Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 25 January 2026

A. Pelov
IMT Atlantique

24 July 2025

Secure ICMPv6 Messages for Network Segment Characterization
draft-pelov-icmpv6-sec-00

Abstract

This document proposes a new ICMPv6 message type, ICMPv6-SEC, designed to convey cryptographically verifiable information using COSE objects and CBOR-encoded certificates. The purpose is to signal segment-specific network characteristics, including high RTT, congestion, policy constraints, and traffic treatment expectations. These messages can describe either the segment beyond the current hop (forward segment) or the local segment on which the source resides. Certificates may be embedded or referenced via DNS using cryptographic hashes. The mechanism is optimized for high-speed environments by allowing the use of static, signed descriptors for destination prefixes.

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 25 January 2026.

Copyright Notice

Table of Contents

1. Introduction

ICMPv6 messages are a fundamental mechanism for communicating control and error information in IPv6 networks. However, existing ICMPv6 message types lack authentication and integrity protection. In high-latency, high-cost, or policy-constrained environments, this deficiency can lead to suboptimal or insecure behavior.

This document introduces ICMPv6-SEC, a new message type that carries a signed COSE object describing network segment characteristics. The signed message may include RTT metrics, availability windows, congestion indicators, traffic marking requirements, or access policies. Certificates for validation can be embedded or referenced via a cryptographic hash.

ICMPv6-SEC messages can describe either:

* The forward segment, i.e., a destination prefix or path region beyond the router issuing the message.

* The local segment, i.e., the link or network on which the sender resides.

The format allows for efficient signaling in high-throughput environments by enabling pre-signed, reusable descriptors.

2. Terminology

* ICMPv6-SEC: The new secure ICMPv6 message type.

* COSE: CBOR Object Signing and Encryption (RFC 8152).

* CBOR: Concise Binary Object Representation (RFC 8949).

* High-RTT Link: A link with round-trip times exceeding conventional internet norms, often seconds or more.

* DiffServ: Differentiated Services Code Points for QoS.

* SCHC: Static Context Header Compression (RFC 8724).

* Forward Segment: A portion of the path toward the packet’s destination.

* Local Segment: The network segment or link on which the sender is located.

* Segment Descriptor: A COSE-signed object describing characteristics of a network region.

3. Message Format

The ICMPv6-SEC message contains:

* Type: TBD (IANA-assigned)

* Code: Usage context (e.g., RTT alert, policy signal)

* Checksum: Standard ICMPv6 checksum

* Payload:

  - CBOR-encoded COSE_Sign1 object (segment descriptor)

  - Optional CBOR certificate

  - Optional SHA-256 certificate hash

  - Timestamp (UTC)

  - Validity duration (seconds)

3.1. Segment Descriptor Structure (CDDL)

```
SegmentDescriptor = {
  scope: "local" / "forward" / "bidirectional" / "pathset",
  prefix: bstr .size 16..32,        ; IPv6 prefix or null for local
  rtt: float32 / null,
  congestion: float32 / null,       ; 0.0 - 1.0 scale
  availability: [tstr, tstr] / null,
  energy-cost: float32 / null,
  marking-required: text / null,    ; e.g., "DSCP=AF42", "SCHC context_id=0xFF123AFF r
ule=3"
  valid-from: tstr,
  valid-to: tstr
}

ICMPv6-SEC = {
  type: uint,
  code: uint,
  cose: COSE_Sign1,
  cert: bstr / null,
  cert-hash: bstr / null,
  timestamp: tstr,
  valid-for: uint
}
```

4. Protocol Semantics

Routers MAY emit ICMPv6-SEC messages:

* Upon detecting misconfigured or non-compliant traffic.

* Proactively, in scheduled intervals.

* In response to discovery probes (see Section 11).

Messages SHOULD include a valid-for duration and timestamp to support caching and prevent replay.

5. Certificate Handling

Certificates used in COSE validation MAY be:

* Embedded directly in the message.

* Referenced via a SHA-256 hash, resolvable through DNS (e.g., a new RR type).

Validation MUST ensure the signature covers the SegmentDescriptor and was created within the claimed validity interval.

6. Host Processing

Receiving hosts MUST:

* Verify the COSE signature.

* Check certificate validity and freshness.

* Match the descriptor scope and prefix to applicable flows.

Hosts SHOULD cache descriptors during their validity window. If multiple descriptors apply to the same prefix with conflicting values, hosts MAY:

* Use the most recently received valid descriptor.

* Apply local policies to prefer descriptors from known routers.

7. Use Cases

7.1. Forward Segment Signaling

A router detects traffic targeting a high-latency or policy-restricted segment. It sends an ICMPv6-SEC message describing the destination prefix and the segment’s properties:

* Expected RTT and variability

* Required DSCP for admission

* Congestion likelihood

* Availability windows for scheduled access

This allows the source to modify behavior preemptively—e.g., adjust timers, enable SCHC, change DSCP.

7.2. Local Segment Signaling

Upon receiving unmarked or misbehaving traffic, a router informs the sender about its own segment characteristics. This may include:

* Policy zones (e.g., quarantine, guest LAN)

* MTU or RTT constraints

* Energy-saving schedule (e.g., LPWAN or time-slot radio)

Sources adapt stack behavior, fall back to compressed protocols, or prioritize retransmission paths accordingly.

8. Optimizations

8.1. Message Rate Limiting

Routers may:

* Emit ICMPv6-SEC no more than once per source/prefix/interval

* Embed timestamp + validity duration in message

* Cache descriptor transmission for repeated flows

8.2. Stateless or Semi-Stateful Generation

Routers MAY use pre-signed descriptors for common segments, eliminating signing on the data path. Stateless ICMPv6-SEC emissions remove per-flow computation burden.

8.3. Certificate Minimization

Compact CBOR-encoded certificates and DNSSEC-pinned hashes are RECOMMENDED to reduce overhead.

8.4. Static Signed Descriptions of Prefixes

For routers operating at high throughput, dynamic message signing can impose untenable computational demands. To address this, static signed segment descriptors can be pre-generated and associated with specific IPv6 prefixes (e.g., 2025:0711::/48). These descriptors can then be reused across all relevant flows without recalculating signatures in real-time. This approach enables highly efficient signaling while maintaining cryptographic integrity and temporal validity through timestamped metadata.

Key benefits of this method include:

* Scalability, by limiting cryptographic operations to a per-prefix basis;

* Efficiency, as it introduces negligible overhead into the data path;

* Security, through deterministic signature validation and replay protection using embedded validity intervals.

9. Segment Scope and Interpretation

Each segment descriptor includes a scope field:

* "local": The message describes the segment on which the sender resides

* "forward": The message describes the segment reachable through a next-hop or destination prefix

* "bidirectional": Characteristics apply in both directions (e.g., satellite relay)

* "pathset": The descriptor includes complex path behavior

Hosts can adjust behavior based on scope—e.g., ignore local metrics for routing but honor forward metrics for preemptive tuning.

10. Interaction with Transport and Application Stacks

ICMPv6-SEC feedback may inform:

* TCP/QUIC Congestion Control: RTT inputs for BBR/CUBIC, ECN calibration

* FEC/SCTP/QUIC Streaming: Adjust bitrate, redundancy, or loss recovery
* MPTCP/Multipath QUIC: Path selection based on segment scoring
* IoT/Embedded Systems: Activate SCHC, reduce keep-alives, etc.

11. Security Considerations

* Authenticity: COSE signatures ensure the source of the signal is verifiable.
* Replay Protection: Valid-from/to timestamps prevent stale reuse.
* Rate Control: Rate limiting and segment caching mitigate signal storms.
* Trust Anchor Management: Certificates should be anchored in DNSSEC or distributed securely.

12. Error Handling

Hosts encountering invalid ICMPv6-SEC messages MUST:

* Discard messages failing signature or validity checks.
* Ignore descriptors referencing unreachable or unverifiable certificates.
* Log or notify operators when encountering repeated failures.

13. IANA Considerations

* A new ICMPv6 message type is required for ICMPv6-SEC.
* A new DNS RR type may be needed to host CBOR-encoded certificates.

14. Future Extensions and Open Issues

14.1. Discovery Mechanism

A host may benefit from querying a router for segment descriptors before sending data. Defining an ICMPv6-SEC echo-request/response mechanism would support proactive policy discovery.

14.2. Certificate Revocation and Update

Mechanisms for revalidating or revoking stale descriptors should be specified. These might include TTLs, revocation flags, or integration with DNSSEC freshness mechanisms.

14.3. Multi-Segment Composition

Describing multiple consecutive segments in one message (via scope: pathset) could enable richer end-to-end context awareness.

14.4. Host Processing Behavior

Clarifying host behavior when receiving conflicting or overlapping descriptors (e.g., caching, priority rules) will help ensure deterministic reactions.

14.5. Trust Bootstrap

Mechanisms to securely distribute initial trust anchors for certificate validation remain an open area. DANE-based models or explicit OS provisioning could be defined.

14.6. Legacy Interoperability

Backward-compatible signaling options (e.g., signed Redirects or DHCP hints) may help inform endpoints without ICMPv6-SEC support.

14.7. Routing and SDN Interfaces

Defining controller interfaces (e.g., YANG modules) for injecting or updating segment descriptors in routers may improve operational scalability.

15. Relevance to the TIPTOP Working Group

The TIPTOP (Taking IP To Other Planets) Working Group at the IETF focuses on enabling IP networking to operate across interplanetary distances. This includes coping with extreme delay, high error rates, intermittent connectivity, and significant asymmetry in network paths. ICMPv6-SEC aligns directly with TIPTOP’s goals by offering a cryptographically verifiable signaling mechanism capable of conveying segment characteristics crucial for deep-space communication scenarios.

ICMPv6-SEC contributes to TIPTOP by enabling:

* Segment-based control-plane signaling that informs endpoints about high-delay links, expected RTT, admission control policies, and availability.

* Resilient and reusable communication of policy and operational constraints through static, long-lived, signed segment descriptors.

* Low-interaction overhead using unidirectional signaling that does not rely on full protocol negotiation.

This mechanism supports scenarios such as:

* Signaling when a destination prefix lies beyond a deep-space relay.

* Informing mobile or orbital systems of local LAN constraints (e.g., power, duty-cycle, or congestion sensitivity).

* Notifying endpoints that specific packet markings or behaviors are required to gain access to scheduled or policy-restricted interplanetary links.

By supporting both "local" and "forward" segment scopes, and providing deterministic, verifiable metadata, ICMPv6-SEC integrates naturally into TIPTOP architectures.

16. Normative References

[RFC4443] Conta, A., Deering, S., and M. Gupta, Ed., "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", STD 89, RFC 4443, DOI 10.17487/RFC4443, March 2006, <https://www.rfc-editor.org/info/rfc4443>.

[RFC8152] Schaad, J., "CBOR Object Signing and Encryption (COSE)", RFC 8152, DOI 10.17487/RFC8152, July 2017, <https://www.rfc-editor.org/info/rfc8152>.

[RFC8610] Birkholz, H., Vigano, C., and C. Bormann, "Concise Data Definition Language (CDDL): A Notational Convention to Express Concise Binary Object Representation (CBOR) and JSON Data Structures", RFC 8610, DOI 10.17487/RFC8610, June 2019, <https://www.rfc-editor.org/info/rfc8610>.

[RFC8724] Minaburo, A., Toutain, L., Gomez, C., Barthel, D., and JC. Zuniga, "SCHC: Generic Framework for Static Context Header Compression and Fragmentation", RFC 8724, DOI 10.17487/RFC8724, April 2020, <https://www.rfc-editor.org/info/rfc8724>.

[RFC8949] Bormann, C. and P. Hoffman, "Concise Binary Object Representation (CBOR)", STD 94, RFC 8949, DOI 10.17487/RFC8949, December 2020, <https://www.rfc-editor.org/info/rfc8949>.

Author’s Address

Alexander Pelov
IMT Atlantique
2bis rue de la Chataigneraie
35536 Cesson-Svign
France
Email: alexander.pelov@imt-atlantique.fr