GNU Radio ile Uygulamalı Haberleşme Sistemleri

Linux Kış Kampı
Eskişehir, 10-13 Şubat 2025

Outline

Quick Recap

SDR Intro

RTL-SDR Installation

Spectrum Monitoring

SDR Architectures

Recap - GNU Radio

- Create a flowgraph that generates # dial tone

Schedule

- First Day: GNU Radio Introduction, DSP, GR Simulation Mode
- **Second Day: SDR Introduction, RTL-SDR, GR Real-Time Mode**
- Third Day: Analog Communications
- Fourth Day: Digital Communications

UNITED STATES FREQUENCY ALLOCATIONS

THE RADIO SPECTRUM

RADIO SERVICES COLOR LEGEND

- AERONAUTICAL MOBILE
- AERONAUTICAL MOBILE SATELLITE
- AERONAUTICAL RADIONAVIGATION
- AMATEUR
- AMATEUR SATELLITE
- BROADCASTING
- BROADCASTING SATELLITE
- EARTH EXPLORATION SATELLITE
- FIXED
- FIXED SATELLITE
- INTER-SATELLITE
- LAND MOBILE
- LAND MOBILE SATELLITE
- MARITIME MOBILE
- MARITIME MOBILE SATELLITE
- MARITIME RADIONAVIGATION
- METEOROLOGICAL
- METEOROLOGICAL SATELLITE
- MOBILE
- MOBILE SATELLITE
- RADIO ASTRONOMY
- RADIODETERMINATION SATELLITE
- RADIOLOCATION
- RADIOLOCATION SATELLITE
- RADIONAVIGATION
- RADIONAVIGATION SATELLITE
- SPACE OPERATION
- SPACE RESEARCH
- STANDARD FREQUENCY AND TIME SIGNAL
- STANDARD FREQUENCY AND TIME SIGNAL SATELLITE

ACTIVITY CODE

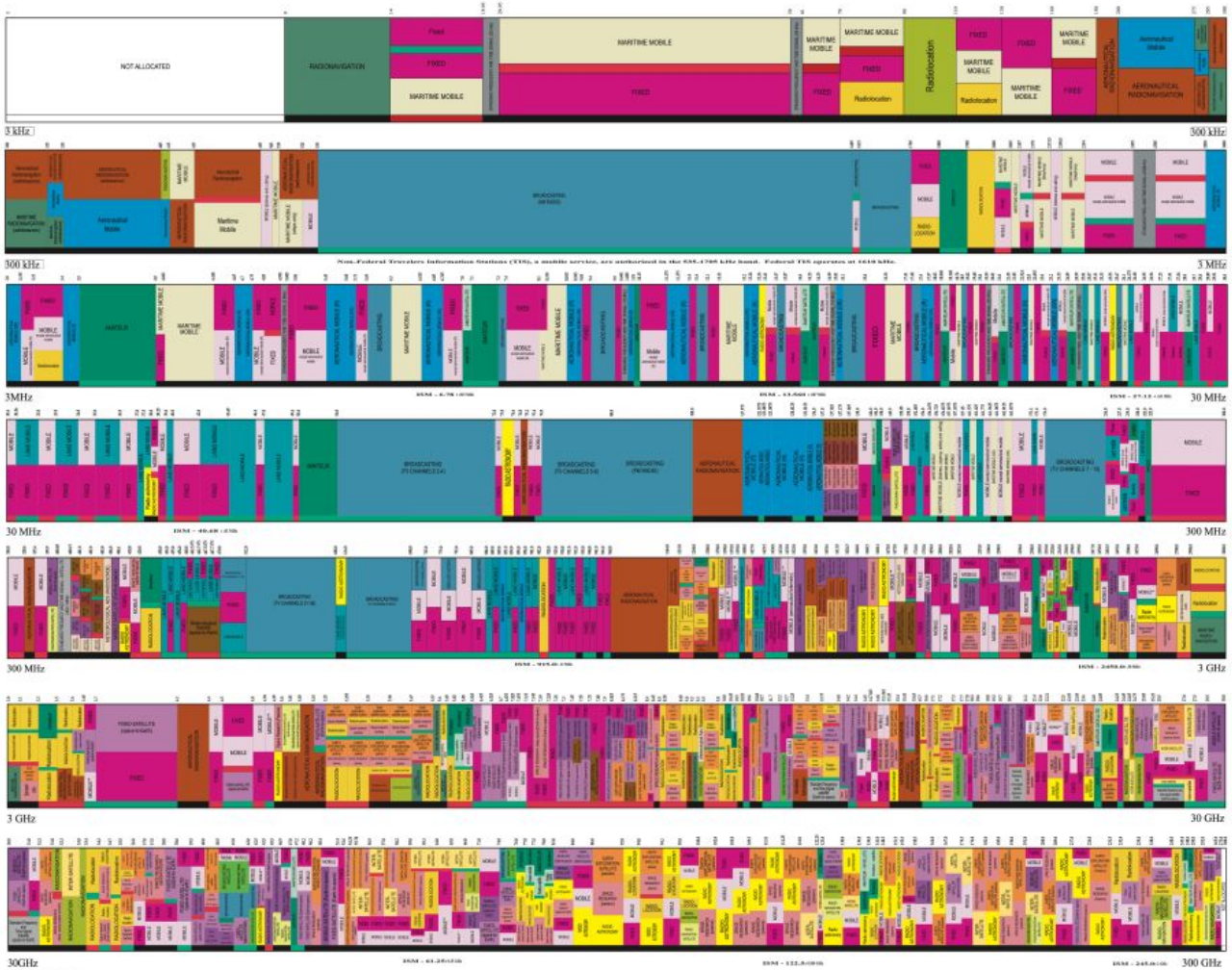
- GOVERNMENT EXCLUSIVE
- GOVERNMENT/NON-GOVERNMENT SHARED
- NON-GOVERNMENT EXCLUSIVE

ALLOCATION USAGE DESIGNATION

SERVICE	EXAMPLE	DESCRIPTION
Primary	FIXED	Capital Letters
Secondary	Mobile	1st Capital with lower case letters

U.S. DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration
Office of Spectrum Management

August 2011



UNITED STATES FREQUENCY ALLOCATIONS

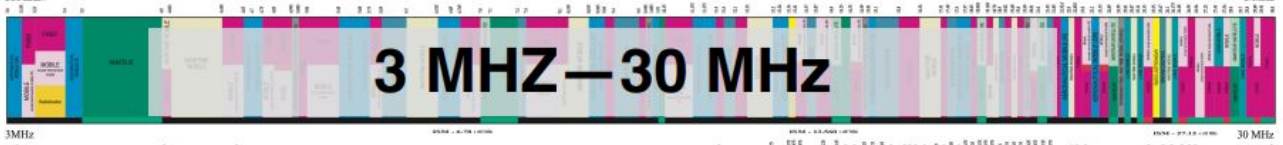
THE RADIO SPECTRUM

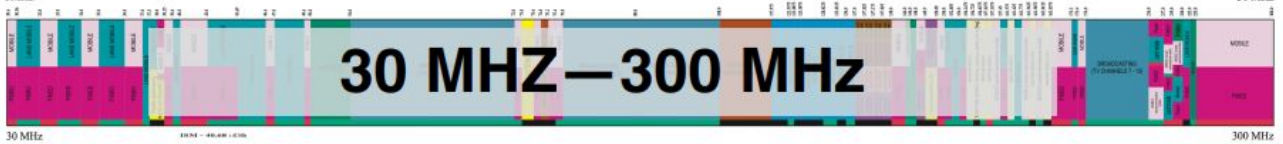
ALLOCATION USAGE DESIGNATION

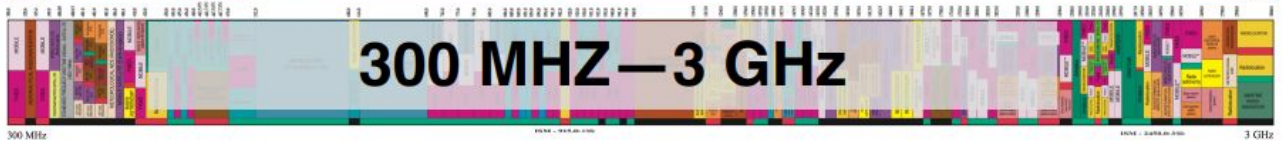
SERVICE	EXAMPLE	DESCRIPTION
Primary	FIXED	Capital Letters
Secondary	Mobile	1st Capital with lower case letters

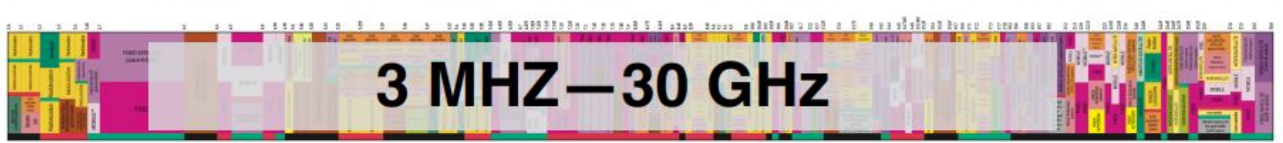
U.S. DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration
Office of Spectrum Management

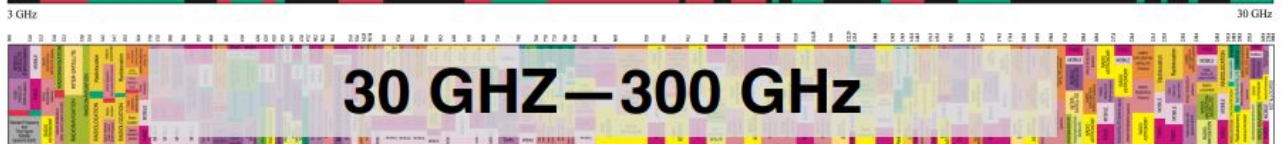
August 2011





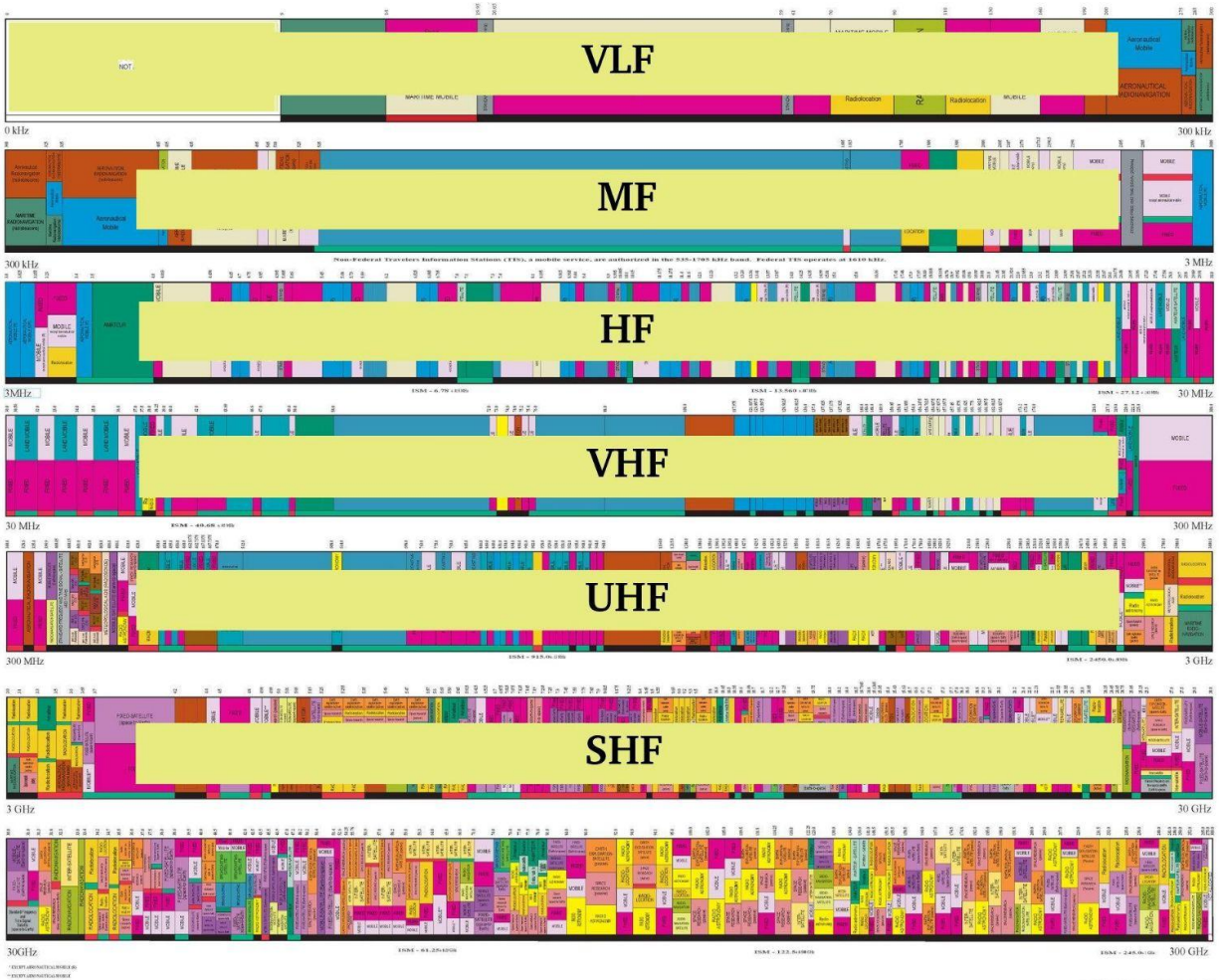






UNITED STATES FREQUENCY ALLOCATIONS

THE RADIO SPECTRUM



RADIO SERVICES COLOR LEGEND

- AERONAUTICAL MOBILE
- AERONAUTICAL MOBILE-SATELLITE
- AERONAUTICAL RADIONAVIGATION
- AMATEUR
- AMATEUR-SATELLITE
- BROADCASTING
- BROADCASTING-SATELLITE
- EARTH EXPLORATION SATELLITE
- FIXED
- FIXED-SATELLITE
- INTER-SATELLITE
- LAND MOBILE
- LAND MOBILE SATELLITE
- MARITIME MOBILE
- MARITIME MOBILE SATELLITE
- MARITIME RADIONAVIGATION
- METEOROLOGICAL
- METEOROLOGICAL SATELLITE
- MOBILE
- MOBILE SATELLITE
- RADIO ASTRONOMY
- RADIODETERMINATION SATELLITE
- RADIOLOCATION
- RADIOLOCATION SATELLITE
- RADIONAVIGATION
- RADIONAVIGATION SATELLITE
- SPACE OPERATION
- SPACE RESEARCH
- STANDARD FREQUENCY AND TIME SIGNAL
- STANDARD FREQUENCY AND TIME SIGNAL SATELLITE

ACTIVITY CODE

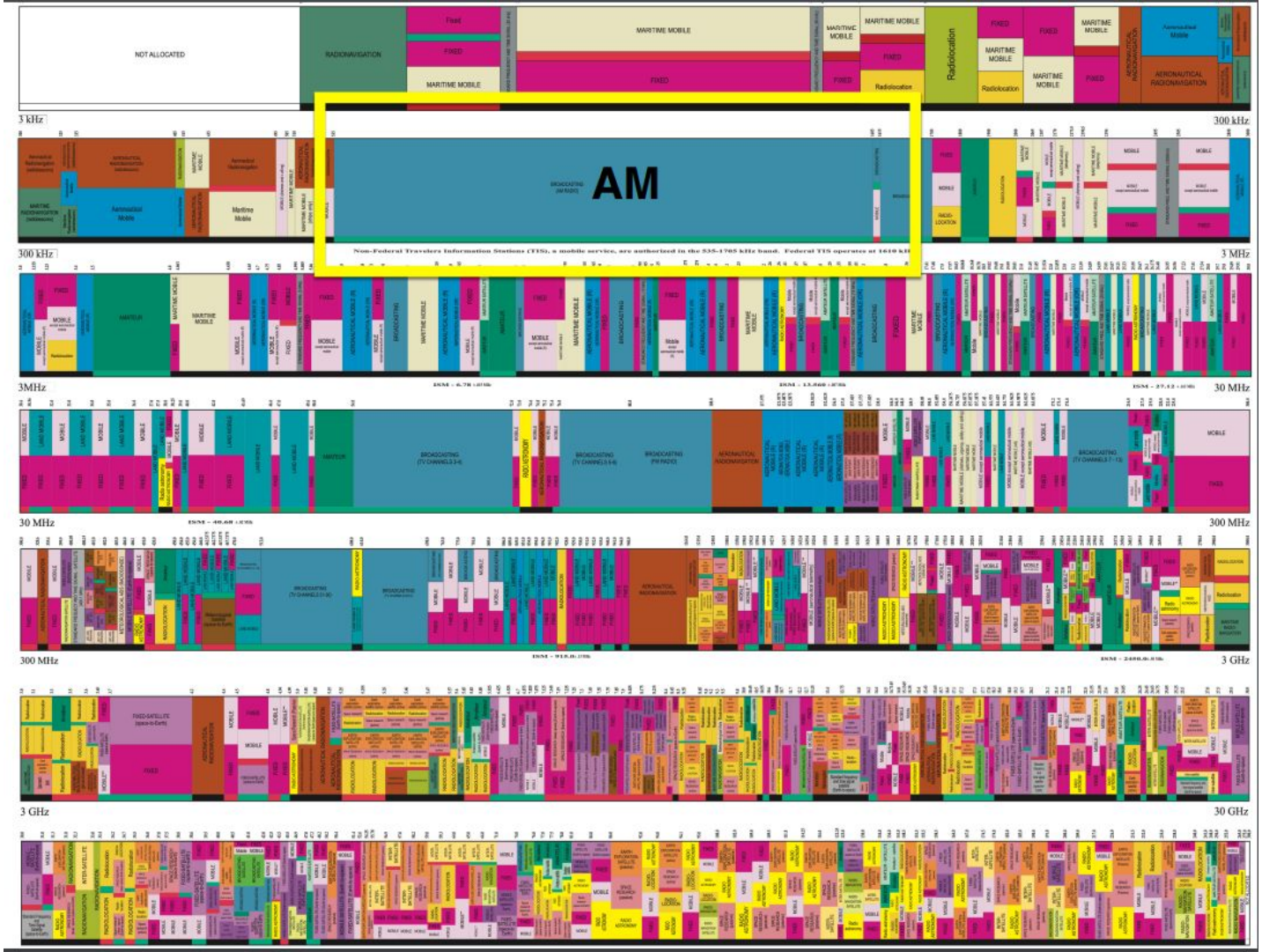
- FEDERAL EXCLUSIVE
- FEDERAL/NON-FEDERAL SHARED
- NON-FEDERAL EXCLUSIVE

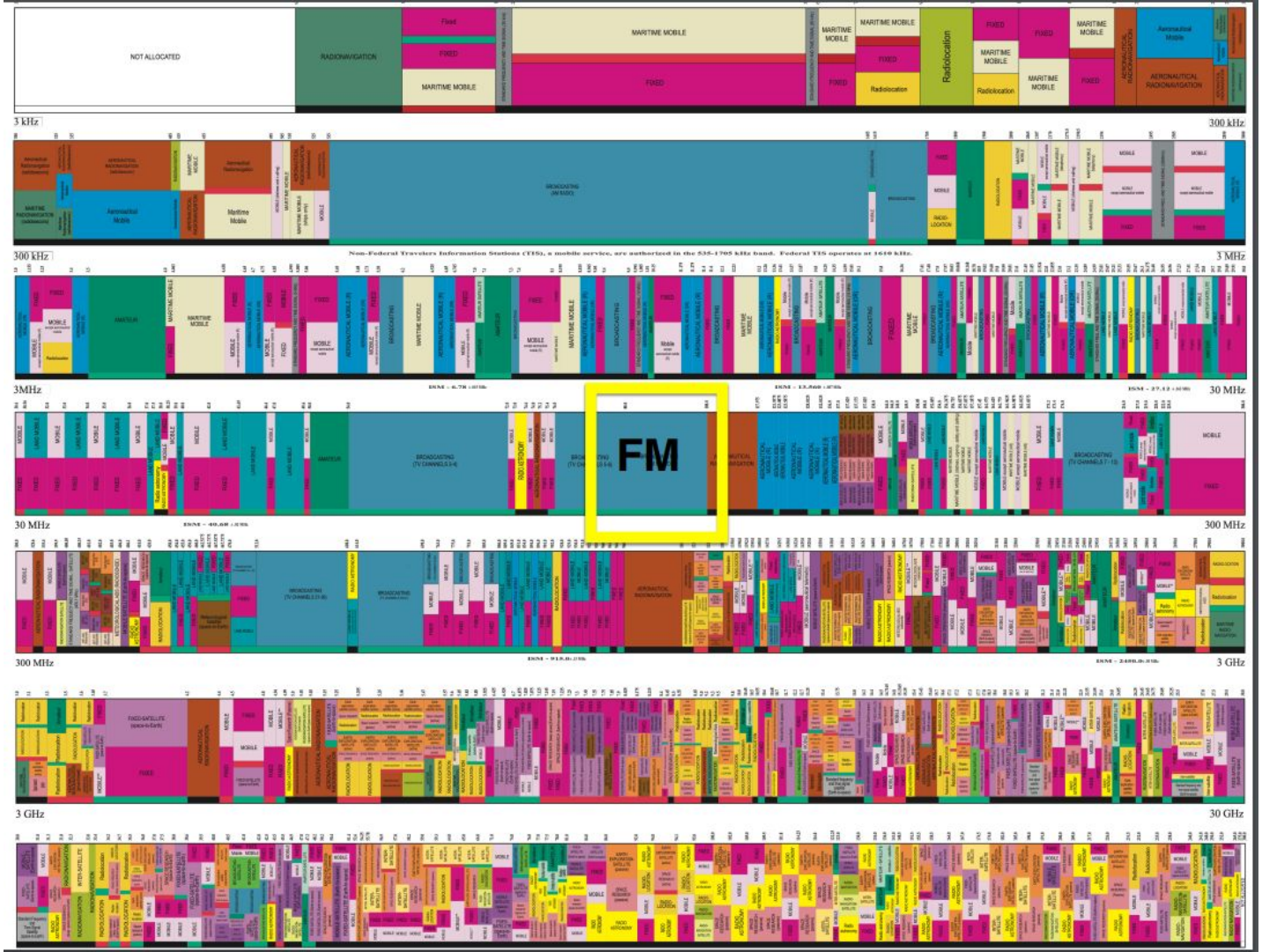
ALLOCATION USAGE DESIGNATION

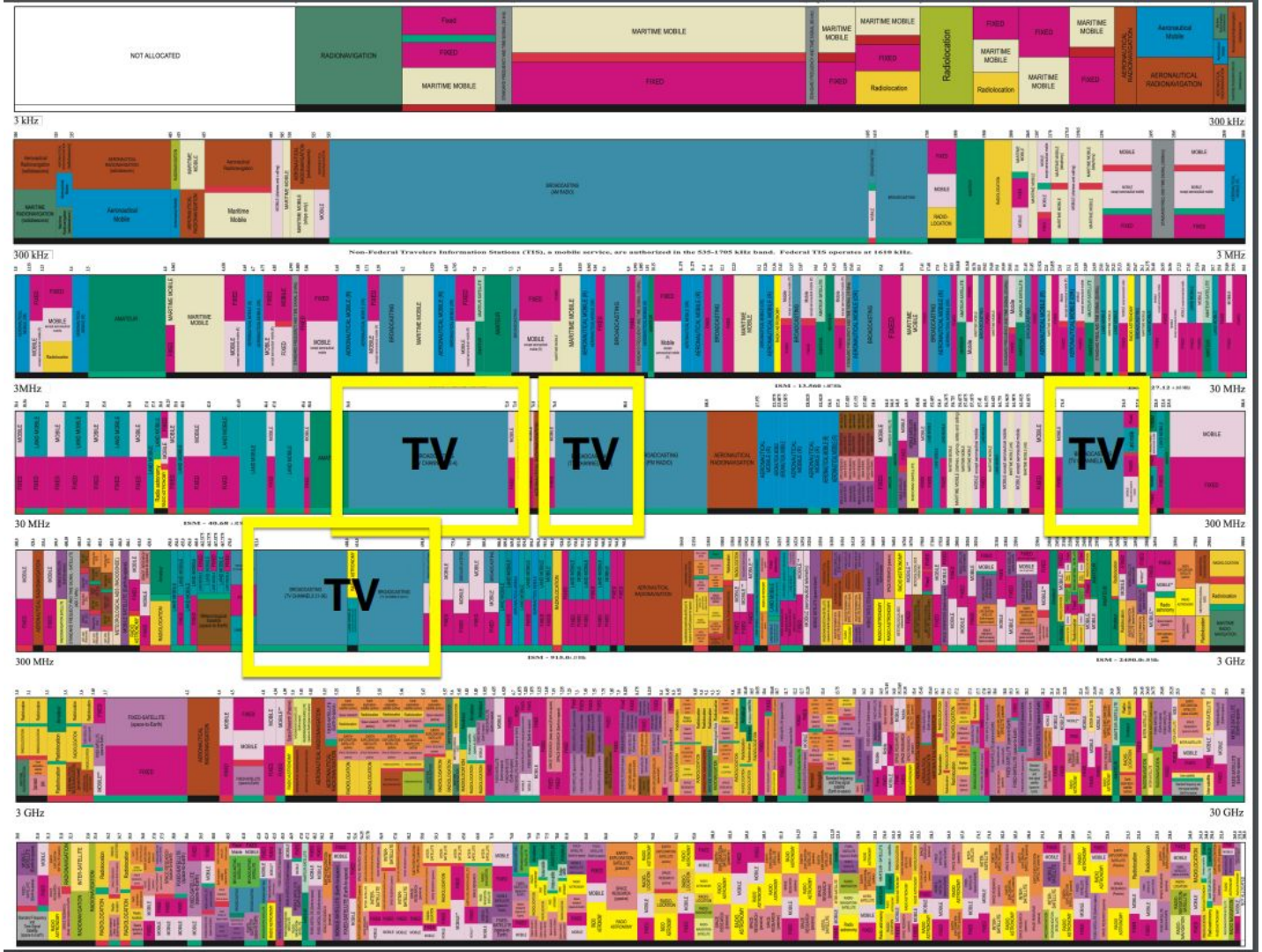
SERVICE	EXAMPLE	DESCRIPTION
Primary	FIXED	Capital Letter
Secondary	Mobile	1st Capital with lower case letter

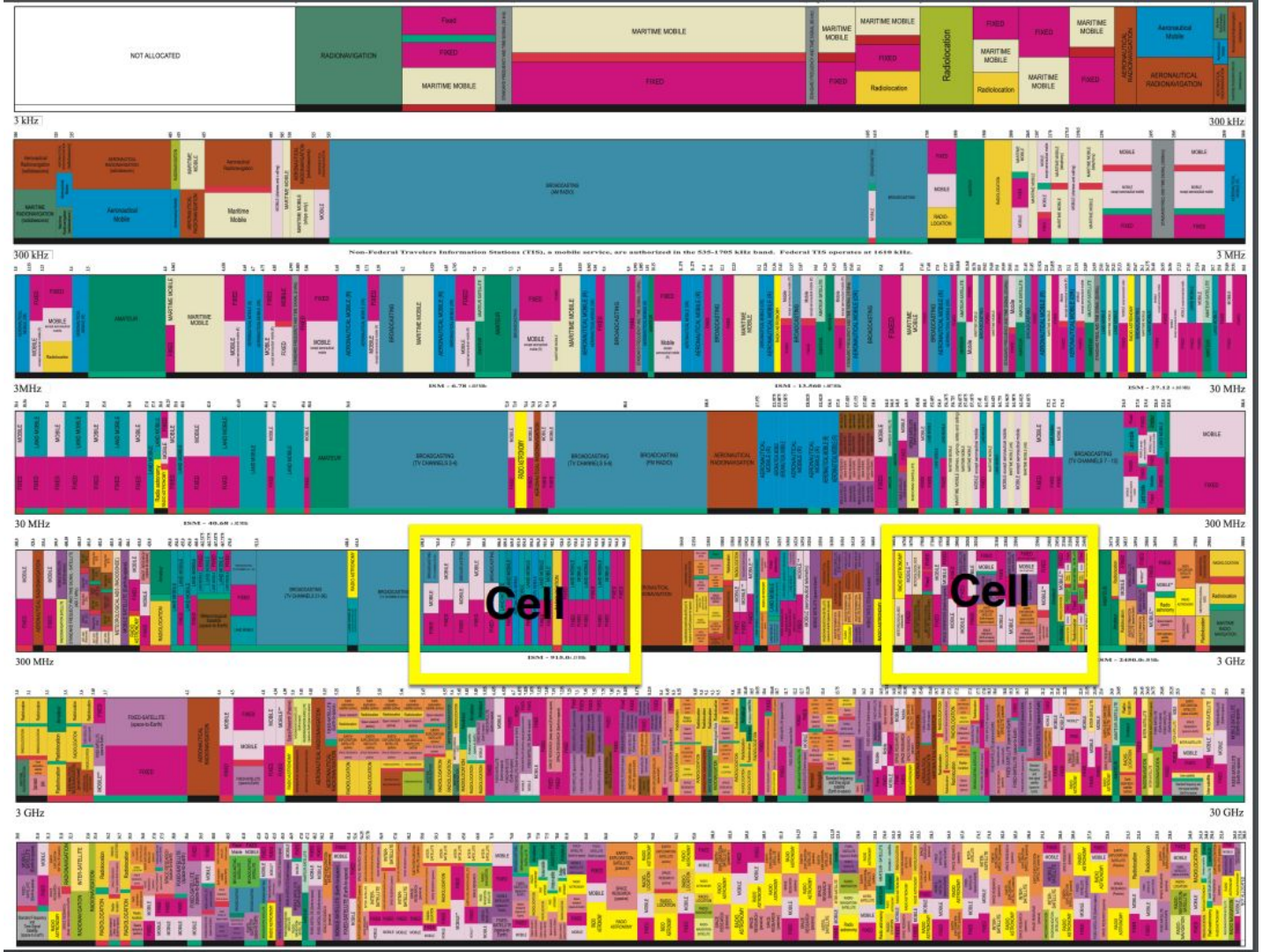
U.S. DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration
Office of Spectrum Management

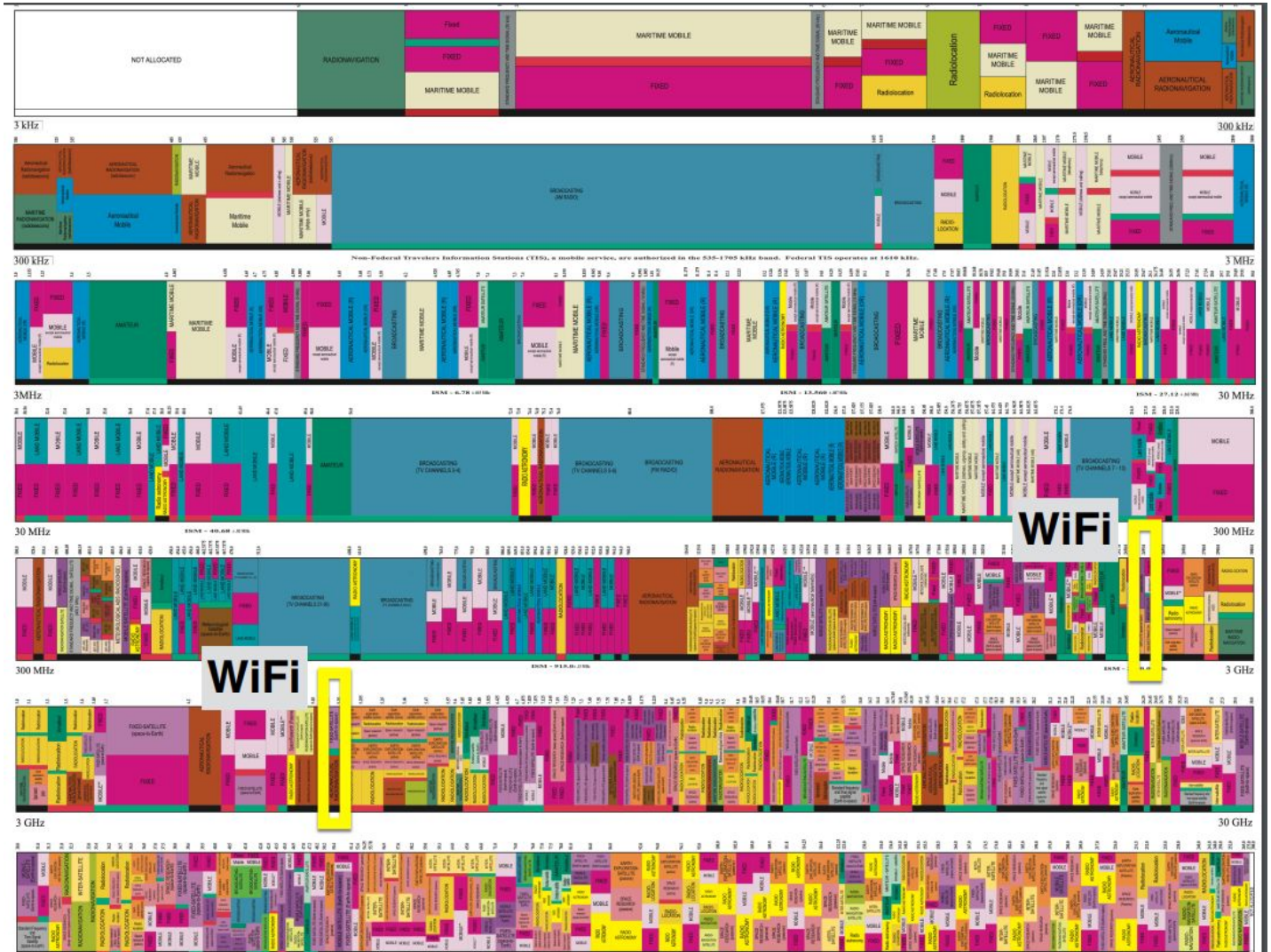
JANUARY 2016

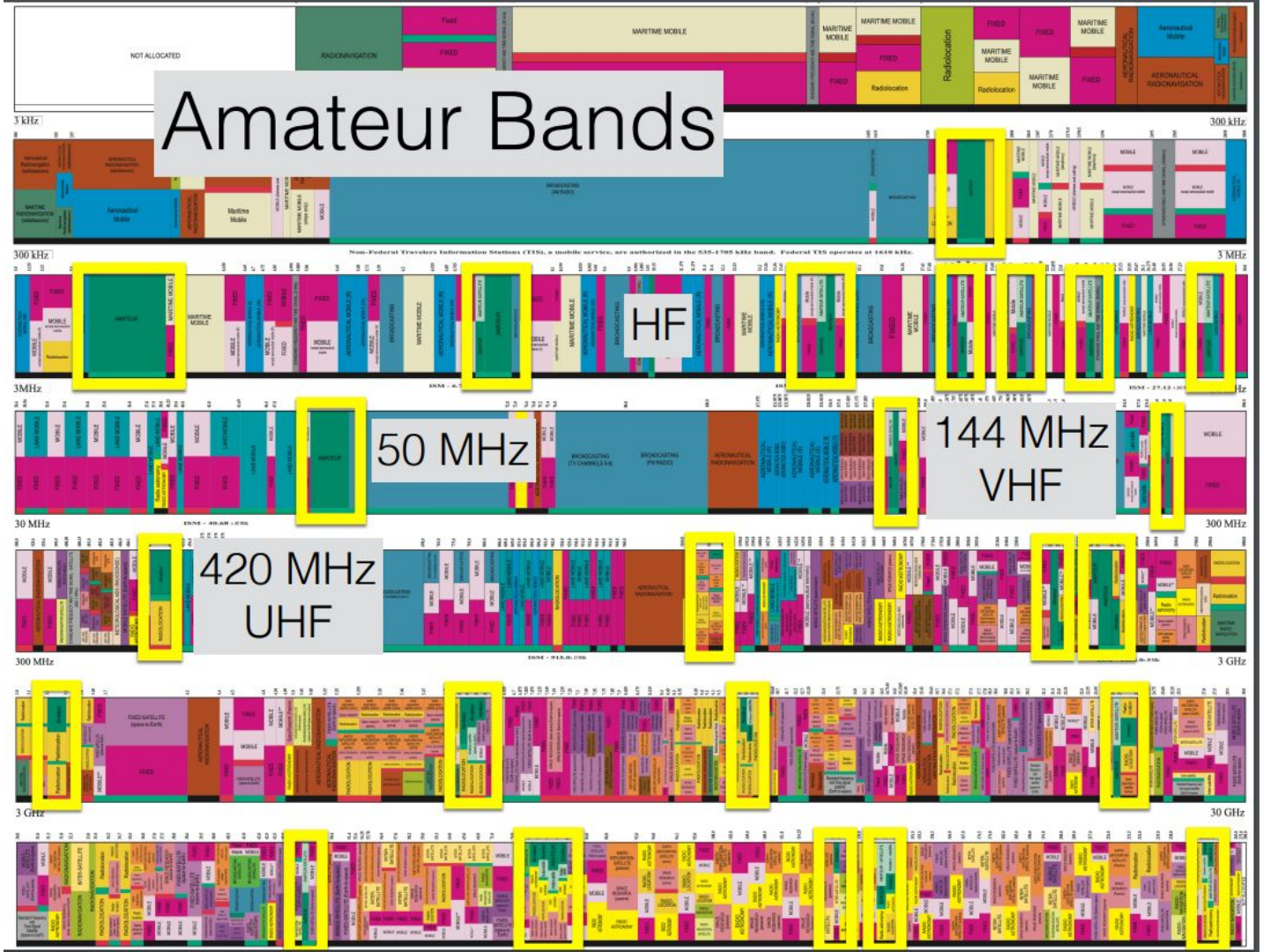

AM
3 kHz
300 kHz
3 MHz
30 MHz
300 MHz
3 GHz
30 GHz
NOT ALLOCATED
RADIONAVIGATION
MARITIME MOBILE
FIXED
Radiolocation
AERONAUTICAL RADIONAVIGATION
Aeronautical Mobile
Maritime Mobile
BROADCASTING (AM RADIO)
Non-Federal Travelers Information Stations (TIS), a mobile service, are authorized in the 535-1705 kHz band. Federal TIS operates at 1610 kH
AMATEUR
BROADCASTING (TV CHANNELS 2-4)
BROADCASTING (TV CHANNELS 5-6)
BROADCASTING (FM RADIO)
BROADCASTING (TV CHANNELS 7 - 13)
AERONAUTICAL RADIONAVIGATION
RADIOLOCATION
FIXED-SATELLITE (space-to-Earth)
MOBILE
ISM - 6.78 ±15k
ISM - 13.560 ±7k
ISM - 27.12 ±16k
ISM - 40.68 ±20k
ISM - 915.0 ±13k
ISM - 2400.0 ±50k


NOT ALLOCATED
RADIONAVIGATION
Fixed
FIXED
MARITIME MOBILE
MARITIME MOBILE
FIXED
Radiolocation
Radiolocation
MARITIME MOBILE
FIXED
MARITIME MOBILE
Radiolocation
FIXED
MARITIME MOBILE
FIXED
AERONAUTICAL RADIONAVIGATION
Aeronautical Mobile
AERONAUTICAL RADIONAVIGATION
3 kHz
300 kHz
300 kHz
Non-Federal Travelers Information Stations (TIS), a mobile service, are authorized in the 535–1705 kHz band. Federal TIS operates at 1610 kHz.
3 MHz
3MHz
30 MHz
FM
30 MHz
300 MHz
300 MHz
3 GHz
3 GHz
30 GHz


NOT ALLOCATED
RADIONAVIGATION
Fixed
FIXED
MARITIME MOBILE
MARITIME MOBILE
FIXED
Radiolocation
Radiolocation
AERONAUTICAL RADIONAVIGATION
Aeronautical Mobile
3 kHz
300 kHz
Aeronautical Mobile
Maritime Mobile
BROADCASTING (AM RADIO)
Non-Federal Travelers Information Stations (TIS), a mobile service, are authorized in the 535–1705 kHz band. Federal TIS operates at 1610 kHz.
300 kHz
3 MHz
3MHz
30 MHz
TV
TV
TV
30 MHz
300 MHz
TV
300 MHz
3 GHz
3 GHz
30 GHz


NOT ALLOCATED
RADIONAVIGATION
Fixed
FIXED
MARITIME MOBILE
MARITIME MOBILE
FIXED
Radiolocation
Aeronautical Mobile
AERONAUTICAL RADIONAVIGATION
3 kHz
300 kHz
Non-Federal Travelers Information Stations (TIS), a mobile service, are authorized in the 535–1705 kHz band. Federal TIS operates at 1610 kHz.
300 kHz
3 MHz
3MHz
30 MHz
30 MHz
300 MHz
Cell
Cell
300 MHz
3 GHz
3 GHz
30 GHz


NOT ALLOCATED
RADIONAVIGATION
Fixed
FIXED
MARITIME MOBILE
MARITIME MOBILE
FIXED
MARITIME MOBILE
FIXED
Radiolocation
Radiolocation
FIXED
MARITIME MOBILE
Radiolocation
FIXED
MARITIME MOBILE
FIXED
AERONAUTICAL RADIONAVIGATION
Aeronautical Mobile
AERONAUTICAL RADIONAVIGATION
3 kHz
300 kHz
BROADCASTING (AM RADIO)
Aeronautical Mobile
Maritime Mobile
300 kHz
3 MHz
Non-Federal Travelers Information Stations (TIS), a mobile service, are authorized in the 535-1705 kHz band. Federal TIS operates at 1610 kHz.
AMATEUR
3MHz
30 MHz
30 MHz
300 MHz
WiFi
WiFi
300 MHz
3 GHz
3 GHz
30 GHz


Amateur Bands
HF
50 MHz
144 MHz
VHF
420 MHz
UHF
3 kHz
300 kHz
3 MHz
30 MHz
300 MHz
3 GHz
30 GHz

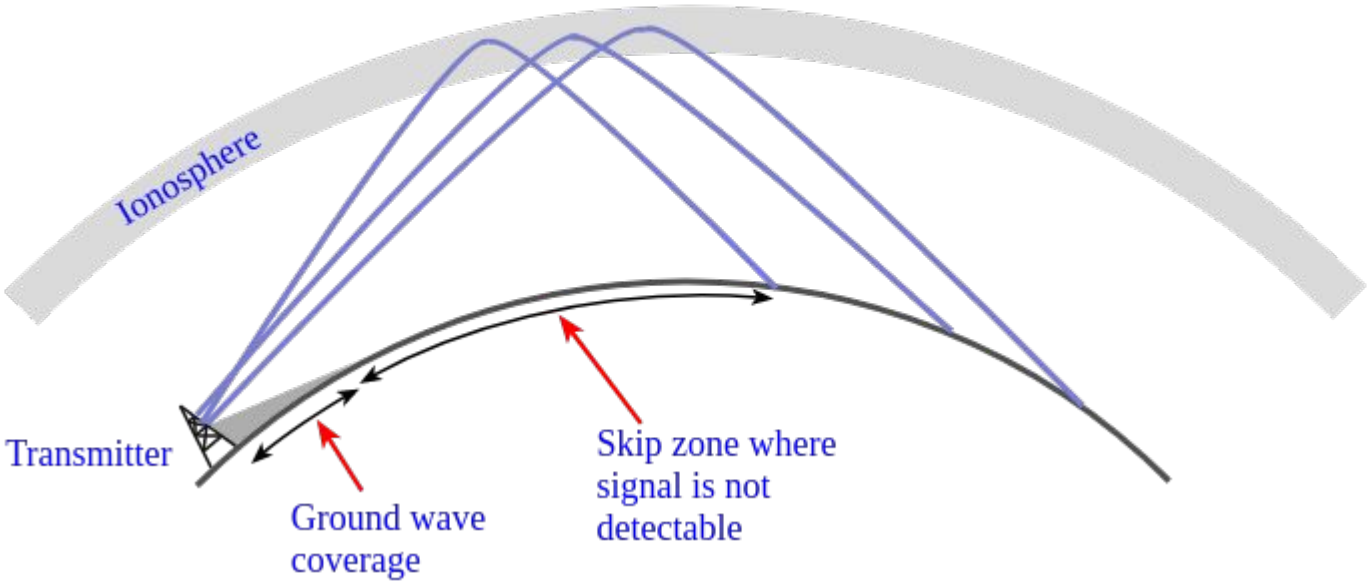
Finding Where You are on the Radio Dial

- Described as Band, Frequency, or Wavelength
- Bands: HF, UHF, VHF
- Frequency: 50 MHz, 144 MHz, 440 MHz
- Wavelength: 6 m, 2 m, 70 cm
- Wavelength (in m) = 300 / (frequency in MHz)

Propagation Modes

- Ground wave
  - Low HF and below, ground acts as waveguide
  - AM radio
- Line-of-Sight (LOS)
  - VHF and above, radio waves only slightly refracted or reflected by the atmosphere
  - FM Radio
- Sky wave
  - For HF, and sometimes VHF, the upper atmosphere acts as a reflector, bouncing radio waves back to earth far from the source
  - Short wave radio

Skywaves & Skip Distance & Skip Zone

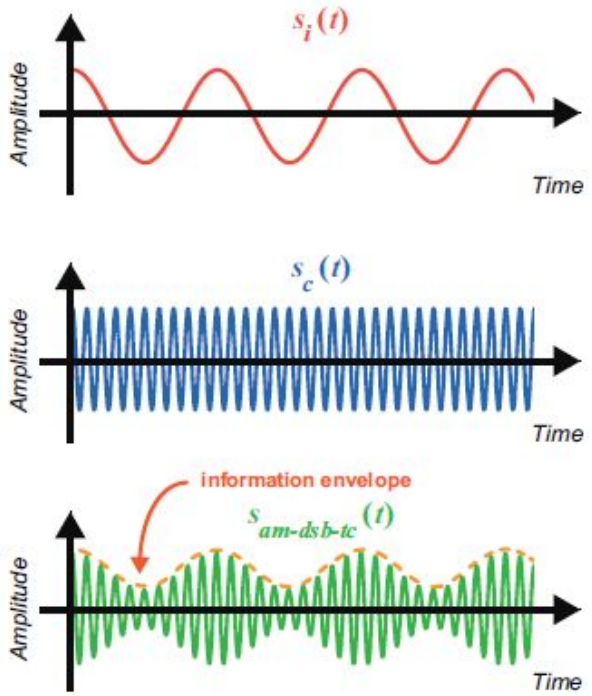


Modulations

- Information is encoded in different ways
  - Morse Code (CW)
  - Amplitude Modulation (AM)
  - Frequency Modulation (FM)
  - Phase modulation (PM)
  - Digital modulations

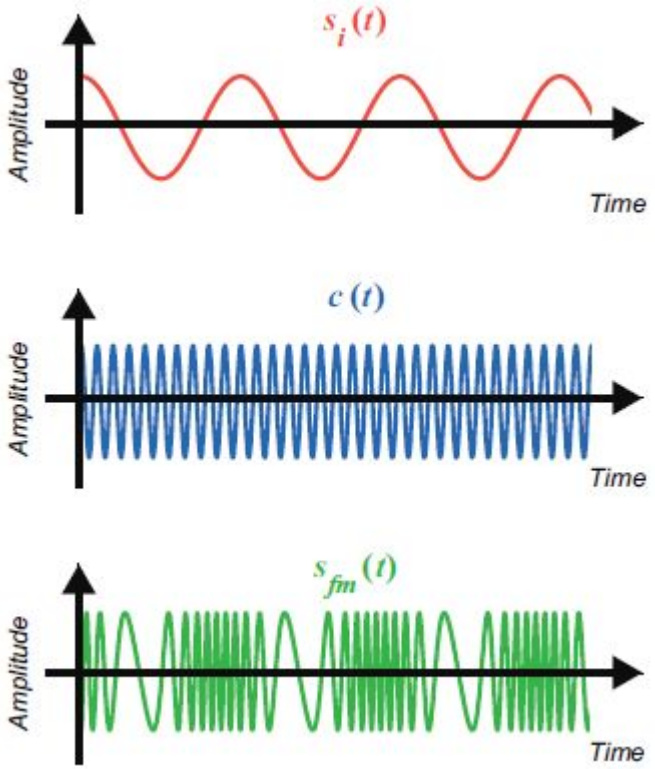
Amplitude Modulation (AM)

- Information encoded in carrier's **amplitude**
- Airband



Frequency Modulation (FM)

- Information encoded in carrier's **frequency**
- Noise resistant



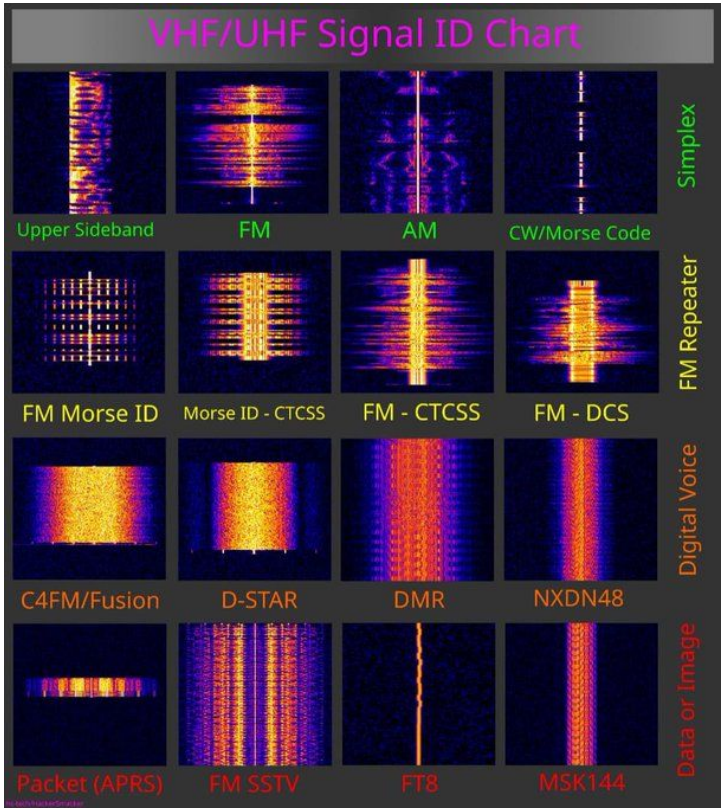
Radios

- Desktop Radios
  - Many modes, complex
  - Mostly HF
  - Lots of modes (FM, SSB, Digital Voice and Data)
  - 100W + Power Amps to 1500 W
- Mobile
  - FM, one or more bands
  - 50 W
- Handheld
  - FM, one or more bands, 5W
  - Simple, but lots of options

Digital Radios

- DStar (ICom, Kenwood)
- C4FM, Wires (Yaesu)
- DMR — Digital Mobile Radio (Lots of companies)

Signal References



What is Software Defined Radio (SDR)?

“A radio in which aspects of functionality are implemented in, or controlled by, software.”

- Flexible functionality
  - the operation of a radio can be changed without making any physical alterations to the device
- Algorithms from DSP and communications theory running as real-time software on a CPU, GPU and/or FPGA
- Joe Mitola first coined the term in 1991

Why SDR?

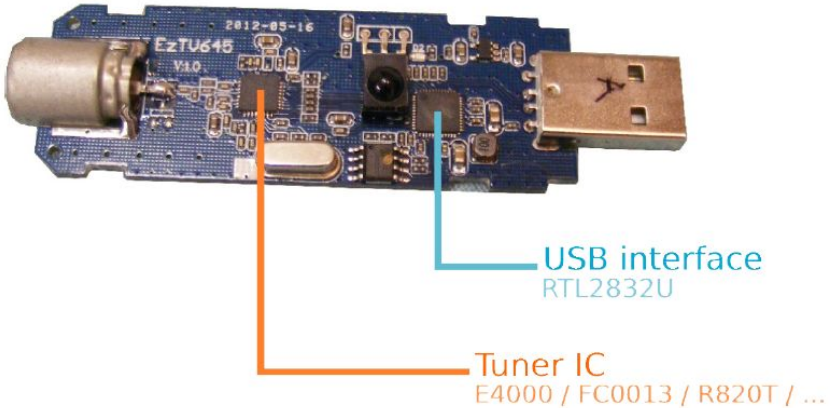
- Traditional radios are hard-wired to specific frequency bands and communication protocols
  - Fixed-function, Black Box
  - Can’t be easily modified, can’t easily access internal values and states
- SDR provides:
  - Flexibility
  - Upgradability
  - Reconfigurability
  - Lower Cost

Key SDR Parameters (Features)

- Frequency (Tuning) Range
- Instantaneous Bandwidth
- Bit resolution
- Interface (USB, Ethernet, PCIe)
- Rx/Tx, half-duplex, full-duplex, MIMO
- Preselectors
- Budget: 50$-...k$

RTL-SDR

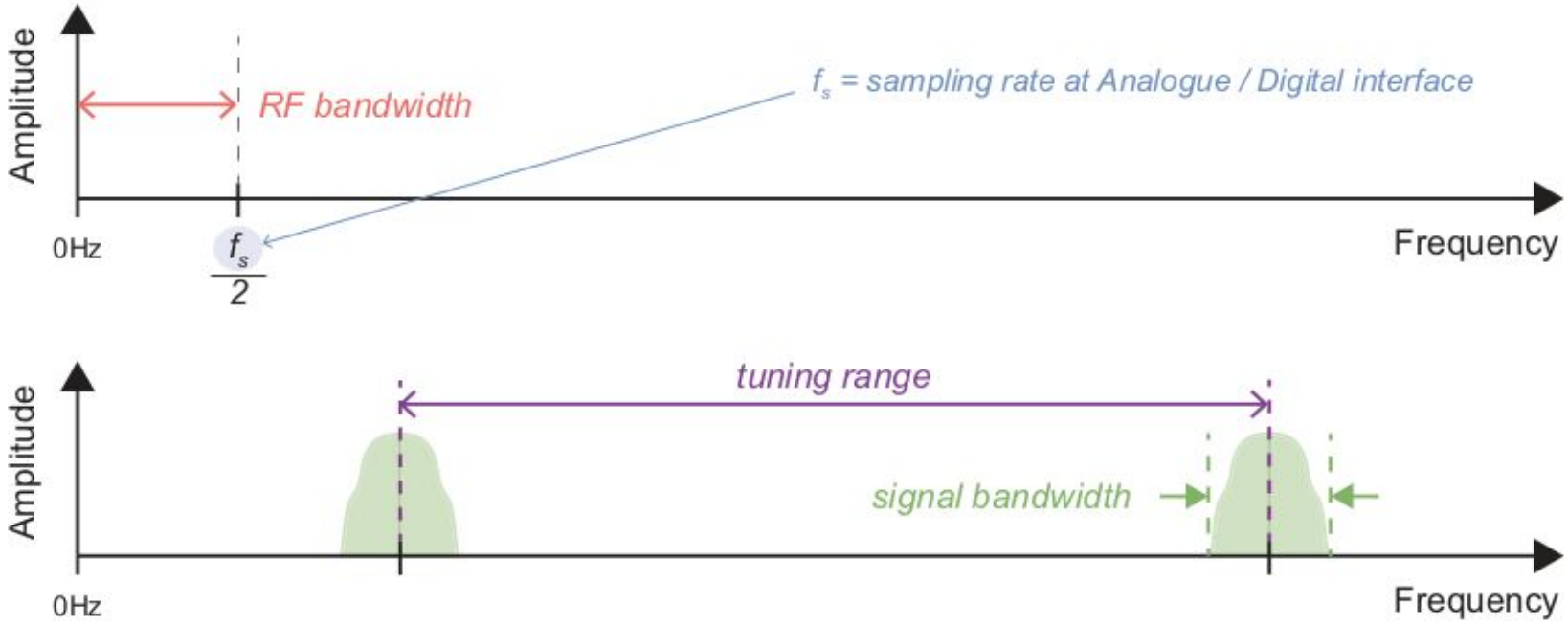
- “I smell a very cheap poor man’s SDR here ☺”
- Cheap man’s radio since 2012
- Hams, DIY, hackers, makers, students,…
- Demodulator
  - Named by RTL2832U chip, DVB-T
- Tuner
  - **R820T**: 24-1766MHz
  - **E4000**: 52-2200MHz



RTL-SDR

- Receive-only
- 8-bit ADC
- 24MHz-1.75GHz (depends on tuner chip)
- 2.4MSPS BW (stable) upto 3.2M
- “*HamItUp*” upconverter
  - HF coverage

Key Radio Terminology and Parameters



RTL-SDR Driver Installation - Linux

- Linux users may blacklist RTL so that default DVB-T driver is not loaded when dongle is plugged in.
  - cd /etc/modprobe.d/
  - sudo gedit blacklist-rtl.conf
  - # append: blacklist dvb_usb_rtl28xxu
  - OR
  - echo "blacklist dvb_usb_rtl28xxu" >> /etc/modprobe.d/blacklist.conf

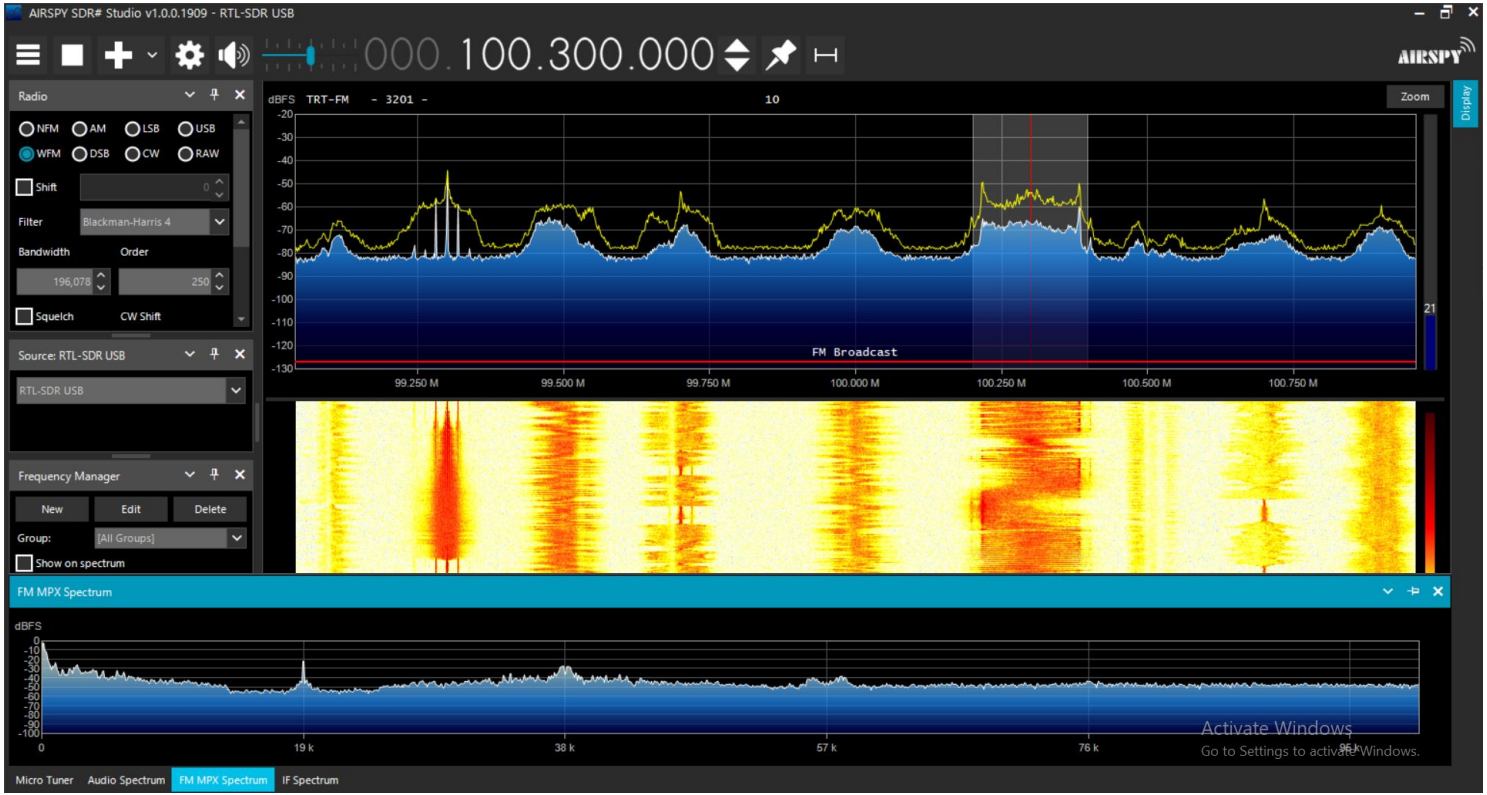
Test your RTL

- run ***rtl_test*** terminal application to check your device is working

“RF” Hello World

- Acquire RF data with RTL-SDR
- Use gqrx as general-purpose SDR application
- Tune to a frequency in FM broadcast band
- Spectrum view
- Spectrogram view
- WBFM demodulation

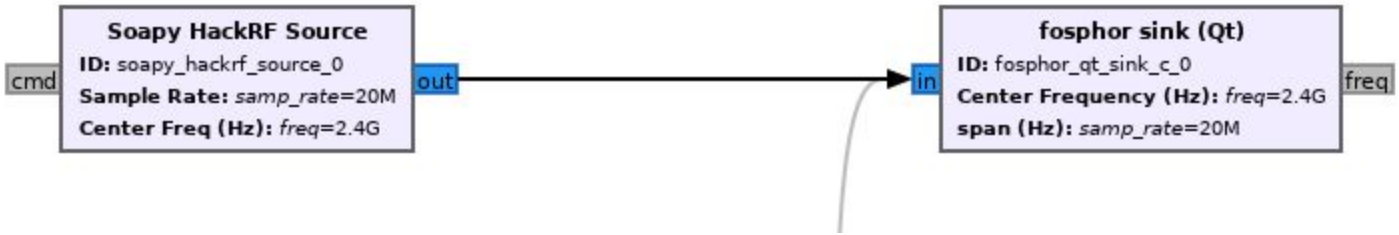
Hello World: WBFM



Capture The Signal (CTS)

- Your instructor is transmitting in one of the ISM bands, your job is to find out what this signal contains?
  - *Hint: Tune to an ISM band frequency, watch the spectrogram!*

RTSA


Soapy HackRF Source
ID: soapy_hackrf_source_0
Sample Rate: samp_rate=20M
Center Freq (Hz): freq=2.4G
cmd
out
fosphor sink (Qt)
ID: fosphor_qt_sink_c_0
Center Frequency (Hz): freq=2.4G
span (Hz): samp_rate=20M
in
freq

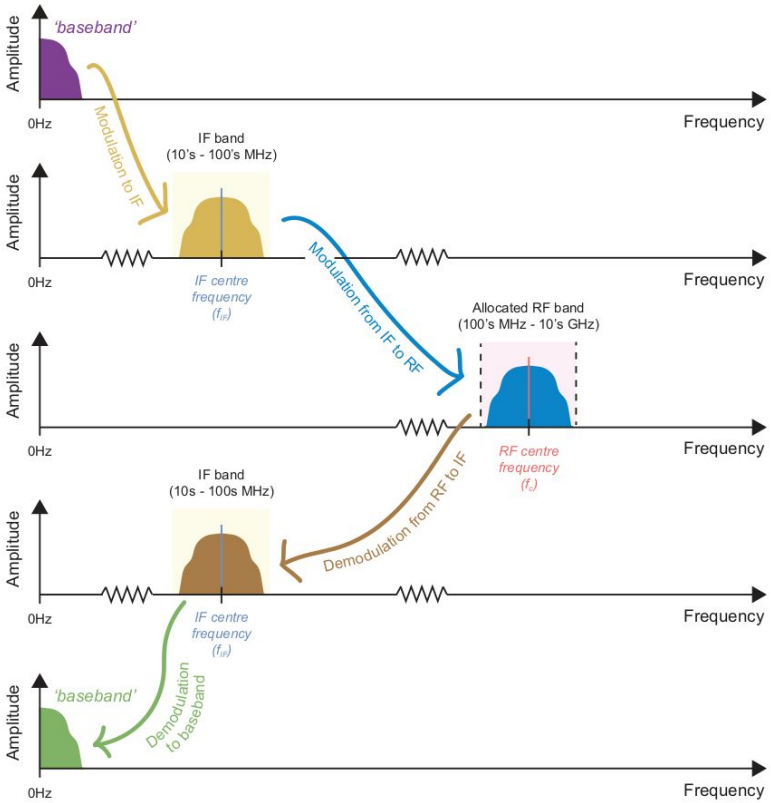
Some Signal Hunting

- VHF airband: 108 and 137 MHz.
  - 108 to 117.95, split into 200 narrow-band channels of 50 kHz. VOR beacons, ILS localizers.
  - 118 to 136.975: amplitude modulation voice transmissions
- Keyfob: 433 MHz
- GSM

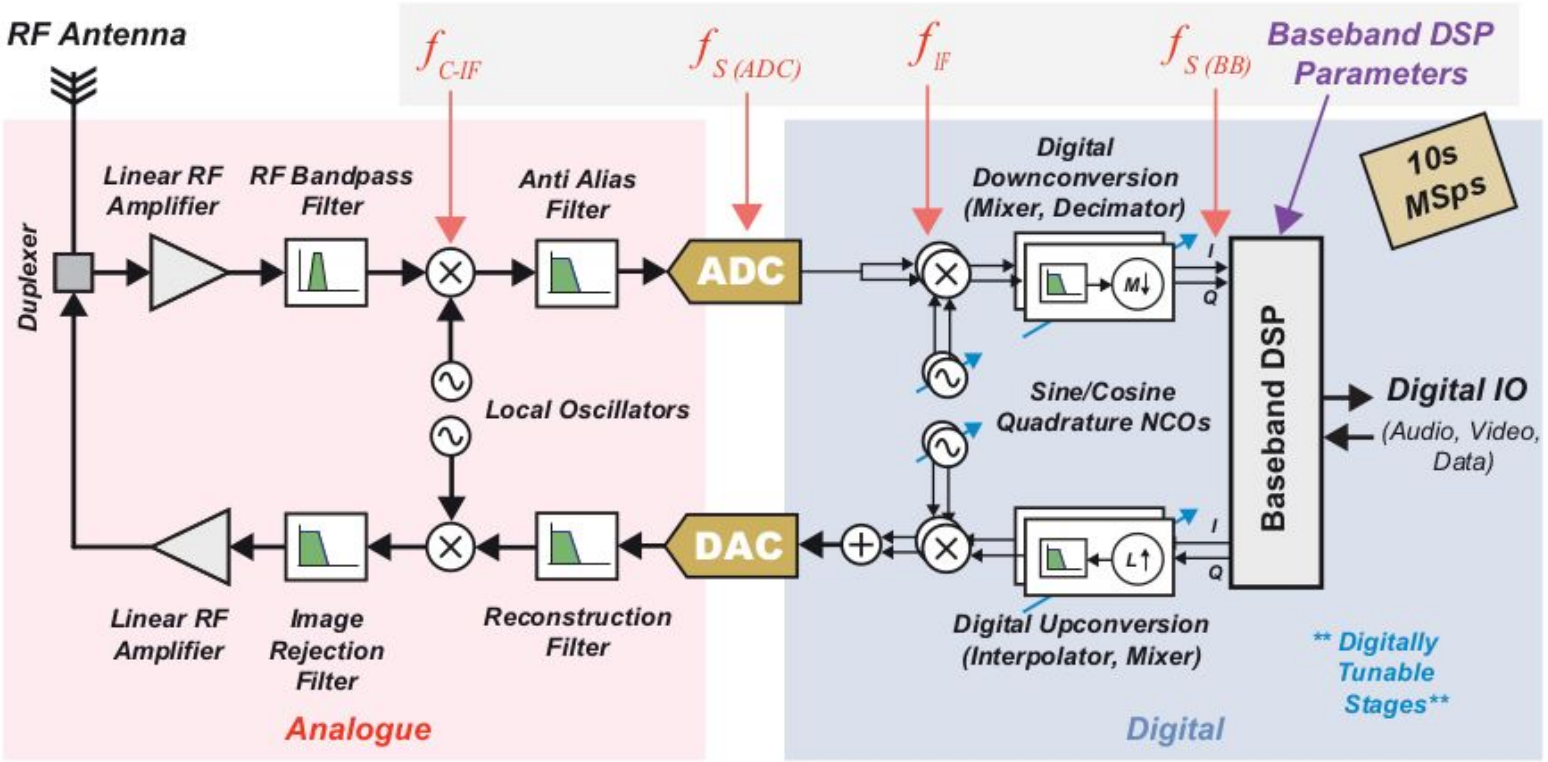
SDR Architectures

- There are **two** primary architectures for radio transmitters
  - One involves **direct** modulation from baseband frequencies to RF frequencies
  - The second (the **superheterodyne**) achieves this transition with two modulation stages: the first from baseband to an Intermediate Frequency (IF), and the second from IF to RF. In each case, the receiver mirrors the operations of the transmitter

Superheterodyne Scheme



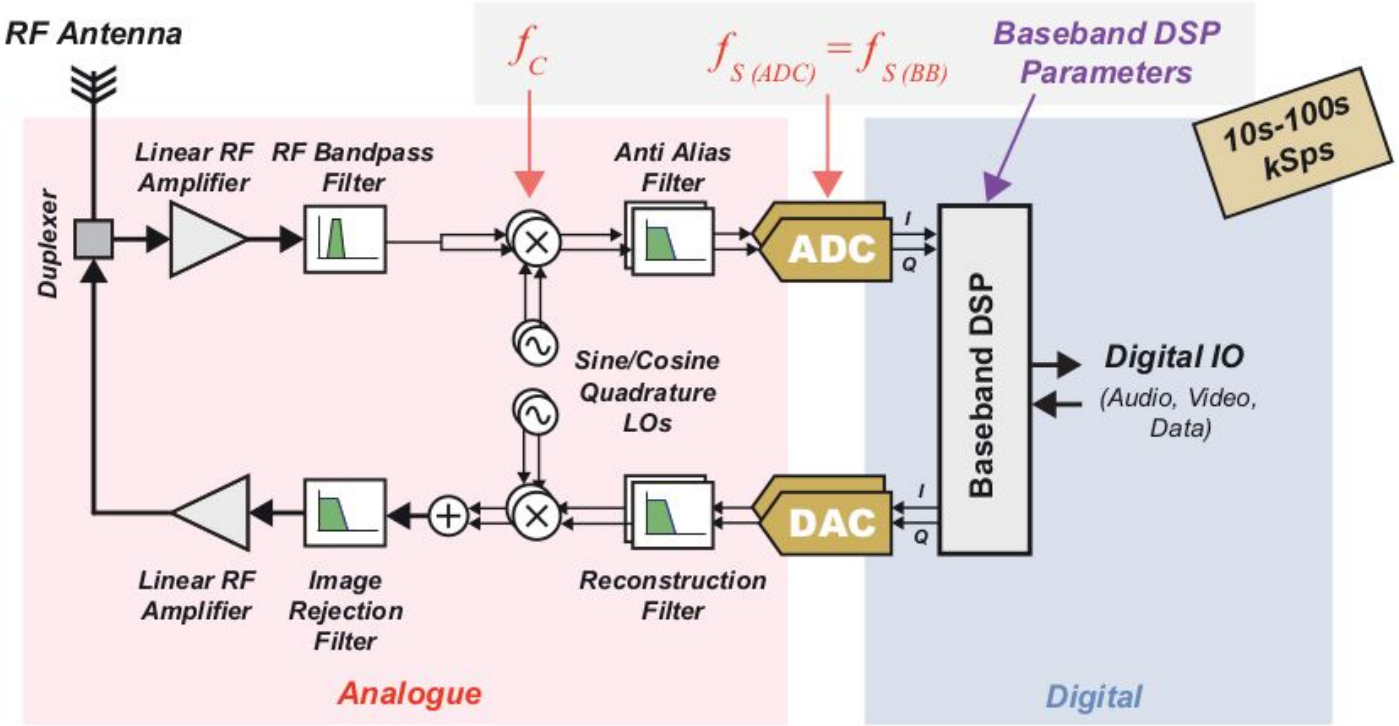
IF-Sampling Software Defined Radio



SDR Architectures: DCR

- Most SDR uses a direct-conversion receiver (DCR) architecture
  - Also called Zero-IF receiver, and homodyne receiver
  - Eliminates the intermediate frequency (IF) by translating the band of interest directly to baseband
  - The frequency of the LO is set to the same frequency as the transmitted/desired RF signal

Baseband-Sampling Software Defined Radio



Direct-RF (Almost-All-Digital) Radio