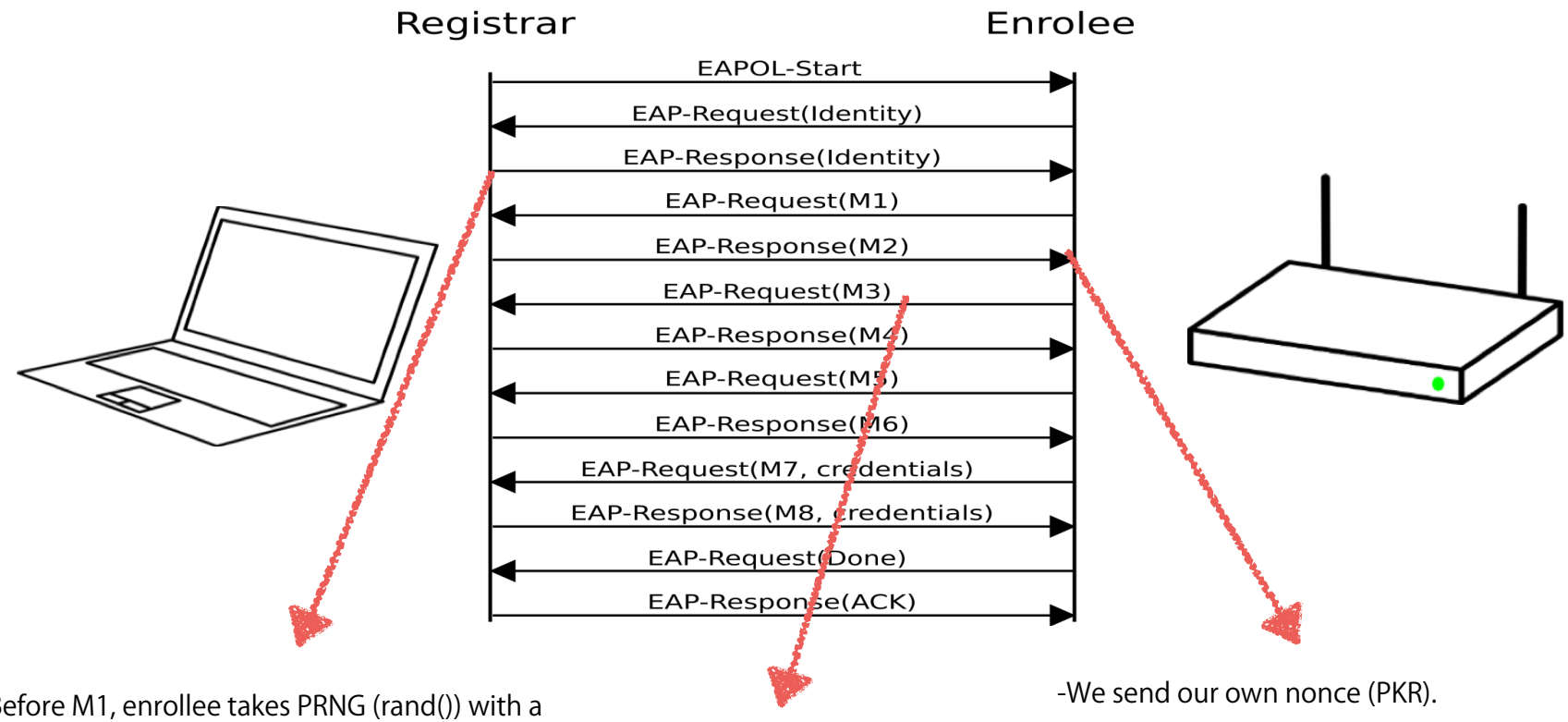

-Before M1, enrollee takes PRNG (rand()) with a seed x (random number.. maybe router's uptime?) and runs it through: rand(x)

-This generates a string of data: 1a2b3c4d5e6f

-Router takes first part "1a2b" and says "this is my nonce.. aka the PKE

-We throughout all this, you know we have PKE, PKR, E-Hash1, E-Hash2. Where are E-S1 and E-S2????

-Well, we know the PRNG that broadcom uses: rand(x). If we can guess the value of x, we can see the next following data. We know we have a match when the PKE matches with our seed (1a2b). Then, the next 256bits are E-S1 and E-S2!!!!

-We send our own nonce (PKR).

-So we find the seed and get a matching PKE: 1a2b. The next data are the E-S1 and E-S2.. E-S1=3c4d and E-S2=5e6f

-Stupid broadcom didn't think this through.