DJ Link Packet Analysis

James Elliott

April 25, 2016

1 Mixer Startup

When the mixer starts up, after it obtains an IP address (or gives up on doing that and self-assigns an address), it sends out what look like a series of packets simply announcing its existence to UDP port 50000 on the broadcast address of the local network.

These have a data length of 37 bytes, appear roughly every 300 milliseconds, and have the content shown in Figure 1.

The tenth byte (inside what is labeled the header) is bolded because its value changes in the different types of packets which follow.

After about three of these packets are sent, another series of three begins. It is not clear what purpose these packets serve, because they are not yet asserting ownership of any device number; perhaps they are used when CDJs are powering up as part of the mechanism the mixer can use to tell them which device number to use based on which network port they are connected to?

In any case, these three packets have a data length of 44 bytes, are again sent to UDP port 50000 on the local network broadcast address, at roughly 300 millisecond intervals, and have the content shown in Figure 2.

The value N at byte 36 is 1, 2, or 3, depending on whether this is the first, second, or third time the packet is sent.

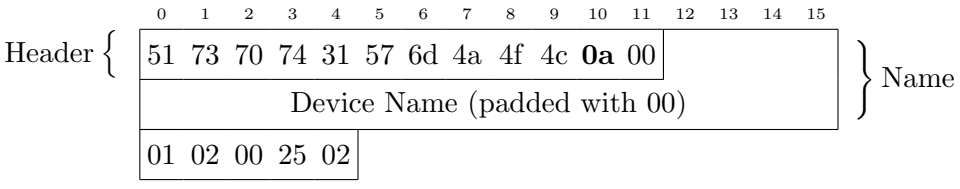

Figure 1: Initial announcement packets from Mixer

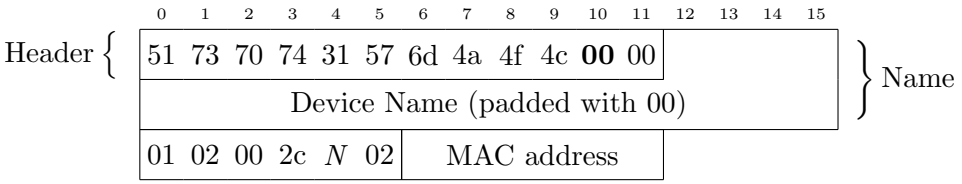

Figure 2: First-stage Mixer device number assignment packets

After these comes another series of three numbered packets. These appear to be claiming the device number for a particular device, as well as announcing the IP address at which it can be found. They have a data length of 50 bytes, and are again sent to UDP port 50000 on the local network broadcast address, at roughly 300 millisecond intervals, with the content shown in Figure 3.

I identify these as claiming/identifying the device number because the value D at byte 46 is the same as the device number that the mixer uses to identify itself (0x21) and the same is true for the corresponding packets seen from the CDJs (they use device numbers 2 and 3, as they are connected to those ports/channels on the mixer).

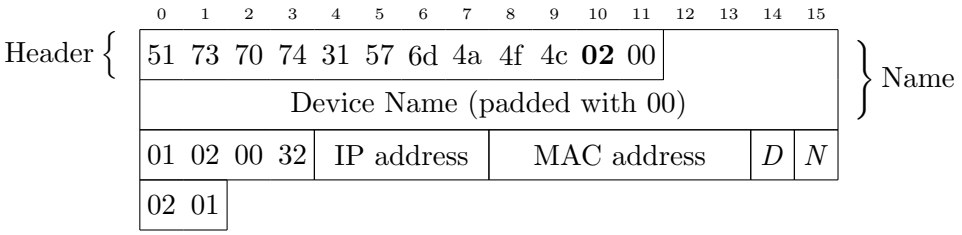

Figure 3: Second-stage Mixer device number assignment packets

As with the previous series of three packets, the value N at byte 47 takes on the values 1, 2, and 3 in the three packets.

These are followed by another three packets, perhaps the last stage of claiming the device number, again at 300 millisecond intervals, to the same port 50000. These shorter packets have 38 bytes of data and the content shown in Figure 4.

As before the value D at byte 36 is the same as the device number that the mixer uses to identify itself (0x21) and N at byte 37 takes on the values 1, 2, and 3 in the three packets.

Once those are sent, the mixer seems to settle down and send what looks

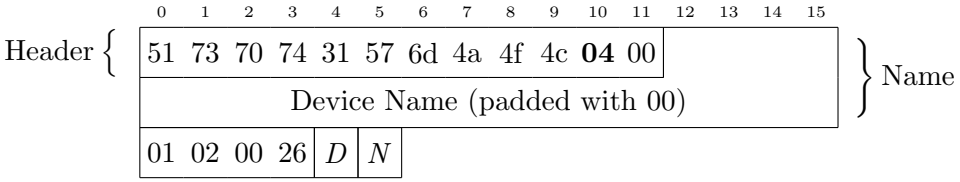

Figure 4: Final-stage Mixer device number assignment packets

like a keep-alive packet to retain presence on the network and ownership of its device number, at a less frequent interval. These packets are 54 bytes long, again sent to port 50000 on the local network broadcast address, roughly every second and a half. They have the content shown in Figure 5.

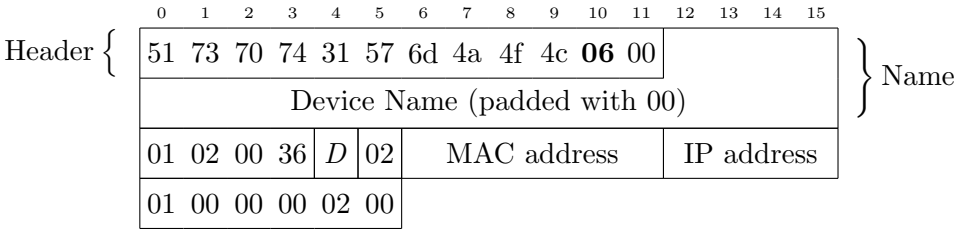

Figure 5: Mixer keep-alive packets

2 CDJ Startup

When a CDJ starts up the procedure and packets are nearly identical, with groups of three packets sent at 300 millisecond intervals to port 50000 of the local network broadcast address. The only difference between Figure 1 and Figure 6 is the final byte, which is 01 for the CDJ, and was 02 for the mixer.

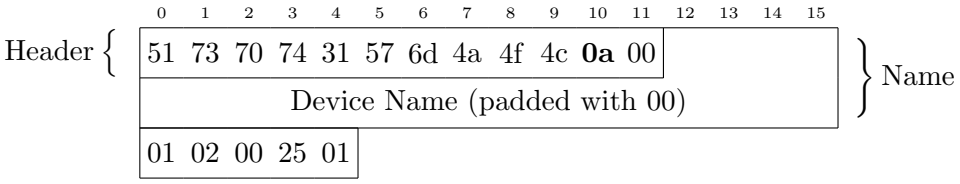

Figure 6: Initial announcement packets from CDJ

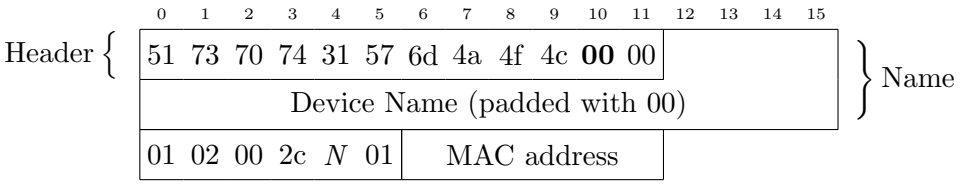

Figure 7: First-stage CDJ device number assignment packets

Similarly, the next series of three packets from the CDJ are nearly identical to those from the mixer. The only differences between Figure 2 and Figure 7 is byte 37 (immediately after the packet counter N), which again is 01 for the CDJ, and was 02 for the mixer.

However it appears that the CDJ skips the second stage of claiming a device number, probably because it is configured to be automatically assigned a device number based on the port of the mixer to which it is connected, and we cannot see a packet that the mixer sent it assigning it that device number. Instead, it jumps right to the end of the third and final stage, sending a single 38-byte packet with header byte 10 set to 04 (which identified the three packets of the third stage when the mixer was starting up), with content identical to Figure 4.

Even though the value of N is 01, this is the only packet in this series that the CDJ sends. It would probably behave differently if configured to assign its own device number (behaving like we saw the mixer behave in claiming its device number).

It then moves to the final keep-alive stage, sending out 54-byte packets with the content shown in Figure 8.

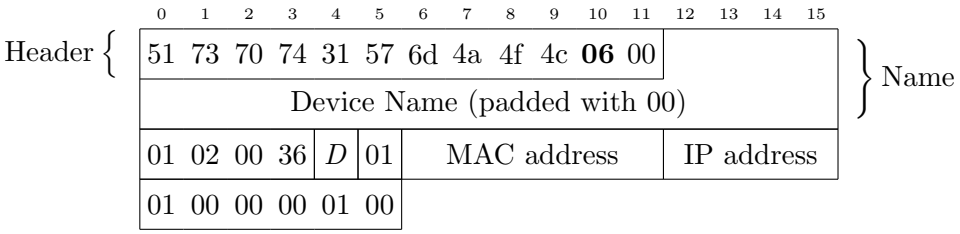

Figure 8: CDJ keep-alive packets

As seems to always be the case when comparing mixer and CDJ packets, the difference between this and Figure 5 is that byte 37 (following the device number D) has the value 01 rather than 02, and the same is true of the

second-to-last byte in each of the packets. (Byte 52 is 01 in Figure 8 and 02 in Figure 5.