Using EAP Keys for Bootstrapping
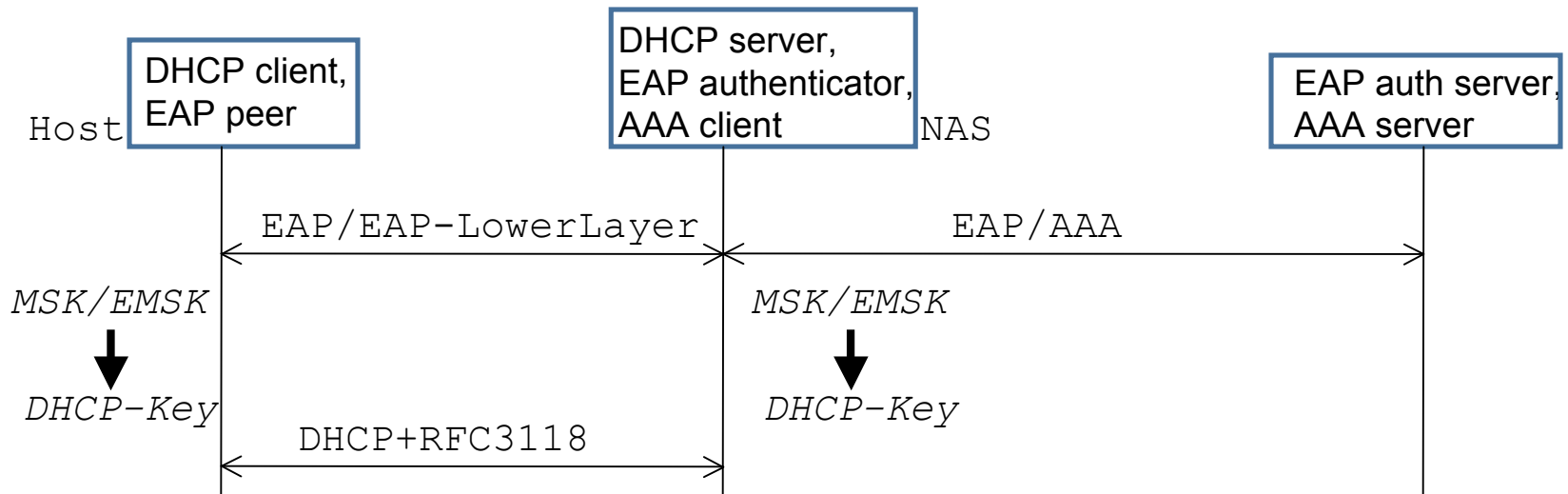# RFC 3118

Problem

- RFC 3118 can secure DHCP but it requires a shared secret between the DHCP client and DHCP server.

- DHCPv4 Threat Analysis (draft-ietf-dhc-v4-threat-analysis-03)

  "The authors believe that only by addressing scalability issues with key distribution can RFC 3118 achieve wide deployment."

Solution

- In networks using EAP for network access authentication, rely on EAP-generated session keys for bootstrapping a security association between DHCP client and server.

Feedback?

- Solution I-Ds exist:
  - draft-yegin-eap-boot-rfc3118-03
  - draft-salowey-dhc-eapkey-3118-00

- Is there interest in
  - providing in-band security for DHCP?
    - As opposed to relying on lower-layer (L1/L2) security…
  - bootstrapping RFC 3118?