“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)
SmartZone

Site 1

Site 2

Site 3
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

• 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 safety 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

<table>
<thead>
<tr>
<th>Uniden Scanners</th>
<th>RadioShack Scanners</th>
</tr>
</thead>
<tbody>
<tr>
<td>• BC235XLT</td>
<td>• PRO-2055</td>
</tr>
<tr>
<td>• BC245XLT</td>
<td>• PRO-2051</td>
</tr>
<tr>
<td>• BC250D</td>
<td>• PRO-2053</td>
</tr>
<tr>
<td>• BC780XLT</td>
<td>• PRO-2052</td>
</tr>
<tr>
<td>• BC785D</td>
<td>• PRO-2067</td>
</tr>
<tr>
<td>• BC895XLT</td>
<td>• PRO-2066</td>
</tr>
<tr>
<td></td>
<td>• PRO-2050</td>
</tr>
<tr>
<td></td>
<td>• PRO-97</td>
</tr>
<tr>
<td></td>
<td>• PRO-95</td>
</tr>
<tr>
<td></td>
<td>• PRO-93</td>
</tr>
<tr>
<td></td>
<td>• PRO-94</td>
</tr>
<tr>
<td></td>
<td>• PRO-92</td>
</tr>
<tr>
<td></td>
<td>• PRO-91</td>
</tr>
<tr>
<td></td>
<td>• PRO-90</td>
</tr>
</tbody>
</table>

This is not a conclusive list
Rebanding
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

• Programming 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

---

<table>
<thead>
<tr>
<th>System</th>
<th>ID</th>
<th>Description</th>
<th>Time</th>
<th>Hits</th>
</tr>
</thead>
<tbody>
<tr>
<td>UCAN SLC</td>
<td>19712</td>
<td>UHP Salt Lake Co</td>
<td>21:29:59</td>
<td>45</td>
</tr>
<tr>
<td>UCAN SLC</td>
<td>00256</td>
<td>SL Co SQ Oquirrh Division (West)</td>
<td>21:29:14</td>
<td>25</td>
</tr>
<tr>
<td>UCAN SLC</td>
<td>00320</td>
<td>SL Co SQ Wasatch Division (East)</td>
<td>21:28:41</td>
<td>44</td>
</tr>
<tr>
<td>UCAN SLC</td>
<td>48032</td>
<td>Park City PD Main</td>
<td>21:28:16</td>
<td>2</td>
</tr>
<tr>
<td>UCAN SLC</td>
<td>09440</td>
<td>Davis Law 2 UHP</td>
<td>21:28:12</td>
<td>38</td>
</tr>
<tr>
<td>UCAN SLC</td>
<td>07520</td>
<td>Prison Perimeter</td>
<td>21:27:01</td>
<td>35</td>
</tr>
<tr>
<td>UCAN SLC</td>
<td>21248</td>
<td>VECC EMS Fire 2</td>
<td>21:26:25</td>
<td>3</td>
</tr>
<tr>
<td>UCAN SLC</td>
<td>44608</td>
<td>Orem PD Ch 1</td>
<td>21:26:17</td>
<td>7</td>
</tr>
<tr>
<td>UCAN SLC</td>
<td>21280</td>
<td>VECC EMS Fire 3</td>
<td>21:25:05</td>
<td>9</td>
</tr>
<tr>
<td>UCAN SLC</td>
<td>21312</td>
<td>VECC EMS Fire 4</td>
<td>21:25:00</td>
<td>13</td>
</tr>
<tr>
<td>UCAN SLC</td>
<td>22368</td>
<td>Gold Cross 1</td>
<td>21:24:16</td>
<td>22</td>
</tr>
<tr>
<td>UCAN SLC</td>
<td>12352</td>
<td>Unidentified - 12352</td>
<td>21:24:02</td>
<td>5</td>
</tr>
<tr>
<td>UCAN SLC</td>
<td>23104</td>
<td>Sandy PD Dispatch</td>
<td>21:23:23</td>
<td>2</td>
</tr>
</tbody>
</table>
Sample Sounds

• Sample Sounds
  – http://www.kb9ukd.com/digital/

• Paging Decoders
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.safecomprogram.gov
- http://www.ojp.usdoj.gov/odp/ta_ictap.htm
- http://www.arrowantenna.com
- http://www.byonics.com
Contact Info

• EMAIL: defcon15@schnivic.net