IP over MPEG-2/DVB (ipdvb) WG

Wednesday, August 3rd, 2005
10:30-12:20 Morning Session II

CHAIR:

Gorry Fairhurst <gorry@erg.abdn.ac.uk>

Active Drafts:

draft-ietf-ipdvb-arch-04.txt
draft-ietf-ipdvb-ule-06.txt
draft-ietf-ipdvb-ar-00.txt
draft-stiemerling-ipdvb-config-01.txt
draft-cruickshank-ipdvb-sec-00.txt
draft-cantillo-ipdvb-s2encaps-00.txt
draft-fair-ipdvb-ar-03.txt (superceded)
draft-montpetit-ipdvb-config-00.txt (expired)

Archive:

http://www.erg.abdn.ac.uk/ipdvb/archive
ftp://ftp.ietf.org/ietf-mail-archive/ipdvb/

4th IETF ipdvb WG meeting

Agenda

1. **Agenda Bashing (10 minutes) - Chair**
   * Agenda changes
   * Scribe for Proceedings
   * Jabber Scribe
2. **Document Status (5 minutes) - Chair**
3. **Unidirectional Lightweight Encapsulation (10 minutes) - GF**

   draft-ipdvb-ule-06.txt
4. **Address Resolution (AR) (15 minutes) - GF**

   draft-ietf-ipdvb-ar-00.txt
5. **IP Address Configuration for ipdvb (10 minutes) - MS**

   draft-stiemerling-ipdvb-config-01.txt

Agenda

6. **ULE Security Extension (20 mins) - HC**

   draft-stiemerling-ipdvb-config-00.txt

7. **IP Encapsulation for DVB-S.2 (20 minutes) - JL**

   draft-cantillo-ipdvb-s2encaps-00.txt

8. **MIP6 & UDLR implications on ipdvb (10 minutes) - ??**

   draft-miloucheva-udlr-mipv6-00.txt

9. **Review of Milestones (10 minutes)**

10. **AOB**

Archive: http://www.erg.abdn.ac.uk/ipdvb/archive

IPR Notice

You MUST disclose any IPR you know of relating to the technology under discussion

When starting a presentation you MUST say if:

- There is IPR associated with your draft
- The restrictions listed in section 5 of RFC 3667 apply to
  - Your draft
  - When asking questions
  - Commenting on a draft

BCP78 (RFC 3667), BCP79 (RFC 3668) and the “Note Well” text

2. Document Status

Gorry Fairhurst <gorry@erg.abdn.ac.uk>

Active IDs

Published RFCs:

None.

RFC Ed Queue:

Framework/Architecture ID (INFO)

draft-ietf-ipdvb-arch-03.txt

Ultra Lightweight Encapsulation (ULE) (for Proposed STD)

draft-ietf-ipdvb-ule-06.txt

IESG Review:

None.

Documents in Last Call:

None.

Active IDs

Individual:

Address Resolution Framework (INFO - AS)
draft-fair-ipdvb-ar-03.txt (Superceded)

Address Resolution Config
draft-montpetit-ipdvb-config-00.txt (expired)
draft-stiemerling-ipdvb-config-01.txt

Other IDs being discussed at this meeting:
draft-cruickshank-ipdvb-sec-00.txt
draft-cantillo-ipdvb-s2encaps-00.txt
draft-miloucheva-udlr-mipv6-00.txt
draft-bormann-rohc-over-802-01.txt

Milestones

Done Draft of a WG Architecture ID
Done Draft of a WG ID on Encapsulation (ULE)
Done Submit Architecture to IESG (for Nov 2004)

Done Draft of a WG ID on AR Framework
Done Submit Encapsulation to IESG

Feb 05 Draft of a WG ID on AR Protocol

Oct 05 Submit AR Framework to IESG

Dec 05 Submit AR Protocol to IESG
Dec 05 Progress ULE RFC along IETF Standards Track

Dec 05 Recharter or close WG?

3. ULE Status

draft-ietf-ipdvb-ule-06.txt

Gorry Fairhurst <gorry@erg.abdn.ac.uk>
Bernhard Collini-Nocker bnocker@cosy.sbg.ac.at

Current Status of ULE

Rev -04
Followed WGLC comments (see IETF-62)

Rev -05
Submitted to IESG for Review

Rev -06
Followed IESG discussion

Changes in Rev -06

This rev followed reviews:

- AD review
- GenART review
- IESG review
- IANA review

Changes (`http://www.erg.abdn.ac.uk/ip-dvb/ids/rfcdiff-ule-06-05.html`)

- Link to arch/framework I-D
- Usage of PP was updated to clarify corner cases
- Figure 1: updated (forward ref)
- Figure 2: fixed 16-bit word alignment error
- Example using IPv6 changed to use Prefix 2001:DB8::/32 (RFC3849)
- IANA section revised (clarification of requirements)
- Name change “Ultra Lightweight” -> “Unidirectional Lightweight”
- NiTs & reordering

This I-D is in the RFC Ed queue with note:

- 1) Clarification of PP overhead
- 2) Text on format_identifier

MPEG Format_identifier

MPEG SI

ULE did not define SI/PSI Information to identify the stream

Lack of an `format_identifier` had two issues:

(i) it can prevent (re)multiplexors forwarding a “stream”

(ii) receivers can not identify the type using SI/PSI tables

Text revised to include an SMPTE-allocated value:

A format_identifier value has been registered for ULE [ULE1]. This 32 bit number has a hexadecimal value of 0x554C4531. Transport Streams that utilise the Programme Map Table (PMT) defined in ISO 13818-1 [ISO-MPEG2] and that use the ULE format defined in this document, SHOULD insert a descriptor with this value in the PMT ES_info descriptor loop.

[ULE1] Registration for format_identifier ULE1, SMPTE Registration Authority, LLC, http://www.smpte-ra.org/ule1.html.

Other Issues

Should ipdvb request a Stream_ID?

- Registries maintained by DVB, ATSC

Should ipdvb request a DVB Data_broadcast_ID?

IP over MPEG-2/DVB Transport (ip-dvb)

Update on known implementations

Receivers

- Open source and commercial Receivers
- Authors say Linux driver conforms to latest ULE spec

Gateways

- Commercial gateway (no Open Source)

http://www.erg.abdn.ac.uk/ipdvb/ipdvb-impl.html

4. AR Status

Marie-Jose Montpetit
(mmontpetit@motorola.com)
Gorry Fairhurst
(gorry@erg.abdn.ac.uk)

Scope of draft

Binding/associating IPv4/IPv6 addresses with MPEG-2 TS.

An IP next hop address must be associated with :

- a Packet ID (PID)
- a Transmission Multiplex
- a L2 frame MAC/NPA address

Describes interaction with well-known protocols:

- DHCP, ARP, and NDP

Guidance on usage in various scenarios

Changes in Rev 00

This rev followed reviews:

- WG adoption as a WG I-D

Changes (`http://www.erg.abdn.ac.uk/ip-dvb/ids/`)

- Inputs from UDLR working group on UDLR, DHCP, NiTs
- Major reordering & reorganising of sections

Changes propose for Rev 01

This I-D requires inputs on:

- ARP scalability, security
- NDP scalability, security
- SEND (with NDP)
- NDP, ARP usage with UDLR
- Use of DHCP, L2TP, PPoE in two-way DVB networks (e.g. RCS)
- Procedures to identify encapsulation used and “platform”

Inputs from users of UDLR most welcome!

5. IP Address configuration for ipdvb

draft-stiemerling-ipdvb-config-01.txt

Martin Stiemerling
(stiemerling@netlab.nec.de)

(slides to follow)

Problem Statement:
IP Address Configuration for IPDVB

draft-stiemerling-ipdvb-config-01.txt

Martin Stiemerling — NEC Network Labs Europe
stiemerling@netlab.nec.de
IPDVB Working Group, 63th IETF meeting

Draft History

- Idea first presented at IETF 61 in Washington
  - Called “XML for Receiver AR Configuration”
- First draft presented at IETF 62
  - Showing the problem space
  - Sketching possible deployment scenarios
  - Sketching possible parameters to be configured

Draft Status (-01)

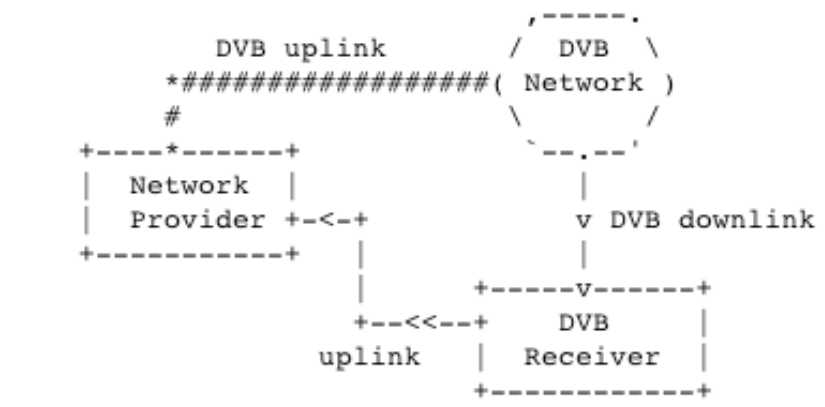
- Updated to RFC 3978 boiler plates
- Mainly editorial changes
- Clarifications on scenarios
- Not enough time to do more work
- Need more input from the WG

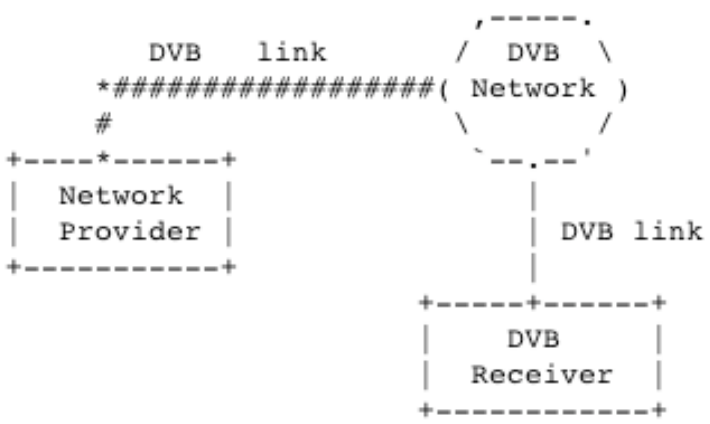
- Diff between -00 & -01 available
  - http://www.stiemerling.org/ietf/ipdvb/draft-stiemerling-ipdvb-config-01-diff-00.html

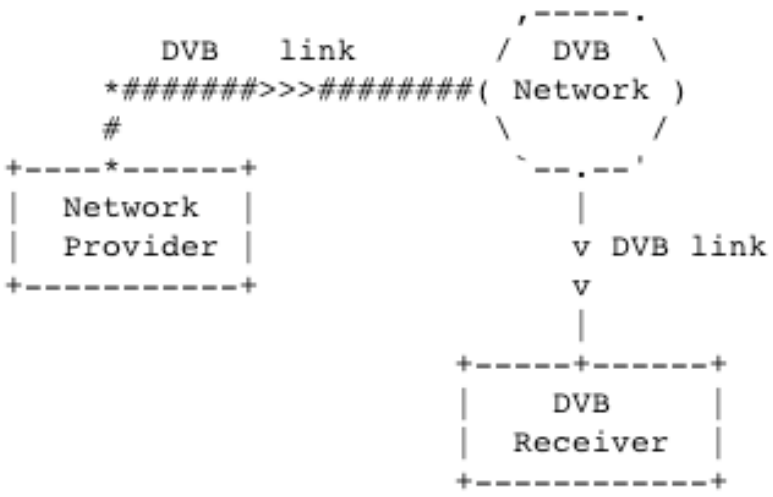
Problem Space

- Configuration of DVB receivers
  - IP address configuration
  - Other IP related configuration (proxies?)
  - Additional configuration (service related)
- Future IPDVB networks require powerful IP address configuration
  - IPDVB networks to be more “embedded” into IP
  - Flexible IP address management
  - Receivers probably not only receivers

Network Scenarios







Configuration Scenarios

- IP configuration available
  - IP pre-configured by the service provider or by users
  - IP service information, such as DNS server, proxies, etc
  - multicast configuration and routing information
  - broadcast configuration ("open bitstream" without any registration, DVB receivers just receive IP streams)
  - security configuration, e.g., keys, policies.
- Complete Bootstrap
  - No IP configuration available at all

Conclusions

- A first attempt on with IP address address configuration.
- Many open questions...
- ...soliciting feedback from the WG
- Future steps
  - Agreeing on scenarios
  - Agreeing on parameters to be configured
  - Start thinking about protocol requirements and a protocol

6. ULE Security Extensions

Haitham Cruickshank
(H.Cruickshank@surrey.ac.uk)
Stephane Combes
(Stephane.Combes@space.alcatel.fr)
Laurence Duquerroy
(Laurence.Duquerroy@space.alcatel.fr)
Sunnil Iyengar
(S.Iyengar@surrey.ac.uk)

IPDVB WG Meeting (IETF-63) - Paris

draft-cruickshank-ipdvb-sec-00.txt
ULE security extensions

Authors: Haitham Cruickshank and Sunil Iyengar *(University of Surrey, UK);*
Stephane Combes and Laurence Duquerroy
(Alcatel Alenia Space, Toulouse, France)

Comments from previous IP-DVB meetings

- Security objectives and the threats should be clearly defined and so need key management in relation to the link.
- Specific requirements on crypto algorithms should be identified, and an example should be worked out.
- There needs to be a statement saying why existing security mechanisms cannot be used.
- A motivation for and an "applicability statement" of the L2 mechanism should be provided in an I-D.
- Other comments:
  - How is the ID space managed? How do link and KM bind?
  - Why not encrypt the whole TS?

UniS

Why do we need ULE security

- This is an additional security mechanism to IP (IPsec), transport or application layer security - not a replacement:
  - For example it can work in parallel with IPsec
- Motivation:
  - Ability to provide security by the wireless/satellite operator in relation to controlling access to the service.
  - Capability to work with non-IP packet formats
  - Protection of the complete PDU including IP addresses and user identity hiding.
  - Protect of identity of the Receiver within the MPEG-2 transmission network. This includes hiding the IPsec tunnel end-point and optionally the receiver L2 identity (MAC/NPA addresses).
  - Transparency to the use of Performance Enhancing Proxies such as TCP PEPs, where IPsec can not be used.
  - Low CPU processing (Receiver decryption is performed at each destination L2 Receiver, instead of each destination IP address, where a Receiver may receive many IP streams.

Security requirements for IP over MPEG-2 TS

- In broadcast networks, data confidentiality is a major requirement against passive threats (using encryption).
- End-to-end security (such as IPsec) and ULE link security should work in parallel without obstructing each other.
- Optional protection of Layer 2 MAC/NPA address is desirable.
- Decoupling of ULE key management functions from ULE encryption is desirable:
  - This will allow the independent definition of these systems such as the re-use of existing security management systems e.g. GDOI and GSAKMP, other systems such as DVB-RCS or the development of new management systems, as required.
- Plus more …

The proposed approach

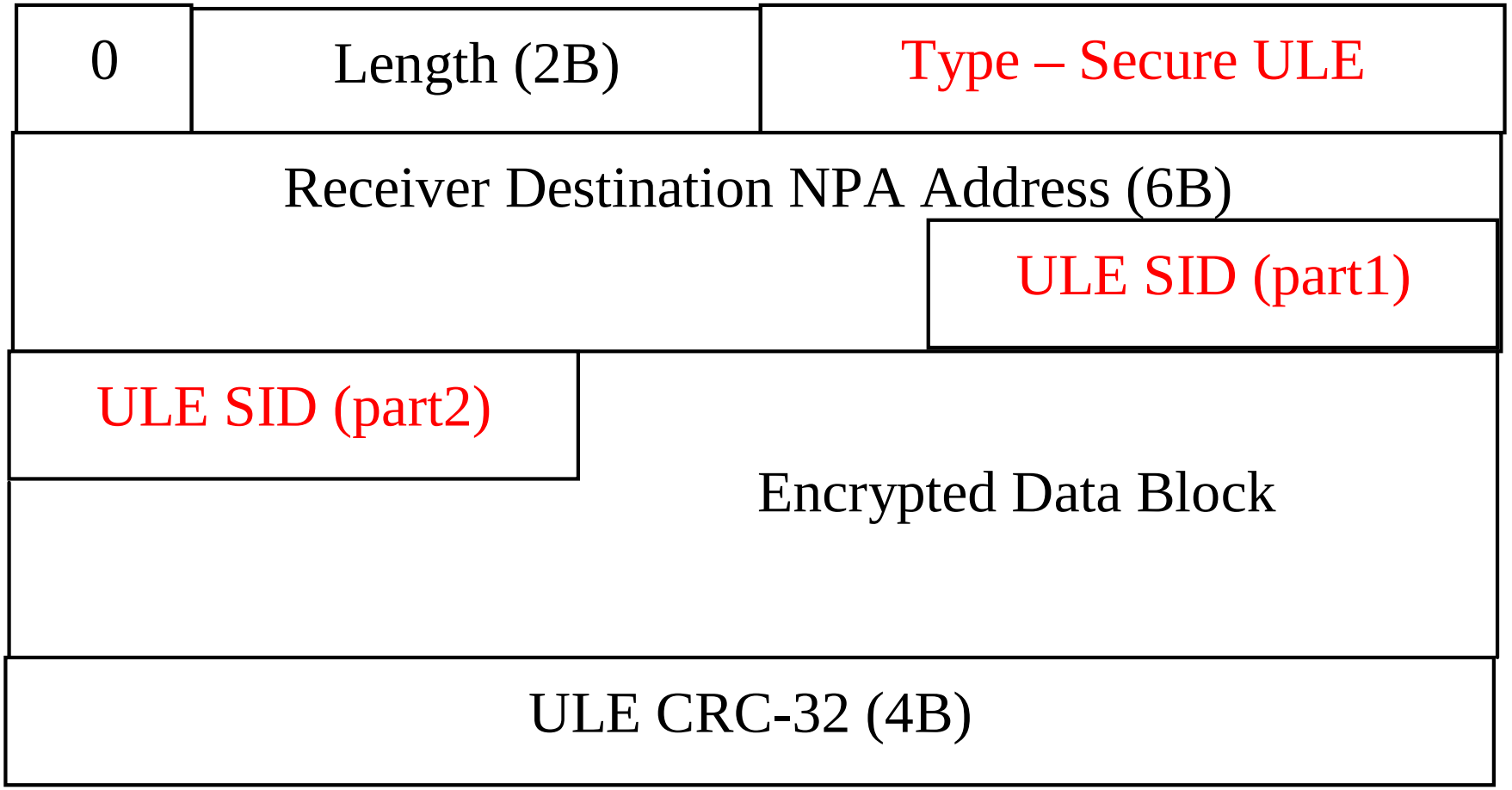
- A new ULE Mandatory Extension header for encryption:
  - The ULE Security IDentifier (ULE-SID) is a 32 bit value (similar to the IPsec SPI).
  - The ULE-SID can be used by a Receiver to filter PDUs in conjunction with the set of MAC/NPA addresses that it wishes to receive.
- Encryption algorithms, key lengths, etc. will be defined making use of the standard IPsec and msec suites.
- key space issue: The main aim of this document is to re-use existing techniques in IPsec architecture as defined in RFC 2401:
  - there is a need for at least two databases for security policy and association similar to the IPsec Security Policy Database (SPD) and Security Association Database (SAD).

ULE receiver identity hiding

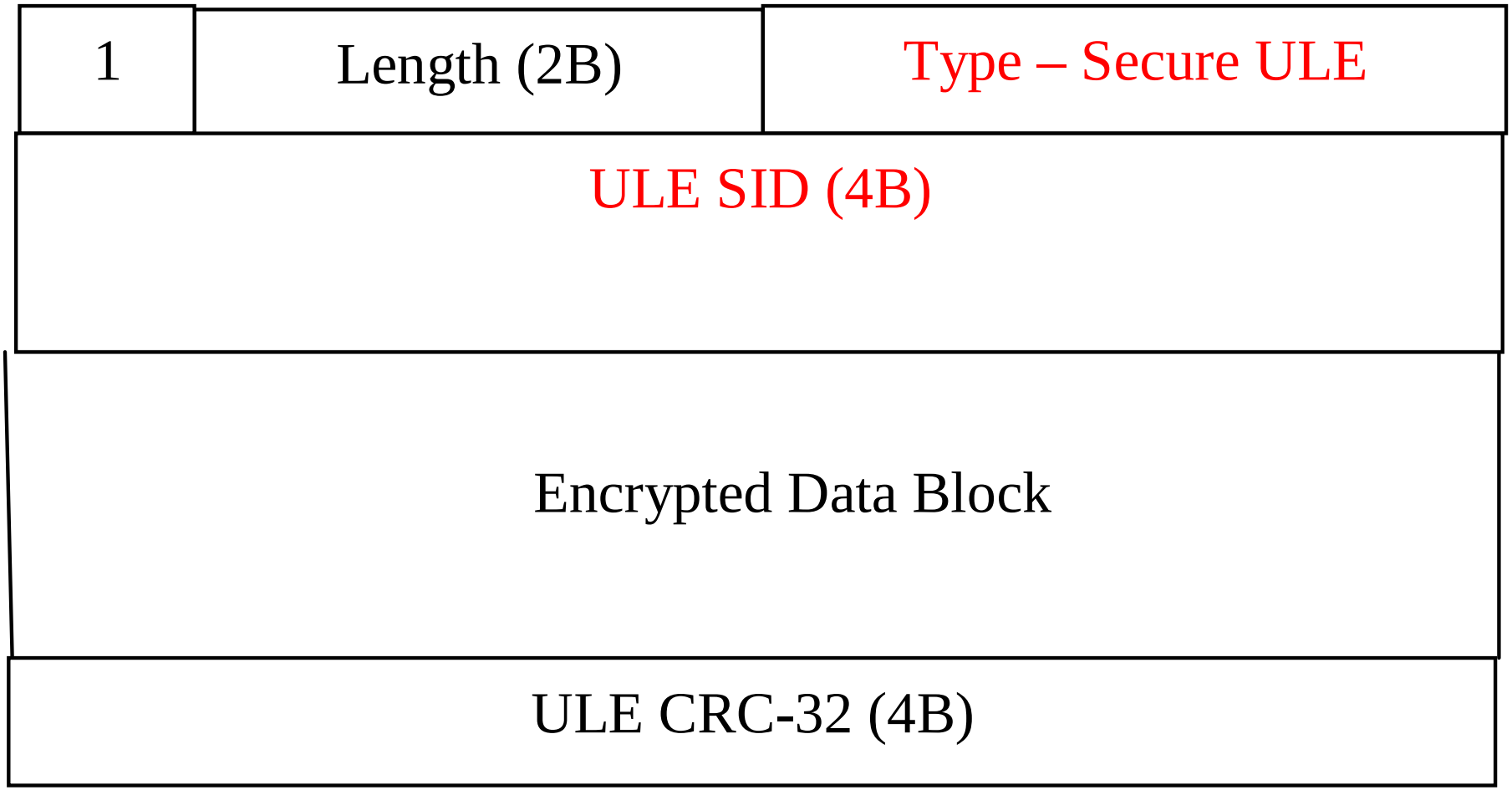
1. First option: We do not use any mac addresses:
   - We use ULE Security session ID for filtering. The D flag in ULE header is set 0.
   - This can ONLY work if the security session ID is unique in the ULE network:
     - Single global security manager that resides near the hub/gateway and controls all secure connections.
2. Second option: We use temporary mac address:
   - If Security session ID is not unique, then we use a temporary mac address for receiver identity hiding, Similar to mobile phones (GSM TMSI).
   - The temporary mac must be decoupled from the current security session and change very slowly and according to some security policy rules.

UniS

SNDU Format for Encryption Header (D=0)



SNDU Format for Encryption Header (D=1)



Future plans and next revision

- Encapsulator and Receiver detailed processing of the ULE security extension.
- Clarify any other comments or requests from from the ip-dvb WG.
- Distance future plans: University of Surrey would like to implement this draft ☺

Questions from IETF-62

What is it that is being protected? (**Security objectives**)

How does the **key management** relate to the link?
- How is the ID space managed?
- How do link and KM bind?

Are there any specific requirements on the **crypto algorithms** that can be used with this approach?

What are the threats? (**Threat analysis**)
Worked example (bits in actual packet sequences)
- E.g., how exactly is the decrypted payload parsed? Padding?

Why aren't we doing this with **existing mechanisms**?

Questions by Carsten Borman, IETF-62

7. IP Encaps for DVB-S.2

draft-cantillo-ipdvb-S2encaps-00.txt

Juan Cantillo (juan.cantillo@ensica.fr)
Jerome Lacan (jerome.lacan@ensica.fr)
Stephane Combes (Stephane.Combes@space.alcatel.fr)

(slides to follow)

Requirements for Transmission of IP Datagrams over DVB-S2

draft-cantillo-ipdvb-S2encaps-00.txt

Juan CANTILLO <juan.cantillo@ensica.fr>
Jérôme LACAN <jerome.lacan@ensica.fr>
Stéphane COMBES <stephane.combes@space.alcatel.fr>

DVB-S2 quick overview

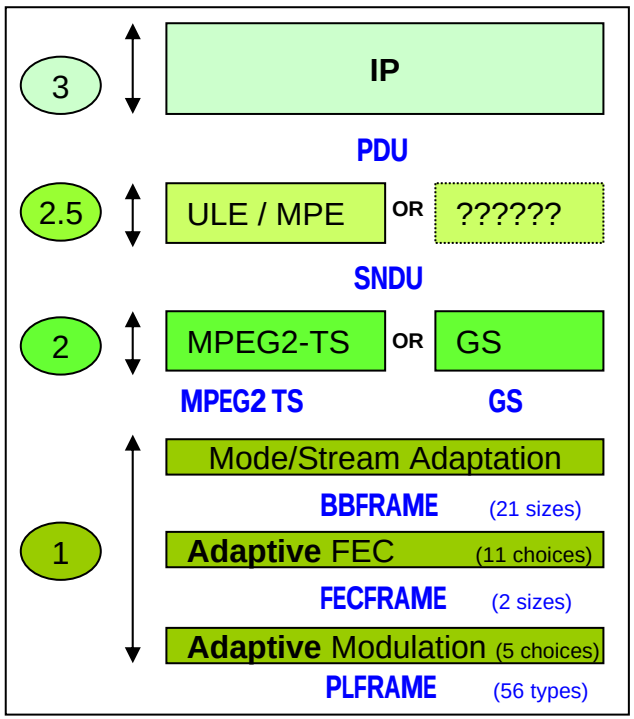
- ETSI 302 307: A new standard for video broadcast and IP distribution, meant to replace DVB-S within few years
  - *“70% of technology providers claimed they will design DVBS-2 compliant products in the next 36 months” (ESA, 2004)*

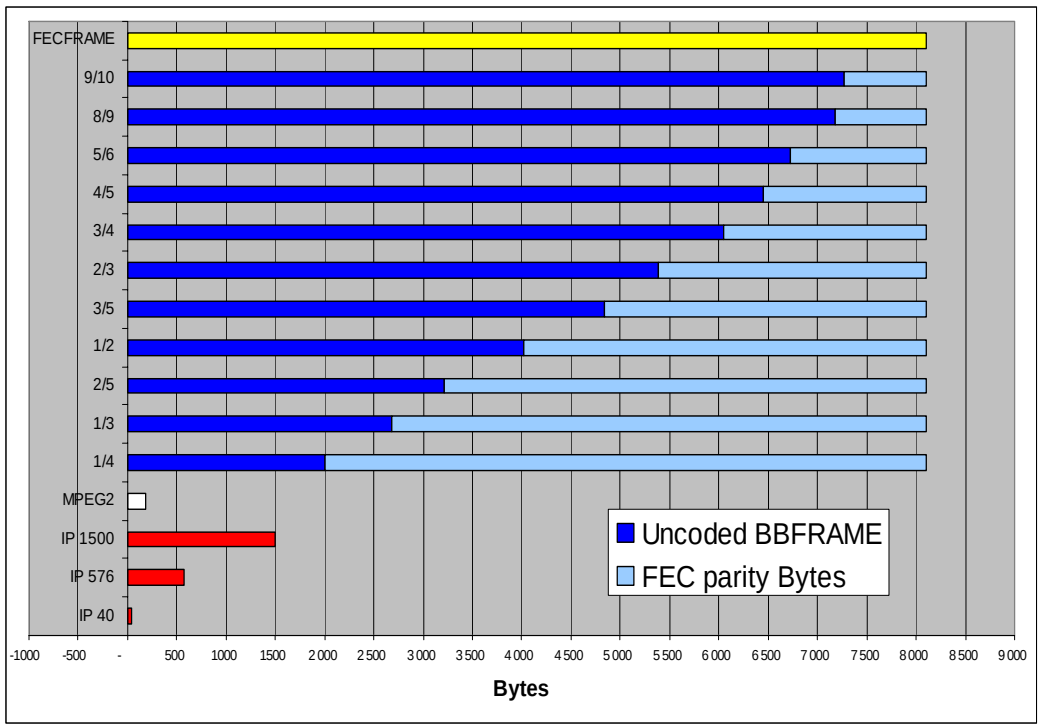
- 30% to 150 % increased throughput compared to DVB-S
  - ☑ *Higher order adaptive MODulations*
  - ☑ *Better and adaptive CODing*
  - ☑ *28 MOD-COD allowed combinations*

- DVBS-2 supports 2 kinds of input data: TS and GS
  - *MPEG2-TS : for legacy and inter-operability reasons*
  - *GENERIC STREAMS: packetized or continuous. “IP-FRIENDLY”*

DVB-S2 architecture and framing

- Uncoded BBFRAMES have variable sizes, between 382 and 7274 B





Generic Streams and IP in DVB-S2

- IP over TS/DVB-S2 with ULE (or MPE) possible
  - *However, ULE and MPE were designed for MPEG2-TS*
  - *constant TS end-to-end delay, bit-rate: not a must for IP services*
- GS designed for IP, but no standard adaptation layer exists yet
  - *If defined, TS layer avoided (less overhead & processing)*
  - *Adaptive & improved MOD-COD raises raises new questions*
- GS specificities motivate the definition of a new adaptation layer
  - *Larger IP fragments, even whole packets in a single BBFRAME*
  - *SAR less important than with DVB-S*
  - *FEC could do SAR error-detection*
  - *Adaptive Coding & Modulation*

Aspects of an adaptation layer for IP/GS/DVB-S2

- Scheduling issues : How to fill the BBFRAMES efficiently?
  - *Complexity vs. delay trade-off*
- Encapsulation issues:
  - *Solution 1 : 1 PDU ➔ 1 header*
  - *Solution 2 : 1 PDU fragment ➔ 1 header*
  - *Solution 3 : use the BBFRAME header*
- Segmentation And Reassembly issues :
  - *Solution 1 : 1 PDU ➔ 1 CRC*
  - *Solution 2 : do not use SAR*
  - *Solution 3 : use FEC and save CRC bytes*
- Security Addressing etc…

Conclusions

- DVB-S2 : a new standard that will replace DVB-S
  - *"DVB-S2 is so powerful that in the course of our lifetime, we will never need to design another system" (Alberto Morello, Chairman of the DVB-S2 TM)*
- Does the scope of the WG cover IP/DVB-S2 ?
  - *IP/DVB-S2 is the future of IP over satellite networks in the forward link*
  - *GS will replace MPEG2-TS for IP. ULE ? 2nd generation ULE?*
- Future work?
  - *Concerning the WG charter?*
  - *Concerning the I-D future ?*

9. Review of Milestones

WG Chair <gorry@erg.abdn.ac.uk>

IP over MPEG-2/DVB Transport (ip-dvb)

1. **Architecture/Requirements** (INFORMATIONAL) - DONE

2. **Encapsulation for MPEG-2 TS - ULE** (STANDARDS TRACK) DONE

3. **Address Resolution Mechanisms for IPv4/IPv6**
   (INFORMATIONAL) - Adopted

4. **Address Resolution Protocol(s)** (STANDARDS TRACK)
   Dynamic Unicast & Multicast - No adopted I-D

Milestones

Done Draft of a WG Architecture ID
Done Draft of a WG ID on Encapsulation (ULE)
Done Submit Architecture to IESG (for Nov 2004)

Done Draft of a WG ID on AR Framework
Done Submit Encapsulation to IESG

Feb 05 Draft of a WG ID on AR Protocol

Oct 05 Submit AR Framework to IESG

Dec 05 Submit AR Protocol to IESG
Dec 05 Progress ULE RFC along IETF Standards Track

Dec 05 Recharter or close WG?