RADEXT Working Group
Internet-Draft
Intended status: Standards Track
Expires: 1 November 2026
P. Seralathan
L. Mukund
Cisco Systems
A. Milton
Hewlett Packard Enterprise (HPE)
30 April 2026

RADIUS Attribute for Persistent Device Identity in MAC-Randomized Environments

draft-seralathan-radext-persistent-devid-00

Abstract

This document defines a new RADIUS attribute, Persistent-Device-Id, that enables Network Access Control (NAC) systems to maintain a stable device identity across Media Access Control (MAC) address changes. Modern operating systems randomize MAC addresses by default, disrupting RADIUS-based authentication, authorization, and accounting workflows that rely on the Calling-Station-Id attribute as a persistent device identifier. The Persistent-Device-Id attribute carries a Globally Unique Identifier (GUID) in RADIUS Access-Accept and Accounting-Request messages, providing a stable correlation key for device profiling, policy enforcement, and regulatory compliance. This document specifies the attribute format, assignment procedures, and usage guidelines for RADIUS clients and servers..

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

The RADIUS protocol [RFC2865] uses the Calling-Station-Id attribute (Type 31) to carry the Media Access Control (MAC) address of the connecting device. This attribute serves as the de facto device identifier in Network Access Control (NAC) deployments, used for device identification, profiling, policy assignment, license counting, and regulatory audit trails.

MAC address randomization as a privacy feature was first introduced during active scanning in iOS 8 (2014). Since 2020, major operating system vendors have adopted randomized MAC addresses by default for network association. [RFC9724] provides a comprehensive taxonomy of MAC address selection policies and documents current OS practices: per-network randomization (PNGM), per-connection randomization (PSGM), periodic rotation (PPGM), and scan-time randomization are now widely deployed across Android [ANDROID-MAC], iOS [APPLE-MAC], Windows [WINDOWS-MAC], and Linux.

Current versions of all major mobile operating systems transmit randomized MAC addresses by default when connecting to wireless networks, disrupting network services that depend on the MAC address as a stable device identifier.

The impact on RADIUS-based NAC systems is significant:

* A single physical device may present different Calling-Station-Id values across connections, creating multiple unrelated endpoint records.

* Device profiling data becomes fragmented across records keyed by different MAC addresses.

* RADIUS Accounting records [RFC2866] cannot be correlated across sessions for the same device.

* License management systems produce inflated device counts.

* Regulatory audit trails required by frameworks such as [HIPAA] and [FISMA] lose device-level continuity.

IEEE 802.11bh-2024 [IEEE80211BH] addresses session continuity at Layer 2 but does not extend to the AAA layer. This document addresses the gap by defining a RADIUS attribute that carries a persistent device identifier above the MAC address layer.

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

Persistent-Device-Id (PDID):

A unique identifier carried within the device’s certificate, typically provisioned during device enrollment by a Mobile Device Management (MDM) system or the NAC server’s own registration process. The RADIUS server extracts this identifier during certificate-based authentication and includes i t in the RADIUS Access-Accept to provide a persistent device identity that survives MAC address changes.

RADIUS Client:

A network device (switch, wireless controller, VPN concentrator) that acts as a RADIUS authenticator per [RFC2865].

RADIUS Server:

A server that processes RADIUS Access-Request messages, performs authentication and authorization, and returns Access-Accept or Access-Reject messages. In this context, the RADIUS server is also the entity that assigns and manages Persistent-Device-Id values.

MAC Address Randomization:

The practice of replacing a device’s hardware-assigned MAC address with a locally-administered, randomly-generated alternative, as described in [RFC9724].

Locally-Administered MAC Address:

A MAC address with the locally-administered bit (bit 1 of the first octet) set to 1. Unlike globally-assigned (burned-in) MAC addresses, a locally-administered address has local significance only, can be assigned by any entity, and is not guaranteed to be globally unique. Randomized MAC addresses use locally-administered addresses.

Identity Correlation Source:

A piece of information available during the RADIUS exchange that can be used to associate a new MAC address with a previously assigned Persistent-Device-Id. Examples include certificate Common Name (from certificate-based EAP methods such as EAP-TLS, EAP-TTLS, or TEAP), MDM device identifier, and IEEE 802.1X authenticated username.

2. Problem Statement

2.1. Calling-Station-Id as Device Identifier

Section 5.31 of [RFC2865] defines the Calling-Station-Id attribute as carrying "the phone number" of the user. In practice, for IEEE 802 networks, this attribute carries the MAC address of the connecting device, formatted as a string of hex digits (e.g., "AA-BB-CC-DD-EE-FF").

NAC systems use Calling-Station-Id as the primary key for:

1. Endpoint record lookup and creation

2. Device profiling and classification

3. Authorization policy evaluation

4. RADIUS Accounting session correlation

5. License and compliance tracking

2.2. Impact of MAC Address Randomization

When a device randomizes its MAC address, the Calling-Station-Id value changes. From the RADIUS server’s perspective, each randomized MAC appears to be a new, unrelated device. This causes:

1. Endpoint Record Proliferation: A single device generates N endpoint records for N different MAC addresses, fragmenting device state.

2. Profiling Data Loss: Attributes collected from network probes (DHCP, HTTP, SNMP, DNS) are stored against a MAC-keyed record. When the MAC changes, the accumulated profiling data is inaccessible for the new session.

3. Accounting Discontinuity: Accounting Start and Stop records [RFC2866] for the same device carry different Calling-Station-Id values, preventing session correlation.

4. License Count Inflation: License management based on unique Calling-Station-Id values produces artificially high counts.

5. Compliance Gaps: Regulatory frameworks requiring device-level audit trails (HIPAA [HIPAA], FISMA [FISMA], PCI-DSS [PCI-DSS]) cannot be satisfied when device identity is ephemeral.

2.3. Limitations of Existing Mechanisms

No existing standard RADIUS attribute provides a persistent device identifier independent of the MAC address. The following existing attributes are insufficient:

Calling-Station-Id (Type 31):

Carries the MAC address, which is now unstable.

User-Name (Type 1):

Identifies the user, not the device. A user may have multiple devices, and conversely, a single device may be shared by several individuals.

NAS-Port-Id (Type 87):

Identifies the network port, not the device.

Class (Type 25):

An opaque value sent by the RADIUS server in Access-Accept and echoed by the NAS in subsequent Accounting-Request messages [RFC2865]. The Class attribute is server-generated per session for accounting grouping and policy context. It is opaque to the NAS, has no defined structure for device identification, and is not guaranteed to persist across sessions or MAC address changes. It cannot serve as a stable device identifier.

Chargeable-User-Identity (CUI) [RFC4372]:

Provides a stable user-level identity for inter-domain roaming and billing. While CUI carries an opaque identifier, it is semantically a user identity, not a device identity. A single user may have multiple devices, and a shared device may serve multiple users. CUI cannot distinguish between devices belonging to the same user. Furthermore, RFC 4372 specifies that the CUI binding lifetime should be temporary (e.g., one billing period), whereas persistent device identification requires a stable identity across the device’s entire enrollment lifecycle. Overloading CUI to carry device identity would violate its defined semantics and conflict with existing CUI deployments used for roaming billing.

Certificate-based EAP fields (EAP-TLS, EAP-TTLS, TEAP):

Available only for certificate-based authentication methods, not for MAC Authentication Bypass (MAB) or credential-based EAP methods.

The absence of a standard attribute has led to vendor-specific workarounds that are mutually incompatible, as described in the following section.

2.4. Current Vendor-Specific Approaches

In the absence of a standard RADIUS attribute for persistent device identity, network access control vendors have independently implemented proprietary solutions to address the MAC address randomization problem. These approaches differ in their choice of RADIUS attribute, encoding format, and client-side parsing requirements.

Some implementations repurpose existing standard RADIUS attributes such as User-Name (Type 1) to carry device identifiers in the Access-Accept message. This approach violates the semantic definition of User-Name in RFC 2865, which specifies it as "the name of the user to be authenticated." Overloading User-Name with device identity creates ambiguity for downstream consumers of RADIUS data, including accounting systems, billing platforms, and compliance audit tools that expect User-Name to contain an actual user identity. It also requires RADIUS clients (NAS devices) to implement vendor-specific logic to distinguish between a true user name and an encoded device identifier.

Other implementations use Vendor-Specific Attributes (Type 26) to carry the persistent device identifier within a vendor-allocated attribute space. While VSAs are a legitimate RADIUS extension mechanism, they are inherently non-interoperable: a RADIUS client from one vendor cannot interpret the VSA encoding of another vendor’s RADIUS server. In multi-vendor enterprise deployments -- where network access devices, RADIUS servers, and policy engines may come from different manufacturers -- VSA-based approaches result in fragmented device identity that cannot be correlated across the infrastructure.

Both approaches share a common deficiency: they require modifications to RADIUS client firmware for each vendor’s proprietary encoding, creating a fragmented ecosystem where persistent device identity is available only within single-vendor deployments. Enterprise networks that use equipment from multiple vendors -- a common scenario in large organizations -- cannot achieve onsistent device identity across their infrastructure.

A standard RADIUS attribute for persistent device identity, as defined in this document, would eliminate this fragmentation by providing a single, interoperable mechanism that all vendors can implement without proprietary extensions or semantic overloading of existing attributes.

3. Persistent-Device-Id Attribute

3.1. Attribute Format

The Persistent-Device-Id attribute is a standard RADIUS attribute with the following format:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |           Value ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Value (variable length string)            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 1: Encoding Persistent-Device-Id Attribute

Type

TBD1 (to be assigned by IANA)

Length

Variable (2 octets for Type and Length, plus the length of the string value)

Data Type

String

Value

A string containing the persistent device identifier extracted from the device’s certificate. Implementations SHOULD use UUID version 4 [RFC9562] in the standard 36-character string representation (e.g., "f47ac10b-58cc-4372-a567-0e02b2c3d479"). The identifier is provisioned into the certificate during device enrollment and is not generated by the RADIUS server.

3.2. String Representation

When UUID version 4 is used as the Persistent-Device-Id, it MUST use the standard string format defined in Section 4 of [RFC9562]:

```
xxxxxxxx-xxxx-4xxx-yxxx-xxxxxxxxxxxx
```

where "x" is a lowercase hexadecimal digit and "y" is one of 8, 9, a, or b. The "4" indicates UUID version 4. This string representation is carried directly in the RADIUS attribute value field.

Example:

```
Persistent-Device-Id = "f47ac10b-58cc-4372-a567-0e02b2c3d479"
```

3.3. Attribute Properties

The following table summarizes the properties of the Persistent-Device-Id attribute:

Attribute Name	Persistent-Device-Id
Attribute Type	TBD1
Value Type	String
Length	Variable
Allowed in	Access-Accept, Accounting-Request, Accounting-Response, CoA-Request
Forbidden in	Access-Request, Access-Reject, Access-Challenge
Presence	OPTIONAL
Maximum Occurrences	1
Encrypted	Yes (as per RADIUS shared secret)

Table 1

4. Security and Deployment Model

This section defines the security and deployment model for the Persistent-Device-Id specification. A clear understanding of the actors, threats addressed, explicit non-goals, and security invariants is essential to evaluate the privacy and security properties of this mechanism.

4.1. Actors

The following actors are relevant to this specification:

1. Device Owner/User: The individual who owns or operates the device. In enterprise environments, this may be an employee using a corporate-issued or BYOD device. The device owner has a legitimate expectation of privacy from passive observers and external networks, while accepting that their employer's network may identify their device for security and compliance purposes.

2. Enterprise Administrator: The network operator responsible for device enrollment, certificate provisioning, NAC policy enforcement, and compliance auditing. The administrator has a legitimate need to persistently identify enrolled devices for security operations.

3. Passive Observer: An entity that can observe Layer 2 frames on the wireless medium or local network segment. This includes any device within radio range of a wireless network. The passive observer is the primary adversary that MAC address randomization is designed to defeat.

4. Rogue Access Point / Man-in-the-Middle: An attacker operating an unauthorized access point to intercept or manipulate network traffic. This actor can observe Layer 2 frames and may attempt to intercept authentication exchanges.

5. External Network: A network operator outside the device's home administrative domain. External networks should not be able to learn the Persistent-Device-Id or correlate device activity across domains.

4.2. Threats Addressed

MAC address randomization was introduced to mitigate the following threats. This specification is designed to preserve these protections:

1. Passive Device Tracking: A passive observer monitors Layer 2 frame headers to track a device’s location and movement patterns using its MAC address. MAC randomization defeats this by changing the MAC address. The Persistent-Device-Id does NOT reintroduce this threat because it is never present in any Layer 2 frame. The identifier value originates from the device certificate exchanged within the encrypted EAP tunnel, and the Persistent-Device-Id RADIUS attribute is carried only in RADIUS messages between the server and authenticator, protected by RADIUS/TLS [I-D.ietf-radext-radiusdtls-bis].

2. Cross-Network Correlation: An adversary correlates a device’s activity across multiple networks using a stable identifier. MAC randomization limits this by using different MAC addresses on different networks. The Persistent-Device-Id does NOT enable cross-network correlation because: (i) the identifier is scoped to the administrative domain that provisioned the certificate, (ii) external networks never see the identifier, and (iii) the RADIUS server MUST NOT share it with external entities.

3. Device Fingerprinting: An attacker combines observable characteristics (probe requests, timing patterns, supported capabilities) to fingerprint a device. The Persistent-Device-Id does not contribute to fingerprinting because it is not observable by any entity other than the RADIUS server and the authenticated NAS.

4.3. Explicit Non-Goals

This specification explicitly does NOT:

1. Enable tracking of unenrolled devices. Devices without certificates (guest, unauthenticated, MAB-only) are completely unaffected by this specification and continue to benefit fully from MAC randomization privacy.

2. Provide a mechanism for cross-network tracking. The Persistent-Device-Id is administratively scoped and MUST NOT be shared across administrative domains.

3. Enable surveillance or monitoring of user behavior. The identifier correlates a device for NAC, compliance, and licensing purposes only. It does not reveal user activity, browsing history, or application usage.

4. Undermine the user's choice to use MAC randomization. The MAC address continues to randomize at Layer 2 as the device vendor intended. The Persistent-Device-Id operates at a different layer (AAA/RADIUS) and is visible only to the enterprise network the device has voluntarily enrolled with.

5. Introduce a covert or hidden identifier. The identifier is explicitly provisioned into the device's certificate during a transparent enrollment process that requires device owner or administrator action.

4.4. Security Invariants

The following security properties MUST hold for any conforming implementation:

1. The Persistent-Device-Id MUST NOT appear in the clear in any Layer 2 frame (Ethernet, Wi-Fi management, or data frames).

2. The Persistent-Device-Id value is derived from the device certificate exchanged within the encrypted EAP tunnel (device to RADIUS server). The Persistent-Device-Id RADIUS attribute MUST only be transmitted within RADIUS messages protected by RADIUS/TLS [I-D.ietf-radext-radiusdtls-bis] (RADIUS server to NAS).

3. The Persistent-Device-Id MUST NOT be derivable from the device's MAC address (randomized or real).

4. The Persistent-Device-Id MUST NOT be observable by passive observers on the wireless medium or local network segment.

5. The Persistent-Device-Id MUST NOT be shared with entities outside the administrative domain without explicit device owner consent.

5. Device Consent and Control

A central concern raised by device vendors and privacy advocates is whether a persistent device identifier undermines the user's control over their device identity. This section specifies the consent and control requirements that ensure the Persistent-Device-Id respects device owner autonomy.

5.1. Consent Model

The Persistent-Device-Id is NEVER assigned to a device without explicit action by the device owner or an authorized administrator. The identifier exists only because a certificate containing it was provisioned onto the device through one of the following consent-based mechanisms:

1. Corporate Device Enrollment (Administrator Consent): An enterprise administrator enrolls the device in a Mobile Device Management (MDM) system. The MDM system generates a certificate containing the Persistent-Device-Id and pushes it to the device. The administrator acts on behalf of the organization, and the device is corporate-owned. The employee is informed of the enrollment through the organization’s acceptable use policy.

2. BYOD Self-Enrollment (User Consent): The device owner voluntarily connects to a provisioning portal (captive portal or onboarding SSID) and follows an enrollment workflow. During this process, the portal generates a certificate containing the Persistent-Device-Id and installs it on the device. The user explicitly initiates and approves this enrollment. On most operating systems (iOS, Android, Windows, macOS), installing a certificate profile requires the user to accept a system-level prompt.

3. MDM-Initiated BYOD Enrollment (User Consent with MDM): The device owner installs an MDM agent application and enrolls their personal device in the organization’s MDM. The MDM provisions the certificate. The user must explicitly install the MDM profile and grant the required permissions, providing informed consent.

5.2. User Control and Opt-Out

The device owner retains full control over the Persistent-Device-Id at all times:

1. Certificate Removal: The device owner can remove the certificate (and with it, the Persistent-Device-Id) at any time by deleting the certificate profile from the device settings. On iOS, this is under Settings > General > VPN & Device Management. On Android, Settings > Security > Credentials. On Windows, certmgr.msc. On macOS, Keychain Access. Once the certificate is removed, the device will no longer present a Persistent-Device-Id during authentication, and the RADIUS server will treat it as a new, unidentified device.

2. MDM Unenrollment: For MDM-managed devices, the device owner can unenroll from the MDM system, which removes the MDM profile and all associated certificates, including the one containing the Persistent-Device-Id.

3. Network Disconnection: The device owner can choose not to connect to the enterprise network. No identifier is transmitted unless the device actively authenticates to the network using the provisioned certificate.

4. No Silent Re-provisioning: The RADIUS server or NAS MUST NOT provision or re-provision a certificate containing a Persistent-Device-Id without the device owner’s or administrator’s explicit action. If a certificate expires or is revoked, a new enrollment process requiring consent is needed.

5.3. Transparency Requirements

Organizations deploying the Persistent-Device-Id SHOULD:

1. Inform device owners, through an acceptable use policy or enrollment notification, that a persistent device identifier will be embedded in the c ertificate and used for network access control, compliance, and licensing purposes.

2. Clearly describe what data is associated with the Persistent-Device-Id (MAC address history, session records, compliance state) and how long it is retained.

3. Provide a documented procedure for device owners to request deletion of their Persistent-Device-Id records, in compliance with applicable privacy regulations (e.g., the General Data Protection Regulation [GDPR] Article 17, the California Consumer Privacy Act).

The above recommendations are expressed as SHOULD to accommodate deployments where equivalent transparency is already provided through existing enterprise acceptable use policies, device management agreements, or where jurisdictional requirements impose alternative notification obligations that satisfy the same intent.

6. Certificate Provisioning Lifecycle

The provisioning of the Persistent-Device-Id into the device’s certificate is outside the scope of the RADIUS protocol. This section provides an informational overview of the lifecycle:

1. Enrollment: The device is enrolled through an MDM system or a NAC registration portal. During enrollment, the system generates a UUID version 4 using a CSPRNG and embeds it in the certificate's Subject Alternative Name (SAN) URI field using the URN format defined in [RFC9562], e.g., "urn:uuid:f47ac10b-58cc-4372-a567-0e02b2c3d479". The certificate is signed by the organization's CA and pushed to the device.

   * The SAN URI field is chosen over the X.509v3 subjectUniqueId field for the following reasons. First, [RFC5280] Section 4.1.2.8 states that conforming CAs "MUST NOT generate certificates with unique identifiers", effectively deprecating subjectUniqueId for new deployments. Second, the SAN extension is the standard mechanism for carrying additional identity forms in X.509 certificates and is universally supported by certificate tooling, MDM systems, and SCEP/EST enrollment protocols. Third, the urn:uuid: namespace is already registered [RFC9562], requiring no new URI scheme registration. The RADIUS server extracts the UUID from the SAN URI by parsing the urn:uuid: prefix and using the remaining string representation directly as the RADIUS attribute value.

2. Consent: Certificate installation requires explicit action -- either by an administrator (corporate MDM push) or by the device owner (accepting a certificate profile prompt during BYOD onboarding). The identifier is never provisioned silently.

3. Authentication: When the device connects to the network, it presents the certificate inside the encrypted EAP tunnel (e.g., EAP-TLS, EAP-TTLS, TEAP). The RADIUS server extracts the Persistent-Device-Id from the SAN URI field and includes it in the Access-Accept message.

4. Renewal: When the certificate approaches expiration, the MDM or NAC system renews it. The renewed certificate must contain the same Persistent-Device-Id as the original, preserving identity continuity.

5. Revocation: When a device is decommissioned, lost, or stolen, the administrator revokes the certificate. The RADIUS server rejects subsequent authentication attempts. The Persistent-Device-Id record may be retained for audit or deleted per the organization's data retention policy.

6. Re-enrollment: If a device is re-enrolled after revocation, a new certificate with a new Persistent-Device-Id should be provisioned. Reuse of a previously revoked identifier is not recommended.

7. Protocol Sequence Diagrams

The following diagram illustrates the complete lifecycle: certificate provisioning, initial authentication with identifier extraction, and re-authentication after MAC address rotation.

```
   Device        MDM/Portal    CA        NAS         RADIUS Server
     |               |          |          |               |
     |  PHASE 1: CERTIFICATE PROVISIONING (one-time)       |
     |               |          |          |               |
     |-- Enroll ---->|          |          |               |
     |  (user consent)          |          |               |
     |               |--CSR---->|          |               |
     |               | (UUID in |          |               |
     |               |  SAN URI)|          |               |
     |               |<-Cert----|          |               |
     |<--Push Cert---|          |          |               |
     | (user accepts |          |          |               |
     |  cert prompt) |          |          |               |
     |               |          |          |               |
     |  PHASE 2: FIRST AUTHENTICATION (certificate-based EAP)|
     |               |          |          |               |
     |-- 802.1X Start -------------------->|               |
     |  (MAC_1 in L2 header)    |          |               |
     |               |          |          |--Acc-Request->|
     |               |          |          | Calling-Stn-Id|
     |               |          |          | = MAC_1       |
     |<============ EAP Tunnel (e.g., EAP-TLS) ============>|
     |  (cert with UUID_A exchanged inside tunnel)         |
     |               |          |          |               |
     |               |          |          |  Server:      |
     |               |          |          |  1.Extract    |
     |               |          |          |    UUID_A     |
     |               |          |          |    from cert  |
     |               |          |          |  2.Store:     |
     |               |          |          |    UUID_A ->  |
     |               |          |          |    MAC_1      |
     |               |          |          |               |
     |               |          |          |<-Acc-Accept---|
     |               |          |          | PDID=UUID_A   |
     |<-- EAP-Success ---------------------|               |
     |               |          |          |--Acct-Req---->|
     |               |          |          | MAC_1,UUID_A  |
```

```
     |               |          |          |               |
     |       PHASE 3: RE-AUTH AFTER MAC ROTATION           |
     |               |          |          |               |
     |  [MAC rotates: MAC_1 -> MAC_2]      |               |
     |               |          |          |               |
     |-- 802.1X Start -------------------->|               |
     |  (MAC_2 in L2 header)    |          |               |
     |               |          |          |--Acc-Request->|
     |               |          |          | Calling-Stn-Id|
     |               |          |          | = MAC_2       |
     |<============ EAP Tunnel (e.g., EAP-TLS) ============>|
     |  (same cert, same UUID_A)           |               |
     |               |          |          |               |
     |               |          |          |  Server:      |
     |               |          |          |  1.Extract    |
     |               |          |          |    UUID_A     |
     |               |          |          |  2.Find       |
     |               |          |          |    existing   |
     |               |          |          |    record     |
     |               |          |          |  3.Add MAC_2  |
     |               |          |          |    to UUID_A  |
     |               |          |          |               |
     |               |          |          |<-Acc-Accept---|
     |               |          |          | PDID=UUID_A   |
     |               |          |          | (same as      |
     |               |          |          |  before)      |
     |<-- EAP-Success ---------------------|               |
     |               |          |          |--Acct-Req---->|
     |               |          |          | MAC_2,UUID_A  |
```

Figure 2: Persistent-ID Lifecycle Management

Key observations: (1) The UUID is provisioned with user/admin consent during enrollment. (2) The UUID originates from the device certificate exchanged within the encrypted EAP tunnel -- it never appears in any Layer 2 frame. The Persistent-Device-Id RADIUS attribute is carried only in RADIUS messages protected by RADIUS/TLS. (3) After MAC rotation, the same UUID is extracted from the same certificate, allowing the RADIUS server to unify device records across MAC changes. (4) Unenrolled devices (no certificate) are unaffected and receive no Persistent-Device-Id.

8. Attribute Assignment Procedures

8.1. Identifier Extraction from Certificate

When a RADIUS server receives an Access-Request containing a certificate-based authentication (e.g., EAP-TLS, EAP-TTLS, TEAP), and the device's certificate contains a persistent device identifier, the server MUST:

1. Extract the persistent device identifier from the device's certificate.

2. Store or update the identifier in association with the device's current Calling-Station-Id (MAC address) for correlation purposes.

3. Include the Persistent-Device-Id attribute in the Access-Accept message.

8.2. Correlation and Retrieval

When a RADIUS server receives an Access-Request and the Calling-Station-Id does not match any stored device record, but the device authenticates via a certificate-based method, the server SHOULD attempt to correlate the request with an existing Persistent-Device-Id by extracting the identifier from the certificate and looking up the stored records.

The primary identity correlation source is the device certificate. If the authentication method is certificate-based (e.g., EAP-TLS, EAP-TTLS, TEAP), the server extracts the persistent device identifier from the certificate and uses it to look up an existing device record. If a matching record is found, the server associates the new MAC address with the existing record.

Note: External device management systems (e.g., MDM) provision the persistent identifier into the device's certificate during enrollment. The identifier reaches the RADIUS server through the certificate-based authentication exchange, not through a separate channel. Therefore, MDM-managed devices are covered by the certificate-based extraction above.

For authentication methods that do not involve certificates (e.g., MAB, credential-based EAP methods, guest access), no persistent device identifier is available in the authentication exchange. In these cases, the RADIUS server does not assign a Persistent-Device-Id, and MAC address randomization continues to result in separate device records per MAC address.

This document does not define alternative mechanisms for persistent device identification in non-certificate-based authentication scenarios. Such mechanisms are outside the scope of this specification.

If the extracted identifier matches an existing record, the server MUST:

1. Associate the new Calling-Station-Id (MAC address) with the existing Persistent-Device-Id record.

2. Include the existing Persistent-Device-Id in the Access-Accept message.

If the device authenticates via a non-certificate-based method, or if the certificate does not contain a persistent device identifier, the server MUST NOT include a Persistent-Device-Id attribute in the Access-Accept.

8.3. Immutability

The Persistent-Device-Id value is determined by the identifier provisioned in the device’s certificate. It MUST NOT be modified by the RADIUS server. If administrative action requires re-identification of a device (e.g., device decommissioning and re-enrollment), a new certificate with a new identifier must be provisioned to the device. The old identifier MUST be retired and MUST NOT be reassigned to a different device.

8.4. Uniqueness

The persistent device identifier provisioned in each device’s certificate MUST be globally unique. The enrollment system (MDM or NAC registration portal) is responsible for ensuring uniqueness during certificate provisioning. The use of UUID version 4 with a CSPRNG during provisioning provides sufficient uniqueness guarantees.

8.5. Concurrency

In deployments where multiple RADIUS server instances process authentication requests concurrently, implementations MUST ensure that the extracted Persistent-Device-Id and its associated MAC address mappings are consistently replicated across all server instances. Since the identifier originates from the certificate (not generated by the server), concurrency risks are limited to MAC address association updates.

Recommended approaches include: 1. Advisory locking on the Calling-Station-Id or identity correlation key before checking for existing assignments. 1. A check-then-act pattern with lock acquisition: acquire lock, re-query for existing assignment, create if absent, release lock. 1. Distributed coordination across server instances in clustered deployments. The lock hold time SHOULD NOT exceed 5 seconds to prevent processing delays.

8.6. NAD and Platform Integration

After receiving the Persistent-Device-Id in the Access-Accept message, the Network Access Device (NAD) associates the identifier with the client session. This enables several downstream use cases beyond the RADIUS exchange itself:

1. Client Session Correlation: The NAD maintains a mapping between the Persistent-Device-Id and the current client session. When the device reconnects with a different randomized MAC address, the NAD can correlate the new session with previous sessions for the same device, preserving continuity for session logs, QoS policies, and access control lists.

2. Device Profiling and Fingerprinting: The NAD or RADIUS server can share the Persistent-Device-Id with endpoint analytics and profiling systems. These systems build device fingerprint profiles -- aggregating attributes such as DHCP options, HTTP user-agent, and CDP/LLDP data -- indexed by the persistent identifier rather than the transient MAC address. This ensures profiling data survives MAC rotation.

3. Location and Presence Analytics: The NAD can include the Persistent-Device-Id in location telemetry messages (e.g., via streaming telemetry or location service protocols) sent to location analytics platforms. This allows location services to track device presence and movement patterns using a stable identifier, even as the MAC address changes between sessions.

4. Cross-Platform Distribution: The RADIUS server or NAD can distribute the Persistent-Device-Id to network management, assurance, and third-party platforms through integration mechanisms such as publish-subscribe frameworks, REST APIs, or event streaming. This enables a consistent device identity across the ecosystem of network services -- including compliance engines, network assurance dashboards, and third-party security tools -- without requiring each platform to independently resolve MAC address changes.

In all cases, the Persistent-Device-Id MUST be treated with the same access control and privacy protections described in this specification. Platforms receiving the identifier MUST NOT expose it to entities outside the administrative domain without explicit device owner consent.

9. Usage in RADIUS Messages

9.1. Access-Accept

When a RADIUS server extracts a Persistent-Device-Id from a device’s certificate during authentication, it SHOULD include the Persistent-Device-Id attribute in the Access-Accept message sent to the RADIUS client (authenticator).

```
RADIUS Server                          RADIUS Client
     |                                         |
     |<--- Access-Request --------------------|
     |     (Calling-Station-Id = random MAC)  |
     |                                         |
     |  [Correlate or assign PDID]             |
     |                                         |
     |---- Access-Accept -------------------->|
     |     (Persistent-Device-Id = UUID)      |
     |     (other authorization attributes)   |
     |                                         |
```

Figure 3: Persistent Device ID in Access Accept

9.2. Accounting-Request

When a RADIUS client has received a Persistent-Device-Id in an Access-Accept, it SHOULD include the Persistent-Device-Id attribute in all subsequent Accounting-Request messages (Accounting-Start, Interim-Update, and Accounting-Stop) for that session.

This enables the RADIUS server to correlate accounting records across sessions where the Calling-Station-Id may differ due to MAC address randomization.

```
   RADIUS Client                         RADIUS Server
         |                                       |
         |---- Accounting-Request (Start) ------>|
         |     (Calling-Station-Id = MAC_1)      |
         |     (Persistent-Device-Id = UUID_A)   |
         |                                       |
         |     [Device reconnects with new MAC]  |
         |                                       |
         |---- Accounting-Request (Start) ------>|
         |     (Calling-Station-Id = MAC_2)      |
         |     (Persistent-Device-Id = UUID_A)   |
         |                                       |
```

Figure 4: Persistent Device ID in Accounting Request

The RADIUS server can now correlate both sessions as belonging to the same device (UUID_A) despite different MAC addresses.

9.3. CoA-Request

A RADIUS server MAY include the Persistent-Device-Id attribute in a Change-of-Authorization (CoA) Request RFC5176 to identify the target device session. The RADIUS client MUST use the Persistent-Device-Id, if present, to identify the session to which the CoA applies, in preference to Calling-Station-Id when both are present.

9.4. Access-Request

The Persistent-Device-Id attribute MUST NOT appear in Access-Request messages. The identifier is extracted from the device’s certificate by the RADIUS server during authentication processing, not supplied by the RADIUS client.

Exception: If a RADIUS client has cached a Persistent-Device-Id from a previous Access-Accept for the same device, and the server’s deployment policy explicitly permits it, the client MAY include the cached Persistent-Device-Id in the Access-Request as a hint to assist correlation. When present in an Access-Request, the server MUST validate the hint against its own records and MUST NOT trust it as authoritative.

9.5. Access-Reject and Access-Challenge

The Persistent-Device-Id attribute MUST NOT appear in Access-Reject or Access-Challenge messages. A Persistent-Device-Id is only included upon successful certificate-based authentication where the certificate contains a valid persistent device identifier.

10. Interaction with Existing Attributes

10.1. Calling-Station-Id (Type 31)

The Persistent-Device-Id attribute supplements but does not replace Calling-Station-Id. The Calling-Station-Id continues to carry the MAC address (randomized or not) as observed by the RADIUS client. Systems that need the current MAC address for network-level operations (e.g., VLAN assignment, ACL application) continue to use Calling-Station-Id for that purpose.

The Persistent-Device-Id provides the stable device-level correlation that Calling-Station-Id can no longer guarantee.

10.2. User-Name (Type 1)

The Persistent-Device-Id identifies a device, not a user. A single User-Name may be associated with multiple Persistent-Device-Id values (one per device), and a single Persistent-Device-Id MAY be associated with multiple User-Name values (if different users authenticate on the same device).

10.3. Acct-Session-Id (Type 44)

The Acct-Session-Id attribute identifies a single session. The Persistent-Device-Id identifies the device across sessions. Together, they enable both session-level and device-level accounting correlation.

10.4. Chargeable-User-Identity [RFC4372]

The Chargeable-User-Identity (CUI) attribute defined in [RFC4372] provides a stable user-level identity for inter-domain roaming and billing. While both CUI and Persistent-Device-Id carry opaque identifiers in RADIUS messages, they serve fundamentally different purposes and cannot be used interchangeably. The key differences are:

1. Semantic Scope: CUI identifies a user (or chargeable entity) for billing purposes. Persistent-Device-Id identifies a physical device. These are orthogonal concepts: a single user may own multiple devices (each requiring a distinct Persistent-Device-Id), and a shared device may authenticate multiple users (each receiving a distinct CUI). Overloading one attribute to serve both purposes would create ambiguity and prevent independent user and device correlation.

2. Identifier Origin: CUI is generated by the home RADIUS server as an opaque token. Persistent-Device-Id is extracted from the device’s certificate (SAN URI field), provisioned by the enrollment system. The RADIUS server does not generate the Persistent-Device-Id; it reads it from the certificate presented during certificate-based EAP authentication. These are different data flows requiring different handling semantics.

3. Binding Lifetime: RFC 4372 explicitly states that the CUI binding "should be temporary -- long enough to be useful for the external applications and not too long such that it can be used to identify the user." A typical CUI lifetime is one billing period. In contrast, the Persistent-Device-Id MUST remain stable for the entire duration the device’s certificate is valid, potentially spanning years, to enable persistent device identification across MAC address changes.

4. Deployment Scope: CUI is designed for cross-network roaming scenarios involving visited and home networks with intermediary proxies. Persistent-Device-Id is scoped to a single administrative domain for NAC, compliance, and audit purposes. A deployment may legitimately need both attributes simultaneously -- CUI for roaming billing and Persistent-Device-Id for device identification -- in the same RADIUS message.

5. Opaqueness Constraint: [RFC4372] mandates that "RADIUS entities other than the Home RADIUS server MUST treat the CUI content as an opaque token, and SHOULD NOT perform operations on its content other than a binary equality comparison test." Any scheme to differentiate user vs. device identity within a CUI value (e.g., using a class prefix or structured encoding) would require intermediaries to inspect and interpret CUI content, directly violating this requirement.

In roaming scenarios, both CUI and Persistent-Device-Id MAY be present in the same RADIUS message, providing independent user-level and device-level correlation without ambiguity or attribute overloading.

10.5. EAP-Message (Type 79)

When certificate-based EAP authentication is used (e.g., EAP-TLS, EAP-TTLS, TEAP), the device’s certificate is the source of the Persistent-Device-Id. The RADIUS server extracts the identifier from the certificate during the EAP exchange and includes it in the Access-Accept. This is the primary and intended use case for this specification.

11. Operational Considerations

11.1. Replication

In deployments with multiple RADIUS servers, the Persistent-Device-Id assignments and the associated MAC address mappings MUST be replicated across all servers. This ensures that a device authenticating to any server in the deployment receives the same Persistent-Device-Id.

The replication mechanism is implementation-specific and outside the scope of this document. Implementations SHOULD provide eventual consistency with a convergence time appropriate for the deployment's authentication rate.

11.2. Proxy Environments

When a RADIUS proxy forwards an Access-Request to an upstream RADIUS server, and the upstream server includes a Persistent-Device-Id in the Access-Accept, the proxy MUST forward the Persistent-Device-Id attribute to the RADIUS client without modification.

A RADIUS proxy MUST NOT modify or strip Persistent-Device-Id attributes. The identifier originates from the device's certificate and is extracted by the authoritative RADIUS server. Proxies that forward Access-Accept messages MUST pass the attribute through unchanged.

11.3. Incremental Deployment

RADIUS clients that do not support the Persistent-Device-Id attribute will ignore it in Access-Accept messages per standard RADIUS behavior (unknown attributes are silently discarded). This allows incremental deployment where RADIUS servers begin including the attribute before all clients are upgraded.

11.4. Pre-Existing Device Records

When a RADIUS server implementing this specification receives an Access-Request for a device that has an existing record (created before Persistent-Device-Id support was deployed), and the device authenticates via a certificate containing a persistent identifier, the server SHOULD:

1. Extract the Persistent-Device-Id from the certificate and associate it with the existing device record.

2. Associate it with the existing device record, preserving all historical data.

3. Include the Persistent-Device-Id in the Access-Accept.

This provides a seamless deployment path for existing deployments.

11.5. Mixed-Mode Operation

During deployment, some device records will have Persistent-Device-Id values and some will not. Implementations MUST support lookups by both Calling-Station-Id (for legacy records) and Persistent-Device-Id (for migrated records) until deployment is complete.

12. Security Considerations

12.1. Identifier Provisioning

The Persistent-Device-Id is provisioned into the device’s certificate by the enrollment system (MDM or NAC registration portal) during device onboarding. The enrollment system MUST use a Cryptographically Secure Pseudo-Random Number Generator (CSPRNG) when generating the identifier to ensure unpredictability. Use of predictable or sequential identifiers would allow an attacker to enumerate devices or anticipate future identifiers. The RADIUS server does not generate identifiers; it extracts them from certificates presented during authentication.

12.2. Transport Security

The Persistent-Device-Id benefits from two layers of transport protection. First, the identifier value originates from the device’s certificate, which is exchanged inside the encrypted EAP tunnel (e.g., EAP-TLS, EAP-TTLS, TEAP) between the supplicant and the RADIUS server. This ensures the identifier is never transmitted in cleartext over the air (wireless) or on the wire (wired), and is not visible to passive observers, neighboring devices, or any entity not party to the authenticated EAP session. This is in stark contrast to the MAC address, which appears in plaintext in every Layer 2 frame header. Second, the Persistent-Device-Id RADIUS attribute is carried within RADIUS messages between the server and the authenticator, protected by the RADIUS shared secret mechanism or, for stronger security, by RADIUS/TLS (RadSec) [I-D.ietf-radext-radiusdtls-bis].

For deployments requiring stronger transport security, RADIUS/TLS (RadSec) [I-D.ietf-radext-radiusdtls-bis] SHOULD be used. [I-D.ietf-radext-deprecating-radius] further deprecates RADIUS over UDP and MD5-based security mechanisms, mandating TLS-based transport for all RADIUS deployments. When RadSec is in use, the Persistent-Device-Id receives the same TLS protection as all other RADIUS attributes.

12.3. Access Control

The Persistent-Device-Id mapping table (associating UUIDs with MAC addresses and device attributes) contains sensitive information. Access to this table MUST be restricted to authorized administrators and audit systems. All access to the mapping table SHOULD be logged.

12.4. Identifier Spoofing

If the Access-Request hint mechanism Section 9.4 is implemented, the RADIUS server MUST validate any client-provided Persistent-Device-Id against its authoritative records. A RADIUS client MUST NOT be trusted as the source of truth for Persistent-Device-Id values.

12.5. Replay Protection

The Persistent-Device-Id does not introduce new replay attack vectors beyond those inherent in the RADIUS protocol. Standard RADIUS replay protections (Request Authenticator, Message-Authenticator attribute [RFC3579]) apply.

13. Privacy Considerations

13.1. Persistent Identification

The Persistent-Device-Id is explicitly designed to enable persistent device identification within an administrative domain. This is its intended purpose for NAC, compliance, and auditing. However, this capability must be balanced against user privacy expectations.

13.2. Scope Limitation

The Persistent-Device-Id SHOULD be scoped to a single administrative domain. A Persistent-Device-Id assigned by one organization’s RADIUS server MUST NOT be shared with other organizations without explicit user consent, except as required by applicable law.

13.3. Data Retention

Organizations deploying Persistent-Device-Id SHOULD establish data retention policies that define: 1. Maximum retention period for Persistent-Device-Id records. 1. Procedures for deleting Persistent-Device-Id records when a device is decommissioned. 1. Procedures for honoring data deletion requests from device owners, where required by applicable privacy regulations (e.g., GDPR Article 17, [GDPR]).

13.4. Relationship to MAC Randomization Goals

MAC address randomization was introduced to prevent cross-network tracking of devices at Layer 2. A key privacy concern is whether introducing a Persistent-Device-Id undermines the privacy benefits of MAC randomization. This specification preserves MAC randomization privacy because the Persistent-Device-Id value originates from the device certificate exchanged within the encrypted EAP tunnel during certificate-based authentication, and the RADIUS attribute is carried only in RADIUS messages protected by RADIUS/TLS. Unlike the MAC address, which is transmitted in plaintext in Layer 2 frames and is visible to any passive observer on the wireless medium or local network segment, the Persistent-Device-Id is never exposed in cleartext over the air or on the wire. Specifically:

1. Transport Protection: The Persistent-Device-Id value originates from the device’s certificate, which is exchanged within the encrypted EAP tunnel (e.g., EAP-TLS, EAP-TTLS, TEAP). The TLS handshake encrypts the certificate exchange, ensuring the identifier is never visible to passive observers, neighboring devices, or any entity not participating in the authenticated session. The Persistent-Device-Id RADIUS attribute is then carried in RADIUS messages protected by the shared secret or by RADIUS/TLS. In contrast, the MAC address is present in every Layer 2 frame header in plaintext and can be captured by any device within radio range (wireless) or on the same network segment (wired). MAC randomization exists precisely because the MAC address lacks this transport protection. The Persistent-Device-Id does not share this vulnerability.

2. Explicit Enrollment and Consent: The Persistent-Device-Id is only present on devices that have been explicitly enrolled through an MDM system or NAC registration portal. The device owner or administrator has voluntarily provisioned the certificate containing the identifier. This is fundamentally different from MAC address tracking, which occurs without the device owner’s knowledge or consent. Unenrolled devices (guest, BYOD without certificates) are not affected by this specification and continue to benefit fully from MAC randomization privacy.

3. Domain-Scoped Visibility: The Persistent-Device-Id is scoped to the administrative domain that provisioned the certificate. It is visible only to the RADIUS server and the authenticator within that domain. It cannot be used for cross-network tracking because external networks never see the identifier -- it is not broadcast, not included in probe requests, and not present in any Layer 2 frame. The MAC address, even when randomized, is visible to every network the device encounters. The Persistent-Device-Id has strictly narrower visibility than even a randomized MAC address.

4. RADIUS Transport Encryption: When the Persistent-Device-Id is included in the RADIUS Access-Accept message from the server to the authenticator, it is protected by the RADIUS shared secret mechanism. For deployments requiring stronger protection, RADIUS/TLS (RadSec) [I-D.ietf-radext-radiusdtls-bis] provides full encryption of the RADIUS transport. Together, the encrypted EAP tunnel protects the certificate exchange (device to server), and RADIUS/TLS protects the attribute transport (server to authenticator), ensuring the identifier is never exposed in cleartext at any point.

Organizations MUST NOT use the Persistent-Device-Id to correlate device activity across independent administrative domains unless the device owner has provided explicit consent.

14. IANA Considerations

14.1. RADIUS Attribute Type

This document requests IANA to allocate a new RADIUS Attribute Type from the "RADIUS Attribute Types" registry (https://www.iana.org/assignments/radius-types/):

Type	Name	Data Type	Reference
TBD1	Persistent-Device-Id	string	[this document]

Table 2

15. References

15.1. Normative References

[I-D.ietf-radext-radiusdtls-bis]
Rieckers, J., Cullen, M., and S. Winter, "RadSec: RADIUS over Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", Work in Progress, Internet-Draft, draft-ietf-radext-radiusdtls-bis-15, 23 February 2026, <https://datatracker.ietf.org/doc/html/draft-ietf-radext-radiusdtls-bis-15>.

[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/rfc/rfc2119>.

[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>.

[RFC2866] Rigney, C., "RADIUS Accounting", RFC 2866, DOI 10.17487/RFC2866, June 2000, <https://www.rfc-editor.org/rfc/rfc2866>.

[RFC3579] Aboba, B. and P. Calhoun, "RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)", RFC 3579, DOI 10.17487/RFC3579, September 2003, <https://www.rfc-editor.org/rfc/rfc3579>.

[RFC5176] Chiba, M., Dommety, G., Eklund, M., Mitton, D., and B. Aboba, "Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)", RFC 5176, DOI 10.17487/RFC5176, January 2008, <https://www.rfc-editor.org/rfc/rfc5176>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/rfc/rfc5280>.

[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/rfc/rfc8174>.

[RFC9562] Davis, K., Peabody, B., and P. Leach, "Universally Unique IDentifiers (UUIDs)", RFC 9562, DOI 10.17487/RFC9562, May 2024, <https://www.rfc-editor.org/rfc/rfc9562>.

15.2. Informative References

[ANDROID-MAC]
Google, "MAC Randomization Behavior", 2023.

[APPLE-MAC]
Apple, "Use private Wi-Fi addresses on Apple devices", 2024.

[FISMA] Congress, U. S., "Federal Information Security Modernization Act of 2014", December 2014.

[GDPR] European Parliament and Council, "Regulation (EU) 2016/679 - General Data Protection Regulation", April 2016.

[HIPAA] Department of Health and Human Services, U. S., "Health Insurance Portability and Accountability Act of 1996", August 1996.

[I-D.ietf-radext-deprecating-radius]
DeKok, A., "Deprecating Insecure Practices in RADIUS", Work in Progress, Internet-Draft, draft-ietf-radext-deprecating-radius-09, 15 March 2026, <https://datatracker.ietf.org/doc/html/draft-ietf-radext-deprecating-radius-09>.

[IANA-RADIUS]
IANA, "RADIUS Attribute Types", n.d., <https://www.iana.org/assignments/radius-types/>.

[IEEE80211BH]
IEEE, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", 2024, <https://standards.ieee.org/ieee/802.11bh/10525/>.

[PCI-DSS] PCI Security Standards Council, "Payment Card Industry Data Security Standard (PCI DSS)", June 2024.

[RFC4372] Adrangi, F., Lior, A., Korhonen, J., and J. Loughney, "Chargeable User Identity", RFC 4372, DOI 10.17487/RFC4372, January 2006, <https://www.rfc-editor.org/rfc/rfc4372>.

[RFC9724] Z炭単iga, JC., Bernardos, CJ., Ed., and A. Andersdotter, "State of Affairs for Randomized and Changing Media Access Control (MAC) Addresses", RFC 9724, DOI 10.17487/RFC9724, March 2025, <https://www.rfc-editor.org/rfc/rfc9724>.

[WINDOWS-MAC]
Microsoft, "MAC address randomization in Windows", 2024.

Appendix A. Use Case Examples

A.1. BYOD with Certificate-Based Authentication

A personal device is onboarded via a provisioning portal and issued a device certificate. The certificate contains a persistent device identifier provisioned during enrollment. The following example uses EAP-TLS, but the same flow applies to any certificate-based EAP method (EAP-TTLS, TEAP).

Step 1: Device connects with MAC_1, authenticates via certificate-based EAP Step 2: RADIUS server extracts Persistent-Device-Id from certificate Step 3: No existing record found for this identifier Step 4: Server stores: PDID -> {MAC_1, cert identity} Step 5: Access-Accept includes Persistent-Device-Id = PDID

[Later, device reconnects with randomized MAC_2]

Step 6: Device connects with MAC_2, authenticates via certificate-based EAP Step 7: RADIUS server extracts same Persistent-Device-Id from certificate Step 8: Server finds existing record for this identifier Step 9: Server adds MAC_2 to the PDID record Step 10: Access-Accept includes same Persistent-Device-Id = PDID

A.2. MDM-Managed Device

A corporate device is enrolled in a Mobile Device Management system. The MDM provisions a device certificate containing a persistent device identifier.

```
Step 1: Device connects with MAC_1, authenticates via certificate-based EAP
Step 2: RADIUS server extracts Persistent-Device-Id from MDM-provisioned certificate
Step 3: No existing record found for this identifier
Step 4: Server stores: PDID -> {MAC_1, cert identity}
Step 5: Access-Accept includes Persistent-Device-Id = PDID

[Later, device reconnects with randomized MAC_2]

Step 6: Device connects with MAC_2, authenticates via certificate-based EAP
Step 7: RADIUS server extracts same Persistent-Device-Id from certificate
Step 8: Server finds existing record
Step 9: Access-Accept includes same Persistent-Device-Id = PDID
```

A.3. Accounting Correlation Across MAC Changes

```
Session 1:
  Accounting-Start: Calling-Station-Id=MAC_1,
                    Persistent-Device-Id=UUID_A,
                    Acct-Session-Id=SES_1
  Accounting-Stop:  Calling-Station-Id=MAC_1,
                    Persistent-Device-Id=UUID_A,
                    Acct-Session-Id=SES_1

Session 2 (same device, new MAC):
  Accounting-Start: Calling-Station-Id=MAC_2,
                    Persistent-Device-Id=UUID_A,
                    Acct-Session-Id=SES_2
  Accounting-Stop:  Calling-Station-Id=MAC_2,
                    Persistent-Device-Id=UUID_A,
                    Acct-Session-Id=SES_2

Correlation: Sessions SES_1 and SES_2 both belong to device UUID_A
             despite different Calling-Station-Id values.
```

A.4. Guest Access Limitations

For unauthenticated guest access (e.g., open hotspot), no identity correlation source is available. In this scenario: Step 1: Device connects with MAC_1, no certificate-based authentication Step 2: RADIUS server has no certificate to extract identifier from Step 3: No Persistent-Device-Id included in Access-Accept Step 4: Device is treated as a new endpoint keyed by MAC_1

[Device reconnects with randomized MAC_2, no certificate-based authentication]

Step 5: Server has no way to correlate MAC_2 with MAC_1
Step 6: Device is treated as a new endpoint keyed by MAC_2

This limitation is inherent: without an identity assertion from the device, persistent identification across MAC changes is not possible without resorting to fingerprinting techniques that undermine the privacy goals of MAC randomization.

Changelog

* 0 - initial draft.

Acknowledgements

The authors thank Suresh Krishnan, Juan Carlos Zuniga, Jerome Henry, Mark Grayson, and Eric Vyncke for their valuable technical review, feedback, and contributions to the development of this specification.

The authors acknowledge the work of the IETF MADINAS working group in documenting the impacts of MAC address randomization, which motivated this specification.

Disclosure of AI Use: The authors used AI-assisted tools for drafting and language editing of this document. All technical concepts and protocol specifications presented are the original intellectual contributions of the authors, developed through years of hands-on engineering work on network access control systems. The authors reviewed, edited, and verified all content and take full responsibility for the accuracy and integrity of this publication.

Authors' Addresses

Premanand Seralathan
Cisco Systems
170 West Tasman Drive
San Jose, 95134
United States of America
Email: pseralat@cisco.com

Laxmi Mukund
Cisco Systems
Cessna Business Park, Kadubeesanahalli
ORR Bangalore 560103
India
Email: lmukund@cisco.com

Antoni Milton
Hewlett Packard Enterprise (HPE)
6280 America Center Dr
San Jose, 95002
United States of America
Email: antoni.milton@hpe.com