ULE Security Extension

draft-ppillai-ipdvb-sule-00.txt

Authors : Prashant Pillai, Yim Fun Hu (University of Bradford)

IPDVB Working Group, 66th IETF Meeting, Montreal

UNIVERSITY OF BRADFORD

10th July 2006

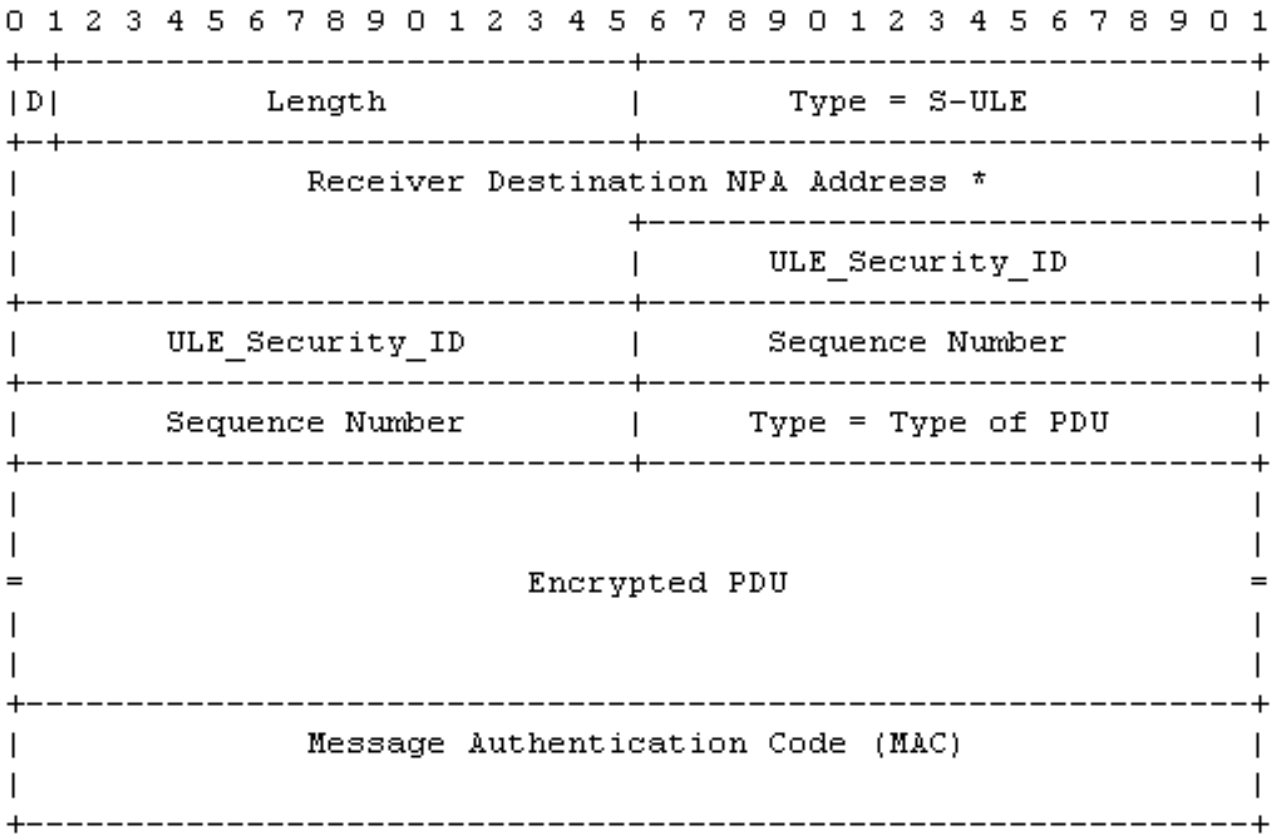
Draft Overview

- This draft describes some additional security requirements that were not addressed in the earlier version of the security requirements document
- It also describes the secure ULE SNDU format
- It also describes the processing procedure of security extension header

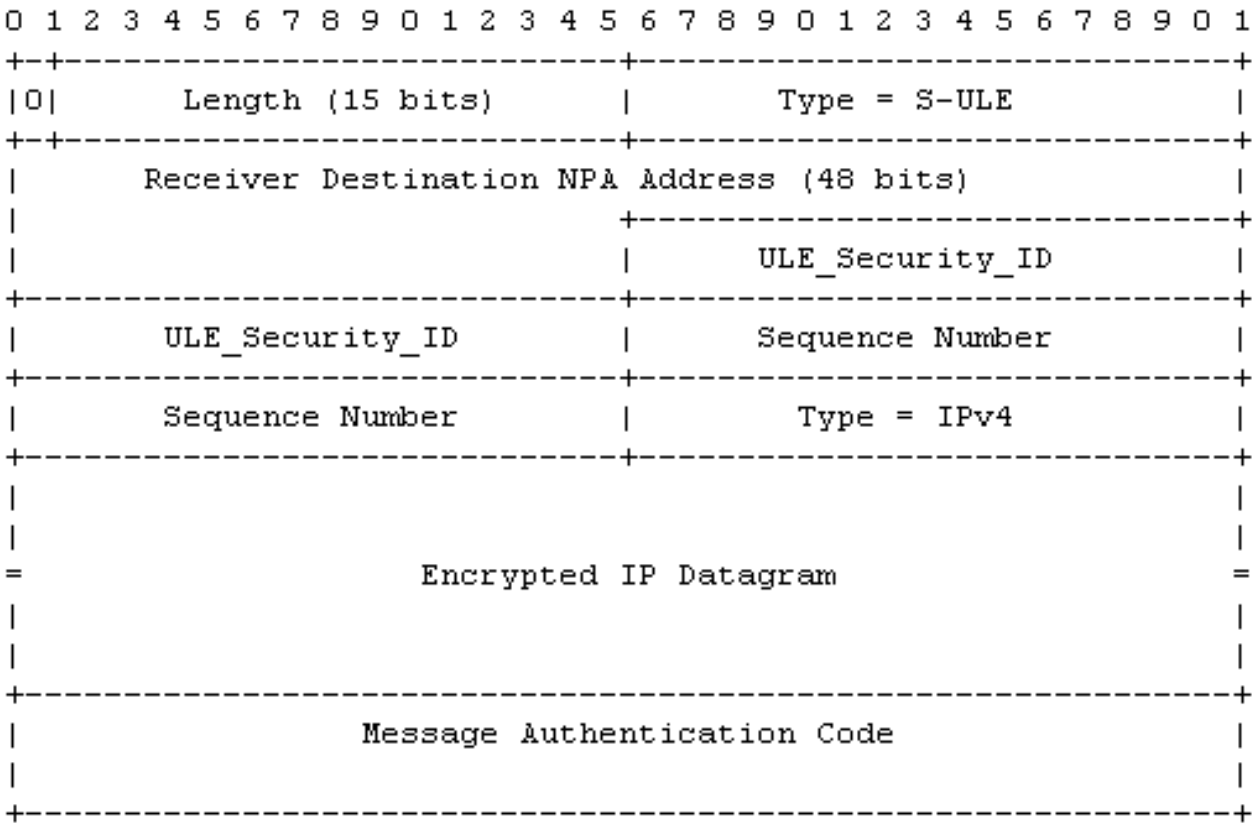
Security Requirement

- Data Confidentiality
- Data Origin Authentication
- Data Integrity
- Replay Attack Countermeasures

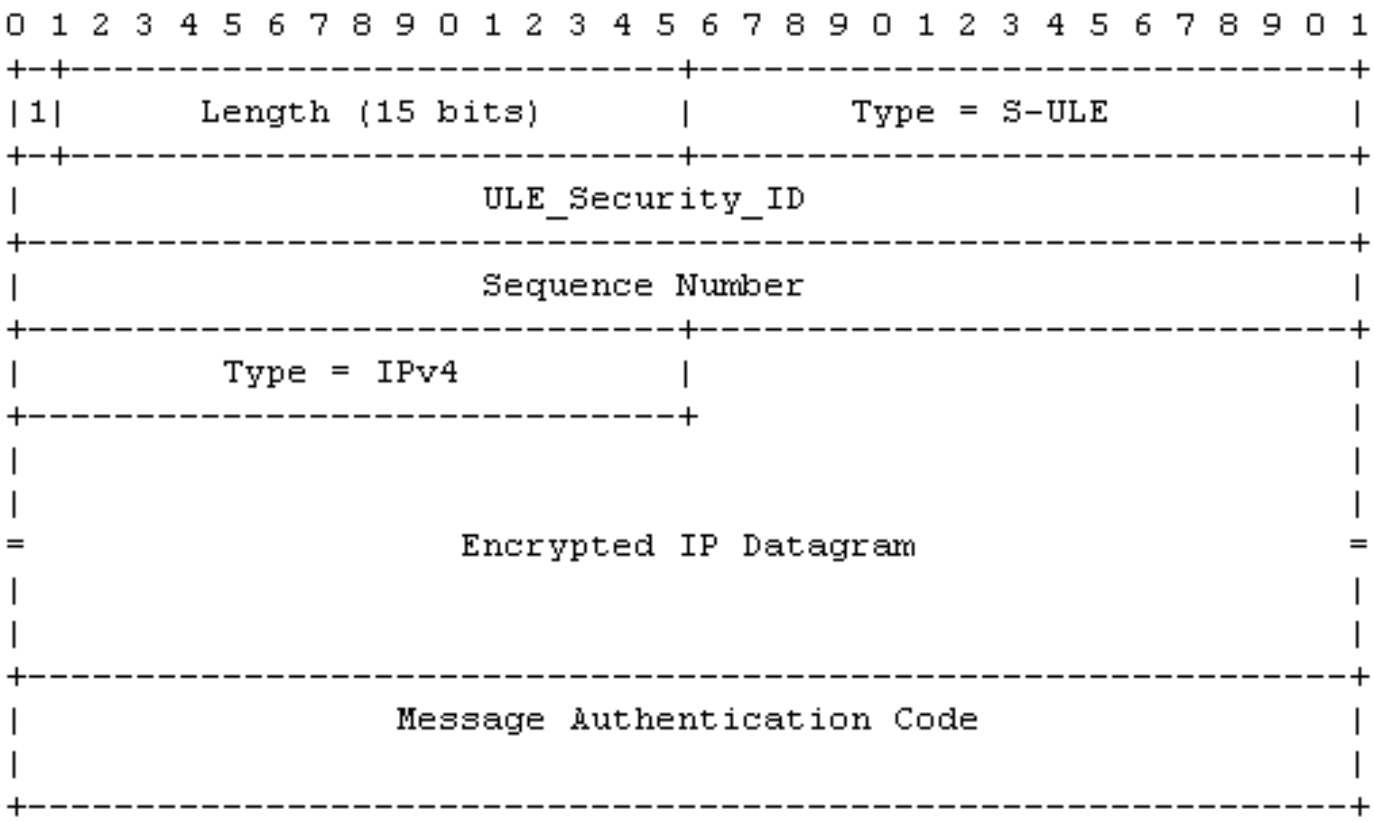
Secure ULE SNDU Format



Secure ULE SNDU Example, D=0



Secure ULE SNDU Example, D=1



Receiver Procedure

- Upon reception of the Secure ULE SNDU, the receiver may first filter the received packets according to the recevier destination NPA address (if present).
- It would then use the ULE_Security_ID to Obtain the security associations between the transmitter and receiver.
- With this the receiver would know the algorithms and keys used for both encryption of the encapsulated PDU and for generation of the message authentication code.
- It would then use the sequence number for filtering out any out-of-sequence packets.
- The next step would be to check the MAC to verify the authenticity and integrity of the received packet. If the calculated MAC does not match the transmitted MAC, then the packet is discarded.
- Finally the encapsulated payload will be decrypted.

Future Plan

- We have combined with the Haitham to define the new draft-cruickshank-ipdvb-sec-02.txt