Skutt KilnLink™ installation considerations for school networks

Our network device (a.k.a. KilnLink Box) will look just like a computer on a network, sending traffic to our server at www.myskutt.com. We use port 80 (for HTTP traffic over TCP/IP). The only thing non-standard about our traffic is that the HTTP header will not have a typical "browser type" in the packets we send.

If the school has a wired guest network we recommend placing our KilnLink Box on that network rather than a production or internal network. This is a best practice for all Internet of Things (IoT) devices.

There are a number of places where successful communication to our server could get hung up. Here are some of the most likely issues:

1. The school may use "whitelisting" to allow access to various websites. If that is true the school will need to add www.myskutt.com to the list. If that solves the problem and allows the KilnLink Box to come online then keep in mind the user's computer will also need to be allowed to interact with www.myskutt.com to see their kiln activity.

2. Some networks are setup to block any unapproved devices, so there is likely a process to register the MAC address of the device with the IT Department in order for it to be allowed onto the network. The MAC address is printed on a sticker on the KilnLink Box, it is 12 characters long.

3. The school might use fixed IP addresses instead of DHCP for dynamic IP assignment. In that case, we will have to configure the device with a static IP address. This is not standard and the KilnLink Box would have to be returned to Skutt with the requested IPv4 static address clearly stated in the RMA. Such an address will take the form of a dotted quad (e.g. 10.0.0.150), and it will be for the internal network not the public facing IP address of the school.

4. The network may require the device to join a domain with an authenticated user account before it's allowed to send any traffic. This could be a show-stopper scenario unless the school can allow an exception on the network.

5. The school might have a network rule somewhere that looks for things that appear to be generating a denial of service attack (DoS). The KilnLink Box is hitting the same address every few seconds, which could trigger a DoS protection routine. If we see the device connect to our server for a limited amount of time after boot up then disconnect for no apparent reason this might be the cause.

6. The school may require traffic to go through a proxy...since we can't configure the device to do so, the school will have to figure out how to allow traffic from KilnLink Box to circumvent the proxy server.

7. The same is true for a captive portal. We have no user interface with which to configure the KilnLink Box for such a network.