IEEE 1722a
Version 1 headers
0.2

Dave Olsen
dave.olsen@harman.com
Version 1 Header

- Defines optional header extensions
  - Initially Signed Packet and Encrypted Packet
- A 1722a stream may contain 0 – 8 header extensions
- All packets in a stream shall use identical header extensions
- Header extensions shall always appear in a fixed order in the packet
- If no header extensions are used then streams shall use version 0 headers
- All future header extensions shall be quadlet based
- Add 8-bit field that is total number of quadlets in header extensions
Version 1 Header

Additional header and payload data
Header Extensions Detail

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>enc</td>
<td>sign</td>
<td>reserved</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

header_extensions
Version 1 Header with Extensions

| subtype data | 00 |
| SRP Stream ID | 04 |
| Header Extensions | 08 |
| 12 |
| 16 |

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 2 0 1 2 3 4 5 6 7 8 9 3 1

- subtype
- sv
- version
- type_specific_data
- stream_id
- reserved
- header_extensions
- header_extensions_length
- header_extension_0
- header_extension_1..6
- header_extension_7

Additional header and payload data
Encryption Header

Encryption Key ID

00
04

Magic Number

08
12
16

Random Data

random_data

EUI-64

magic_number

7/30/2012

IEEE 1722a Version 1 Header
Signed Packet Header

EUI-64

Signature

subtype data

Stream ID
Signed Packet Questions

• Signature includes all packet data from DA to end of packet not including the Ethernet CRC
• Do we need a trailer for Signed Packets?
• The packet signature should be at the end of the packets, especially if the packet is a data packet. Having to store the entire packet and then calculate the signature would increase latency.
Encrypted Packet Question

• Which sections of the packet are encrypted?
  – Magic Number
  – Random Number
  – StreamID (Stream ID needs to move to after header extensions)
  – Payload

• Do we need an encryption trailer to guarantee packet integrity?

• The encrypted payload should be a mapped block defined in the header_extensions bitmap. This would allow the sections of the packet to be arrange in the most reasonable manner.