Fondation RESTENA
IETF-71, Philadelphia, PA, USA

How to prevent RADIUS packet fragmentation when using EAP?

Problem Statement

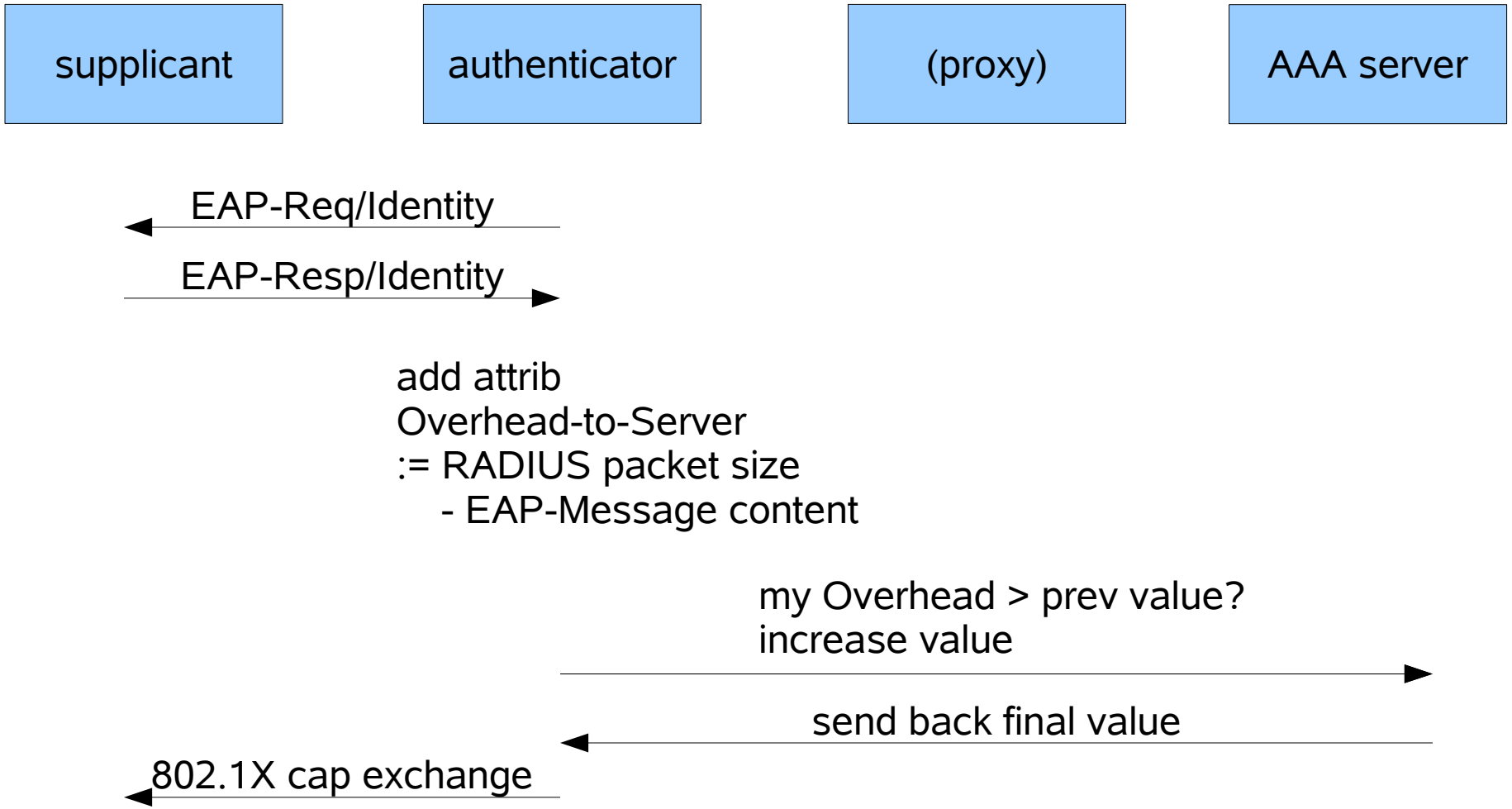
- some EAP payloads require client to send a lot of data to the server (EAP-TLS, possibly EAP-TNC)
- Clients can send upto their own link MTU
- Authenticator adds RADIUS wrap around EAP-Message
- resulting RADIUS packet may be >MTU limit from authenticator to AAA server
- practical experience: creates problems with equipment en route

Questions...

- What to do?
  - Tell supplicant how big EAP fragments should be
- How to do it?
  - find out RADIUS overhead during EAP-Response/Identity
  - send back info in Access-Challenge to authenticator
  - use IEEE 802.1X capability exchange to tell supplicant

work flow


RESTENA


supplicant
authenticator
(proxy)
AAA server
EAP-Req/Identity
EAP-Resp/Identity
add attrib
Overhead-to-Server
:= RADIUS packet size
- EAP-Message content
my Overhead > prev value?
increase value
send back final value
802.1X cap exchange

to be considered

- EAP-Resp/Identity is small, can be expected not to be fragmented
- Do authenticators/proxies treat all Access-Requests that contain an EAP-Message equally?
- Will this ever be implemented?
- How about the other way around? I.e. how does server know how much EAP content to put into Access-Challenge at max?

Thank you!

Questions?