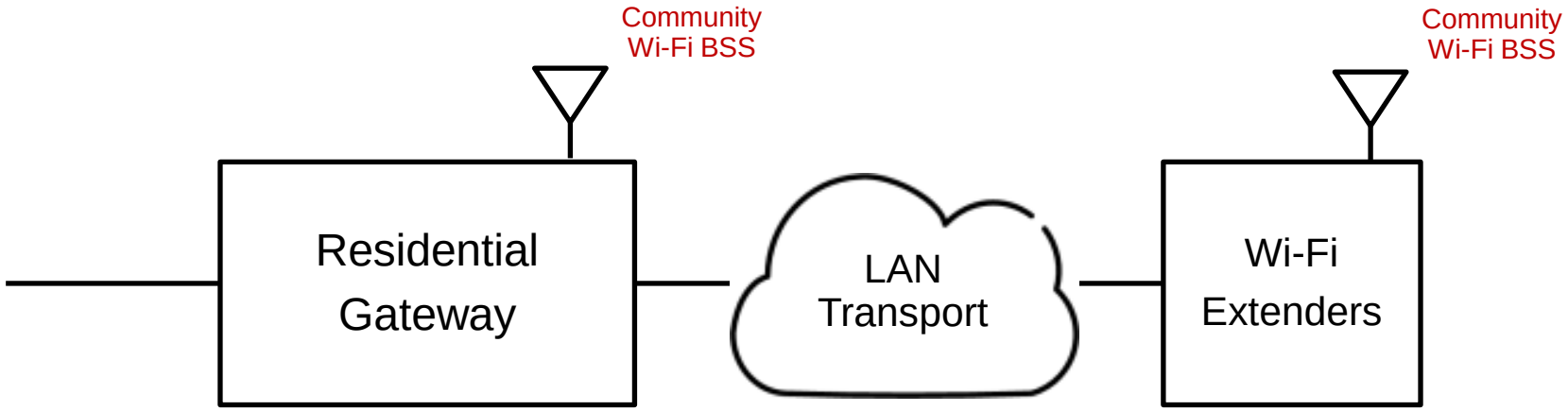
L2 Security Use Case – Wi-Fi Community Range Extenders

Contributed by Philippe Klein, PhD

philippe.klein@broadcom.com

IEEE 802 Interim Meeting, Budapest May 2016

Use case: Community Wi-Fi Architecture With Wi-Fi Extenders

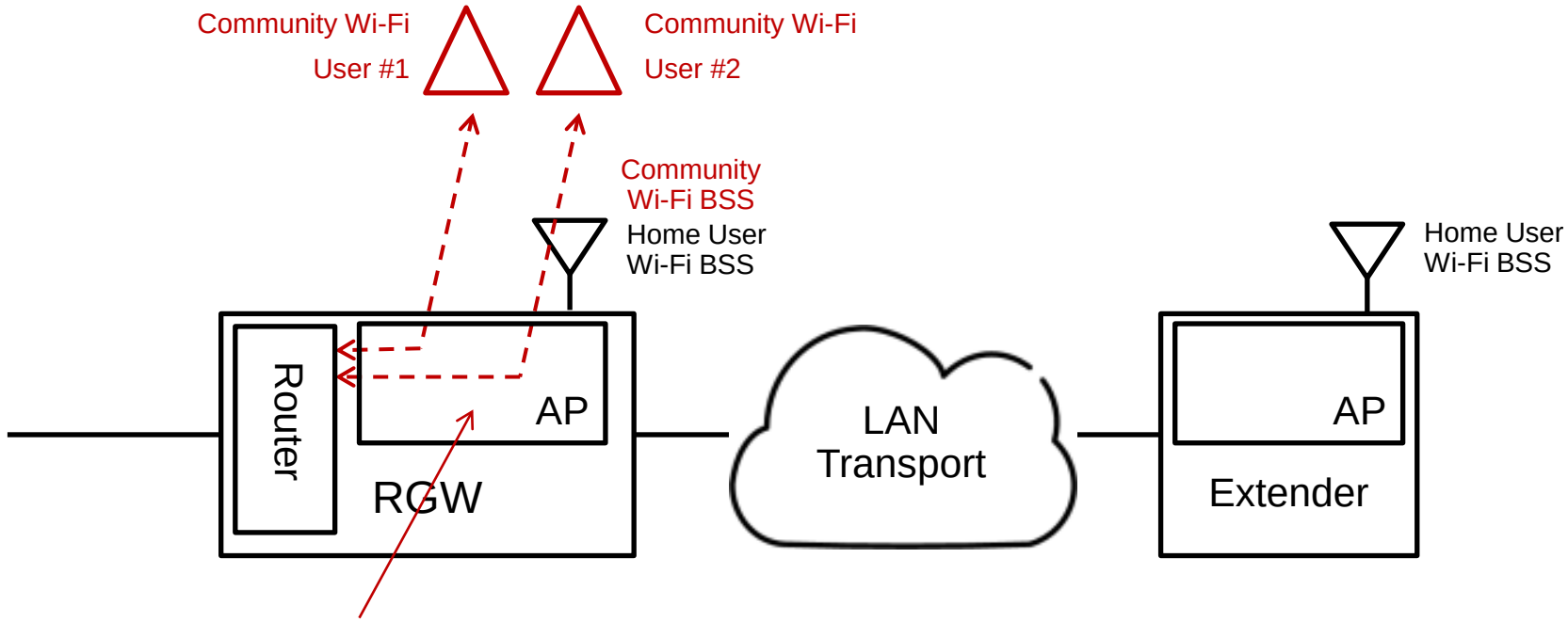


One or more Wi-Fi Extenders are connected to the main Wi-Fi Gateway via a local area network (LAN).

Wi-Fi Extenders could be distributed using many different LAN transport technologies, including:

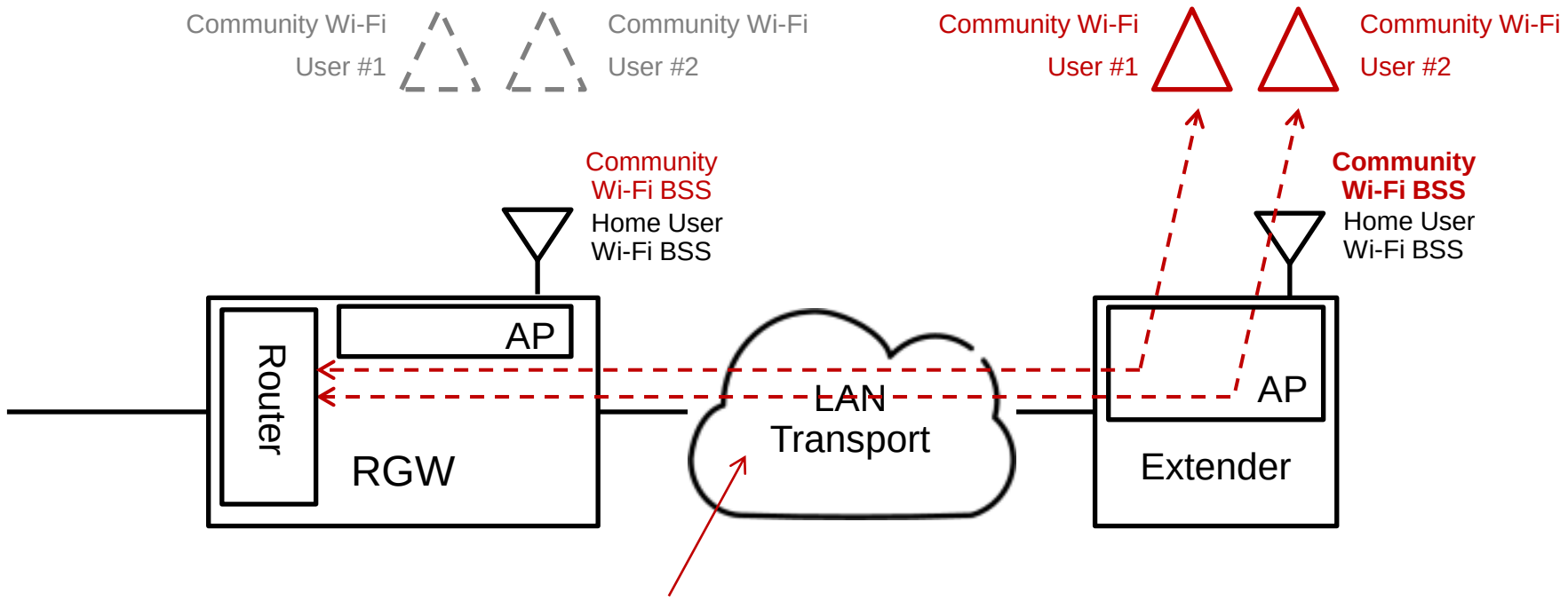
- *Ethernet*
- *Coax Power*
- *Line Communications*
- *Wireless*

Community Wi-Fi Traffic Privacy w/o Community Wi-Fi Range Extenders



The traffic isolation between the Community Wi-Fi users is provided by **disabling the AP's local routing** for the Community Wi-Fi BSS

Community Wi-Fi Traffic Privacy with Community Wi-Fi Range Extenders



The traffic isolation between the Community Wi-Fi users **SHALL be maintained** over the backbone links

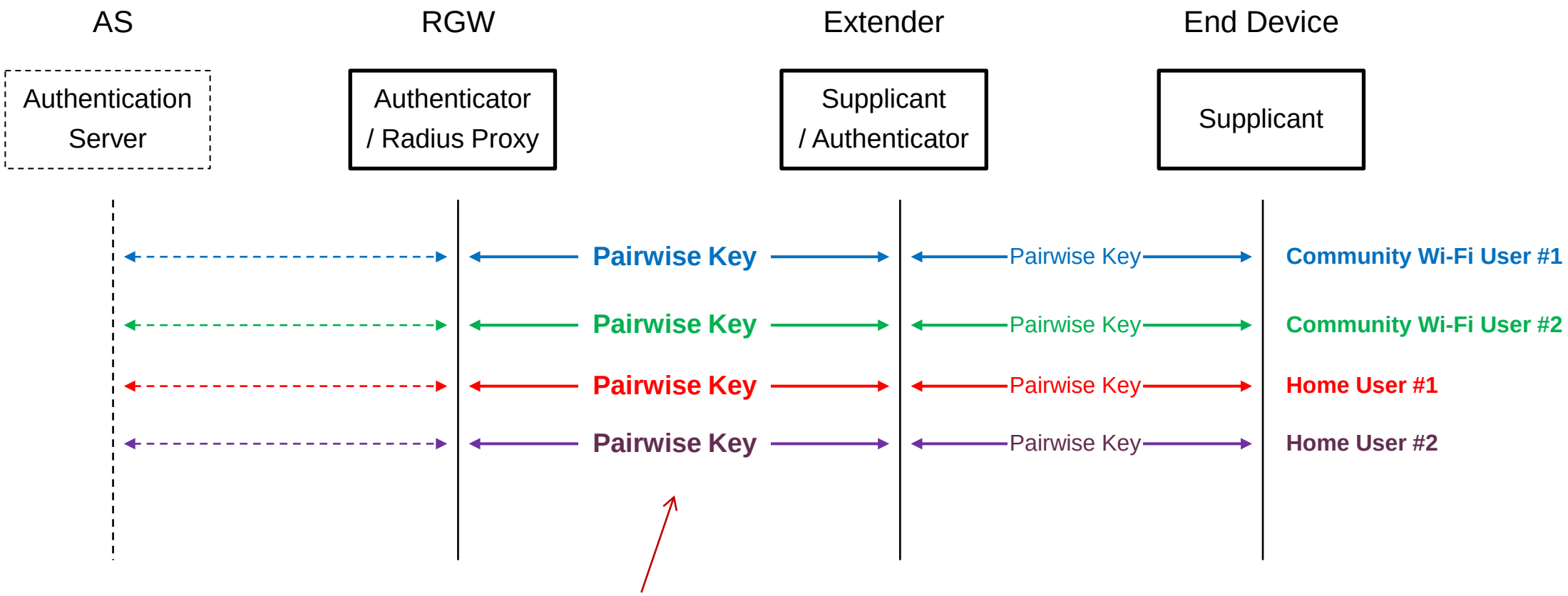
Traffic isolation between Home Users

- Traffic isolation is not limited to Home users vs Community Wi-Fi users
- Traffic isolation will also apply between users of various Home SSIDs such:
  - Home user
  - Children
  - Guest
  - or Specialized services such
    - Home automation
    - Home security
    - E-Health
    - …

*“Some US operators have as many as 1 million truck rolls a year, where most of the problems found are Wi-Fi related with one of the most frequent calls operators get is to **ask for the Wi-Fi password** in the home: responsible for **20% of calls** i.e. 200K truck rolls “*

(source: Faultline, Apr 2016)

L2 Traffic Isolation – Pairwise Key



These pairwise keys need to be created dynamically when End device users join the network

BROADCOM

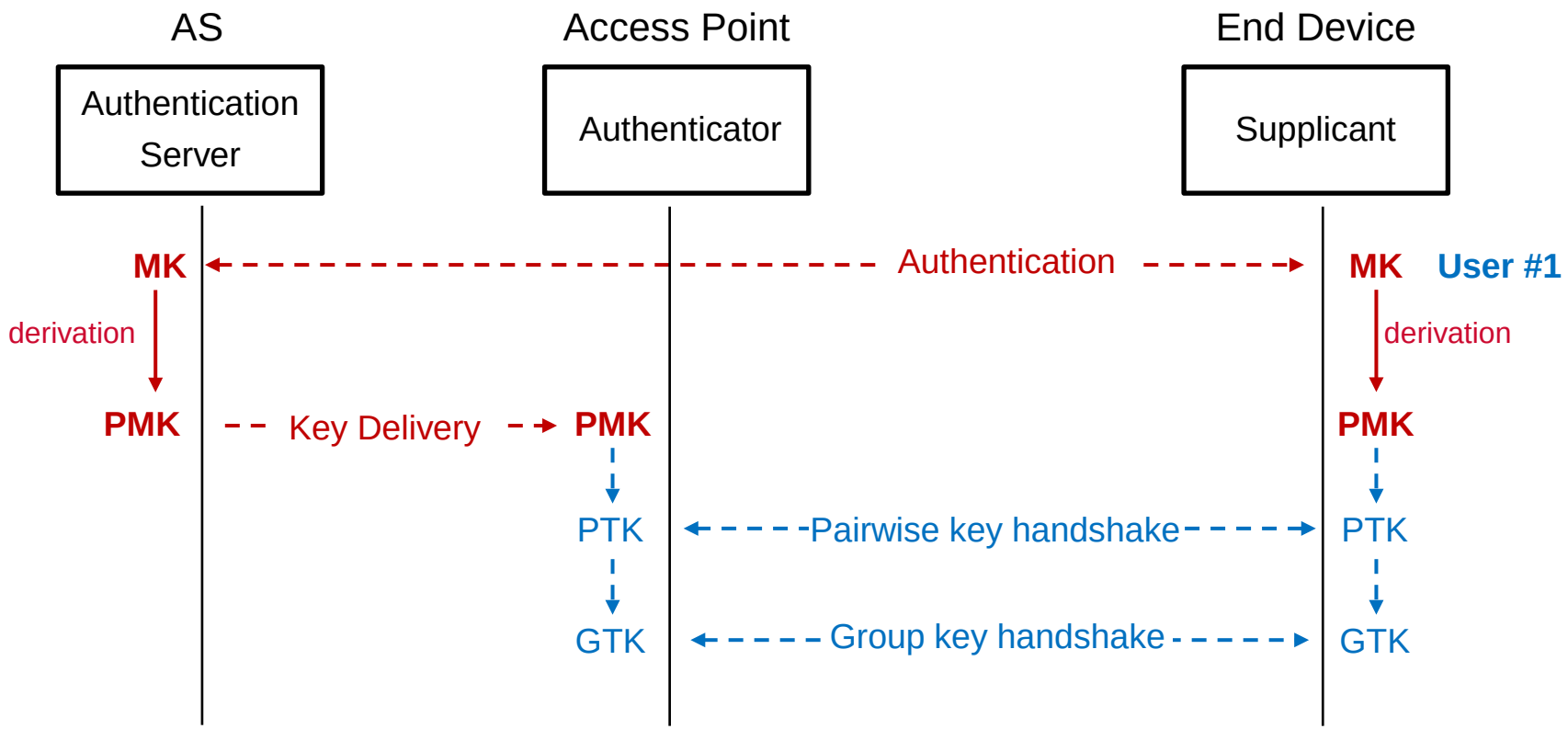
Pairwise Key Generation for the backbone link

- The delay of creating a new CA to generate a pairwise key **during the End Device wireless authentication** could be **too expensive**…

  …especially for Wireless Fast Roaming when the End Device re-associates to a different extender.

- How could this be resolved ?
- Since 802.11i is already implemented in wireless devices, could it be “extended” to resolve the issue here ?
- Let me explain…

IEEE 802.11i Protocol



MK Master key

PMK Pairwise Master Key

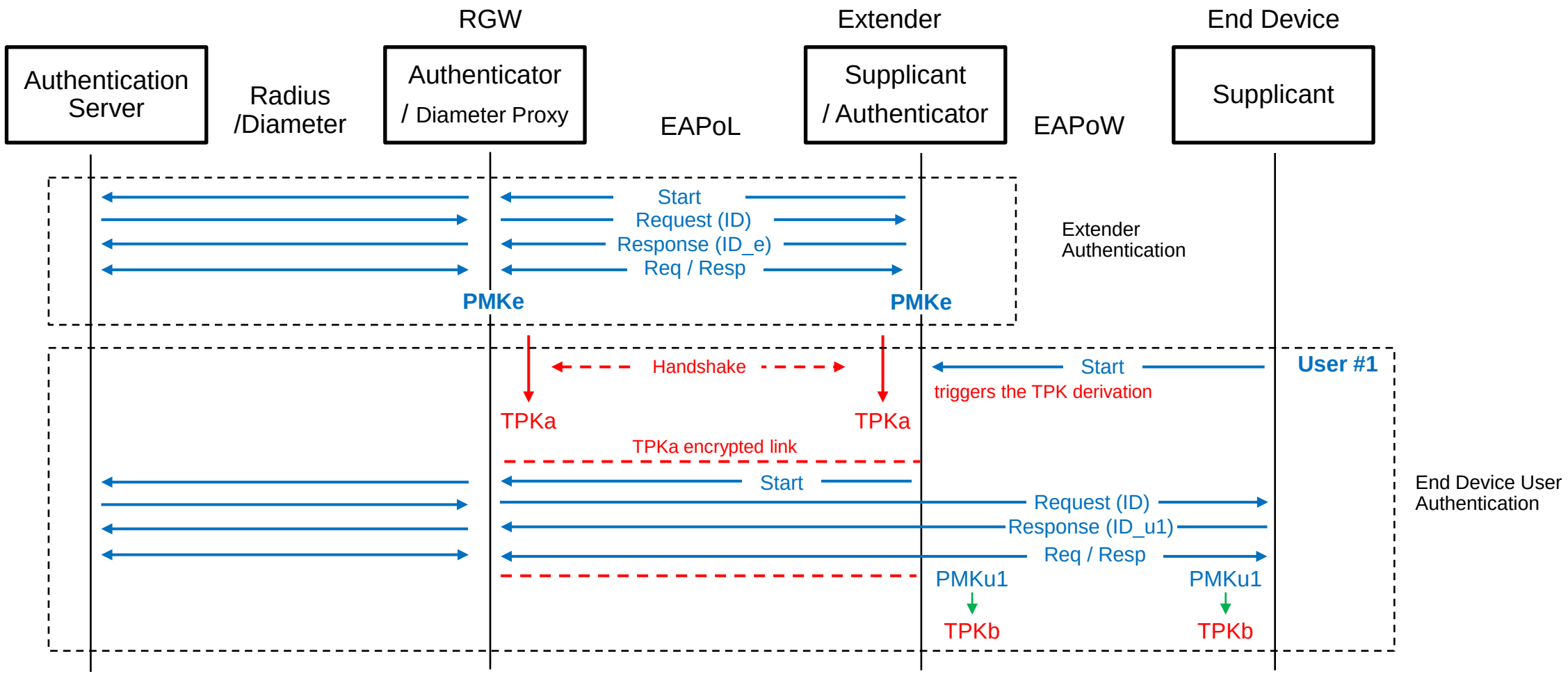
PTK Pairwise Transient Key

GTK Group Transient Key

Proposal: “Cascaded” Authentication

1. Extenders as supplicants are authenticated and share a PMK with their Authenticators
2. Authenticated extenders then act as Authenticators to the end devices
3. When triggered by a supplicant authentication request, they run an handshake with their authenticators to derive a PTK
4. Then they act as proxy to the EAP authentication of the supplicant

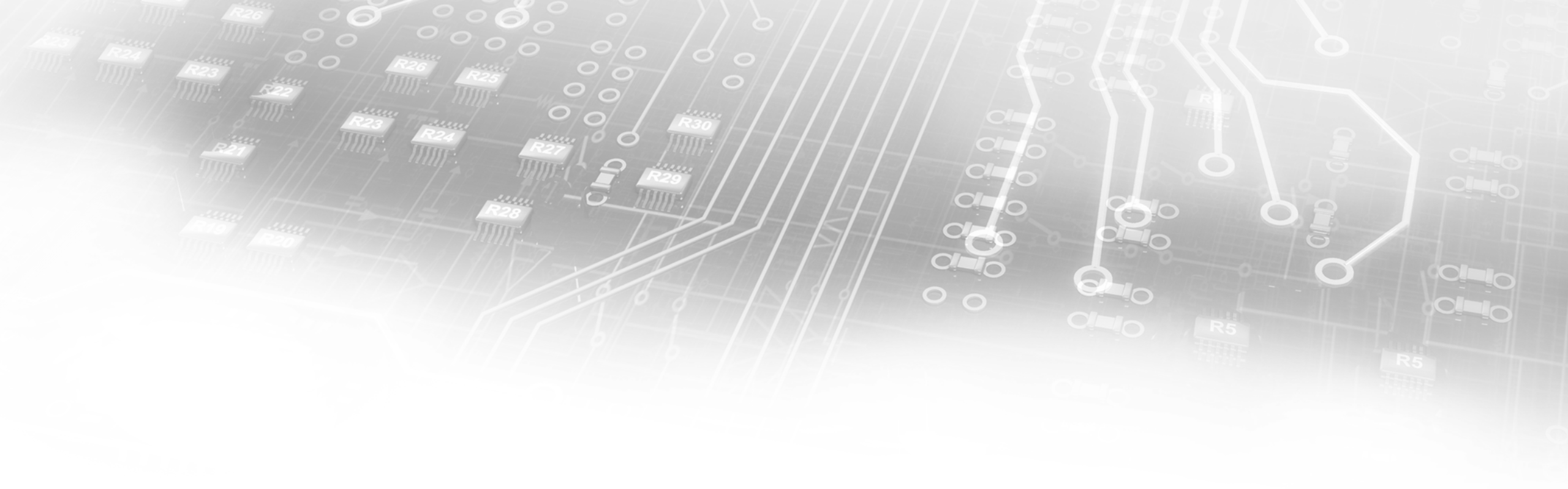
EAP “Cascaded” Authentication

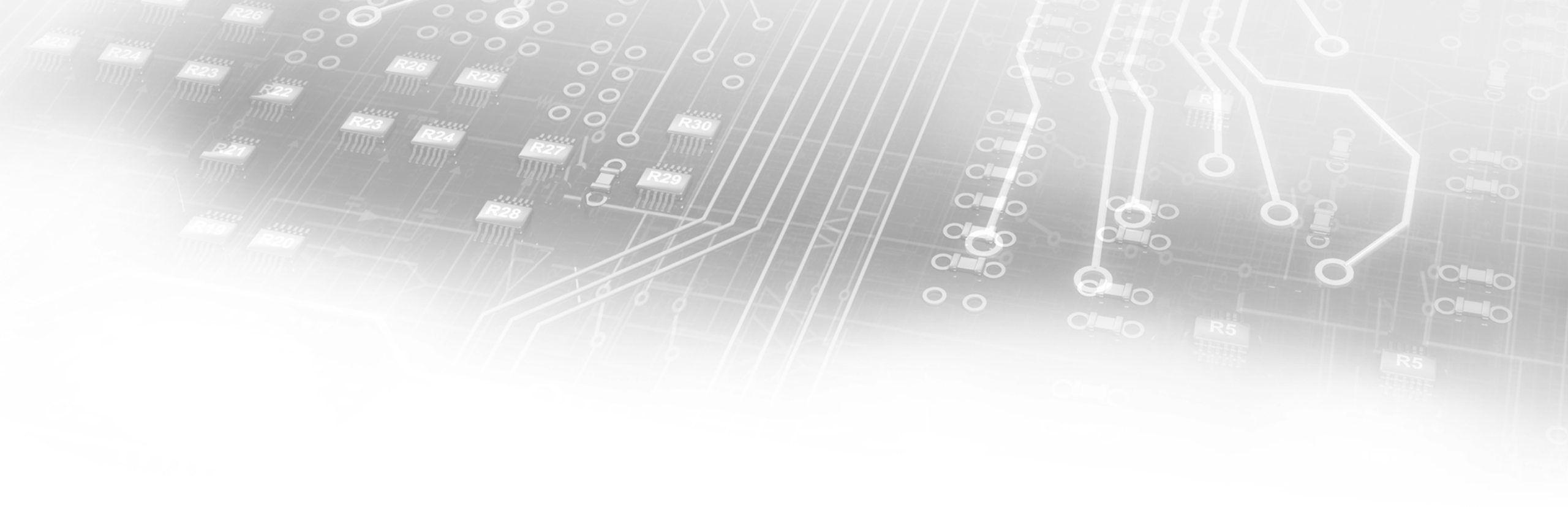


PMK = Pairwise Master Key

TPK = Transient Pairwise Key

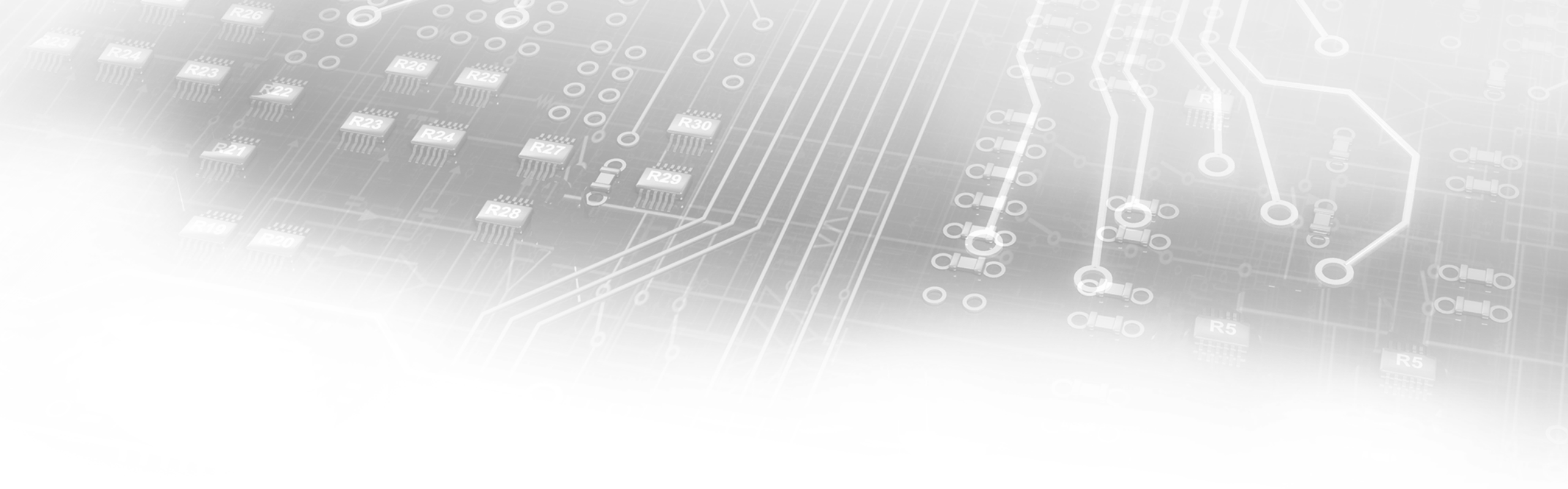
Q: Are there better alternatives ?





Questions ?

BROADCOM®



Thank You !