Enabling the KeyPad on Vertex VX-427A Radios

Brian Rasnow (brian@rasnowpeak.com)

Summary. The Vertex Standard VX-427 radio (Fig. 1) is programmed through Vertex's CE89 software. The later generation VX-427A requires CE94 software. CE94 in its default configuration disables the radio's keypad. This paper describes a hack to enable it.

Figure 1. Vertex VX427A.

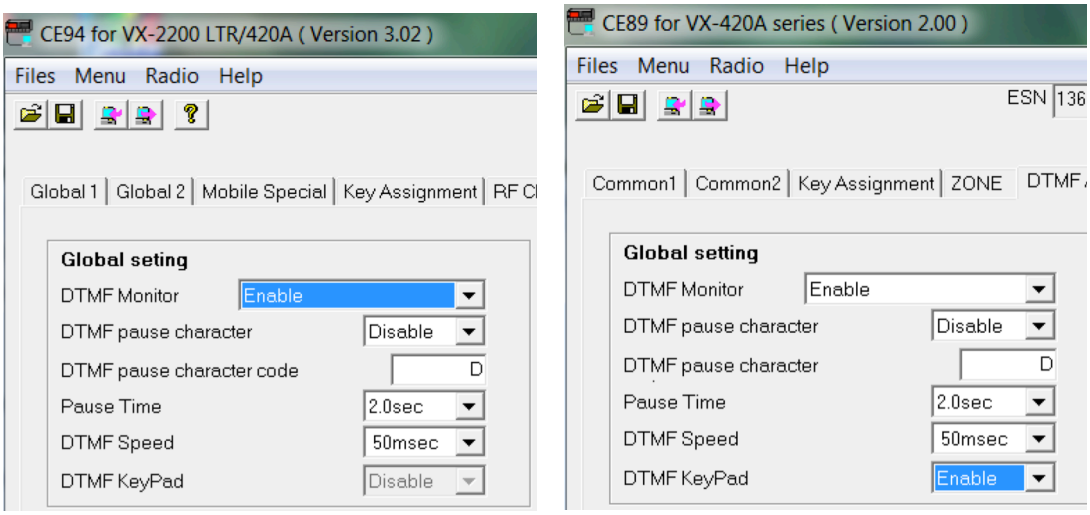

Figure 2. CE94 software for the Vertex VX427A has the DTMF KeyPad disabled and unselectable (left). CE89 (which doesn't recognize the "A" radios in spite of the title) has a functional KeyPad button.

Methods. Using CE89, 2 parameter files were saved differing only in the settings of the KeyPad switch. These are 23kB binary files with no obvious format, and no documentation that I could find. Comparing the files using a Unix terminal:

```
$ ls *.H89
dtmfDis.H89  dtmfEn.H89
$ cmp -l *.H89
  386 102 142
```

Byte 386 is the only difference, so it must correspond to the KeyPad being disabled (102) or enabled (142). The Unix utility od (octal dump) shows the files in that neighborhood:

```
$ od -x  dtmfDis.H89 | more
…
0000560      7b83    596e    bc4e    84b4    040c    0408    ffff    ffff
0000600      42a0    0000    0000    0000    0000    0000    0000    0000
0000620      0000    0000    0000    0000    0000    0000    0000    0000

$ od -x  dtmfEn.H89 | more
…
0000560      7b83    596e    bc4e    84b4    040c    0408    ffff    ffff
0000600      62a0    0000    0000    0000    0000    0000    0000    0000
0000620      0000    0000    0000    0000    0000    0000    0000    0000
```

Byte 600_8 equals 42_{16} in the disabled file and 62_{16} in the enabled file. Looking at CE94 files at that location:

```
$ od -x u4Tst.H94 | grep 0000600
0000600      42a0    0000    0000    0000    0000    0000    0000    0000
```

This suggests changing the 42_{16} at location 600_8 to 64_{16} might enable DTMF. Although there are various Unix tools to edit binary files (along with low level fopen/fread/fwrite), a freeware hex editor for OSX called iHex is an easy download from Apple's AppStore. Flipping that bit and saving changed the state of CE94 (Figure 3).

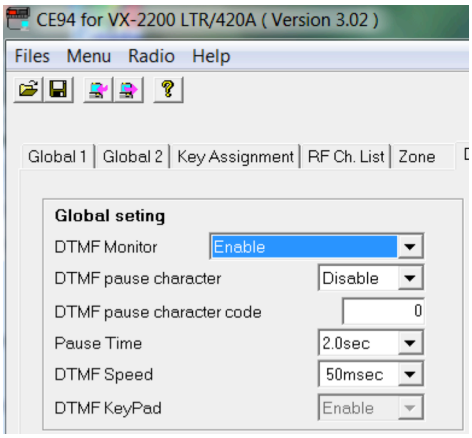

Figure 3. Modified file enables the KeyPad.

Conclusions. One doesn't need a lot (any) documentation to modify software behavior. The key to this hack was the ability to modify CE89 and take advantage of its similarity to the broken CE94. The tools to find and change this needle-in-a-haystack are free and simple to use. The trick is to know where and how to use them. One can make an analogy to a surgeon using a scalpel – a simple (sharp) knife, but wielded with extreme care. Changing one byte of the 23kB file did the trick, but it took some detective work to find that one byte.