V.24 Data as discovered

Released to further amateur radio - 10/31/2017
Work credited to: Anthony Casciato, KT9AC; John Yaldwyn, ZL4JY and others

- STUN adds the following leading 0831000000 bytes
- Next are the number of bytes to expect in a line in addition to the 11 Voice bytes and "0831" leading characters. (i.e. 18, 10, 13 or 12, including itself).
- STUN ID is next (i.e. 63 hex or 99 in decimal)
- 07 = Un-numbered Information UI - Information payload with encoded voice
- Next Byte is the "Site ID". Defaults to "1" in the Quantar and translates to "$03". Site ID goes between 1 and 63, matching up to Hex $03 to $fb.
- Record number is next – 62 thru 73, these repeat throughout the transmission
- Individual lines excluding the 11 voice bytes have various data (voice bytes are underlined below)
- Voice bytes (underlined below) are random depending on IMBE encoding, or a fixed pattern for "Silent" or "1011Hz P25 pattern"
    a. Silent: "040cfd7bfb7df27b3d9e44" (all records)
    b. 1011Hz Test Pattern: "09b0880cc621f680a82600" (even records)
    c. 1011Hz Test Pattern: "09b0880cc621f680a82601" (odd records)

- Fd 01 = Address 253, Frame type RR (Receive Ready, or keepalive)
    - Example: "0831000000 02 63 fd 01" (63 is StunID 99 in decimal)
- 07 03 = Address 07, Frame Type 03 (Un-numbered Information UI - Information payload with encoded voice

LDU1:

Record 62:

0831000000 18 63 07 03 62 02020c0b1b641a21a0 09b0880cc621f680a82600 00

In above example: $64 is DBM, $21 is RSSI, $a0 is BER
Decimal to RSSI measured: 0dbm=117, -10dbm=113, -20dbm=103, -30dbm=93, -40dbm=83, -50dbm=73, -60dbm=63, -70dbm=53, -80dbm=43, -90dbm=33, -100dbm=23
BER ($a0) is a number between 0 and 255, median is 128 for no errors. Value increases with more errors (no measurement standard available yet).

Record 63:

0831000000 10 63 07 03 63 09b0880cc621f680a82601000e

Record 64:

0831000000 13 63 07 03 64 00000000 09b0880cc621f680a82600 02

Byte 1 "00" denotes Group Call versus "03" Individual Call.
Green is Clear 0000, Secure 0040, Non-OFB 9000

Record 65:
0831000000 13 63 07 03 65 00000100 09b0880cc621f680a82601 02
Destination/TalkGroup $0001 = TG 1
If Record 64 “Individual Call” this field is *Called Radio Unit*

Record 66:
0831000000 13 63 07 03 66 00000100 09b0880cc621f680a82600 02
Source/RadioID - $000001 = ID 1
The “Calling Radio” if Record 64 Individual Call is set

Record 67:
0831000000 13 63 07 03 67 b5752d00 09b0880cc621f680a82601 02
TBD

Record 68:
0831000000 13 63 07 03 68 a012eb00 09b0880cc621f680a82600 02

Record 69:
0831000000 13 63 07 03 69 4fe09600 09b0880cc621f680a82601 02

Record 6a:
0831000000 12 63 07 03 6a 000006 09b0880cc621f680a82600 00
Low-speed data Byte1

LDU2:
Record 6b:
0831000000 18 63 07 03 6b 02020c0b1b641a21a0 09b0880cc621f680a82601 00
Repeat of Record 62, same data now in LDU2

Record 6c:
0831000000 10 63 07 03 6c 09b0880cc621f680a8260000 0e

Record 6d:
0831000000 13 63 07 03 6d 00000000 09b0880cc621f680a82601 02

Record 6e:
0831000000 13 63 07 03 6e 00000000 09b0880cc621f680a82600 02

Record 6f:
0831000000 13 63 07 03 6f 00000000 09b0880cc621f680a82601 02

Record 70:
0831000000 13 63 07 03 70 80000000 09b0880cc621f680a82600 02
AlgID 80/Clear,84/AES,9F/DES-XL,81/DES-OFB
0000 = Common Key Reference Slot (CKR)

Record 71:
0831000000 13 63 07 03 71 acb8a400 09b0880cc621f680a82601 02

Record 72:
0831000000 13 63 07 03 72 9bdc7500 09b0880cc621f680a82600 02

Record 73:
0831000000 12 63 07 03 73 00000a 09b0880cc621f680a82601 00
Low-speed data Byte2

Data checks:

- Make sure bytes are Hex and not garbage (hex unpacked data from Cisco STUN)
- StunID valid range between 1 and 255 (text fields)
- Data length of each line (based on 6th byte formula) – key to using TCP for transport to ensure internet delays and "sliding window TCP" aren't sending hundreds of pent-up bytes where say 50 are expected. OK to skip delayed data since P25 allows for "late entry" feature and no loss of conversation. This is how you deal with public internet links.
- RSSI values below -115dbm (aka Brick Wall) are muted properly to avoid "robot" or "pixelization". Over-write voice frames with silent frames
- Quantar will send "out-of-band" signaling when analog detected. Need to block that out from keying nodes without audio or open squelch.
- Looking for P25 "turn off code" when data transmission ends:
    - StunID + SiteID + "03000202250b";
    - If you don't catch it, might have delay up to 5 seconds before keepalives re-appear.
- Difference between RT/RT mode and Non-RT mode
    - One byte difference – "04" versus "02" in code
    - Third byte past the SiteID
    - AstroTAC Comparator uses "04" and does not send 62 and 6b lines – issues for systems that expect "back-to-back" comms (RT/RT mode). Work in progress to resolve
- Validate TGID between 1 and 65535 (text field)
- Validate RadioID between 1 and 9999999 (text field)
- Validate RSSI value between 0 and 255 (text field)
- Validate BER value between 0 and 255 (text field)
- Validate DBM value between 0 and 255 (text field)
- Validate suspected Secure bytes and Algo ($aa=ADP, $84=AES-256, $9f=DES-XL, $81=DES-OFB)

Innovations:

- Dump captured complete "superframe" of Lines 62-73 into SQL Database for later development/reporting use
- Create summary SQL line for transmission stats for Website
- Voting is possible based on RSSI "high-watermark" comparison. Better method to align up multiple receivers and their records as they come in (see patents).
- System built using original STUN and TCP transport