networkRADIUS

Session Identifiers

FOR FAST RE-AUTHENTICATION

RECAP

- RFC 5247 defines Session-ID

```
Session-Id

      The EAP Session-Id uniquely identifies an EAP authentication

      exchange between an EAP peer (as identified by the Peer-Id(s)) and

      server (as identified by the Server-Id(s))
```

THE REQUIREMENT

- RFC 5247 Section 1.4 says:

> … EAP method
>
> specifications developed after the publication of this document MUST
>
> define the Peer-Id, Server-Id, and Session-Id.

THE PROBLEM

- This has been done for existing EAP methods… mostly
- EAP-Session-ID has not been defined for fast re-authentication for
  - EAP-SIM
  - EAP-AKA
- But no Session ID derivation was defined for:
  - EAP-AKA’
  - PEAP

WHY?

- TLS-based EAP methods do not have this problem
  - They cache TLS information, and can always derive the keys
- Non-TLS based EAP methods cannot use the same information
  - it does not exist for fast re-authentication
  - it must instead be derived from the cached information
- Vendor EAP methods are likely to have this problem, too
- Session-Id derivation needed for ERP (RFC 6696) and FILS (IEEE 802.11ai)

PROPOSAL

- Based in Jouni Malinen's comments to the EMU mailing list:
- EAP-AKA Session-Id = 0x17 || NONCE_S || MAC
- EAP-AKA' Session-Id = 0x32 || RAND || AUTN

  Session-Id = 0x32 || NONCE_S || MAC
- EAP-SIM Session-Id = 0x12 || NONCE_S || MAC
- PEAP Session-Id = 0x19 || client.random || server.random

UPDATES

- Updates 5247 (EAP key management framework)
- Should also update
  - RFC 4186 (EAP-SIM)
  - RFC 4187 (EAP-AKA)
  - RFC 5448 (EAP-AKA’)
  - RFC 5247 (PEAP)

QUESTIONS?