Network Working Group
Internet-Draft: draft-joetansey-alvc-schc-lpwan-00
Intended status: Experimental
Expires: February 27, 2026

Joe Tansey
Cisco

August 28, 2025

ALVC over LPWAN: SCHC Fragmentation, Priority, and Security

Abstract

This document specifies a transport profile for carrying the Adaptive
Layered Voice Codec (ALVC) over constrained Low-Power Wide-Area Networks (LPWANs) using Static Context Header Compression and fragmentation (SCHC). It defines an ALVC object model, fragment headers, priority scheduling, unequal error protection, receiver behavior, and a CoAP mapping supporting progressive playback under regional duty-cycle limitations.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working
documents as Internet-Drafts. The list of current Internet-Drafts is
at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months
and may be updated, replaced, or obsoleted by other documents at any
time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on February 27, 2026.

Table of Contents

1. Introduction

LPWAN links have small MTUs, long airtimes, and strict duty cycles, which make continuous audio streaming impractical. This profile defines the carriage of ALVC objects over LPWAN using SCHC fragmentation, enabling store-and-forward voice with early base-layer playback and progressive refinement. Gateways may cache fragments and perform store-and-forward across backhaul links with heterogeneous reliability and delay.

This document is a companion to the Adaptive Layered Voice Codec (ALVC) specification [ALVC-CODEC].

2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174].

3. ALVC Object Model

An ALVC Message comprises: optional Transcript, mandatory Layer-0, and zero or more Enhancement layers. Each layer is divided into fragments sized to the transport payload. Messages may arrive out of order. Gateways SHOULD prioritize Layer-0 recovery before enhancements.

4. ALVC Fragment Header

Each SCHC payload carrying ALVC includes an inner ALVC header with fields: MsgID, LayerID, Sequence number, Total fragments, TTL, Flags, and optional CRC16. Flags include BASE, ENH, FEC present, encrypted.

5. Priority and Scheduling

Priority order is Transcript (highest), then Layer-0, then Enhancements. Retransmissions SHOULD favor missing Layer-0 fragments.
Senders SHOULD emit a burst of early Layer-0 fragments to reach playable audio, then interleave enhancements in a deficit-round-robin manner. Gateways MAY reorder to favor base recovery.

6. Unequal Error Protection

Layer-0 SHOULD use stronger redundancy (for example, plus 20-30% parity) using Reed-Solomon or fountain codes. Enhancements MAY use reduced FEC or none. A MIC at the SCHC level is RECOMMENDED. Inner CRC16 is OPTIONAL when OSCORE is used.

7. Loss Handling and Parity Slicing

CRC-only detection is not sufficient. This profile specifies parity slicing for Layer-0 fragments using systematic FEC. Enhancements MAY use best-effort delivery with optional light FEC. Gateways MUST prioritize Layer-0 recovery over Enhancements. A header flag indicates when FEC is present.

8. Receiver Behavior and Progress Reporting

Receivers MUST permit early playback once all Layer-0 fragments for the initial window are received. Enhancement fragments MUST be applied idempotently. Progress MAY be reported as weighted completion across layers. Decoders SHOULD persist partial messages across reboots when permitted by policy.

9. CoAP and OSCORE Mapping

ALVC groups MAY be exposed as CoAP resources and transferred using Block-Wise over SCHC. OSCORE [RFC8613] provides confidentiality, integrity, and replay protection. Gateways SHOULD minimize metadata leakage by padding or batching transmissions where feasible.

10. Congestion Control and Duty-Cycle

Senders MUST respect regional duty-cycle rules. Gateways MAY throttle enhancement layers under congestion. ACK-on-Error for Layer-0 is RECOMMENDED to bound recovery latency without incurring per-fragment acknowledgments.

11. Parameter Sets

Example (informative): LoRaWAN SF10, payload 80 bytes. Layer-0 at 800 bps for 20 seconds requires about 25 fragments; one enhancement layer may require about 50 fragments. Total transfer time spreads over one to two minutes with duty-cycle limitations.

12. Security Considerations

Threats include spoofing, replay, and privacy leakage via transcripts.
Mitigations include OSCORE, AEAD, and transcript redaction policies.
Implementations MUST zeroize keys on gateway reboot and SHOULD use hardware-backed keystores.

13. Privacy Considerations

Voice content is sensitive. Systems SHOULD apply data minimization and retention limits. Transcript-only modes MAY be used where voice

is not required.

14. IANA Considerations

This document has no IANA actions.

15. Acknowledgments

Thanks to reviewers for feedback on SCHC operation and voice layering.

16. References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC8174] Leiba, B., "Ambiguity of Uppercase Key Words", BCP 14, RFC 8174, May 2017.

[RFC8724] Minaburo, A., et al., "SCHC for LPWAN", RFC 8724, April 2020.

[RFC9363] Minaburo, A., et al., "SCHC over LoRaWAN", RFC 9363, November 2022.

[RFC7252] Shelby, Z., et al., "The Constrained Application Protocol (CoAP)", RFC 7252, June 2014.

[RFC8613] Selander, G., et al., "Object Security for Constrained RESTful Environments (OSCORE)", RFC 8613, July 2019.

[ALVC-CODEC] Tansey, J., "Adaptive Layered Voice Codec (ALVC) for LPWAN Store-and-Forward", Internet-Draft, draft-joetansey-alvc-codec-00 (work in progress), August 2025.

Authors' Addresses

Joe Tansey
Cisco Systems
170 West Tasman Dr
San Jose, CA 95134
United States

Email: joetanse@cisco.com