Geneve Security Requirements

Migault, Boutros, Wings, Krishnan

History

- Feb 27 2018 Call for adoption version 03
- Oct 12 2018 version 04
- Nov 11 2018 version 05
- March 21 2019 version 06
  - Clarified the distinction between Operational versus Geneve Mechanism Security requirements
  - Uniformizes requirements for authentication and encryption
  - Match each requirements with DTLS and IPsec

Status

The draft derives security requirements based on:

- Threat model (provided by the draft)
- Specification of Geneve (current version 12)

The security requirements are:

- Operational: check list to securely deploy Geneve
- Protocol: check list for a Geneve Security Mechanism
    - if ever such mechanism needs to be defined.

Status

Security requirements are closely tighten to the Geneve specification (version 12):

- Reveals some incoherence in the Geneve
- Currently stalled
    - waiting for these incoherence to be addressed

Geneve & DTLS

Comments from Geneve co-authors:

- The use of DTLS is sufficient to secure Geneve deployments
- Security capabilities for Transit Devices are not necessary

Geneve & DTLS

In fact:

- DTLS/IPsec cannot secure Geneve overlays (in general)
  - Transit Devices make Geneve Security Mechanism implemented through Geneve Options.
- NVE and Transit Devices MUST be able to operate with the same level of security
  - Geneve Options are interpreted by Transit Device or NVE.
  - Transit Devices creates three party communications with a lot of complexity.

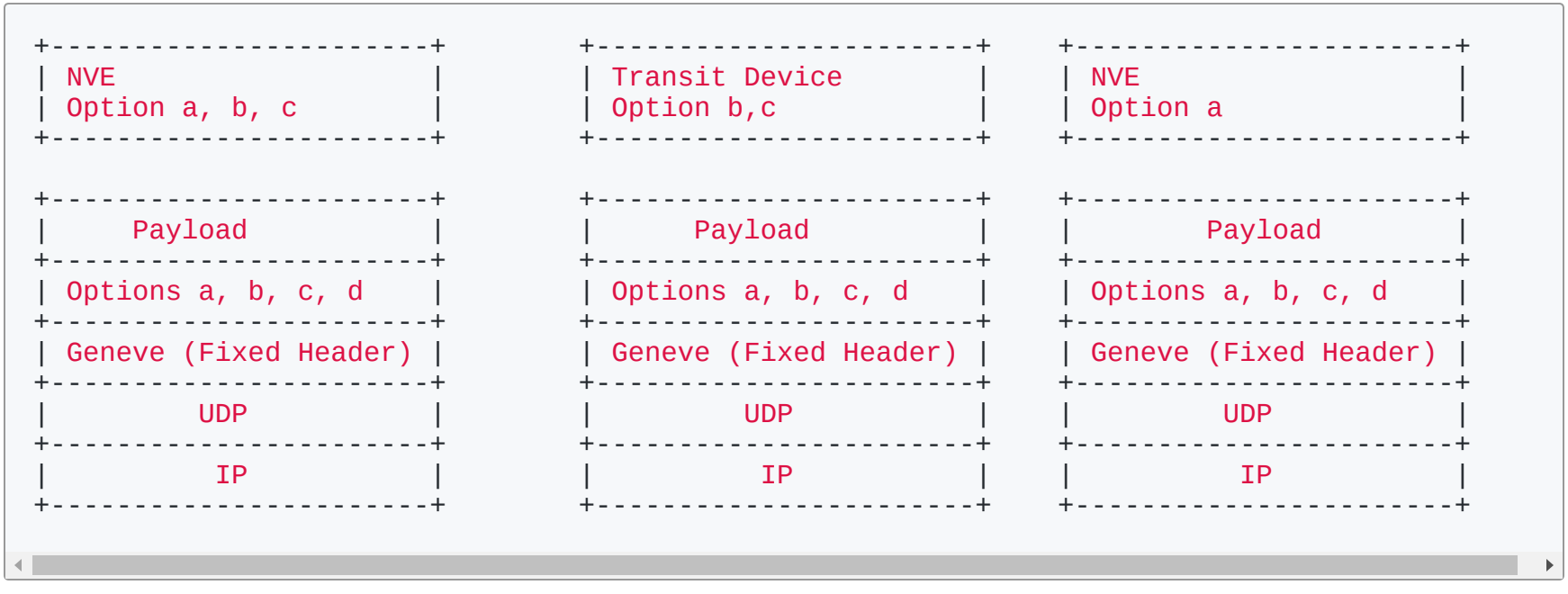
Geneve & DTLS

The overall concern of complexity provided by security is a consequence of the Geneve architecture

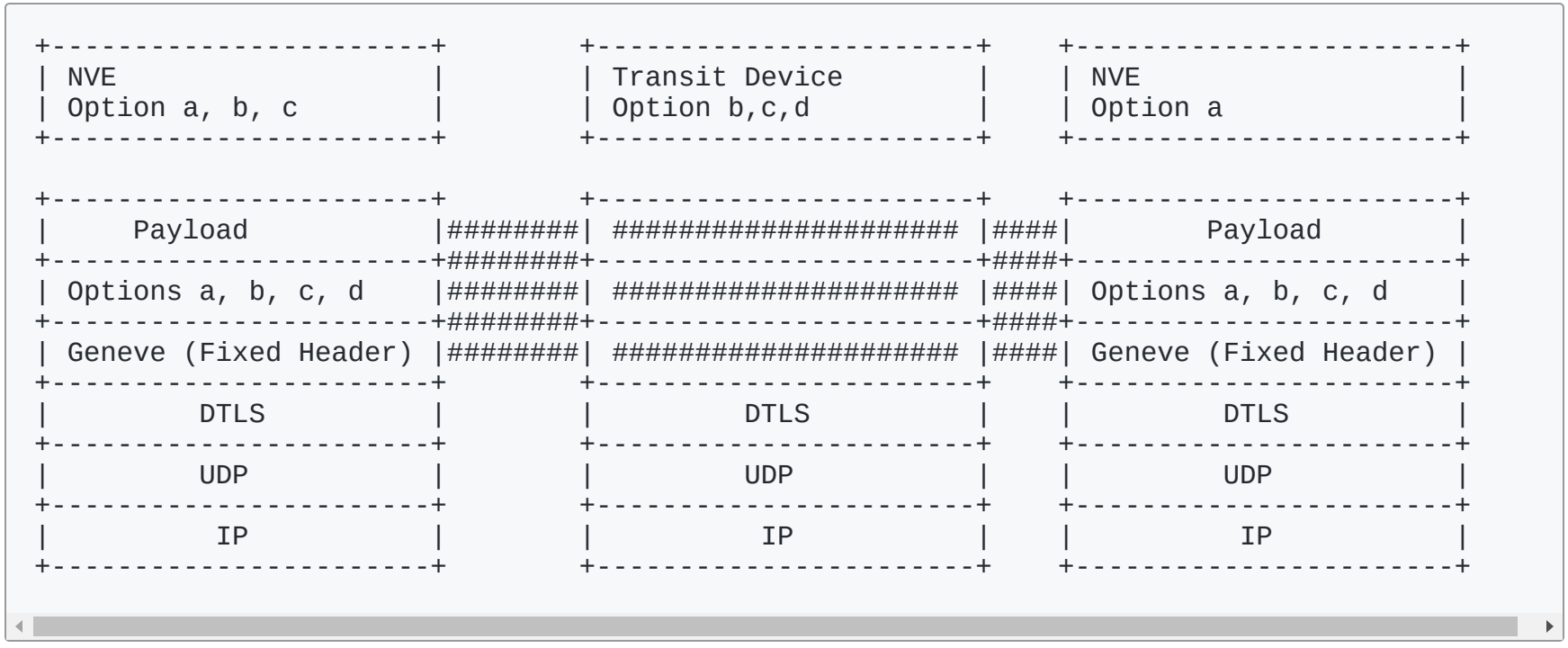
- (At least my understanding of it)

Geneve & DTLS

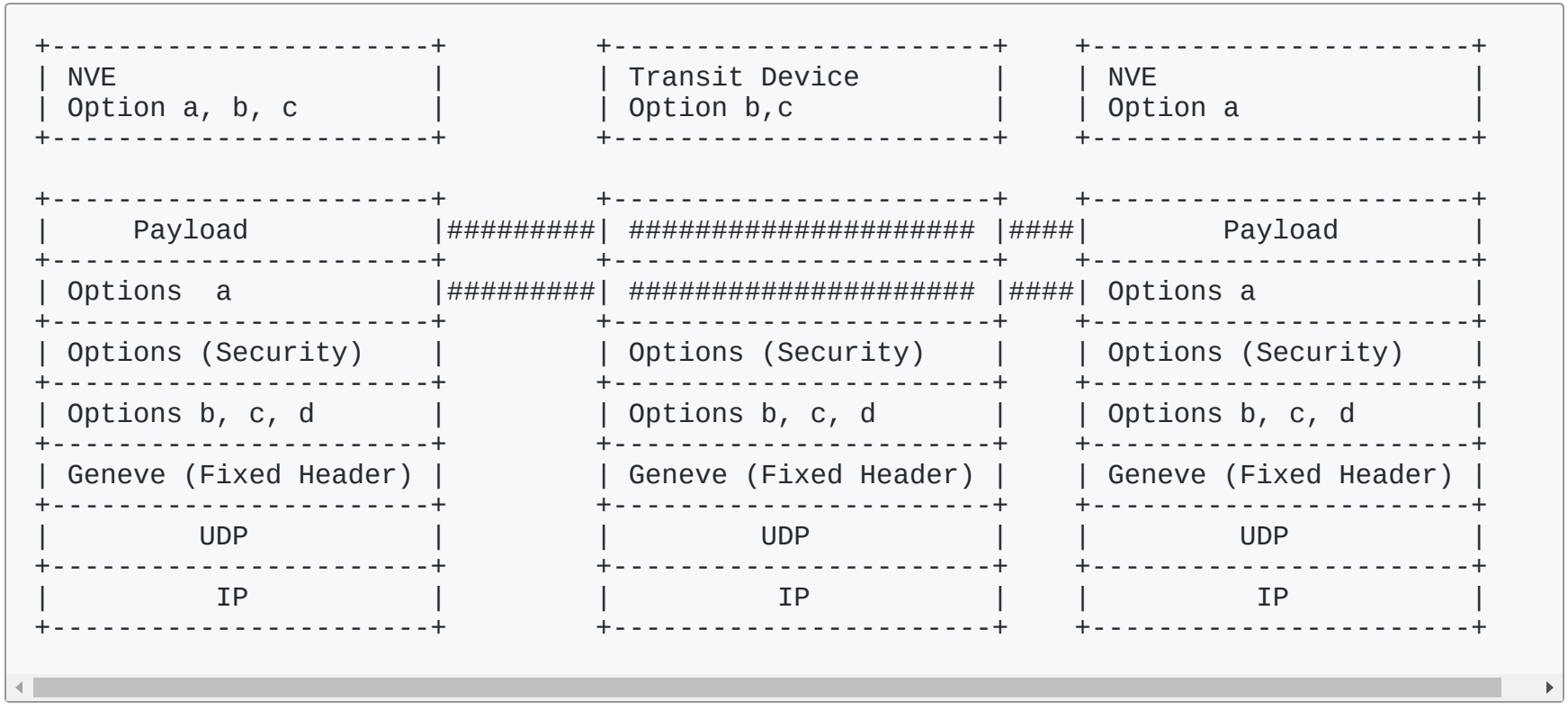
Options a,b,c are treated by the NVE (a) and the Transit Device (b,c)



Geneve & DTLS


NVE
Option a, b, c
Transit Device
Option b,c,d
NVE
Option a
Payload
Options a, b, c, d
Geneve (Fixed Header)
DTLS
UDP
IP
Payload
Options a, b, c, d
Geneve (Fixed Header)
DTLS
UDP
IP
Payload
Options a, b, c, d
Geneve (Fixed Header)
DTLS
UDP
IP

Geneve & DTLS


NVE
Option a, b, c
Transit Device
Option b,c
NVE
Option a
Payload
Options a
Options (Security)
Options b, c, d
Geneve (Fixed Header)
UDP
IP
Payload
Options a
Options (Security)
Options b, c, d
Geneve (Fixed Header)
UDP
IP

Geneve & DTLS/IPsec

Transit Devices prevents end-to-end security with Geneve

- IPsec/DTLS cannot be considered as a way to secure Geneve

Transit Device are optional

- incompatibility between end-to-end security and transit devices does not make them OPTIONAL

Geneve and end-to-end protocol

Geneve co-authors seems to be willing to have Geneve as an end-to-end protocol:

- End-to-end protocols are much easier to secure than three party protocols
- Geneve could probably benefit from already defined security protocols (DTLS, IPsec)

Do we need Transit Device ?

Analysis of the Transit Devices

There is currenlty no use case for Transit Devices

- Transit Devices are limited to read, process a Geneve Option (prevents Telemetry)

Transit Devices are on-path devices that do not follow middleboxes recommendations

- Explicit signaling to the end points
- ...

Transit Devices are incompatible with UDP encapsulation:

- Transit Devices interpret Geneve Packets based on heuristics that will ossify the Geneve
- ports are not reserved

Analysis of the Transit Devices

Transit Device are likely to modify on-path packets

```
if DTLS:
    BYPASS
else: ## No possible guarantee
    Procees Geneve Option
```

Conclusion

Transit Devices:

- Introduce a lot of architecture or protocol complexity
  - Not addressed yet by current specifications
- Security complexity reflects the architecture complexity
- Do not have use cases

Next steps:

- Adoption of the security requirement as a WG document
- Remove the Transit Devices from the specification
- Update the security analysis

We expect this will address the concerns of the Geneve co-authors.