Simple Authentication for ALC and NORM

IETF81, Québec City

V. Roca

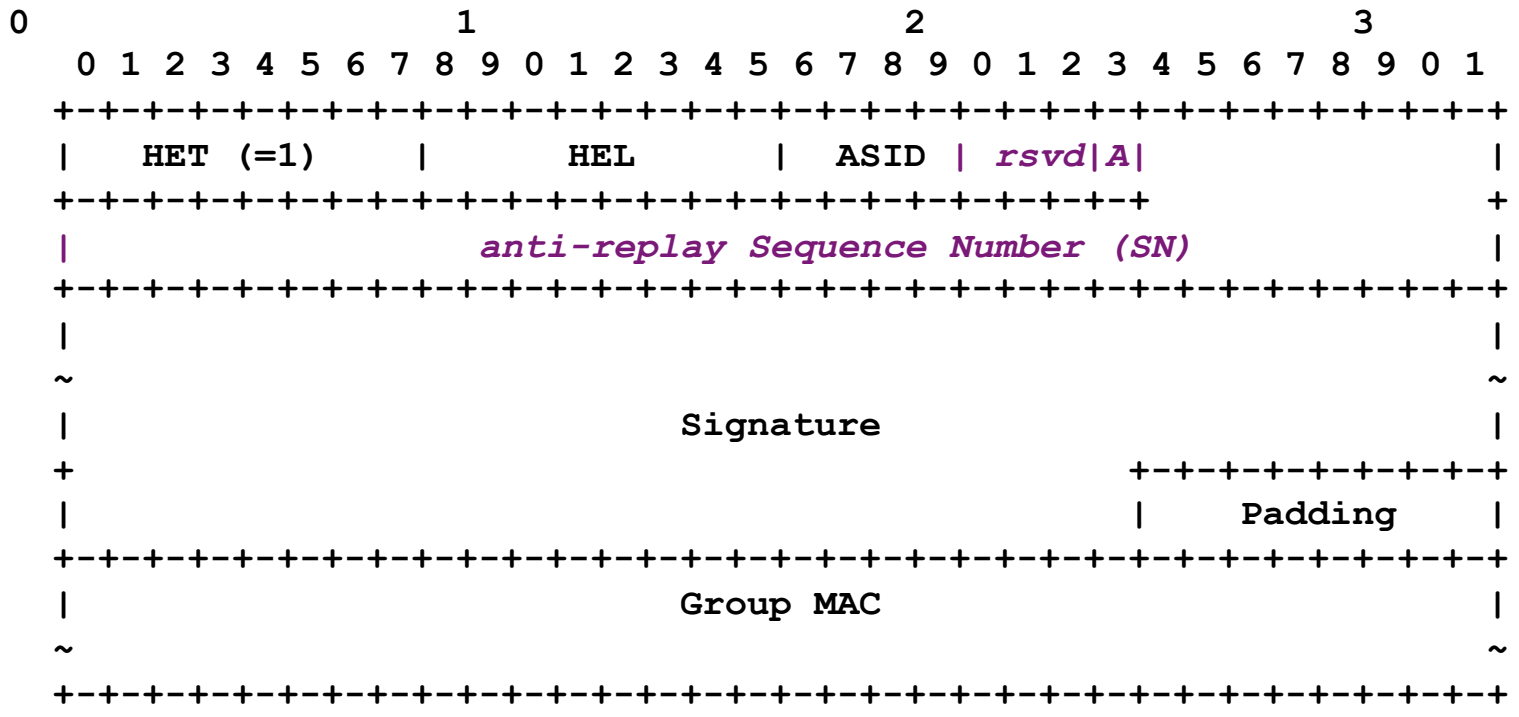
informatiques mathématiques

I-D update, after David's comments

- comment: "Can replay be used as a DoS attack, consuming resources?"
  - true with the combined signature/group MAC
    - **replaying a valid packet is an easy way to bypass the "light" group MAC filtering ☹**
    - **added an anti-replay mechanism**
    - **anti-replay MUST be used**
  - what about other authentication schemes?
    - **added anti-replay as an *option***
    - **using anti-replay is RECOMMENDED**

I-D update… (cont')

- anti-replay format
  - **added a 3-bit "reserved" field**
  - **added a 1-bit "A" flag: indicates the presence of the SN field**
  - **added a 40-bits anti-replay sequence number ("SN") field**
    - provides sufficient space, even for high speed transmissions, for most situations



I-D update… (cont')

- what are the consequences of not using anti-replay when optional?
  - NORM:
    - **NORM "sequence number" feature to provide anti-replay is no longer considered as suitable, given the small field size (16 bits)**
    - **using the anti-replay mechanism is now RECOMMENDED**
  - ALC:
    - **more robust in front of replay attacks, there's just a small risk when using EXT_TIME header extensions**
    - **clarification added to the "Security Considerations" section**