RoE authentication, control packets and e2e security

Jouni Korhonen
8/11/2015

Background 1/2

- ❑ Do we need to protect the RoE traffic?
  - – Depending on the deployment: YES.

- ❑ Two observations:
  - – First: Traffic that goes over the air to/from UE is typically already protected by the cellular system – both user traffic and control traffic that get transported over RoE data flows.
  - – Second: RoE control flows are only between REs and RECs, thus the cellular system security does not apply.

Background 2/2

- Do we need to authenticate REs?
  - Depending on the deployment: YES:

- When a deployment decides and desires it should be possible for REs and RECs to mutually authenticate each other before allowing e.g. REs to join the system.

- It makes sense to reuse existing mechanism already standardized (and deployed) solutions for this kind of “Port Access Control” -> IEEE 802.1X.

Observations 1/2

- RoE control flows get terminated at the local CPUs – not the switch.
- There is no reason to protect RoE data flows.
- The protection must be e2e even it there is a network between REs and RECs.
- There is no reason to protect anything else but the RoE content itself - the RoE payload.
- The protection overhead may be significant (e.g. a new record layer).

Observations 2/2

- ❑ For the access control and mutual authentication IEEE 802.1X must be used.

- ❑ IEEE 1904.3 should define one must support authentication method (if the whole mechanism is used):
  - – E.g. EAP-TTLSv0 (RFC5281) as the must support method.

Conclusion and Proposal

- However, the current IEEE1904.3 PAR does not say a word about 1) authentication or 2) e2e security!

- Proposal to plain neglect any specifications for mandatory or optional security features in the specification for now.
  - May add a forward looking note that security features may need to be added later on (would need a PAR revision).