Standard Communication with Network Elements
Internet-Draft
Intended status: Informational
Expires: 10 May 2026

S. Mishra
Verizon
Z. Sarker
Nokia
A. Tomar
Meta
K. Abbas
Verizon

6 November 2025

Applicability & Manageability Considerations for SCONE
draft-ietf-scone-applicability-manageability-00

Abstract

This document describes the Applicability and Manageability considerations for providing throughput guidance to application endpoints. This guidance is specifically addressed within the context of telecommunications service provider networks utilizing the Standard Communication with Network Elements (SCONE) protocol.

Discussion Venues

This note is to be removed before publishing as an RFC.

Discussion of this document takes place on the Standard Communication with Network Elements Working Group mailing list (scone@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/scone.

Source for this draft and an issue tracker can be found at https://github.com/ietf-wg-scone/appman.

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 10 May 2026.

Table of Contents

1. Introduction

The SCONE protocol [I-D.ietf-scone-protocol] provides a signaling mechanism that enables on-path SCONE-capable Network Elements to communicate the advisory maximum allowable bit rate to application endpoints, which is particularly relevant for adaptive bit-rate applications. This document addresses the Applicability and Manageability considerations for deploying the SCONE protocol within telecommunications service provider networks.

SCONE operates based on a UDP 4-tuple. Network Elements capable of rate limiting at this granularity can send notifications of the advisory maximum allowable bit rate in each direction of the observed traffic. Such Network Elements may also drop or delay packets within the corresponding UDP 4-tuple flows. This implies that on-path SCONE-capable Network Elements (referred to as SCONE Network Elements in the rest of this document) are assumed to have the following capabilities: detect and maintain UDP 4-tuple flows, be aware of or configurable with rate-limiting policies, and identify flows that carry SCONE packets in order to insert throughput advice into those packets.

In this document, on-path SCONE Network Elements are generally considered within the _access_ portion of the Telecommunications provider’s network. However, multiple SCONE Network Elements may exist along a path between the communicating peers. Depending on their configuration and roles they are likely to generate different throughput advices for the SCONE enabled application traffic flows, especially when different _access_ technologies are in use. For example, the SCONE protocol in a wireless access network element may operate differently from one in a fixed broadband network. Wi-Fi networks provide another example, where enforcement is often per user or per Service Set Identifier (SSID), but visibility into individual UDP 4-tuples may be limited. Among access networks, mobile networks offer the most fine-grained visibility into traffic flows and can act on individual flows. For example, in mobile networks, the User Plane Function (UPF) in 5G [_5G-Arch] and the Packet Data Network Gateway (P-GW) in 4G [_4G-Arch] can generate throughput advice to guide adaptive bit-rates applications on a per-flow basis. In contrast, wireline broadband networks typically apply rate limiting at a centralized Broadband Network Gateway (BNG) or at aggregation points serving multiple Customer Premises Equipment (CPE) devices.

Accordingly, Applicability and Manageability considerations must encompass a wide range of access-network scenarios, each of which handles per-flow rate limiting differently. However, the scope of this document is limited to discussing the core Applicability and Manageability considerations for the SCONE protocol.

2. Terms and Definitions

This document uses terms and definitions described in [I-D.ietf-scone-protocol].

3. Applicability and Manageability Considerations

3.1. Flow session awareness

SCONE signaling operates only over established sessions. SCONE Network Elements ought to be able to unambiguously associate throughput advice with application flows. Each session is bound to an IP address and port, ensuring SCONE packets are routed precisely without affecting unrelated traffic.

3.2. Per-Flow Signaling

Throughput advice is applied on a UDP 4-tuple basis. SCONE Network Elements ought to maintain flow-specific context to ensure signaling correctness. This enables applications to receive targeted throughput advice while preventing unintended impact on unrelated flows.

3.3. QoS awareness

Quality of Service (QoS) may be enforced by networks through a variety of mechanisms. In certain deployments, network operators may choose to apply distinct QoS policies to SCONE-enabled flows. The SCONE Network Element responsible for inserting SCONE advice is not required to interpret or enforce QoS policies; its role is limited to the signaling of the advisory throughput information. It is expected that network operators shall be able to identify SCONE-enabled flows and, where appropriate, provide throughput advice in accordance to their policy objectives.

3.4. SCONE Hint to the Network

SCONE-aware applications ought to provide hints to the SCONE Network Elements, enabling it to generate appropriate throughput advice for a given UDP 4-tuple. Such hints prevent unnecessary default rate-limiting, allow the network to signal the maximum allowable bit rate, and reduce CPU overhead by eliminating additional classification steps.

3.5. Retransmission of Advised Bit-Rate

Packet loss or non-delivery of SCONE advice reduces its effectiveness. Both SCONE Network Elements and application endpoints should support retransmission or periodic re-sending of SCONE packets to ensure reliable delivery. Conformance depends on the behavior of both network and application endpoint.

3.6. Frequency of Updates

The rate at which SCONE updates are issued depends on flow characteristics and available computational resources. Excessively frequent updates may increase CPU load, while infrequent updates may reduce advisory effectiveness. Network Operators can define adjustable update intervals based on application requirements, network capacity, and operational constraints.

3.7. Dynamic Updates

Dynamic rate limits updates can be enforced by the network during active application sessions due to:

* Changes in access network type (requiring updated throughput advice)

* Changes in Subscriber policy (e.g., exceeding usage thresholds)

In such cases, the SCONE Network Elements need to be able to initiate SCONE packets to provide updated advice, or applications should generate SCONE packets frequently enough to trigger network responses.

3.8. Monitoring and Logging

SCONE signaling can be integrated into existing operational and management frameworks to enable monitoring, troubleshooting, and fault isolation. Metrics of interest include:

* Rate of SCONE advisory messages issued per session

* Correlation between SCONE advisories and user-plane throughput changes

* Error conditions where SCONE signaling fails to reach the intended endpoints

3.9. Conformance Monitoring

Networks providing SCONE throughput advice ought to implement mechanisms to measure compliance, either per application flow or in aggregate. This allows operators to validate advisory effectiveness and adjust policies. Due to flow awareness, such mechanisms are typically implemented in a SCONE Network Element but may also be implemented elsewhere in the network.

3.10. Standards Compliance

SCONE signaling is expected to traverse the existing data path associated with the UDP 4-tuple flow for which the Network Element intends to send the advisory bit-rate.

3.11. Interworking with Other Congestion Management Mechanisms

SCONE operates independently of transport-layer mechanisms such as Explicit Congestion Notification (ECN) or Low Latency, Low Loss, and Scalable throughput (L4S). Operators would benefit from harmonizing multiple congestion signaling methods by policy or scope deployments to manage conflicting feedback.

4. Security Considerations

Security considerations are included separately in the SCONE protocol documents.

5. IANA Considerations

This document has no IANA actions.

References

References

Normative References

[I-D.ietf-scone-protocol]
Thomson, M., Huitema, C., Oku, K., Joras, M., and M. Ihlar, "Standard Communication with Network Elements (SCONE) Protocol", Internet-Draft, draft-ietf-scone-protocol, Work in Progress , July 2025, <https://datatracker.ietf.org/doc/draft-ietf-scone-protocol/>.

Informative References

[_4G-Arch] 3GPP, "System Architecture for the Evolved Packet Core (EPC)", 1 June 2020, <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=24300>.

[_5G-Arch] 3GPP, "System Architecture for the 5G System (5GS)", 7 January 2025, <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144>.

Acknowledgments

The authors thank Wesley Eddy, Renjie Tang, Kevin Smith, Tina Tsou, Tianji Jiang, Lucas Pardue, and Martin Thomson for their helpful comments and contributions to this document. The authors also thank members of the SCONE Working Group for their review and support throughout the development of this document.

Authors' Addresses

Sanjay Mishra
Verizon
Email: sanjay.mishra@verizon.com

Zaheduzzaman Sarker
Nokia
Email: zaheduzzaman.sarker@nokia.com

Anoop Tomar
Meta
Email: anooptomar@meta.com

Khurram Abbas
Verizon
Email: khurram.abbas@verizonwireless.com