Geneve Security Requirements

Migault, Boutros, Wings, Krishnan

Goals

Geneve security without transit devices

Geneve security with transit devices

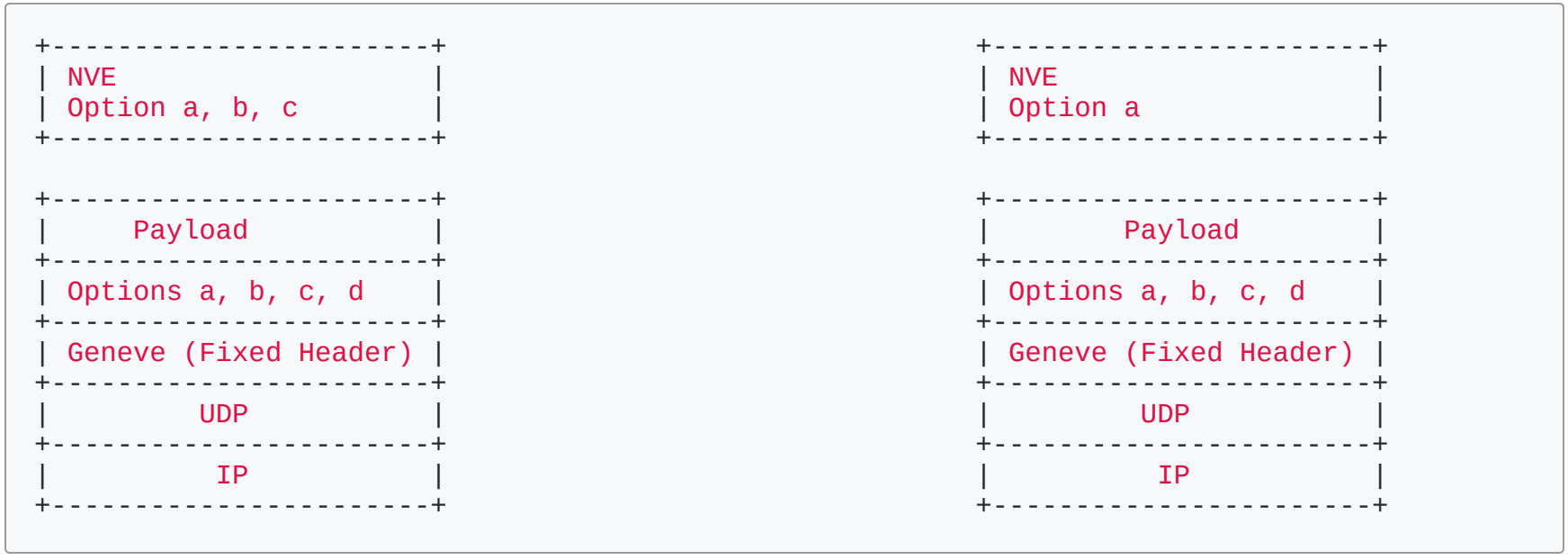
- Problem
- Moving forward

Geneve NVE-to-NVE

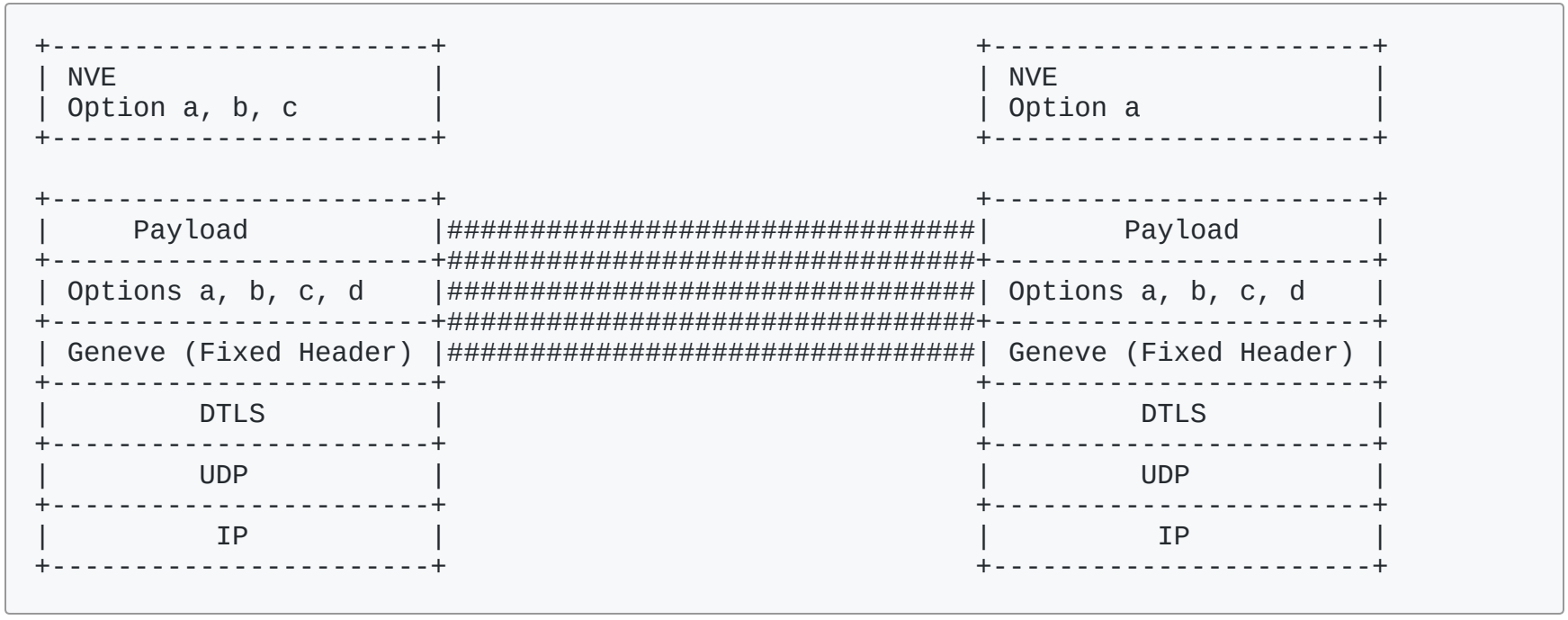
In a NVE-to-NVE communication without transit devices:

- Options a,b,c are treated by the NVE
- DTLS or IPsec are very well known protocol to secure this communication

Geneve NVE-to-NVE



Geneve NVE-to-NVE



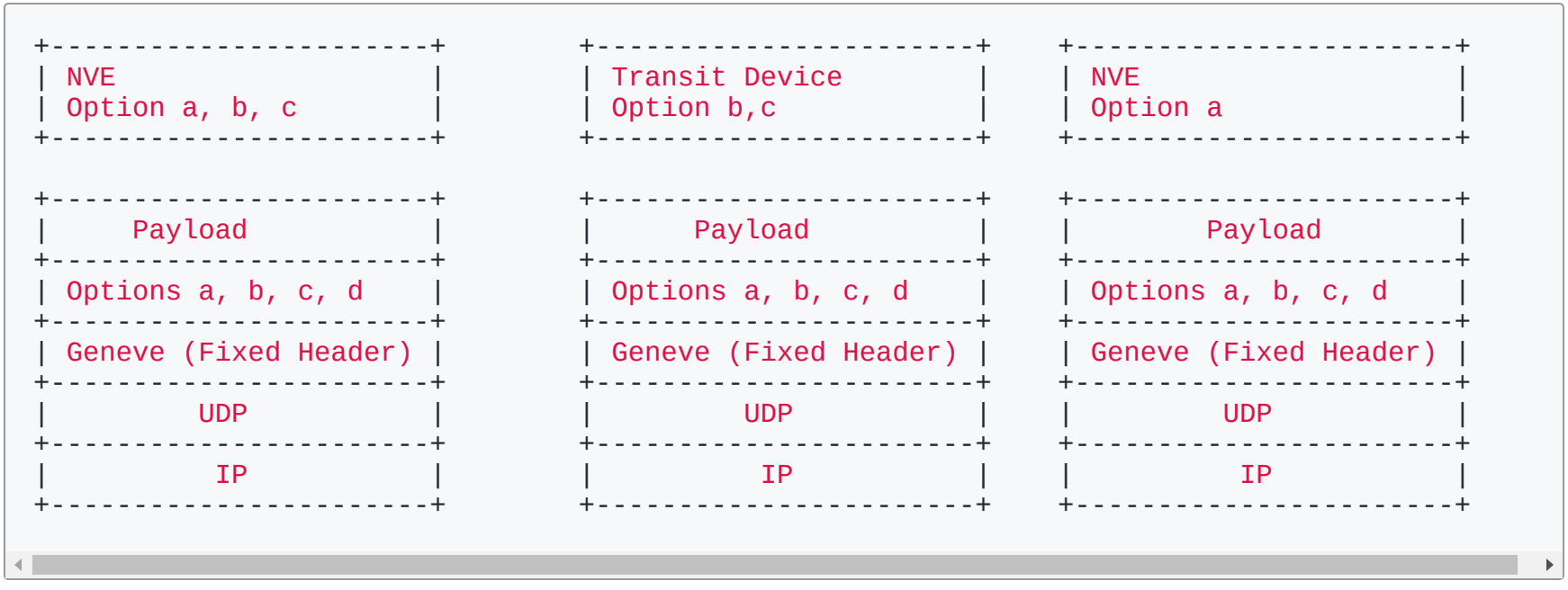
Geneve with Transit Devices

Options a,b,c are treated by the NVE (a) and the Transit Device (b,c)

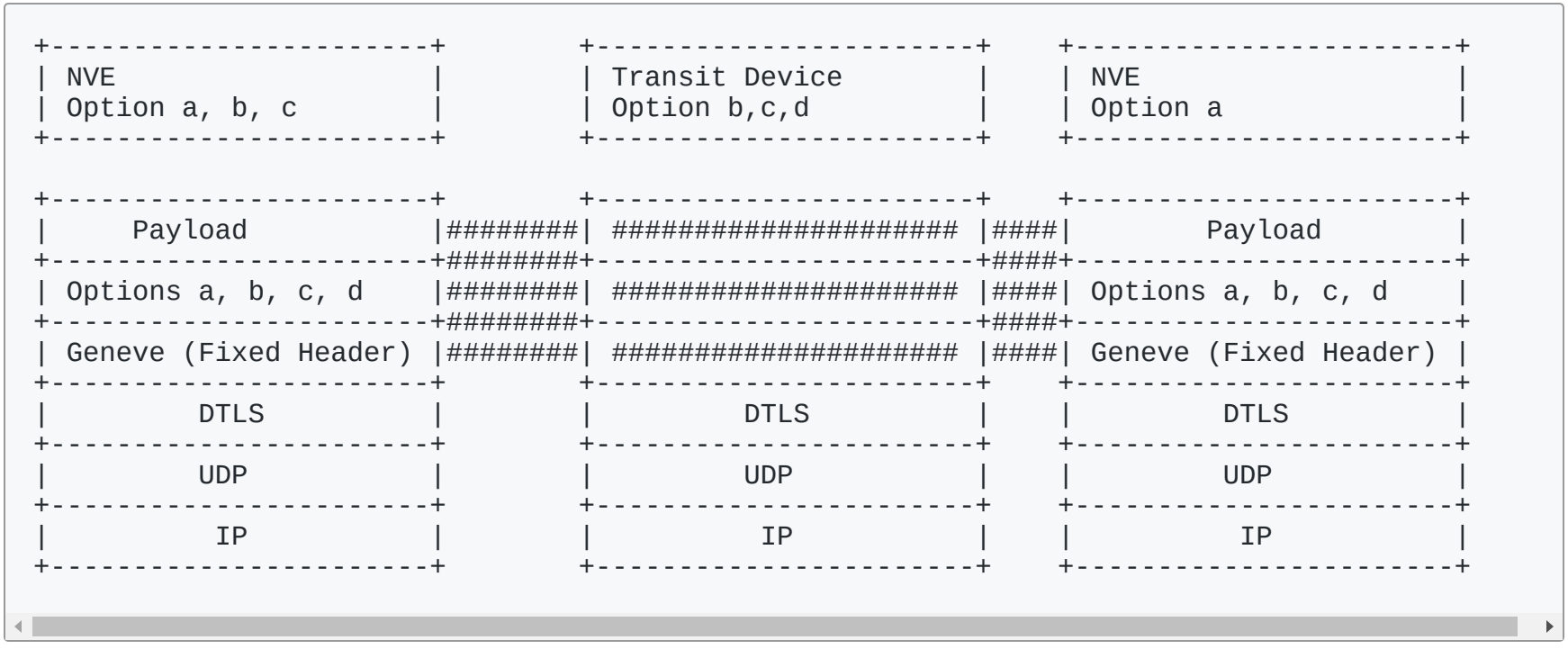
The problem of DTLS is that it is either:

- activated: Transit device does not see it
- not activated: no protection

Geneve with Transit Devices



Geneve with Transit Devices

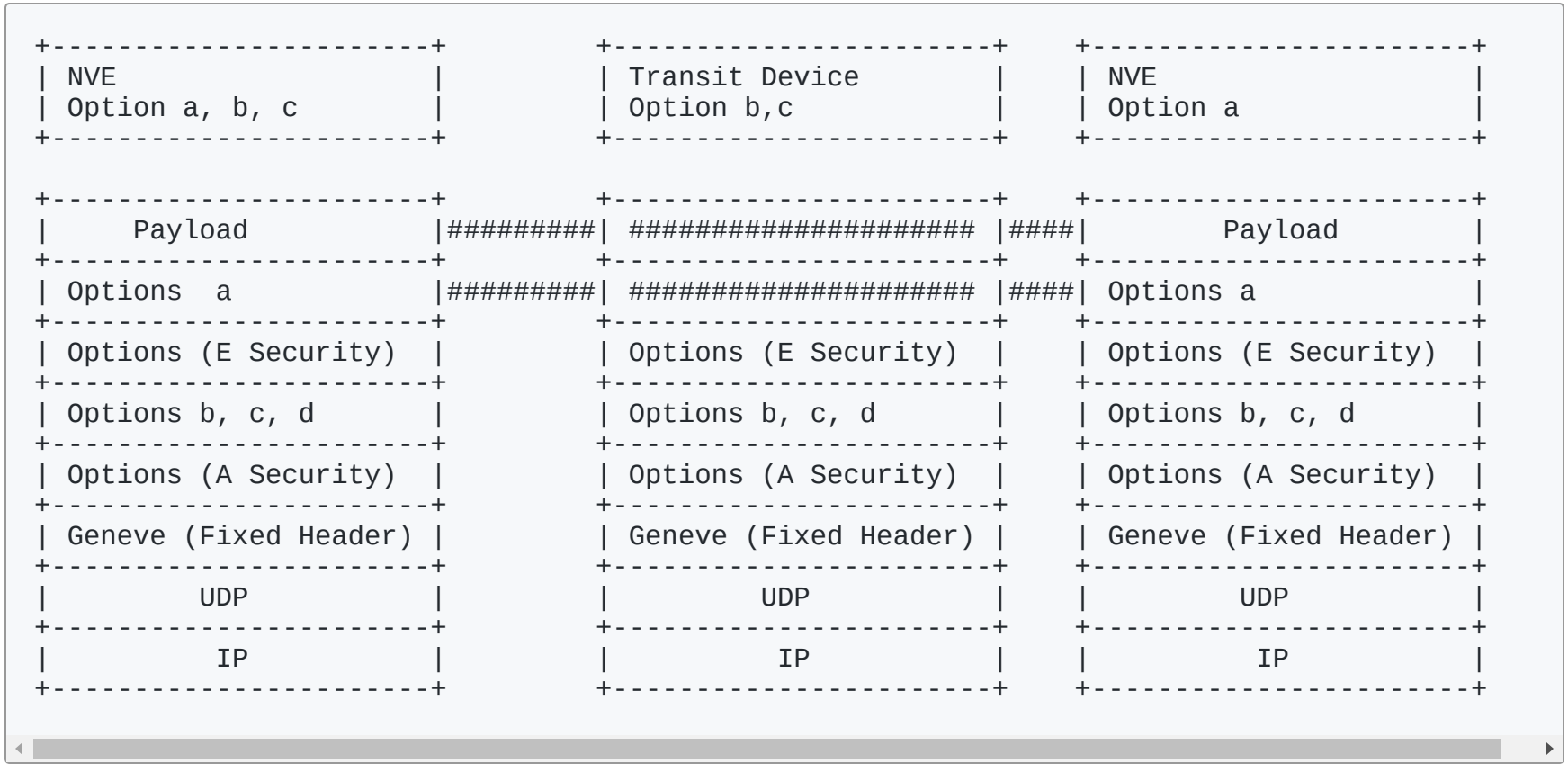


Transit Devices

The current Geneve specification mentions TD can ONLY READ Geneve Options.

- We need to enforce that actions are limited to READ and detect write
    - authentication
- We need to be able to be able to limit the options a TD can read
    - encryption

Geneve with Transit Devices



Transit Devices

Transit Devices are not defined in the NVO3 architecture (RFC8014):

- more work is needed to specify their place in the architecture.
- there is a need to clarify the boundaries between TD and NVE

Typically, what happens wen multiple transit devices are on path ?

- should a option visible to a TD be visible to all TD ?
- should options visible to a TD be only visible to that TD ?
- could an option for a TD be encrypted, authenticated ?

Next Steps

Define Transit Devices

Define Security Requirements

Define Security Architecture, Encrypted / Authenticated options