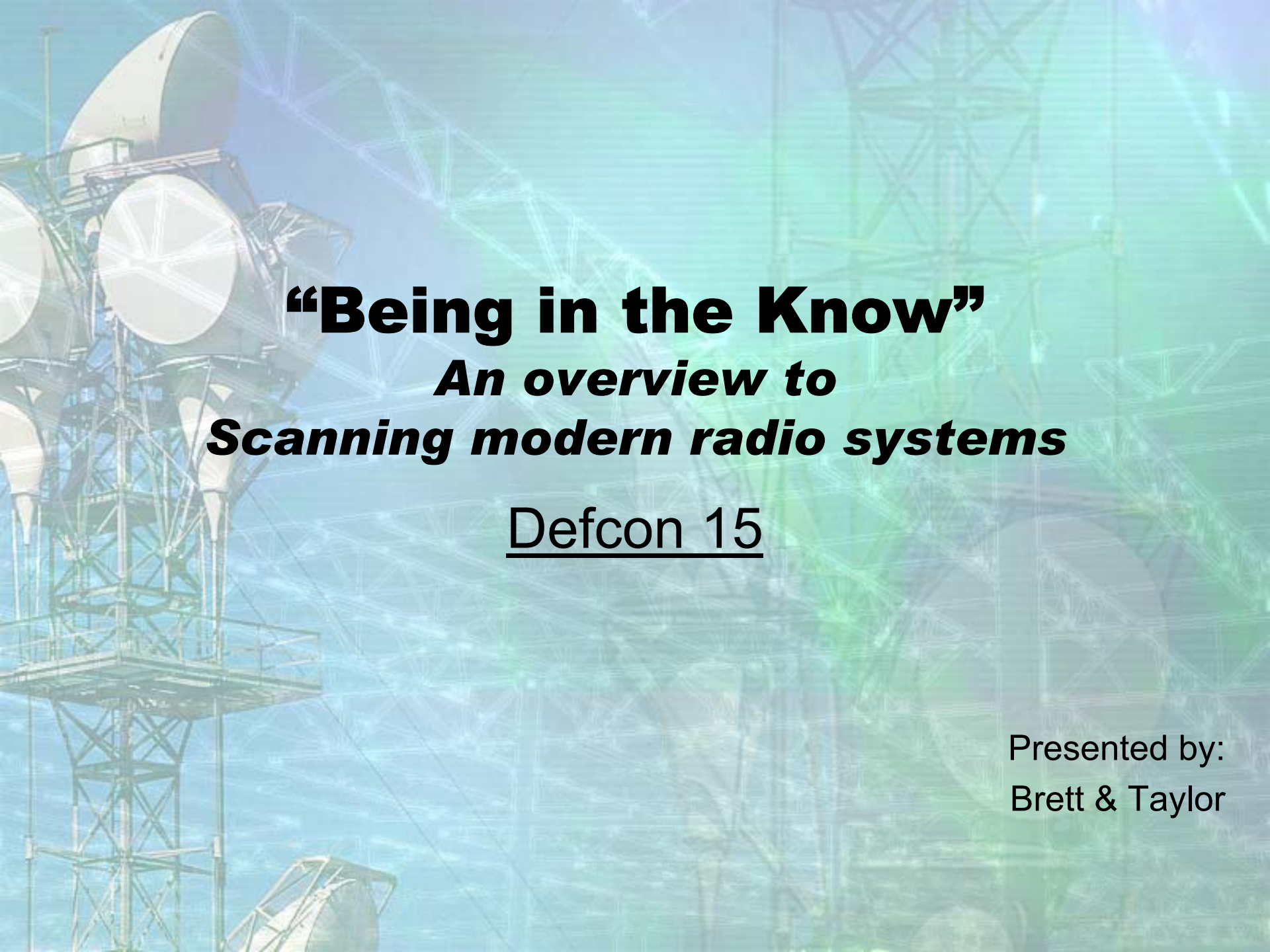


“Being in the Know”

An overview to Scanning modern radio systems

Defcon 15

Presented by:
Brett & Taylor

The Basics

- Simplex
  - One frequency shared by multiple stations
  - Limited coverage
- Tones
  - Continuous Tone Coded Squelch System (CTCSS)
    - Private Line (PL)
  - Digital Coded Squelch (DCS)
- Repeaters
  - Two frequencies (input & output)
  - Increased Coverage

So you want to listen to stuff

- Back in the day it was easy…
- You just dialed in the frequency and you were good to go.
  - 154.905 Utah Highway Patrol SLC
  - 155.505 Statewide
  - 154.2350 SLCO Fire Dispatch
- Not quite as easy these days…
  - Trunked, Digital, Encrypted, etc

What is Trunked Radio

- Users are grouped by Talk Group rather than Frequency
- Radios monitor a central channel called the Control Channel
- When a user keys the radio the control channel tells other what frequency to move to
- When done, users return to the control channel and wait for the next call

System Types

- Ericsson (EDACS)
  - Enhanced Digital Access Communication System
- E.F Johnson (LTR)
  - Logical Trunked Radio
- Motorola
  - Probably the most common type of system

Ericsson

Enhanced Digital Access Communication System (EDACS)

EDACS - Overview

- Central Control Channel
- Each frequency is assigned an LCN
  - Logical Channel Number
- Controller tells radios what LCN to switch to when radio traffic is present
- Frequencies must be entered in LCN order to scan properly

E.F Johnson
Logical Trunked Radio (LTR)

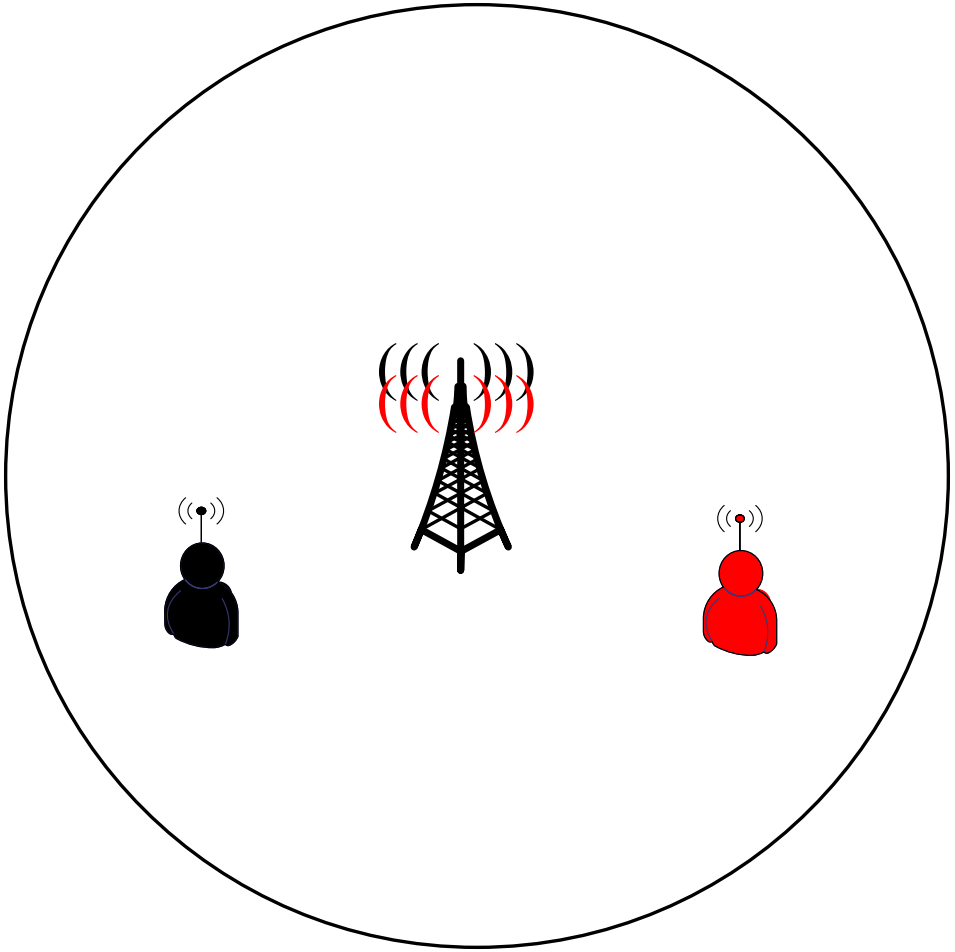
This is what The Riviera Runs

LTR - Overview

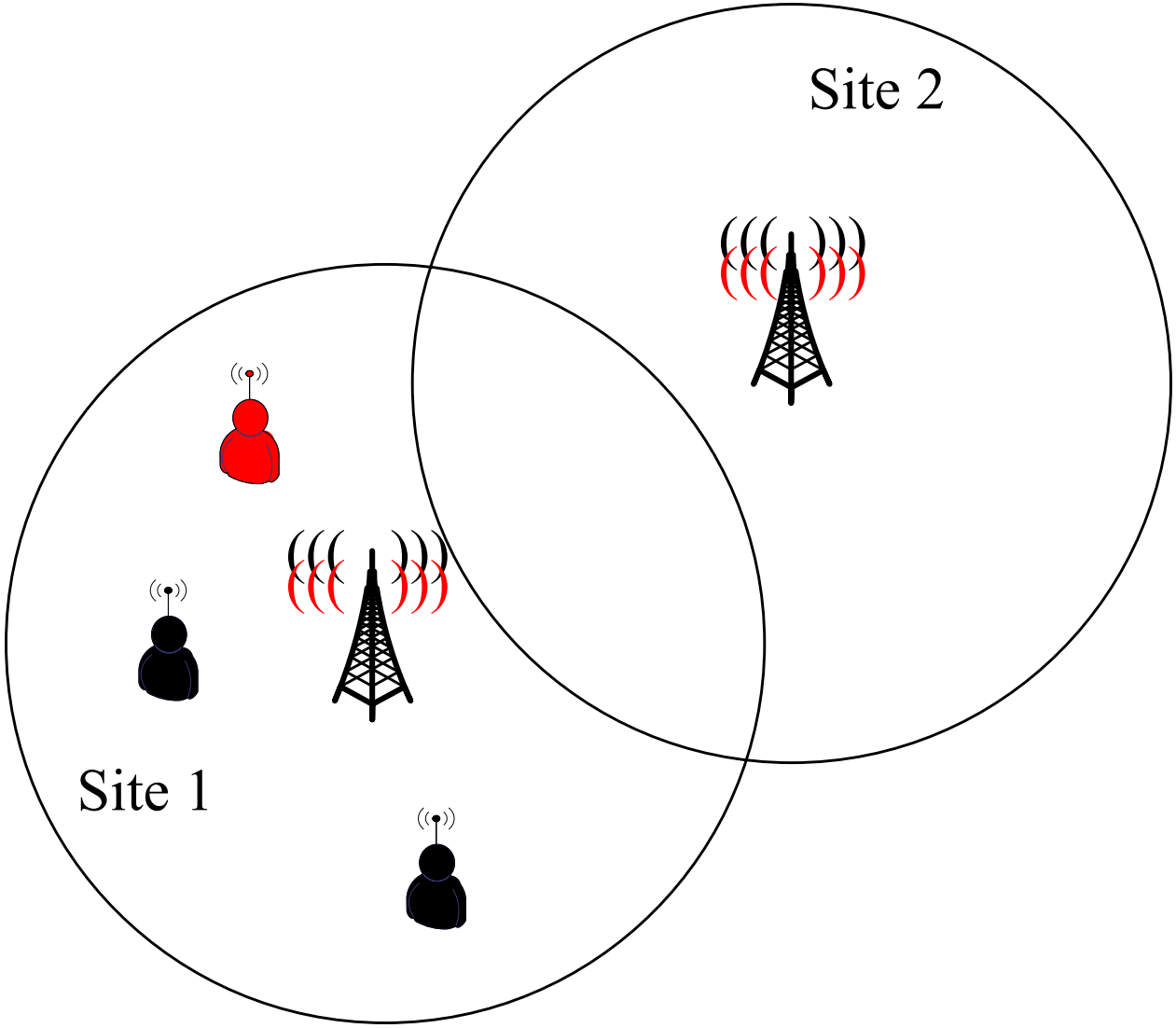
- Decentralized Model
- Uses sub-audible data on each frequency to control system
- Each frequency is assigned an LCN
  - Logical Channel Number
- Users are assigned to a specific LCN and only move if it is busy
- Frequencies must be entered in LCN order to scan properly

Motorola
SmartNet & SmartZone

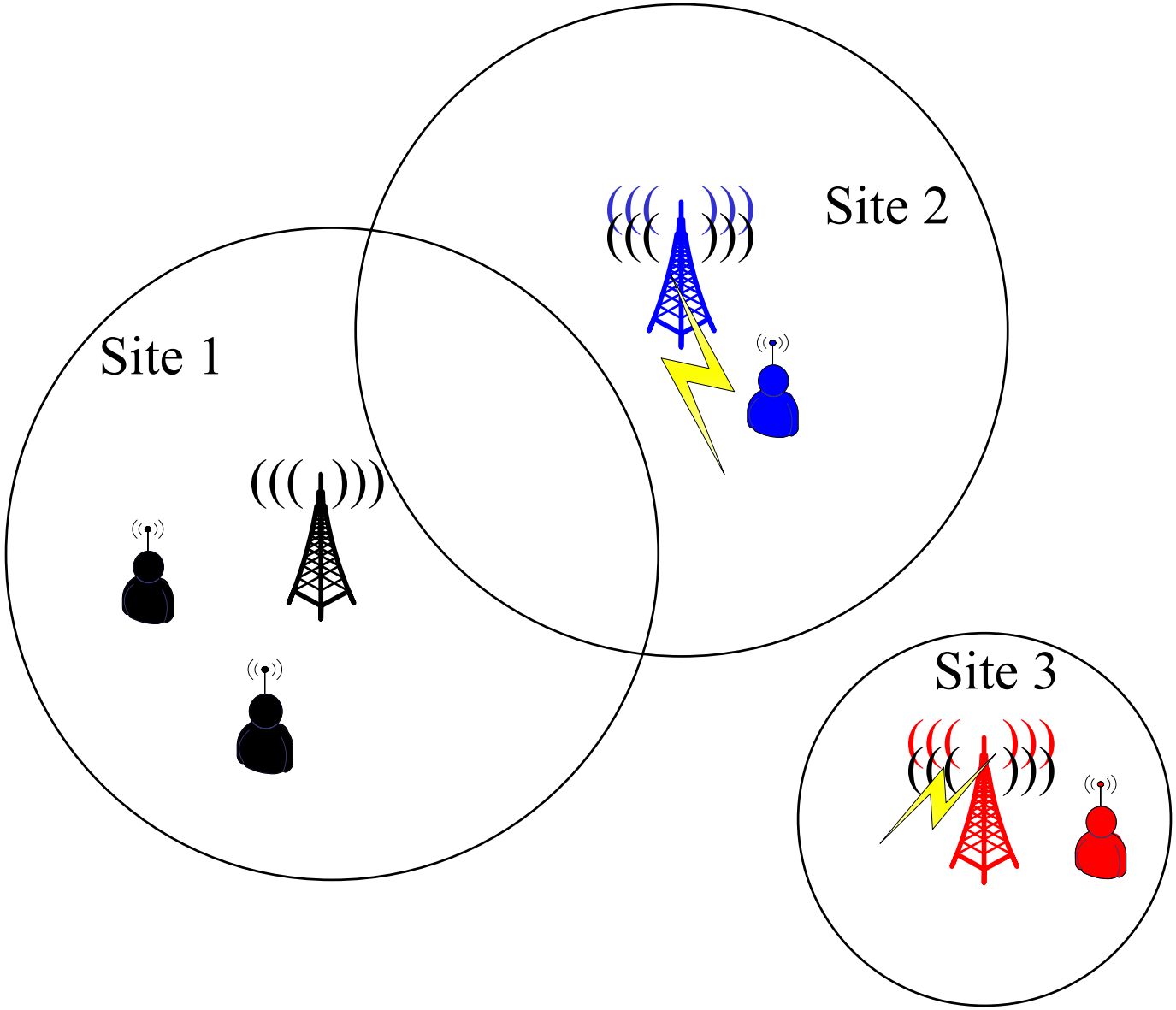
SmartNet (Site)



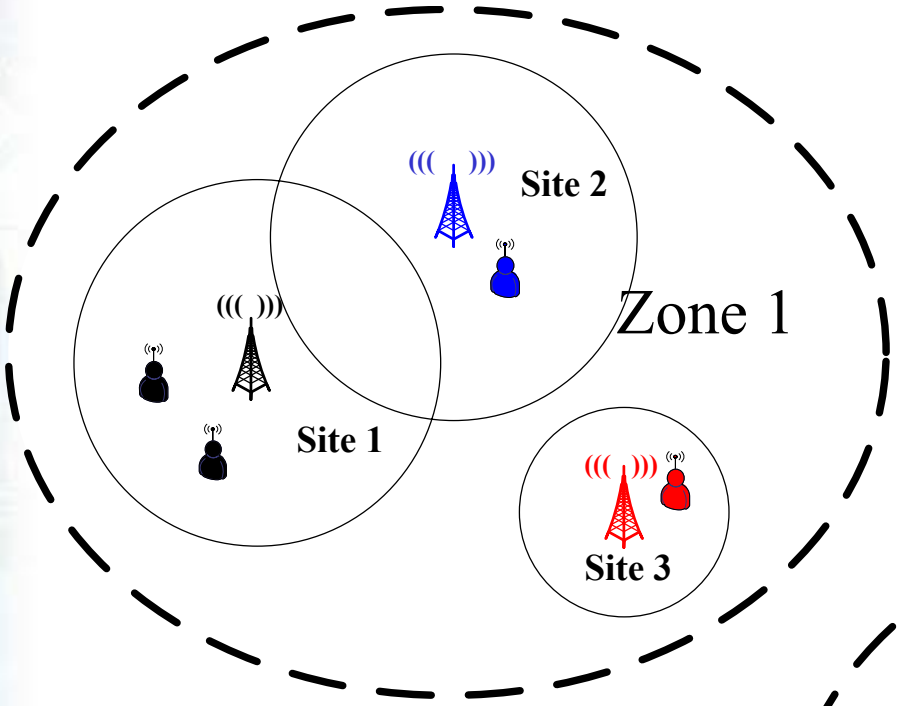
SmartNet (Simulcast)

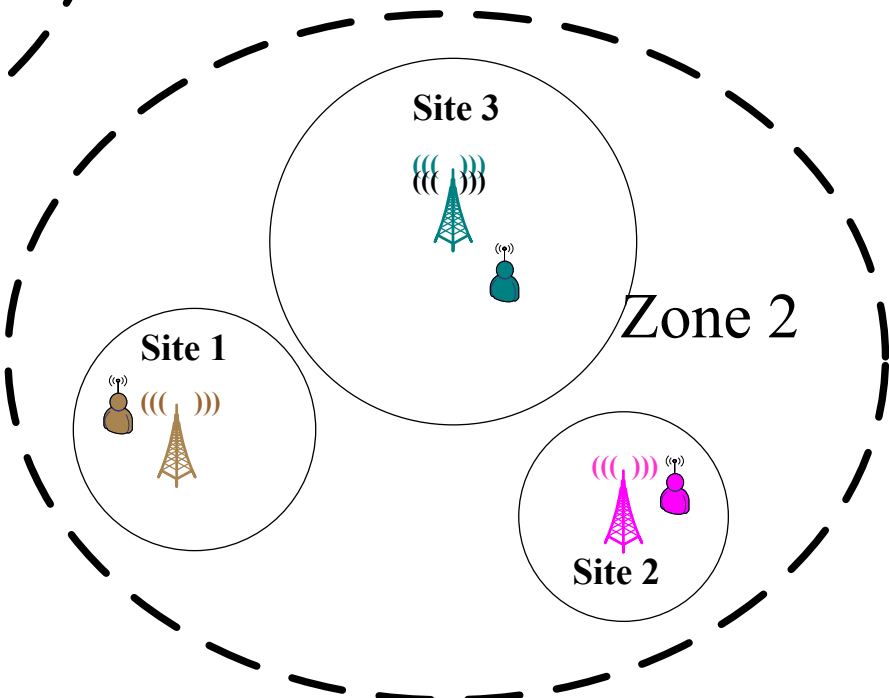


SmartZone



SmartZone OmniLink





UCAN

- Motorola Smart Zone Omni Link
- Established in 1997
- Operational in January 2002
- Over 120 Agencies use the system
  - Consisting of over 15,300 radios
  - 38 Known Sites (many with simulcast)
- 2002 Olympics
  - 8.5 million transmissions
  - 5.5 per second


UCAN Site
Clayton Peak

APCO 25

APCO 25

- What is APCO 25?
  - Association of Public Safety Communications Officials International.
  - APCO 25 brings together representatives from many local, state and federal government agencies who evaluate basic technologies in advanced land mobile radio.

APCO 25 Benefits

- Provides enhanced functionality with equipment and capabilities focused on public safety needs.
- Improved spectrum efficiency.
- Ensures competition among multiple vendors through Open Systems Architecture.
- Allows effective, efficient, and reliable interoperability

APCO 25

- So what does that all mean for us.

- We will still be able to listen to the public saftey transmissions.
- APCO 25 Helps ensure this.

Rebanding

Rebanding

- Rebanding (also called Reconfiguration) refers to changes to the 800 MHz band plan that are taking place nationwide
- In the late 1990's, the FCC realized that they had a problem with Nextel.

Why won't my scanner work after rebanding?

- Well, depending on what you listen to, it might work.
- If you listen to EDACS or LTR (or conventional), you will just need to reprogram the new frequencies and logical channel numbers (LCN).
- However, if you listen to Motorola systems (which still comprise the largest number of public safety systems), your scanner will have a problem.

How will my scanner work after rebanding?

- Motorola has several options when it comes to rebanding. They could:
- 1. Just change their channelization and make no other changes to the data.
- 2. Use the control channel format used for P25 systems.
- 3. Use a completely new control channel format specifically for rebanded systems.
- 4. Something else... No vendor has a fix.

Scanners that will NOT work

Uniden Scanners

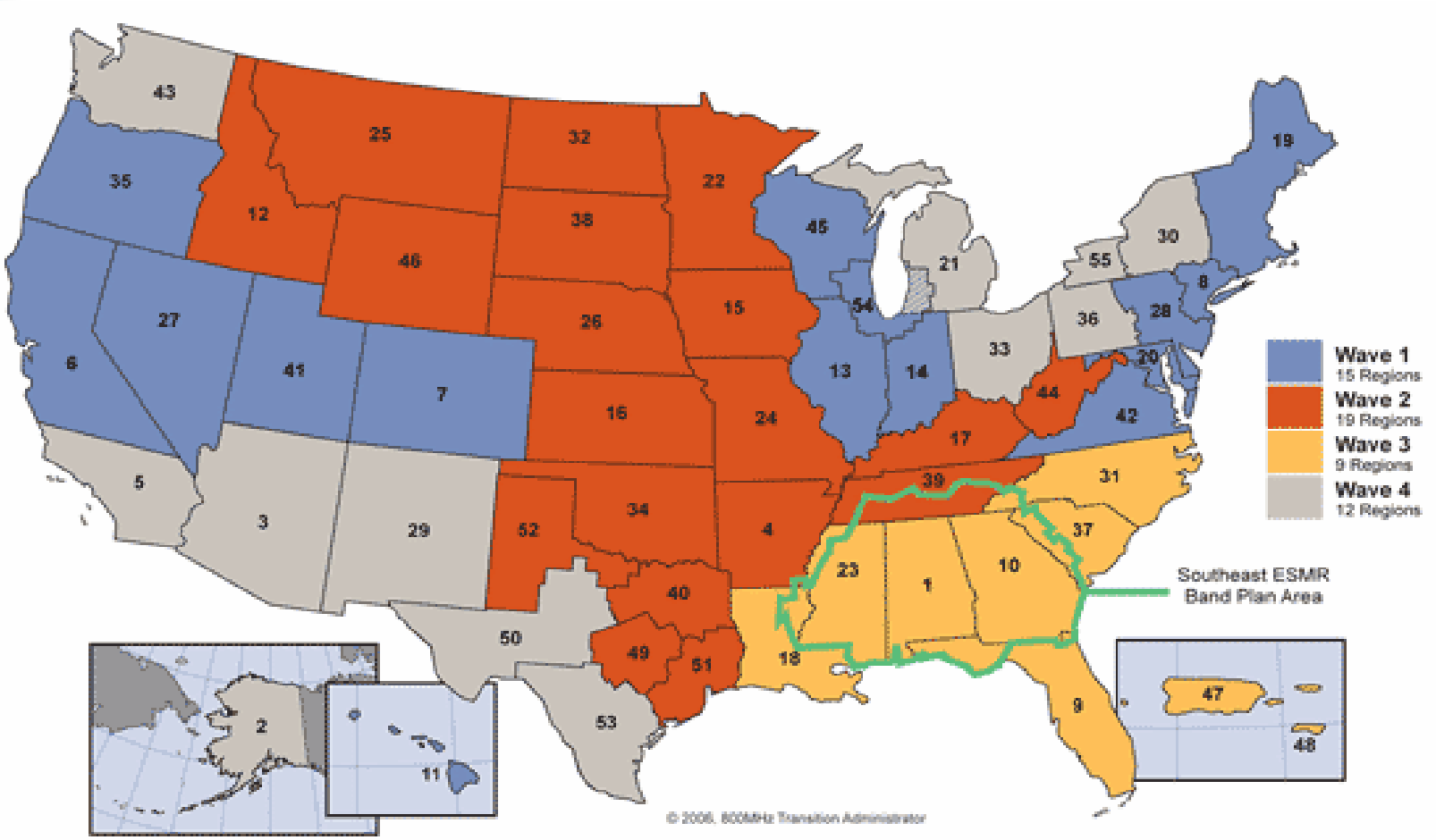
- BC235XLT
- BC245XLT
- BC250D
- BC780XLT
- BC785D
- BC895XLT

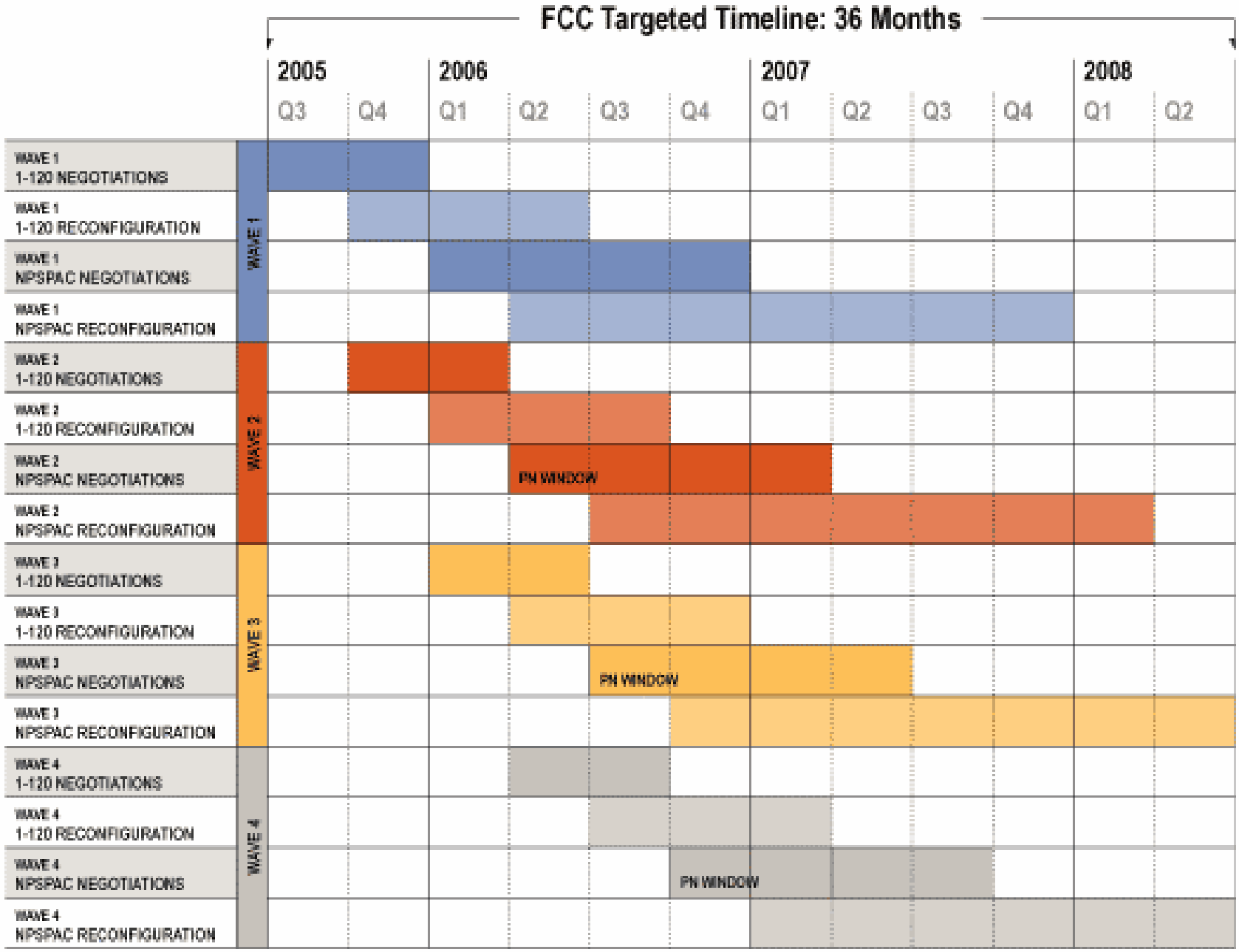
This is not a conclusive list

RadioShack Scanners

- PRO-2055
- PRO-2051
- PRO-2053
- PRO-2052
- PRO-2067
- PRO-2066
- PRO-2050
- PRO-97
- PRO-95
- PRO-93
- PRO-94
- PRO-92
- PRO-91
- PRO-90

Rebanding


Wave 1
15 Regions
Wave 2
19 Regions
Wave 3
9 Regions
Wave 4
12 Regions
Southeast ESMR
Band Plan Area
© 2006, 800MHz Transition Administrator



NOTE: PN window is the period during which Public Notice announces the start of NPSPAC region negotiations

Hardware

Hardware

- Radio Shack Trunking
- Pro-97
- This unit does NOT support rebanding.

- www.radioshack.com

Hardware

- Radio Shack Trunking
- Pro-96 (Digital)
- This unit does support rebanding.

- www.radioshack.com

Hardware

- Uniden Trunking
- BR330T / BCD396T (Digital)
- This unit does support Rebanding.

- www.uniden.com

Hardware

- AR8600MKIIB – non trunking (Conventional)
- Great for monitoring aircraft, public safety, broadcast, shortwave, etc.

- http://www.aorusa.com

Coming Soon (October 2007)

- GRE PSR-500 Trunking Scanner
  - Traditionally an OEM for Radio Shack
  - Starting to go direct
- Very similar to the Pro-96
- Fully dynamic memory
- Full review in Pop Com

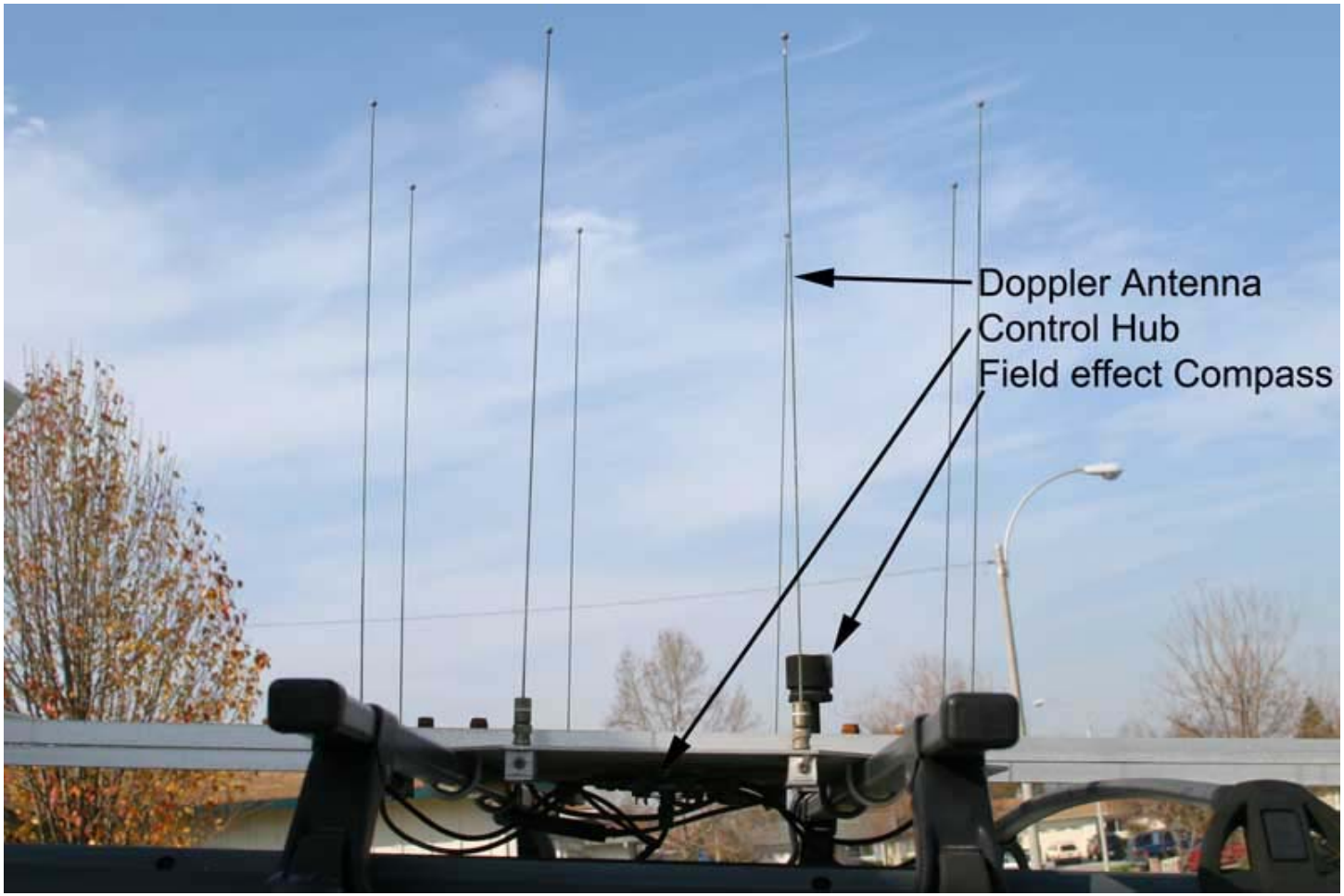
Finding Stuff

Close Call

- Uniden Specific Feature
  - Other vendors may call it something different
- Instantly tunes to nearby signals
  - Hotel Security, Police, FRS
  - Etc…

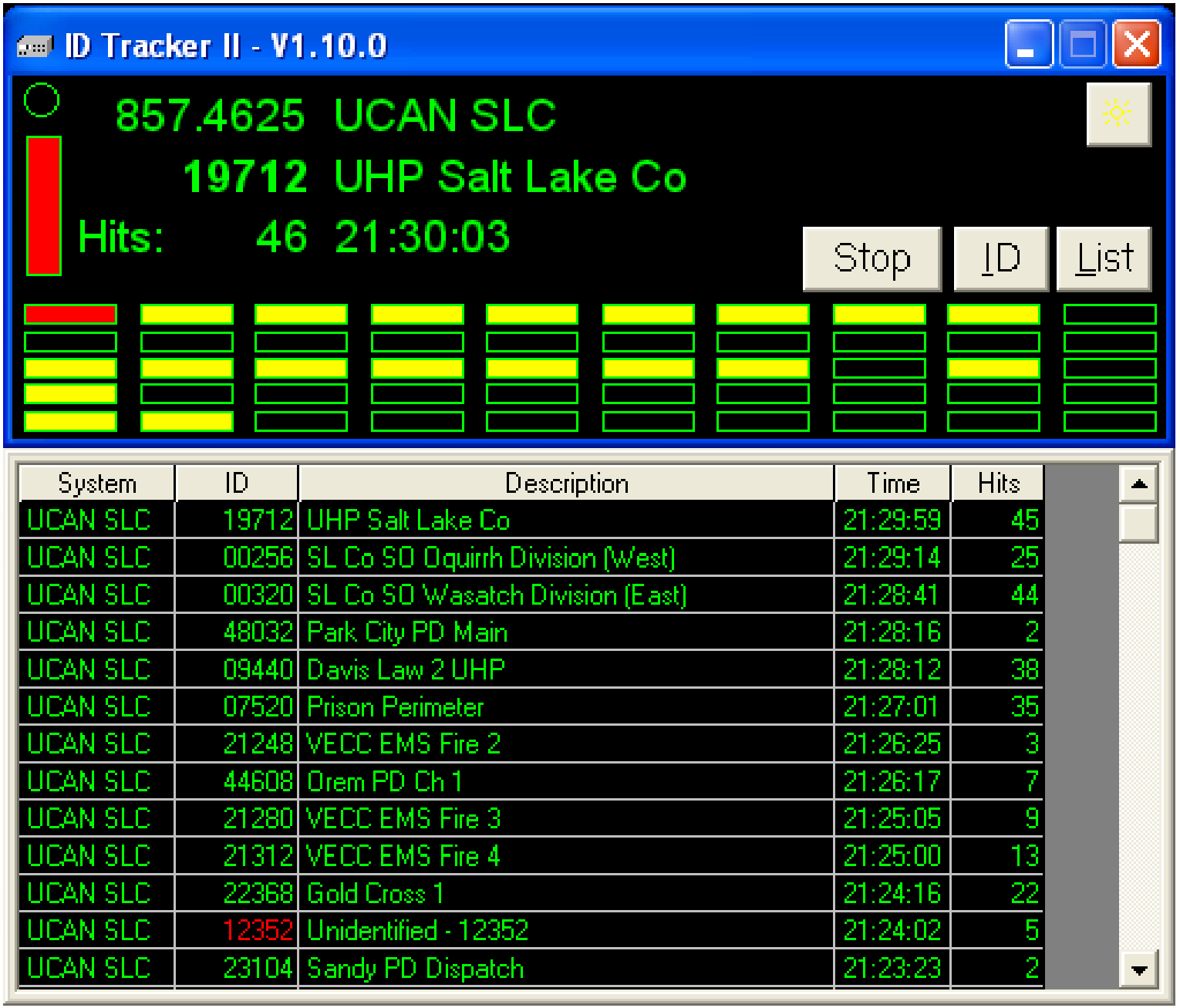
Demo

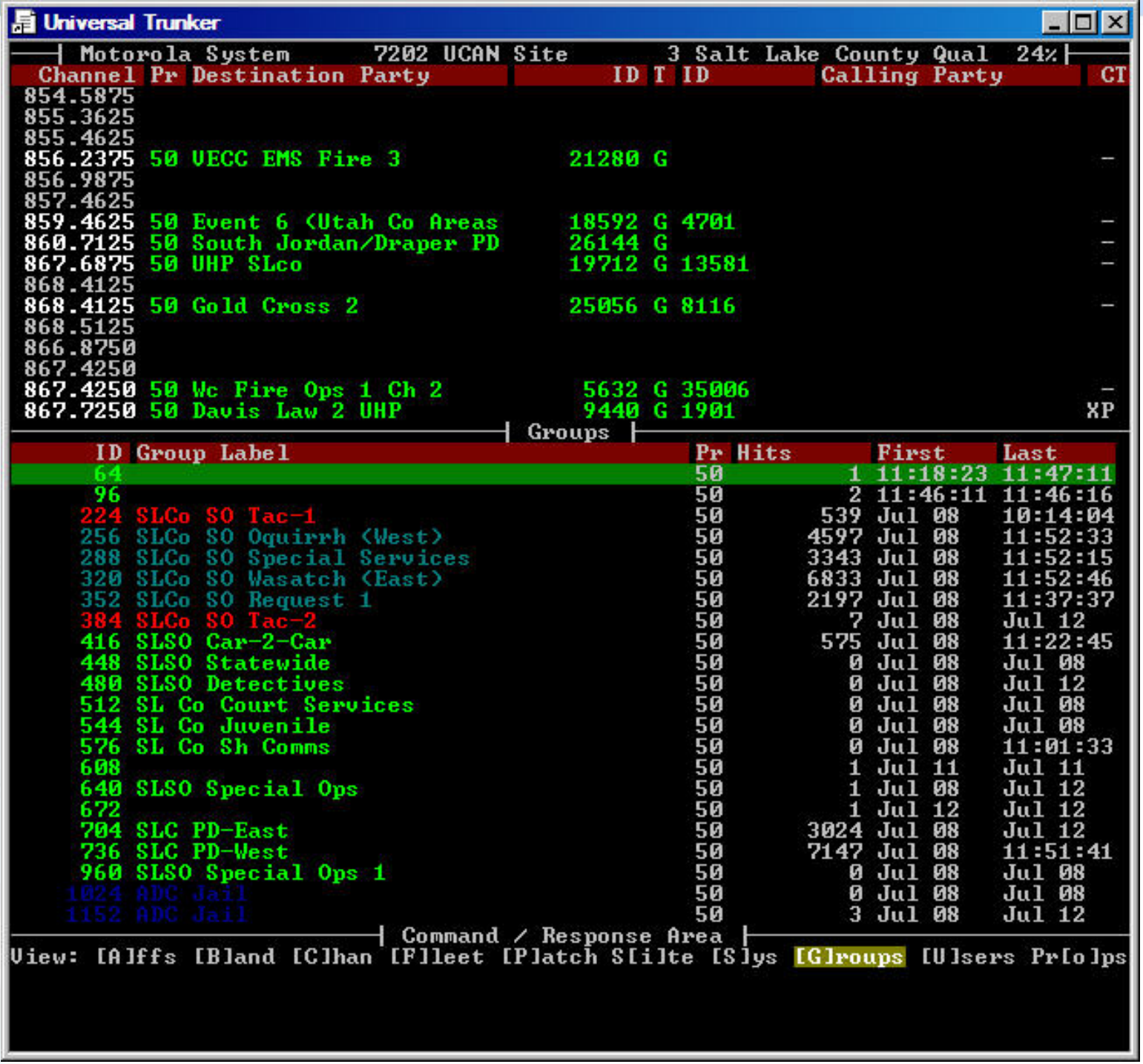
Direction Finding (DF) Transmitter Hunt



Software

- Frequency Database
  - www.radioreference.com
- Scanner Control / Recording
  - Trunk Star Elite/Pro
    - http://scanstar.com/
  - Scanner Recorder v1.9
    - http://www.davee.com/scanrec/
  - ID Tracker II*
    - http://bellsouthpwp.net/k/d/kd5eis/IDTracker/IDTracker.htm
- Trunk Monitoring
  - UniTrunker*
    - http://wiki.radioreference.com/index.php/UniTrunker
- Programing Software
  - Butel
    - http://www.butel.nl/


ID Tracker II - V1.10.0
857.4625 UCAN SLC
19712 UHP Salt Lake Co
Hits: 46 21:30:03
Stop
ID
List
System ID Description Time Hits
UCAN SLC 19712 UHP Salt Lake Co 21:29:59 45
UCAN SLC 00256 SL Co SO Oquirrh Division (West) 21:29:14 25
UCAN SLC 00320 SL Co SO Wasatch Division (East) 21:28:41 44
UCAN SLC 48032 Park City PD Main 21:28:16 2
UCAN SLC 09440 Davis Law 2 UHP 21:28:12 38
UCAN SLC 07520 Prison Perimeter 21:27:01 35
UCAN SLC 21248 VECC EMS Fire 2 21:26:25 3
UCAN SLC 44608 Orem PD Ch 1 21:26:17 7
UCAN SLC 21280 VECC EMS Fire 3 21:25:05 9
UCAN SLC 21312 VECC EMS Fire 4 21:25:00 13
UCAN SLC 22368 Gold Cross 1 21:24:16 22
UCAN SLC 12352 Unidentified - 12352 21:24:02 5
UCAN SLC 23104 Sandy PD Dispatch 21:23:23 2


Universal Trunker
Motorola System 7202 UCAN Site 3 Salt Lake County Qual 24%
Channel Pr Destination Party ID T ID Calling Party CT
854.5875
855.3625
855.4625
856.2375 50 UECC EMS Fire 3 21280 G -
856.9875
857.4625
859.4625 50 Event 6 (Utah Co Areas 18592 G 4701 -
860.7125 50 South Jordan/Draper PD 26144 G -
867.6875 50 UHP SLco 19712 G 13581 -
868.4125
868.4125 50 Gold Cross 2 25056 G 8116 -
868.5125
866.8750
867.4250
867.4250 50 Wc Fire Ops 1 Ch 2 5632 G 35006 -
867.7250 50 Davis Law 2 UHP 9440 G 1901 XP
Groups
ID Group Label Pr Hits First Last
64 50 1 11:18:23 11:47:11
96 50 2 11:46:11 11:46:16
224 SLCo SO Tac-1 50 539 Jul 08 10:14:04
256 SLCo SO Oquirrh (West) 50 4597 Jul 08 11:52:33
288 SLCo SO Special Services 50 3343 Jul 08 11:52:15
320 SLCo SO Wasatch (East) 50 6833 Jul 08 11:52:46
352 SLCo SO Request 1 50 2197 Jul 08 11:37:37
384 SLCo SO Tac-2 50 7 Jul 08 Jul 12
416 SLSO Car-2-Car 50 575 Jul 08 11:22:45
448 SLSO Statewide 50 0 Jul 08 Jul 08
480 SLSO Detectives 50 0 Jul 08 Jul 12
512 SL Co Court Services 50 0 Jul 08 Jul 08
544 SL Co Juvenile 50 0 Jul 08 Jul 08
576 SL Co Sh Comms 50 0 Jul 08 11:01:33
608 50 1 Jul 11 Jul 11
640 SLSO Special Ops 50 1 Jul 08 Jul 12
672 50 1 Jul 12 Jul 12
704 SLC PD-East 50 3024 Jul 08 Jul 12
736 SLC PD-West 50 7147 Jul 08 11:51:41
960 SLSO Special Ops 1 50 0 Jul 08 Jul 08
1024 ADC Jail 50 0 Jul 08 Jul 08
1152 ADC Jail 50 3 Jul 08 Jul 12
Command / Response Area
View: [A]ffs [B]and [C]han [F]leet [P]atch S[i]te [S]ys [G]roups [U]sers Pr[o]ps

Sample Sounds

- Sample Sounds
  - http://www.kb9ukd.com/digital/
- Paging Decoders
  - http://www.discriminator.nl/software/index-en.html

Stuff to listen to here in Vegas and check-out at home.

Frequencies & Systems

- Vice is great
  - 155.1150
- Goons
  - DC14: 464.5125 with a DCS of 131
  - DC15: 464.2125 with a DCS of 131 (Security)
  - DC15: 469.3250 with a DCS of 131 (Speaker)
- Hotel Security
  - LTR System

See the CD for a much larger list

Fun Stuff

- Drive Thru & Retail
  - Frequently on VHF/UHF frequencies
    - Business Band
      - Dot Frequencies (Blue, Red, Green, etc)
    - FRS & GMRS
- Media Remotes
  - Listen to the news as it is being recorded
- Wireless Mics
  - You can listen to the traffic stop
  - Track 3 (519.050 podium mic)

References

- http://www.radioreference.com
- http://www.signalharbor.com/ttt/index.html
- http://www.safecomprogram.gov
- http://unihedron.com/projects/spectrum/
- http://www.ojp.usdoj.gov/odp/ta_ictap.htm
- http://www.heritage.org/Research/HomelandDefense/bg2021.cfm
- http://www.arrowantenna.com
- http://www.byonics.com
- http://www.apcointl.org/frequency/project25/index.html

Contact Info

- EMAIL: defcon15@schnivic.net