SCONE
Internet-Draft
Intended status: Informational
Expires: 31 July 2026

S. Gundavelli
M. Grayson
Cisco Systems
J. Redmore
CableLabs
J. Padden
Nova Labs

27 January 2026

SCONE Applicability for IEEE 802.11 Access Networks
draft-gundavelli-scone-wifi-applicability-00

Abstract

This document describes the applicability of the Standard Communication with Network Elements (SCONE) protocol to IEEE 802.11 based access networks. SCONE defines a mechanism by which an on-path network element can provide advisory downlink throughput guidance to QUIC endpoints. The SCONE protocol is access agnostic and does not assume any specific access technology.

In IEEE 802.11 deployments, such constraints may be derived at access points or controllers that combine policy awareness, with visibility into access network conditions. This document explains how existing SCONE roles and throughput advice semantics apply in these deployments without assuming any specific IEEE 802.11 MAC or PHY behavior.

This document does not define new protocol extensions and does not modify SCONE behavior. Its purpose is to clarify deployment considerations for IEEE 802.11 environments.

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 31 July 2026.

Table of Contents

1. Introduction

SCONE [I-D.ietf-scone-protocol] provides a mechanism for on-path network elements to convey advisory uplink throughput guidance to QUIC [RFC9000] endpoints. The guidance reflects throughput constraints that apply along the network path. SCONE is access agnostic and does not assume any specific access technology.

IEEE 802.11 [IEEE80211-2024] access networks are widely deployed across enterprise, residential, and public hotspots. In these networks, throughput constraints may arise from administrative policy or service differentiation and may be applied at different points in

the access network, including access points, wireless controllers, or gateways. These characteristics motivate an applicability discussion for IEEE 802.11, without altering the access-agnostic design of SCONE.

In enterprise IEEE 802.11 deployments, throughput constraints are commonly derived from subscriber, device, or service policy conveyed through Authentication, Authorization, and Accounting (AAA) systems over RADIUS protocol ([RFC2865]). Access points or controllers enforce such policies as part of the session management function in the access network. SCONE can be used in these environments to expose the resulting throughput guidance to QUIC endpoints, without assuming or relying on IEEE 802.11 MAC or PHY behavior.

This document describes how existing SCONE roles and throughput advice semantics apply to common IEEE 802.11 deployment models. It does not define new protocol behavior and does not specify how throughput constraints are derived or enforced within the access network.

1.1. 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] when, and only when, they appear in all capitals, as shown here.

1.2. Terminology

All the terms used in this document are to be interpreted as defined in the IETF SCONE [I-D.ietf-scone-protocol], QUIC [RFC9000] and IEEE 802.11 [IEEE80211-2024] specifications. For convenience, the definitions for some of the terms are provided below.

STA (Station) - IEEE 802.11 Station

AP (Access Point) - IEEE 802.11 Access Point

AAA - Authentication, Authorization and Accounting

2. IEEE 802.11 Deployment Models and Policy Considerations

IEEE 802.11 access networks are commonly deployed based on two dominant architectural models, distinguished by whether control and policy functions are distributed at the access point or centralized in a controller. While implementations vary, most deployments follow one of these two approaches. In addition, many deployments use cloud-managed systems to host configuration, monitoring, and policy distribution functions outside the local network. These management systems typically do not participate directly in data forwarding.

In all deployment models, AAA systems are commonly used to host network credentials and policy elements that influence access and service treatment. These systems provide a consistent source of policy configuration, regardless of whether enforcement is applied locally at the access point, centrally at a controller, or based on configuration distributed through cloud-managed systems. In smaller or less complex deployments, policy and credential information is configured locally on the access point or controller without the use of an external AAA system.

The following subsections describe these deployment models and identify where SCONE network element functionality may reside.

2.1. Distributed Access Point Deployment

In the distributed access point deployment model, the IEEE 802.11 Access Point (AP) performs radio termination, policy enforcement, and local data forwarding, without a centralized controller in the data path. This model is commonly used in residential networks, small enterprises, and branch deployments.

Authentication and authorization are performed during association using standard IEEE 802.11 mechanisms. Policy information may be conveyed to the AP through a AAA system over RADIUS protocol, or configured locally in these deployments. Based on these interfaces, the AP applies policy for the associated station.

Throughput constraints in this model are enforced directly at the AP. When such constraints are applied, the AP functions as an on-path network element capable of exposing advisory throughput guidance using SCONE for flows traversing the access network.

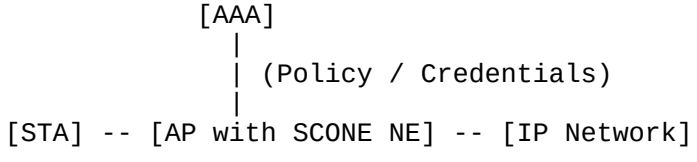

Figure 1: Distributed Access Point Deployment with SCONE Network Element

2.2. Centralized Controller-Based Deployment

In the centralized controller-based deployment model, the Access Points operate under the control of a wireless controller that performs centralized coordination and policy control across multiple APs. Data forwarding may be centralized at the controller or distributed at the APs, depending on deployment design, while policy decisions are typically made centrally. Authentication and authorization are commonly handled through centralized interaction with AAA system. Policy information obtained during authorization is applied consistently across APs serving the associated station. This model is widely used in enterprise and campus environments where centralized policy control and mobility management are required.

Throughput constraints in this model may be enforced either at the controller or at the access points under controller direction. The SCONE network element function resides at the point in the data path where such constraints are applied. In deployments where enforcement remains local to the access point, SCONE placement is similar to the distributed access point model described in Section 2.1.

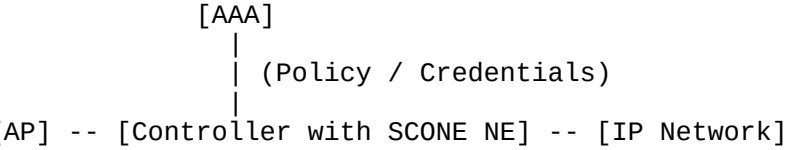

Figure 2: Centralized Controller-Based Deployment with SCONE Network Element

2.3. Cloud-Managed Deployment

In cloud-managed deployments, the Access Points are configured and monitored using a remote management system hosted outside the local access network. These systems provide centralized configuration and monitoring functions, while data forwarding remains within the local network. The cloud management system does not participate in data forwarding or SCONE signaling. However, it can interwork with the SCONE NE on rate guidance estimates.

Authentication and authorization are commonly performed using AAA systems, with policy information conveyed either directly to the access points or through configuration distributed by the cloud management system. In smaller deployments, equivalent policy information may be configured locally.

Throughput constraints in this model are enforced locally at the access point. When such constraints are applied, the access point represents the on-path network element capable of exposing advisory throughput guidance using SCONE.

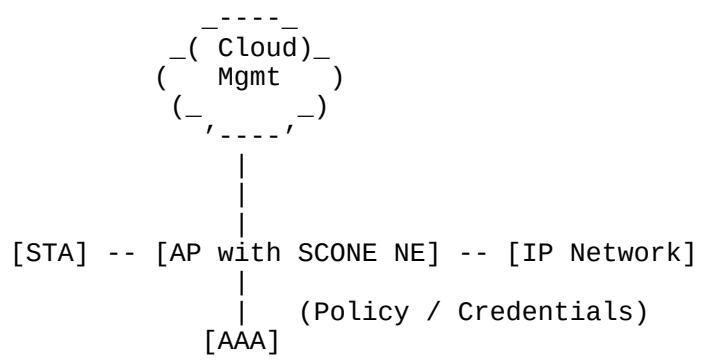

Figure 3: Cloud-Managed Deployment and SCONE Placement

2.4. Policy Based Throughput Constraints

Many enterprise and service-provider Wi-Fi deployments rely on AAA infrastructure for policy and authentication, commonly using RADIUS. During authentication, the access point or controller acts as an AAA client and may receive authorization attributes that override locally configured WLAN policy.

AAA-based policy mechanisms are commonly used to convey per-user parameters such as maximum uplink and downlink throughput, traffic shaping or policing profiles, session duration limits, or QoS classification. These parameters reflect administrative or subscription-based policy and are enforced by the access point or controller.

While no standardized AAA attribute defines per-user Wi-Fi throughput, vendor-specific attributes are widely deployed to convey bandwidth limits or rate profiles. Despite differences in representation, these attributes share a common semantic meaning: a bounded, policy-defined sustainable throughput for a user session.

When such policy-based throughput constraints are enforced in the data path, SCONE signaling may be used to expose corresponding advisory throughput guidance to endpoints. SCONE reflects the outcome of applied policy without exposing AAA attributes, policy rules, or authentication state.

3. IEEE 802.11 Specific Implementation Considerations

In IEEE 802.11 deployments, the access point is the enforcement point for access policy and traffic treatment. As part of normal operation, the access point has continuous visibility into activity within its Basic Service Set (BSS), covering both uplink and downlink transmissions for associated stations. This visibility is intrinsic to IEEE 802.11 operation and is independent of higher-layer protocols.

The access point maintains access-local operational context related to the shared wireless medium and connected stations. This context may include, but is not limited to:

* PHY Rate (MCS Index)

* Channel Load

* Queue Backlog (Buffer Status)

* Packet Error Rate (PER) / Retries

* Station Signal Strength (SNR/RSSI)

* Active Contending Stations

Such information is maintained to support normal access network operation and enforcement and does not require any SCONE-specific functionality.

In practice, access points may use this access-local context, together with subscription-based policy, to determine throughput constraints that can be sustainably enforced. These determinations may vary over time due to changes in the active station set, mobility, interference, or traffic patterns.

This document does not specify how throughput constraints are determined and does not require the use of any particular IEEE 802.11 parameters or estimation techniques. When SCONE is used in an IEEE 802.11 deployment, the SCONE Network Element exposes advisory throughput guidance that reflects the outcome of air interface and policy conditions

3.1. Inter Access Point Handovers

In IEEE 802.11 deployments, stations may move between access points due to mobility, radio conditions, or load management. When a station transitions to a new access point, the data path for active flows also moves. Since SCONE throughput guidance reflects locally enforced constraints and is carried in-band, continuity of guidance across access point transitions is desirable to avoid extended gaps in updates. Each access point independently observes its local radio and network conditions and can generate SCONE throughput guidance based on locally applied policy and enforcement. After a transition, the new access point can generate updated guidance that reflects its own conditions.

In many deployments, a limited amount of per-station context is transferred between access points or coordinated through a controller during mobility events. This context may include policy or enforcement-related information. Where such context is available, it may be used by the new access point to initialize SCONE-related state for ongoing sessions and reduce delay before updated guidance is provided.

This document does not require access points to exchange per-flow SCONE timers or define any specific state transfer mechanism. SCONE guidance remains advisory, and endpoints are expected to tolerate brief changes or gaps in guidance following mobility events. The generation and update of SCONE throughput guidance after a transition remains a local decision at the new access point.

4. IANA Considerations

This document does not define any new protocol mechanisms, or require any registry updates. Therefore, it does not require any IANA actions.

5. Security Considerations

This document does not define new protocol mechanisms and does not introduce new threats beyond those described in the SCONE protocol specification.

SCONE capability is negotiated end to end between QUIC endpoints using SCONE protocol elements. After negotiation, throughput advice values carried in SCONE packets may be inserted, updated, or removed by on path network elements. The throughput advice value is not authenticated, and endpoints cannot guarantee that a received value was inserted by a particular on-path network element.

In IEEE 802.11 deployments, throughput constraints may reflect policy-based configuration, including policies informed by Authentication, Authorization, and Accounting (AAA) systems over RADIUS protocol . This document does not require exposure of AAA attributes, authentication state, or other sensitive policy information to endpoints explicitly.

Exposing throughput constraints through SCONE to an endpoint can reveal limited information about network policy or service differentiation through inference. This disclosure risk is inherent to SCONE signaling and is not specific to IEEE 802.11 deployments. Operators should consider the granularity and update frequency of throughput advice to limit unnecessary exposure. Endpoints are free to ignore advice they consider incorrect or inappropriate.

6. Acknowledgements

Thanks to Marting Thompson for reviewing this document and providing some review feedback. Also, thanks to the discussions in Wireless Broadband Alliance on the use of SCONE for Wi-Fi environments.

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[I-D.ietf-scone-protocol] Thomson, M., Huitema, C., Oku, K., Joras, M., and L. M. Ihlar, "Standard Communication with Network Elements (SCONE) Protocol", Work in Progress, Internet-Draft, draft-ietf-scone-protocol-04, 14 December 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-scone-protocol-04>.

7.2. Informative References

[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, DOI 10.17487/RFC2865, June 2000, <https://www.rfc-editor.org/rfc/rfc2865>.

[RFC9000] Iyengar, J., Ed. and M. Thomson, Ed., "QUIC: A UDP-Based Multiplexed and Secure Transport", RFC 9000, DOI 10.17487/RFC9000, May 2021, <https://www.rfc-editor.org/rfc/rfc9000>.

[IEEE80211-2024] IEEE, "IEEE Standard for Information Technology— Telecommunications and Information Exchange between Systems— Local and Metropolitan Area Networks— Specific Requirements— Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", IEEE Std 802.11-2024, 28 April 2025, <https://standards.ieee.org/ieee/802.11/10548/>.

Authors' Addresses

Sri Gundavelli
Cisco Systems
510 McCarthy Blvd
Milpitas, CA 95035
United States of America
Email: sgundave@cisco.com

Mark Grayson
Cisco Systems
10 New Square Park
Feltham
TW14 8HA
United Kingdom
Email: mgrayson@cisco.com

Joshua Redmore
CableLabs
858 Coal Creek Cr.
Louisville, 80027
United States of America
Email: j.redmore@cablelabs.com

Joey Padden
Nova Labs
Boulder, Colorado
United States of America
Email: jpadden@nova-labs.com