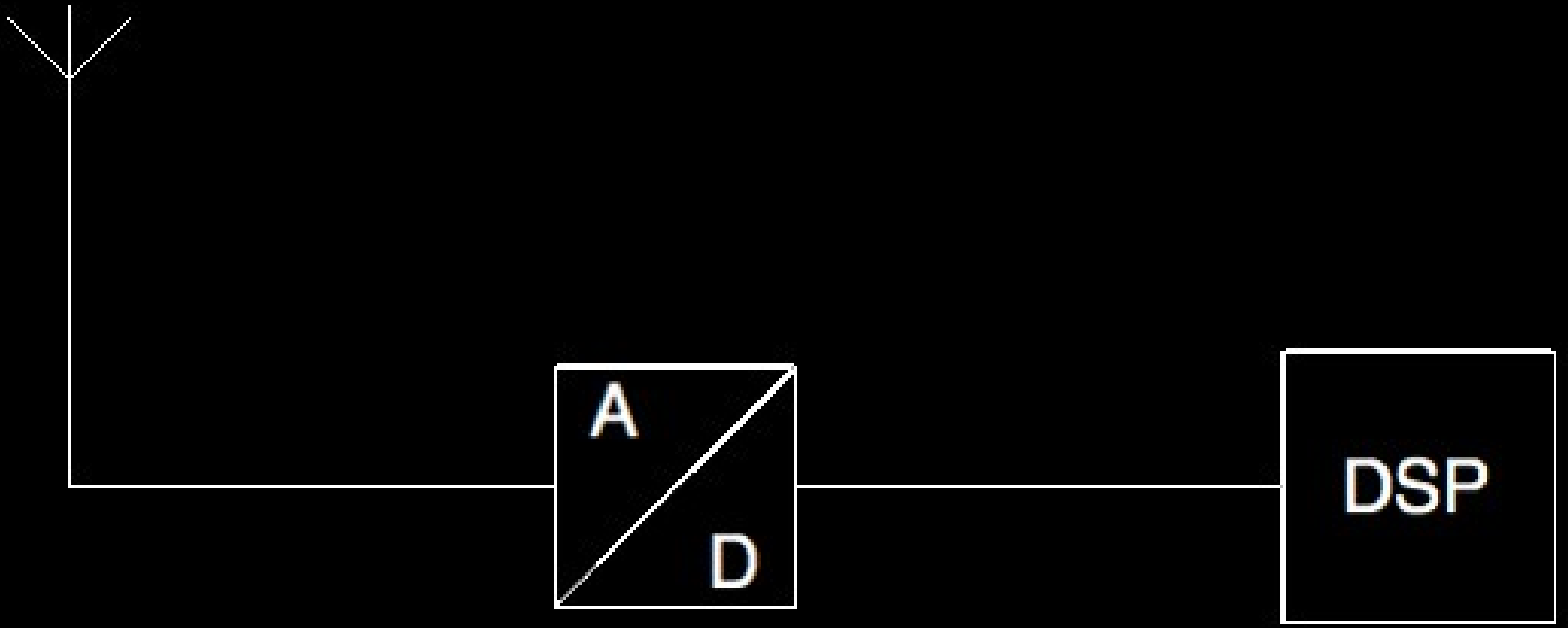
Computer geek, ham radio operator, electronics fiddler, RC pilot, cat and dog servant, etc...

A Brief History of Radio

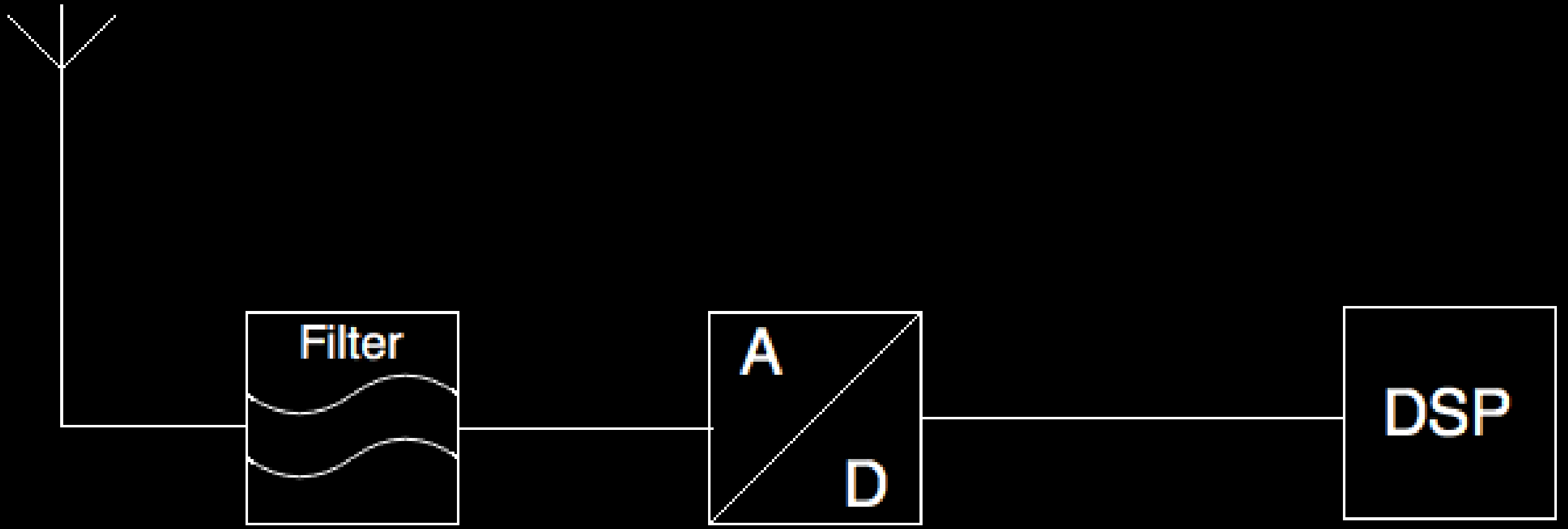
- Spark-gap transmitter (late 1800s to early 1900s)
- Crystal radio receiver (early 1900s through around 1930)
- Vacuum tubes (early 1900s)
- Transistor radios (mid-1950s onward)
- Software-defined radios (mid-1980s, more widespread mid-90s)

What is SDR?

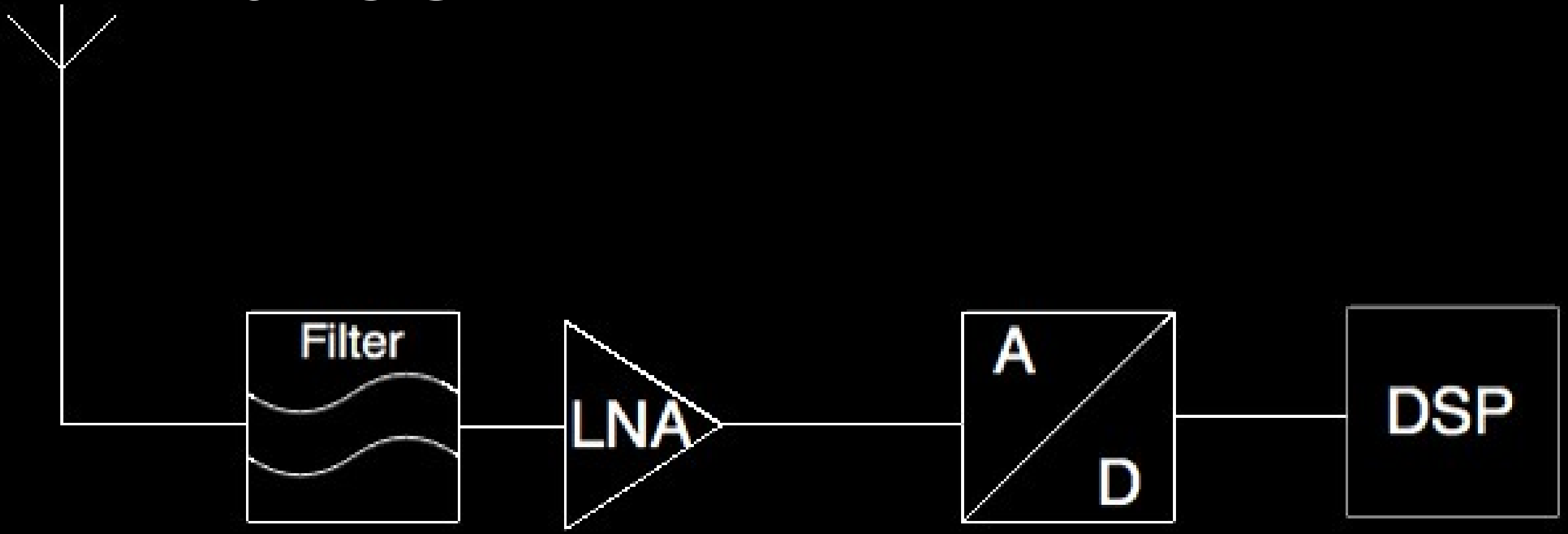
What is SDR?



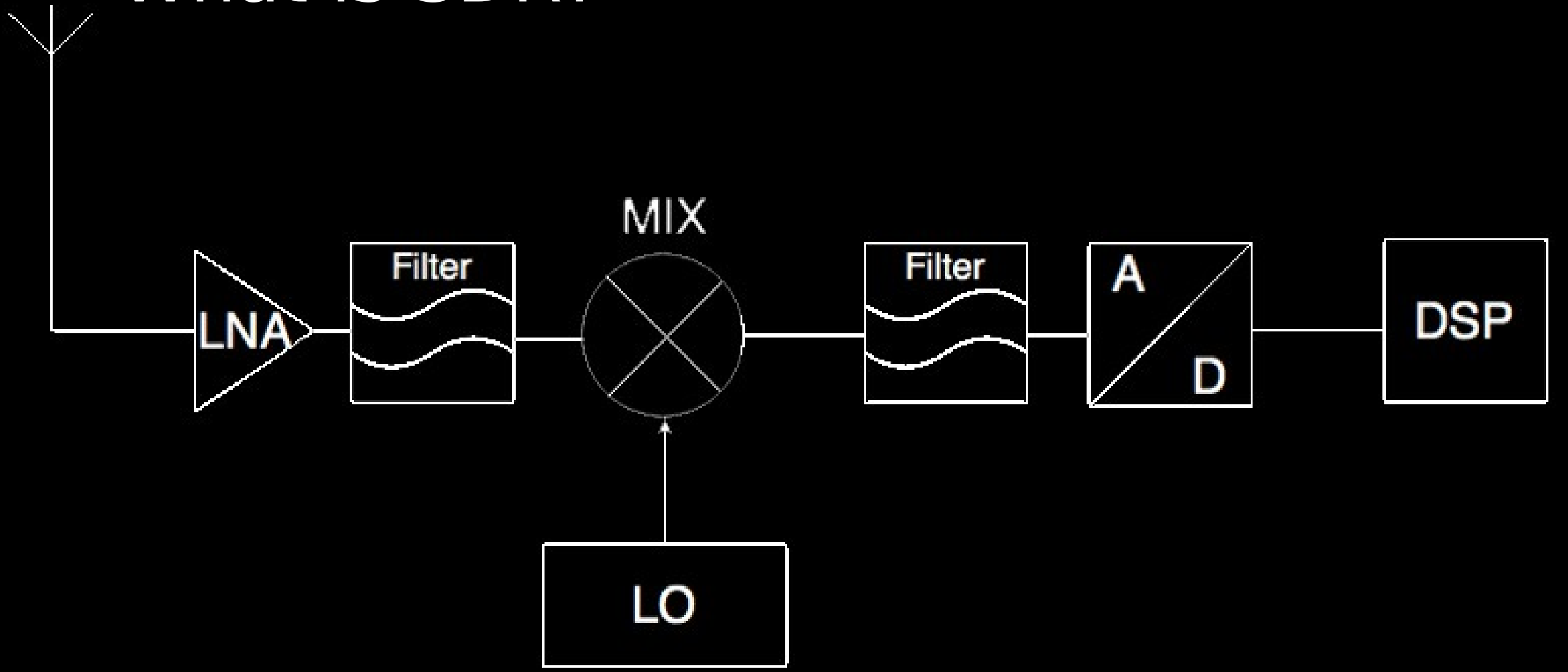
What is SDR?



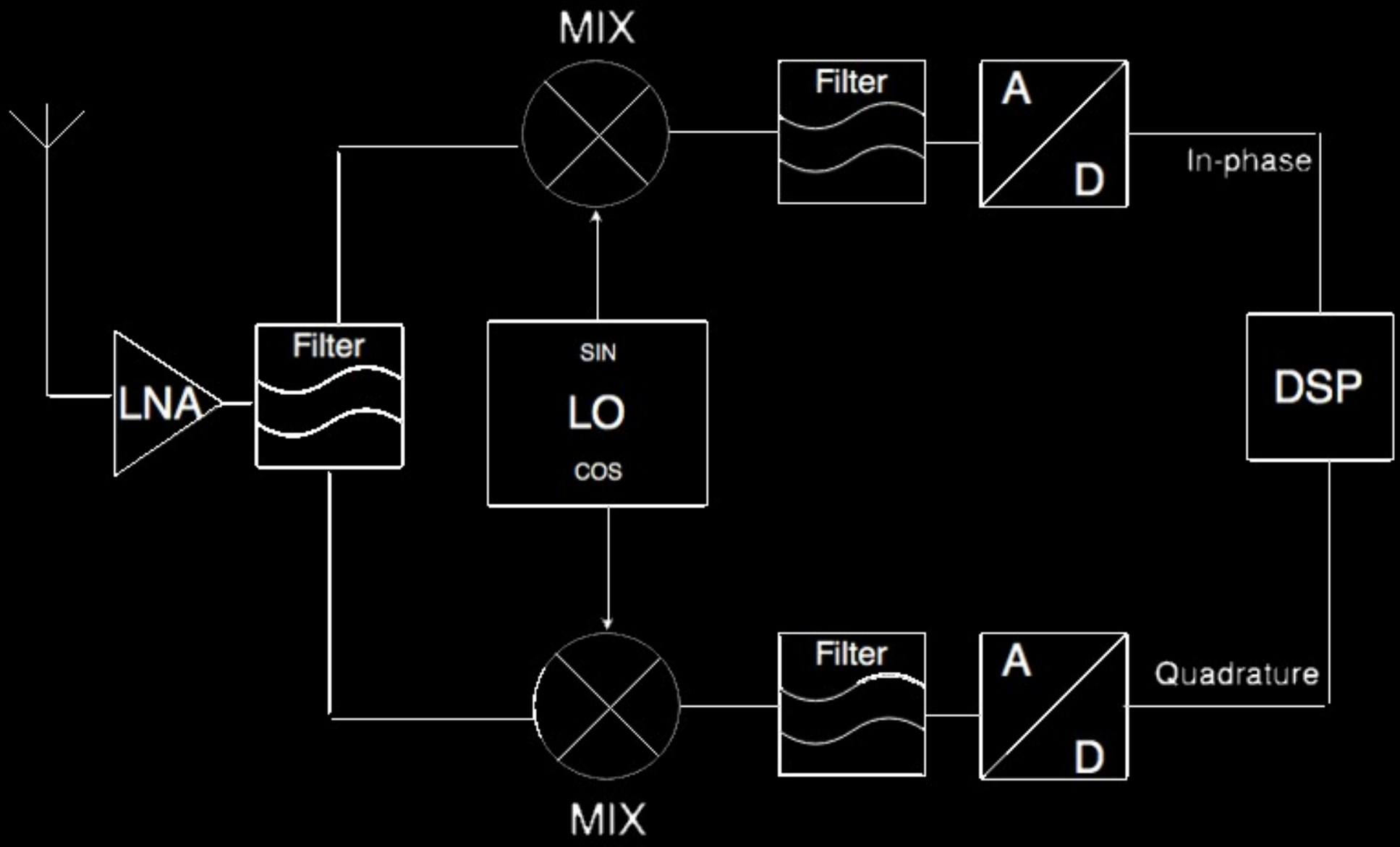
What is SDR?



What is SDR?

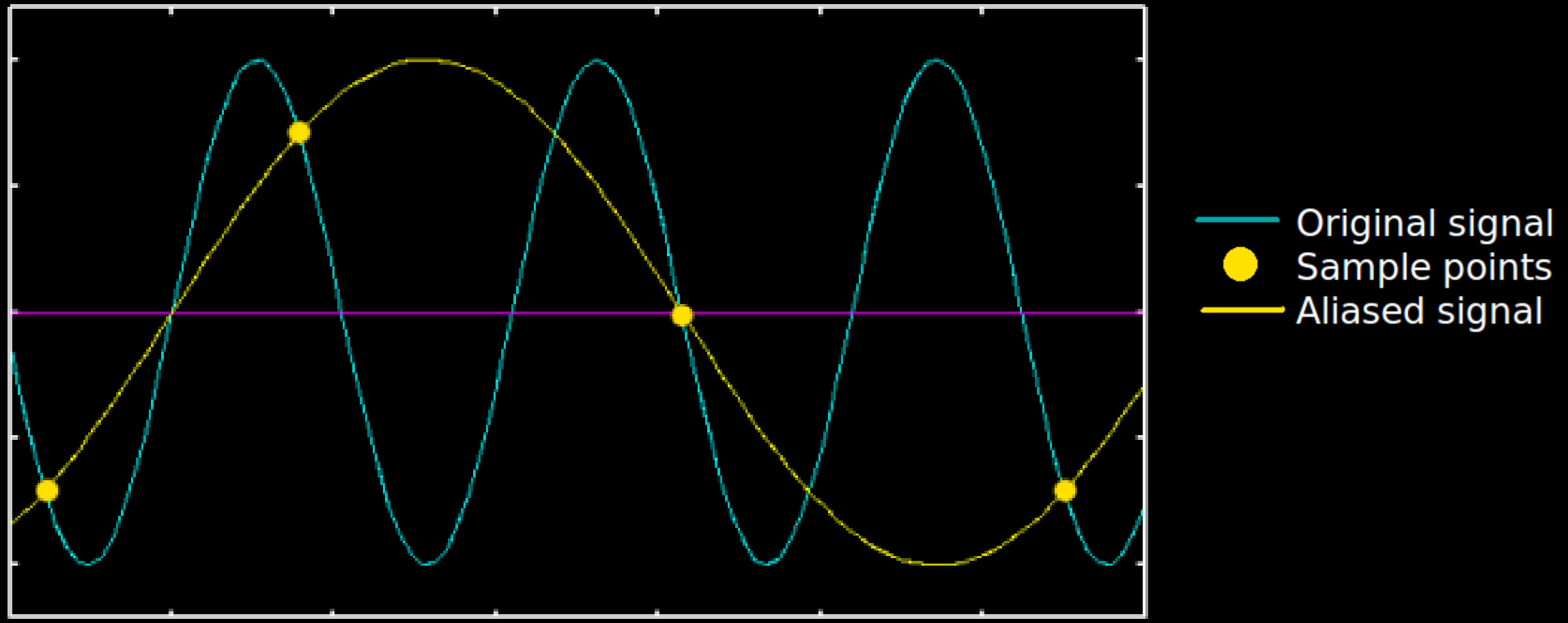


What is SDR?


MIX
Filter
A
D
In-phase
LNA
Filter
SIN
LO
COS
DSP
Filter
A
D
Quadrature
MIX

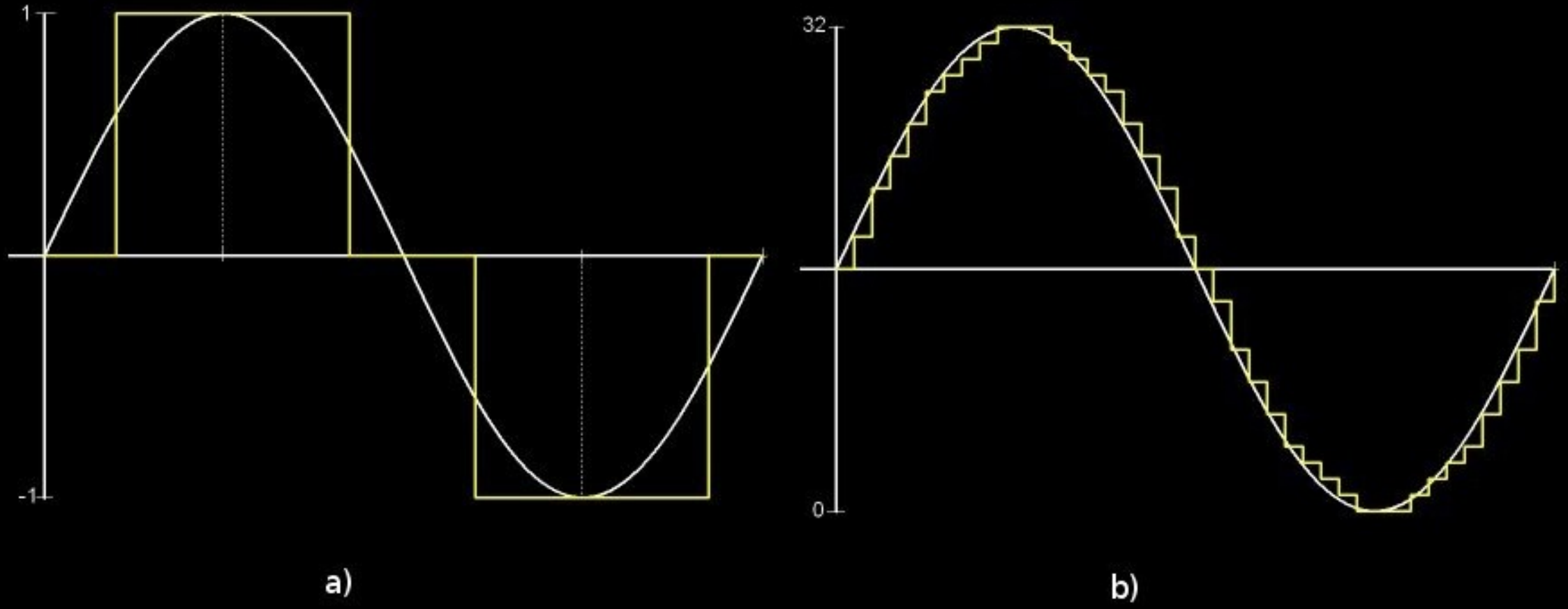
You mentioned this Nyquist guy...

Sample at a rate at least twice the frequency of the signal, otherwise...

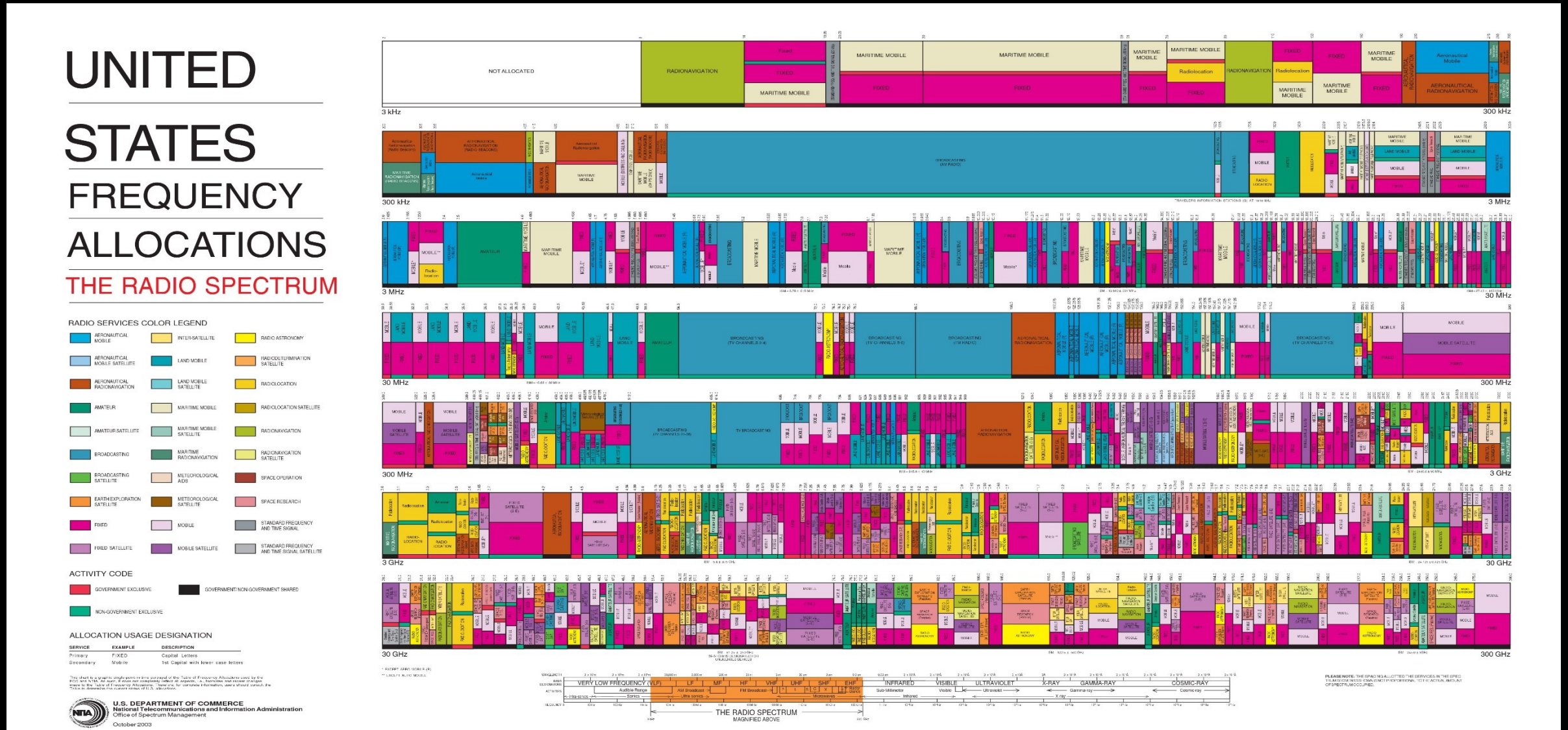


Is sample rate the only important thing?

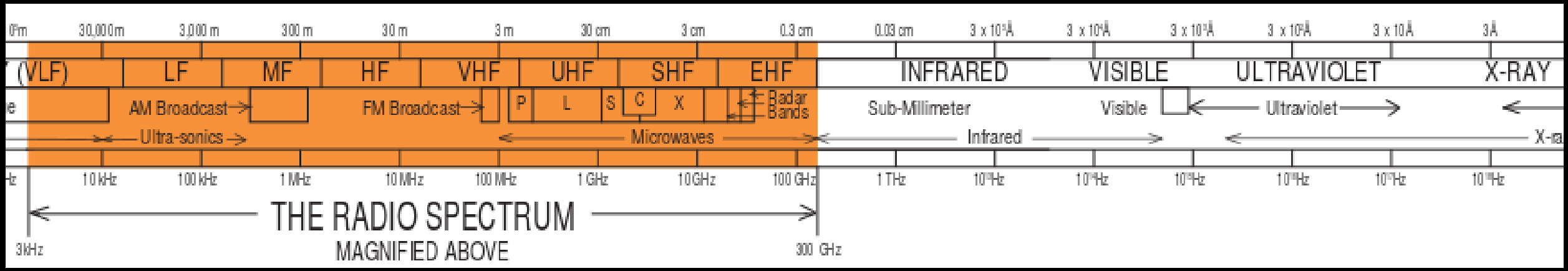
Bit depth is important to amplitude-modulated signals & dynamic range



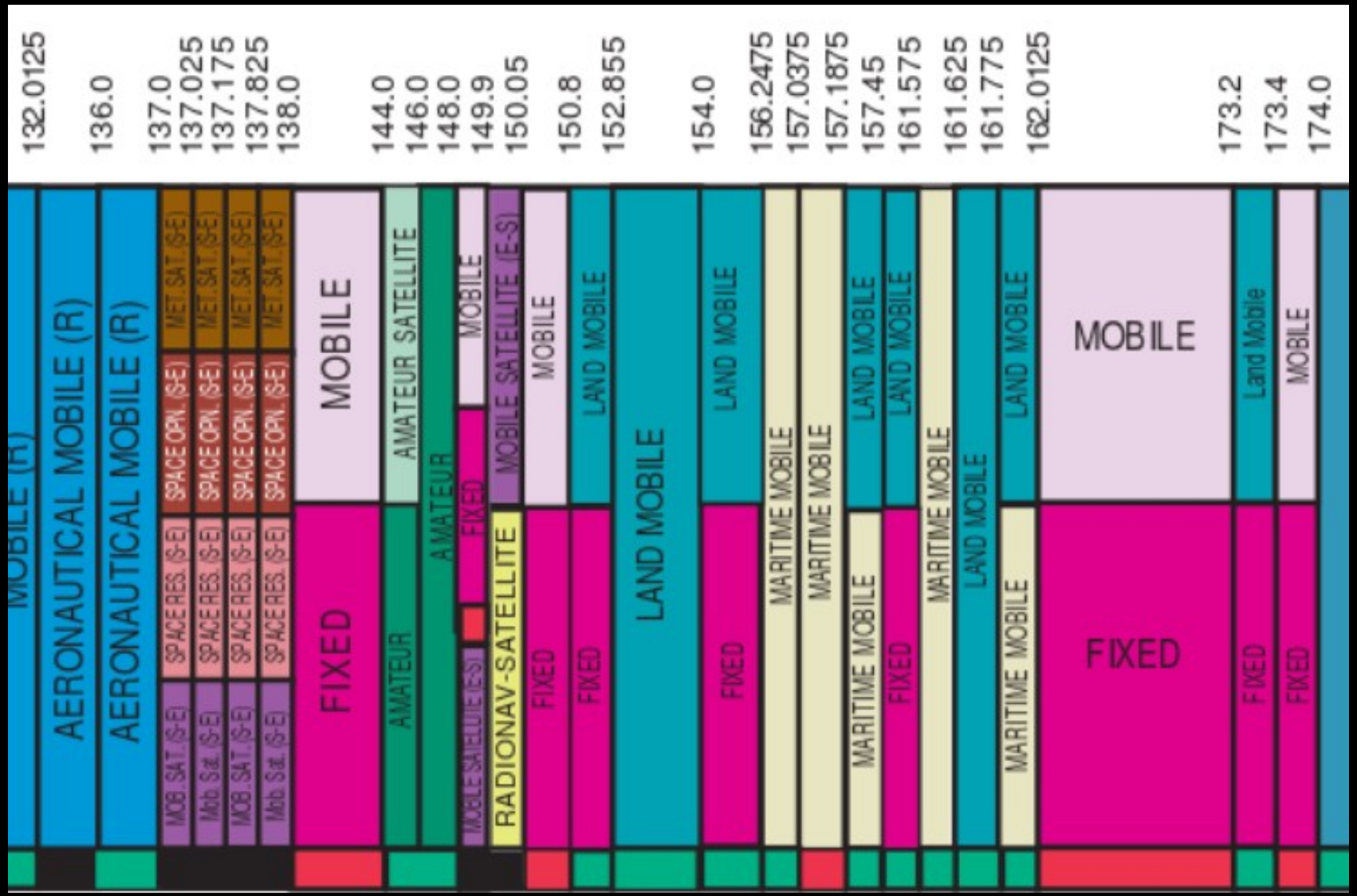
Okay, so what are we actually receiving?



Okay, so what are we actually receiving?

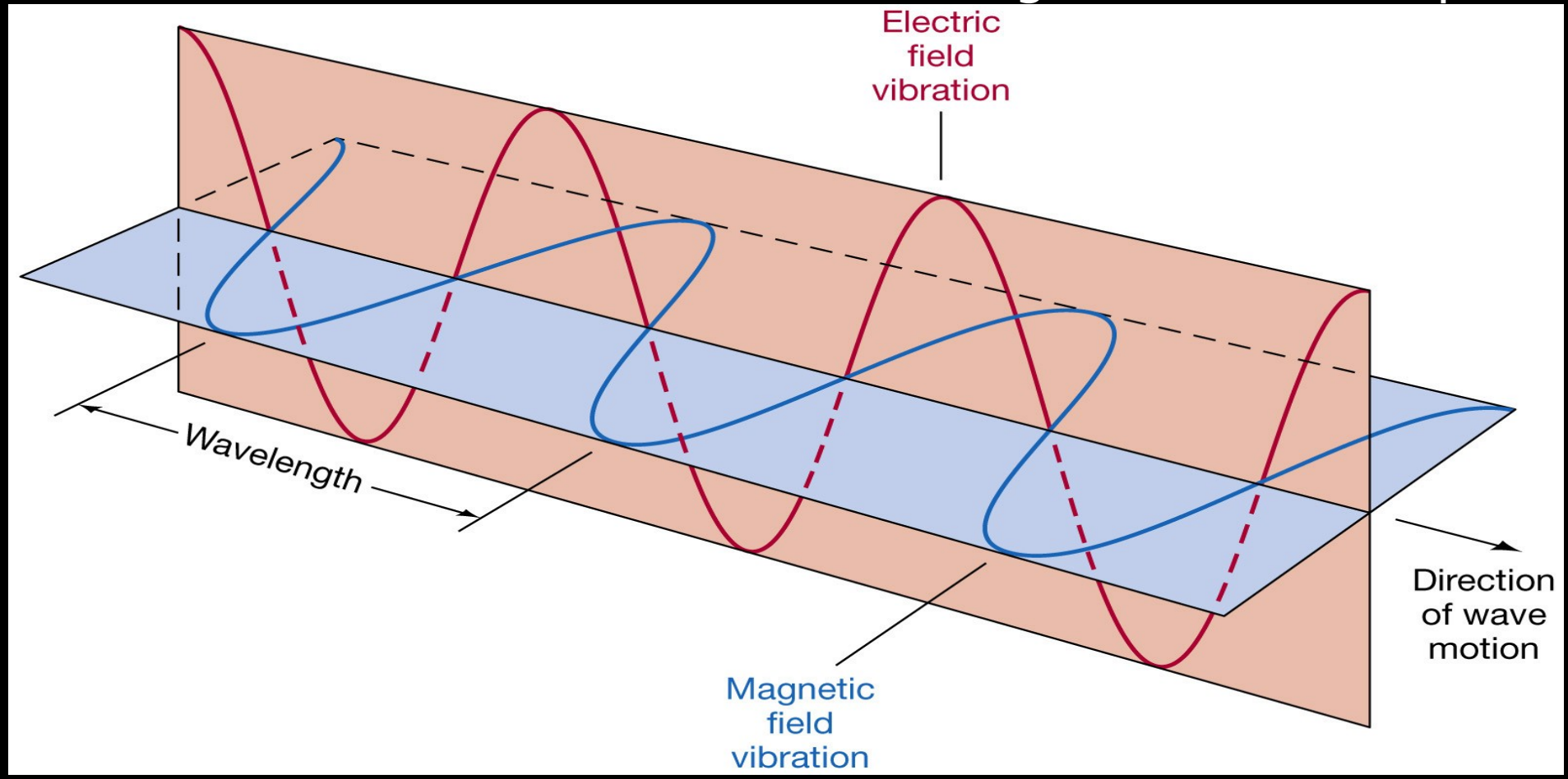


Okay, so what are we actually receiving?



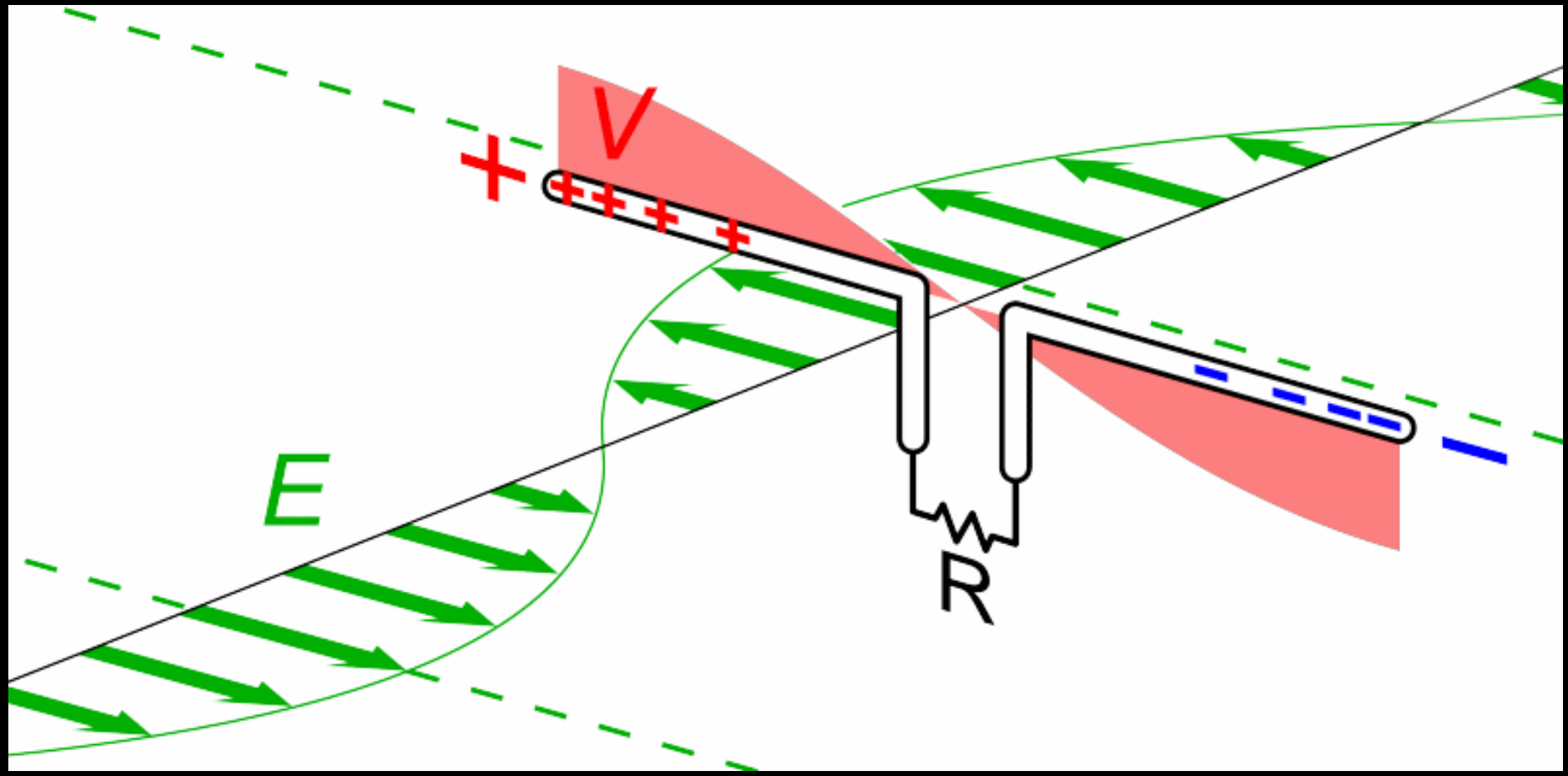
But what is an electromagnetic wave?

Transverse wave with electric field and magnetic field components



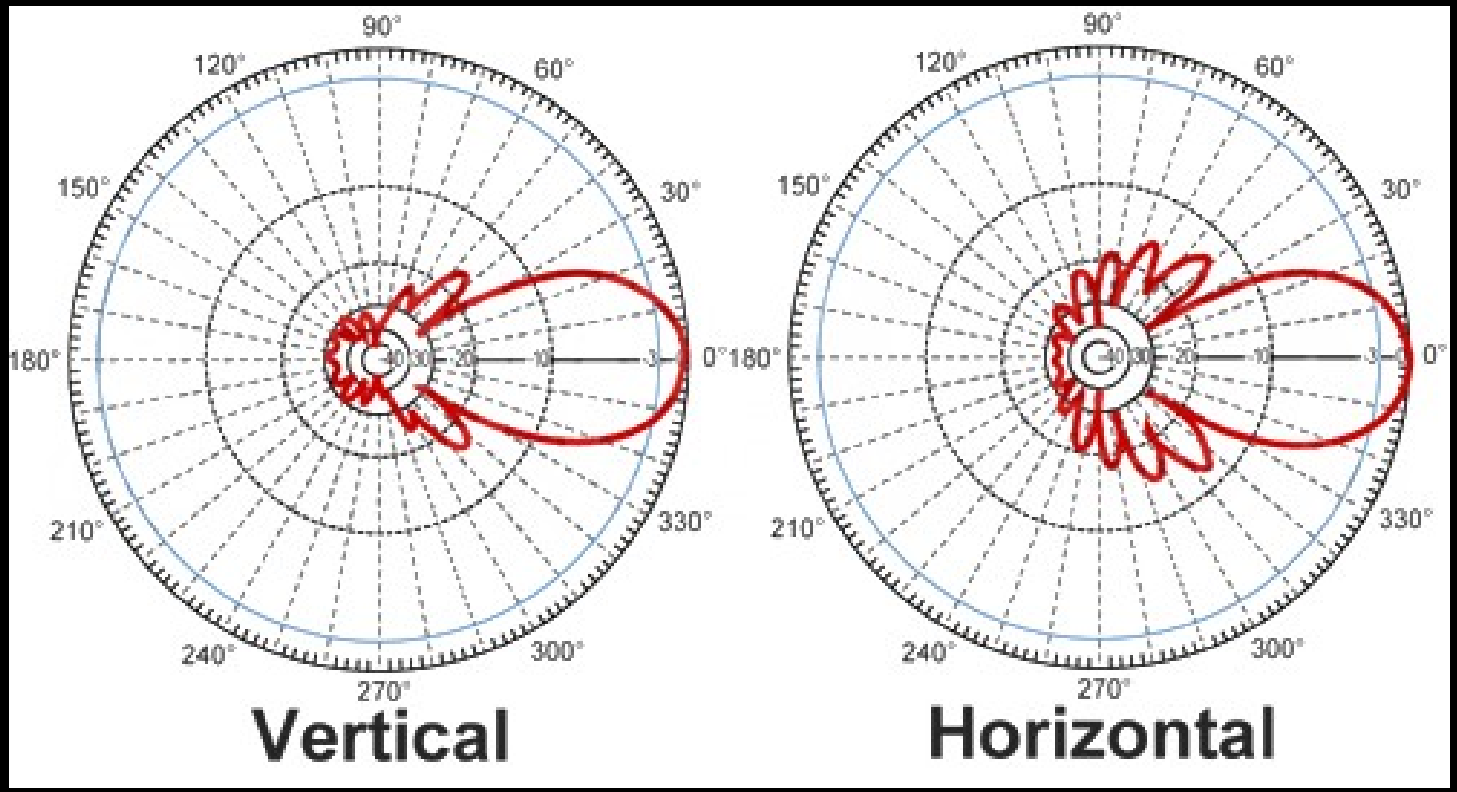
How do we receive the wave?

With an antenna!



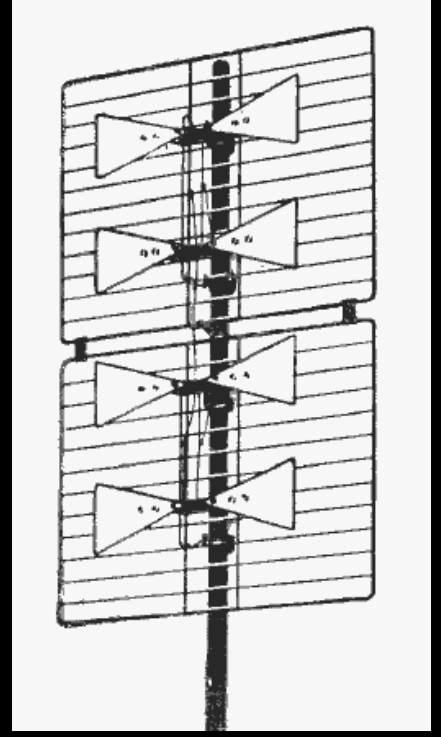
Tell me more about antennas...

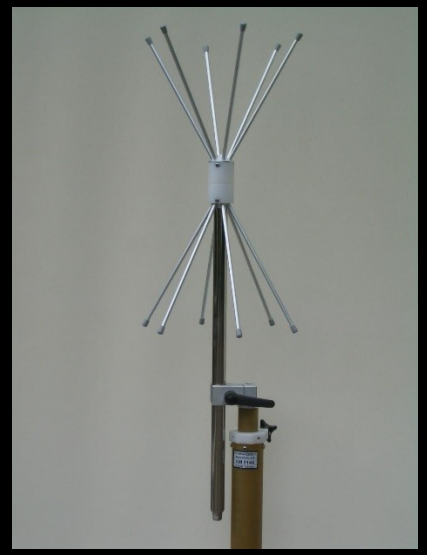
- Tuned to radiate for frequency and bandwidth
- Gain expressed in dBi (tTX power expressed in dBm)
- Polar radiation charts



MOAR ANTENNAS

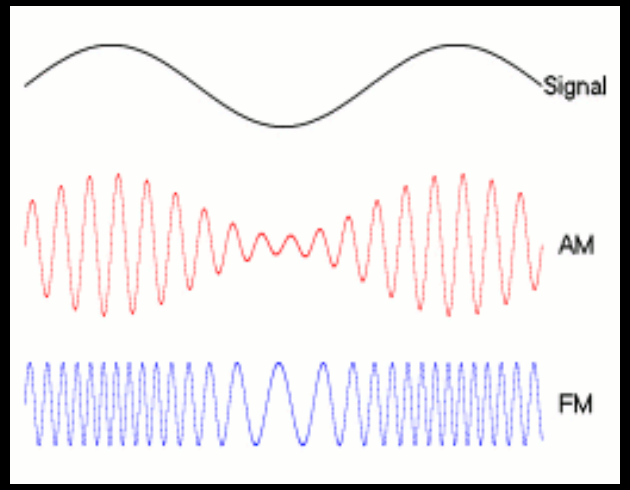
Many different types...

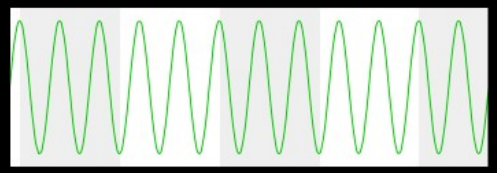


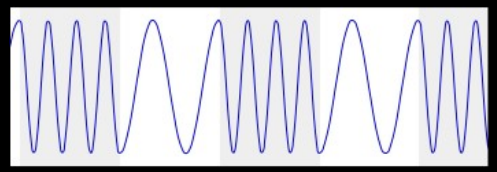


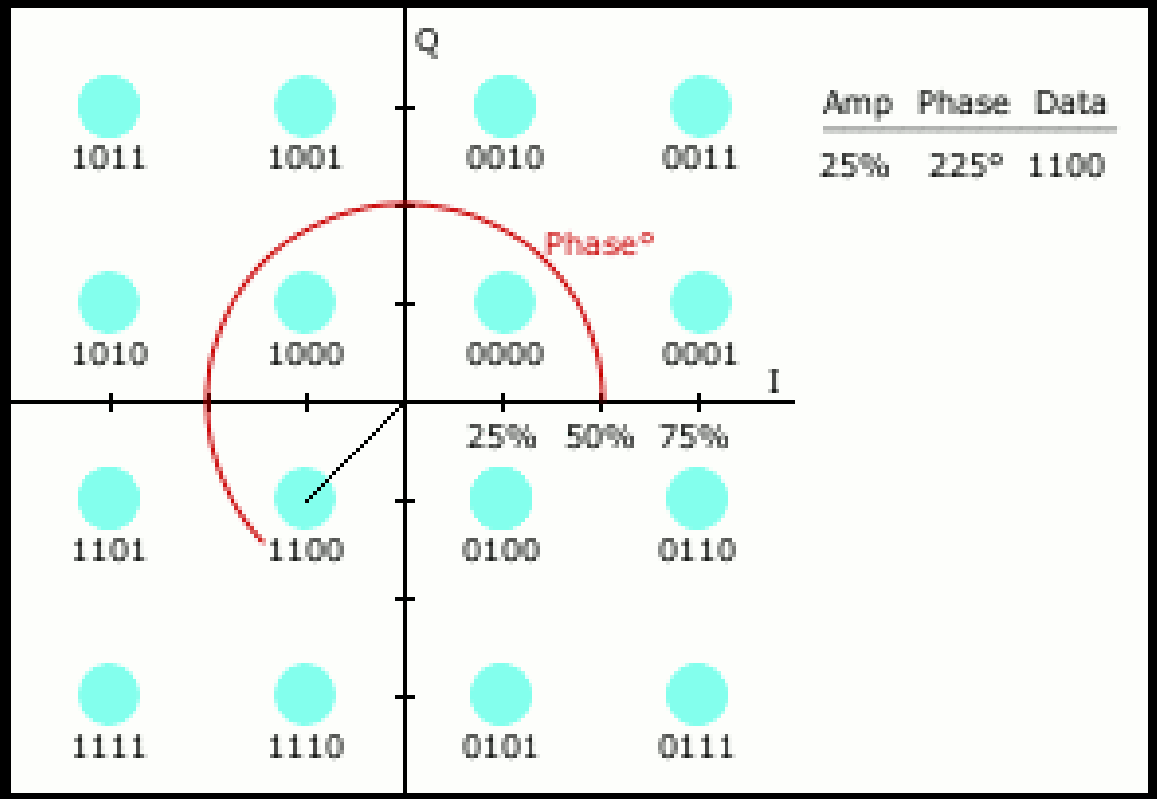
So how do we use all this to communicate?

- Modulation!
  - Analog
    - AM
    - FM
  - Digital
    - OOK
    - FSK
    - PSK
    - QAM
    - OFDM









Just how much data can we send?

Ask information theorists!

- Channel capacity
- Shannon-Hartley theorem

$$Capacity \approx 0.332 \times Bandwidth \times 10 \log(10) \frac{Signal}{Noise}$$

- Example:
  - 20MHz bandwidth
  - -70dB signal
  - -90dB noise
  - 86mbit/sec
  - Better SNR? -60dB signal, -110dB noise, 112mbit/sec
  - Double bandwidth? -60dB signal, -110dB noise, 40MHz BW, 225mbit/sec

Where do I go to learn more?

- For RF:
  - Amateur Radio license! Today (Tuesday) at 7pm
    - http://conham.org/exams.html
    - http://www.kb6nu.com/study-guides/
    - http://www.arrl.org/ham-radio-license-manual
  - ARRL Handbook, http://www.arrl.org/arrl-handbook-2015
  - RF for non-RF engineers, http://www.ti.com/lit/ml/slap127/slap127.pdf
  - NXP RF Basics, https://www.youtube.com/watch?v=FVmTooGICNc
- For SDR:
  - Michael Ossman's videos, http://greatscottgadgets.com/sdr/
  - Wireless CTF training, http://sdr.ninja/training-events/sdr-wctf/

How do I find you?

- Twitter: @explodinglemur
- Github: https://github.com/explodinglemur
- Blahg: http://blog.explodinglemur.org