HARMAN

HDCP IIA over 1722a Discussion

Version 3

Dave Olsen 8/13/2012

AKG by HARMAN harman/kardon by HARMAN Infinity by HARMAN JBL by HARMAN lexicon by HARMAN mark levinson by HARMAN

Sample Topology

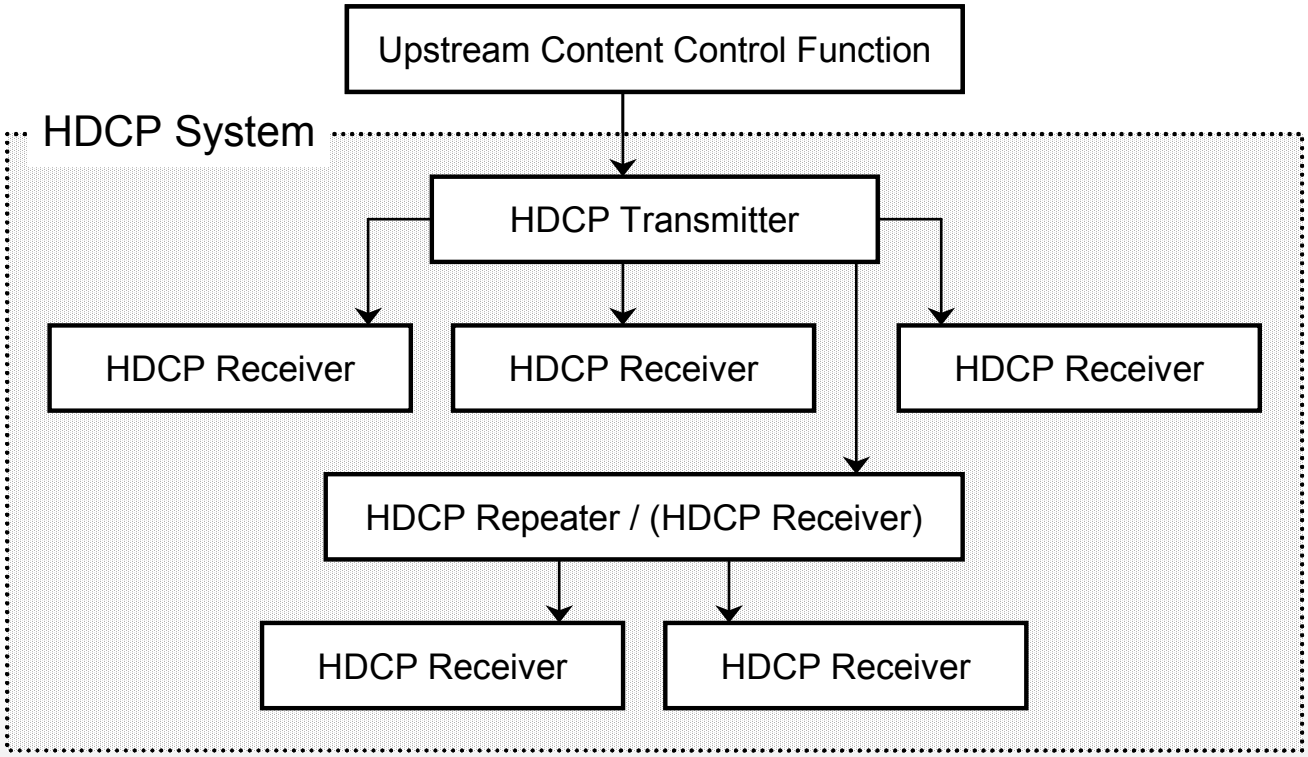


Figure 1.1. Sample Connection Topology of an HDCP System

Requirements

HARMAN

- **Authentication and Key Exchange (AKE) – The HDCP Receiver's public key certificate is verified by the HDCP Transmitter. A Master Key *km* is exchanged.**
- **Locality Check – The HDCP Transmitter enforces locality on the content by requiring that the Round Trip Time (RTT) between a pair of messages is not more than 7 ms.**
- **Session Key Exchange (SKE) – The HDCP Transmitter exchanges Session Key *ks* with the HDCP Receiver.**
- **Authentication with Repeaters – The step is performed by the HDCP Transmitter only with HDCP Repeaters. In this step, the repeater assembles downstream topology information and forwards it to the upstream HDCP Transmitter.**

Requirements

HARMAN

- A reliable, bidirectional packet protocol (e.g., TCP/IP) is used to transport messages used for the HDCP authentication protocol from the HDCP Transmitter to the HDCP Receiver, and vice versa.
- Each packet must contain exactly one message. Each packet payload commences with a msg_id specifying the message type, followed by parameters specific to each message.
- In the case of TCP/IP, packets use an IP address and port number determined by procedures above the HDCP layer.

Reliable Packet Protocol

HARMAN

- **AECP – AVDECC Enumeration Control Protocol**
  - Acknowledged Message Protocol
  - Will need a new message type
    - Can we reserve a type for this?
- **HDCP IIA max packet size is ~5000 bytes (see page 66 “System Renewability Message”)**
  - How does this fit with “each packet must contain exactly one message”
  - This will require a fragmentation message type in AECP
  - ACK and retry each fragment independently
    - This will require changes to 1722.1
    - We need a proposal quickly
    - For Draft 21 with would be needed in the next month, by 7/25/2012

Locality Check

HARMAN

- **Locality Check message should be sent on the same reliable transport as other messages**
  - No extra issues

Addressing

HARMAN

- **All AECP message are unicast**
- **Discovery will by ADP**
  - No extra issues

Other

HARMAN

The *integrity* of many values in the system is protected by fail-safe mechanisms of the protocol. Values that are not protected in this manner require active measures beyond the protocol to ensure integrity. Such values are noted in the table as requiring integrity. Core Functions must be implemented in Hardware.

What does this mean to be in Hardware?

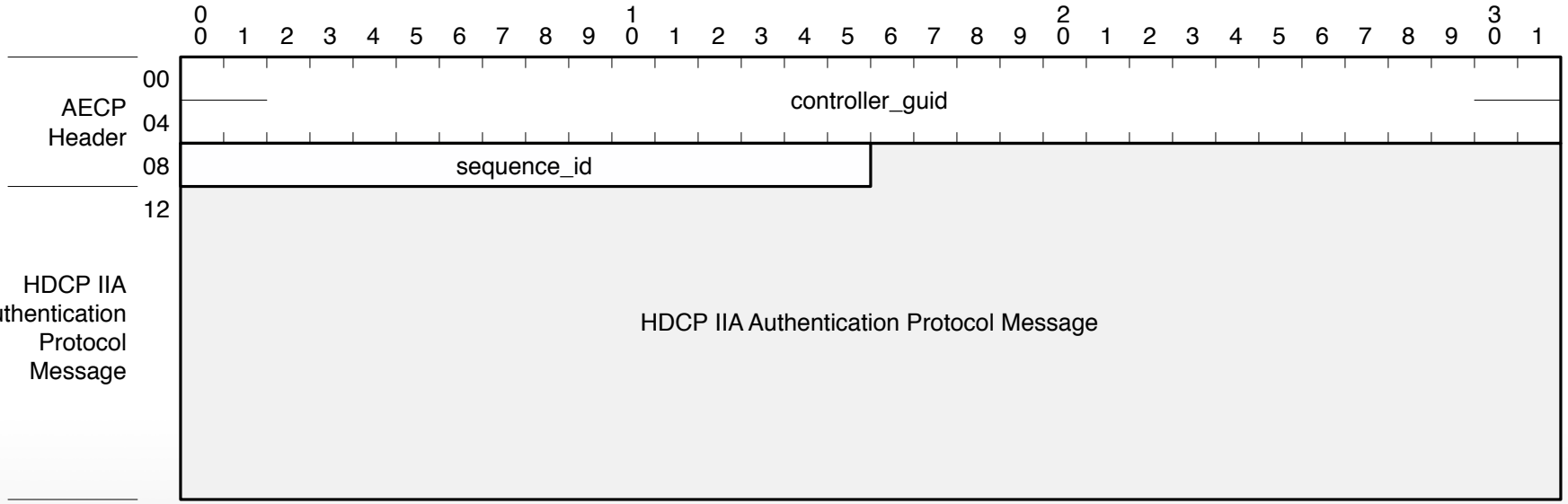
This is not a 1722a issue, but may be an issue for implementers.

HDCP IIA Packet Formats

Use AVDECC Enumeration and Control Protocol as defined in 9.2

HDCP IIA Authentication Protocol Messages are defined in HDCP IIA Section 4

NOTE: Add a 16-bit reserved field to align payload on 32-bit boundary



HDCP IIA Packet Formats

HARMAN

- **All fields are used as defined**
  - Target_guid
  - Controller_guid
  - Sequence_id
  - Message_type
  - NOTE: Need to request a command and response message type from 1722.1
- **Message_id is new HDCP Authentication Protocol Message/Response**
  - Need new entry in Table 9.1
  - Only valid responses to HDCP APM messages are
    - SUCCESS (packet received)
    - NOT_IMPLEMENTED (I don't support HDCP APM)
  - All other protocol transactions/errors/status are handled in APM
  - Are retries defined by AECP???? Retries are defined per message, so we need to define this for IIA

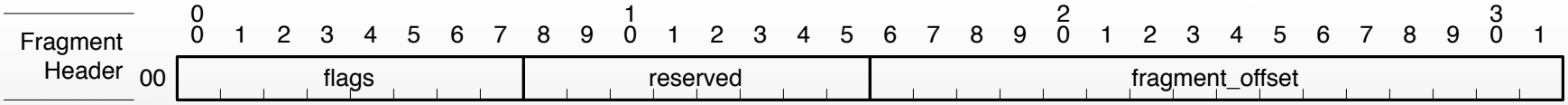
HDCP IIA Packet Formats

All HCDP APM packets use a version 1 Fragmentation Header to accommodate packet sizes greater than 1500 bytes.

NOTE: Max length of a 1722.1 packet is limited to 11-bits, but there is a SHALL for AECP that limits to 524 bytes.

Move fragmentation to the 1722.1 APM format header, remove fragmentation from the Version 1 header.

Shall we propose this as comment for 1722.1? Group feels that this should be proposed as a comment 1722.1



HDCP Packet transport

HARMAN

- HDCP defined stream data is transported in a transport stream
- Since AVTP supports transport streams no additional definition is needed.
- See http://grouper.ieee.org/groups/1722/contributions/1722a_Klaus-Wagenbrenner_PES_TS_sync_encryption.pdf

WHERE SOUND MATTERS

AKG by HARMAN
harman/kardon by HARMAN
Infinity by HARMAN
JBL by HARMAN
Lexicon by HARMAN
Mark Levinson by HARMAN