

Digital Mobile Radio (DMR)

@Crypt0s

Who we are:

- We are a hacker/maker space
- We are a non profit 501(c)(3)
- Everything you see here was donated by the community
- Everything you see here is free for public use (although some may require minor training)



Our mission is to foster creative and technical growth through open collaboration by providing tools and resources within the greater Baltimore-Washington Metro area.

Unall{Ø}cated

Get Involved!

- You can donate your time
- You can donate your knowledge
- You can donate your unused equipment
- You can donate supplies
- Lastly we also have overhead and we would appreciate a one time donation or even better you can become a member.



This space many of us call home is completely run based on community donations, every little bit helps and ensures we can keep the door open and keep classes like this free for anyone interested in attending.

Unall{Ø}cated

No matter the day there is almost always something going on here and events can be found on the following social media outlets.



www.unallocatedspace.org



meetup.com/Unallocated-Space/



[@unallocated](https://twitter.com/unallocated)



<https://unallocatedspace.slack.com>



facebook.com/Unallocated/



<https://groups.google.com/forum/#!forum/unallocated-space>

Unall{Ø}cated

Who Am I?



@Crypt0s



Department 13 Red Team Director || Penetration Tester



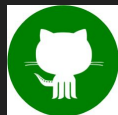
Former President / Current Board Member Emeritus



Hacking, breaking protocols, programming

+1

Other Projects: FakeDNS, Killerbee, and a few others...



<https://github.com/crypt0s> <-- These slides will be posted here

What Will We Learn Today?

1. Who Where and Why of DMR
2. Technical details of physical layer
3. Terminology (Talkgroup, Timeslot, Contact, ect...)
4. How to use a repeater
5. Operating a “Hotspot” repeater
6. Programming your radio
7. Question and Answer segment

What Do You Need to Get Started???

Ham Radio Callsign <http://www.arrl.org/getting-your-technician-license>

DMR ID from <https://www.radioid.net/>

Brandmeister Account (if you want to run your own repeater/hotspot):
<https://brandmeister.network/?page=register>

A Radio:

- RadioOddity GD-77
- Tytera MD380
- Anytone at-d868uv || BTech DMR 6x2 (my favorite)

What is it, Where is it used, and Why?

What - A digital comms mode which uses 4-level Frequency Shift Keying

Where - All over the United States as commercial, safety, and amateur

Why - Numerous advantages over analog transmission including:

- Improved voice quality
- View current speaker information
- Ability to split users into groups
- “Manufacturer features” (discussed later)

Technical Details

Bandwidth: 12.5khz

Modulation Type: 4-level FSK (Multi-FSK where each frequency represents 2 bits)

TDMA with 2 Time Slots each 30ms long

Error Correction with Reed-Solomon or Trellis Coding

Digital Mode so duty cycle is much lower than analog modes

Utilizes a Vocoder so you sound like a robot (A vocoder matches sounds it hears to tones in a lookup table)

Digital so it sounds great until suddenly you just can't talk, vs analog where you just sound progressively worse and hope whomever you're calling can hear you.

Technical Details: Continued

DMR is a specification which many manufacturers have their own implementation of. These may be compatible with other manufacturers. Motorola TRBO is one example.

There are three tiers:

1. Basic, no repeaters, don't get radios that do this.
2. Full functionality, digital voice with two timeslots and repeaters
3. The above, plus trunking and IP over DMR (among other features)

Tough Talk - The Terminology of DMR

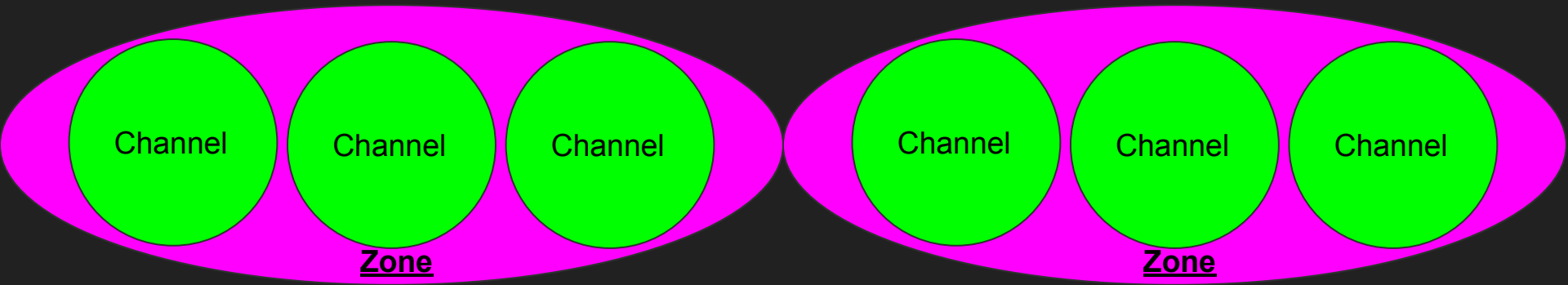
We'll start with the widest concepts and end with the narrowest

There are 5 major new concepts in DMR:

- Zones
- Channels
- Timeslots
- Contacts (Talkgroups, IDs)
- DMR IDs

We need some diagrams...

Tough Talk - The Terminology of DMR



A **ZONE** contains several geographically-close *channels*
Usually a *channel* can be selected using your radios selector knob and
a **ZONE** can be changed through another button

Tough Talk - The Terminology of DMR

Channel 1

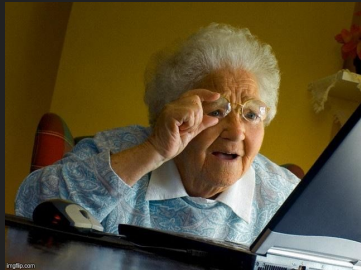
Name: Repeat 1
TX Freq 433Mhz
RX Freq 415Mhz
TIMESLOT 2
Contact 1

Channel 2

Name: Repeat 1
TX Freq 433Mhz
RX Freq 415Mhz
TIMESLOT 1
Contact 2

Channel 3

Name: Repeat 2
TX Freq 421Mhz
RX Freq 426Mhz
TIMESLOT 1
Contact 2



A **ZONE** contains several *channels*

Channels contain information about a repeater and a **contact** on that repeater

A **contact** on a repeater is also known as a **talkgroup** but it could also be a **DMR ID**

A *channel* is usually named after the repeater/**contact** combo it's using

Talkgroups and DMR IDs



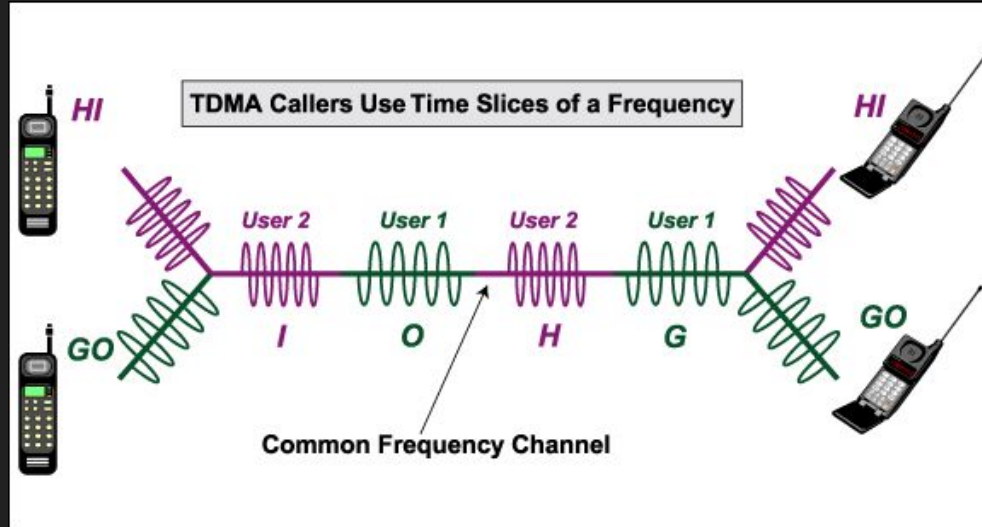
Talkgroup - Basically a chatroom, but its name is a special number within a number range which is assigned only to chat rooms

DMR ID - Basically your username. It's unique and (supposedly) locked to your ham radio callsign, so people can use it to look up your callsign and therefore your address (you do know the FCC publishes your address with your callsign, right?)

Wait, wait, wait...you missed something, Crypt0s

Timeslots. Wibbly-Wobbly Timeslots.

DMR has this neat feature where the hotspot can transmit to someone else while you talk to it



Currently, most radios have two timeslots (TS). TS1 and TS2 are used to break up multiple talkgroups because repeaters can still only transmit from up to two talkgroups at once.

Terminology Review

A ZONE has many *channels* which communicate with *talkgroups* which are set to specific TIMESLOTS. TIMESLOTS allow a repeater to time-slice it's operation so that it can do multiple things "simultaneously" on the same frequency.

By programming my radio with a ZONE containing *channels* with the frequency of a repeater, the ID of a *talkgroup*, and a TIMESLOT, I can communicate with people.

Some repeaters force specific *talkgroups* to specific TIMESLOTS, and I will need to know the organization of my repeater before I attempt to use it.

Reminder: I'll post these online and help with ?'s

How to Use a

It's the most fun wo

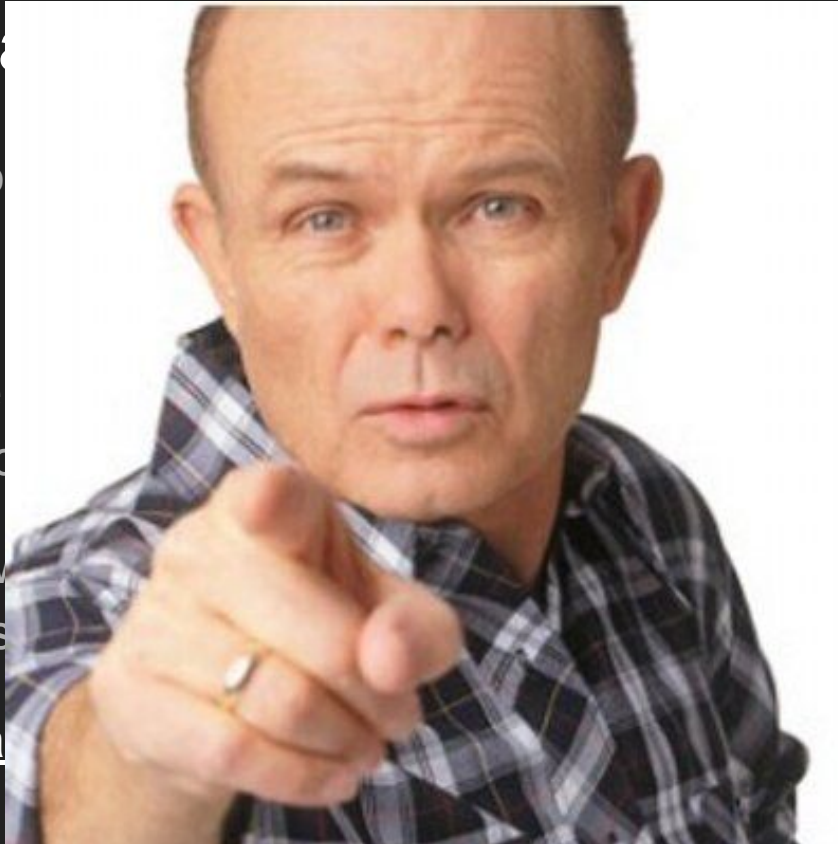
Kerchunk - To key

You should be able
9990 and get your o

Kerchunking a TG v
Use new talkgroups

Don't Be a Dumb

When you talk on a talkgroup, you are being re-broadcast around the world.
There could be thousands of people listening to you on some popular talkgroups!



can communicate with

unk" onto talkgroup
the "Parrot" talkgroup.

ing that talk group!
er.

How To Use Repeaters, Continued

I want to get onto the Wireless Village Talkgroup on my local repeater

1. Ensure the repeater allows User-Defined talk groups and that you're using the correct timeslot for that
2. Select the correct zone
3. Choose the channel with my desired talkgroup (31337) as the contact
4. Key the Push-to-talk, holding down the button for a second or two
5. Release the PTT
6. Push the PTT and speak, you will now be communicating with the TG

Optional: Utilize hose.brandmeister.network to ensure that you're reaching the TG on the network.

There Aren't Any Repeaters Near Me Tho.

Sorry to hear that dude, you should run your own Hotspot!

Purchase a Raspberry Pi and an MMDVM Hat. I have some instructions on how to do that here: <https://bit.ly/2Tbh0UA>

Lets dive into how that actually works by looking at my brandmeister account!

Programming Your Radio

[LIVE DEMO, DOOMED TO FAILURE]

Question / Answer Segment

What did I not cover that you need?

Did I mess something up?

Where in the world is Carmen Sandiego?

Why did Penny always help out Inspector Gadget? I mean, she was in school!

<https://t.co/IELU5HxNE9>