

RADEXT Working Group
Internet-Draft
Intended status: Standards Track
Expires: 13 October 2022

J. Henry
N. Cam-Winget
Cisco Systems, Inc.
11 April 2022

RADIUS attributes for Randomized and Changing MAC addresses
draft-henry-radext-stable-mac-identifier-01

Abstract

This document describes the means by which a Stable MAC address identifier can be signaled to a Authentication Authorization and Accounting (AAA) server.

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 13 October 2022.

Copyright Notice

Copyright (c) 2022 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the [Trust Legal Provisions](#) and are provided without warranty as described in the Revised BSD License.

Table of Contents

1.	Introduction	2
2.	Use cases	3
2.1.	Stable Machine Identifier provided to the Wireless Infrastructure	4
2.1.1.	General Use Cases	4
2.1.2.	Special scenarios	6
2.1.3.	Failure Handling	7
2.2.	Stable RADIUS machine identifier	7
2.2.1.	General Use cases	8
2.2.2.	Special scenarios	9
2.2.3.	Failure Handling	9
2.3.	Stable NAS and stable RADIUS machine identifiers	9
2.3.1.	General cases	9
2.3.2.	Special scenarios	10
2.3.3.	Failure Handling	11
3.	Stable-Machine-Identifier	11
4.	Attribute table	11
5.	Diameter Consideration	12
6.	Security & Privacy Considerations	12
7.	IANA Considerations	12
8.	References	12
8.1.	Normative References	12
8.2.	Informative References	13
	Acknowledgments	14
	Authors' Addresses	14

[1.](#) Introduction

In many cases where a client establishes communication over a wireless network, an observer (as defined in [\[RFC6973\]](#)) might monitor the client MAC address and the associated traffic. Although the traffic payload itself may be protected (e.g. encrypted in some way), the outer header is commonly not obfuscated. When the client is a personal device (as defined in IEEE 802E), observing the client traffic may allow an attacker to characterize, from the traffic, the associated user activity. For this reason, many vendors of personal devices have started operating under a Randomized and Changing MAC address (RCM) scheme, where the visible and external MAC address changes over time, so as to make device tracking and fingerprinting more difficult. An account of these efforts can be found in [\[ZUNIGA\]](#) [draft-ietf-madinas-mac-address-randomization](#).

Such RCM scheme does not necessarily mean that the client intends to obfuscate the machine identifier from all infrastructure devices. In many cases, the intent is to hide the MAC address from external observers. For example, a wireless infrastructure may use a stable

identifier for the client to provide service continuity within a RADIUS accounting session, between the Access Point (AP) or the Wireless LAN controller (WLC), acting as a Network Access Server [NAS]) and the RADIUS server; with the stable identifier being independent from the RCM. In this scenario, the NAS is the means for the client to access network services, and the client may expect or need service continuity. Continuity might include for example obtaining the same IP address from the DHCP server, the continued access to cached resources or the persistence of established exchange pathways. In many of these cases, the provider of the service needs to be informed that a new RCM matches a previously connected object that should continue to obtain the same service, independently of the changed MAC address. When this happens, it is useful for the continuity of network services that the wireless infrastructure, acting as the NAS, exchanges with the RADIUS server about the client capability to provide an identity independent from the RCM. For this purpose, this document specifies a Stable Machine Identifier attribute.

[2.](#) Use cases

The attributes in this document are intended to be applicable across a wide variety of network access scenarios in which RADIUS is involved:

- * In some cases, the client may provide a machine identity to the NAS, after the authentication has completed and the client has established a trusted and secure connection to the AP, that the NAS interprets as stable. The client may then have not provided a stable machine identifier (SMI) to the RADIUS server, for example because the 802.1X/EAP process authenticated the user, but not the machine (that is then identified with a MAC address that may change).
- * There are cases where the client may provide a machine identity to the RADIUS server during the authentication phase, and that the

RADIUS server interprets as stable, but may not provide a stable machine identifier directly to the NAS. In some cases, the NAS cannot see the stable machine identity provided to the RADIUS server (for example because it is provided within a tunnel).

- * In other cases, the client may provide a machine identifier to the RADIUS server during the authentication phase that the RADIUS server interprets as stable, and may also provide a machine identifier to the NAS after the establishment of a trusted and secure connection to the AP, that the NAS interprets as stable. The machine identifier provided to the NAS and the RADIUS server may not be the same.

It should be noted that cases where both the NAS and the RADIUS server are unable to determine a stable machine identifier for the client are not considered in this document. Additionally, the machine identifier provided to the NAS or the RADIUS server may not be the SMI attribute in this document. However, the machine identifier is interpreted as stable by the receiving side.

This section further describes these use cases.

[2.1](#). Stable Machine Identifier provided to the Wireless Infrastructure

In this scenario, the client initially attaches to the network in a constrained state and proceeds through the 802.1X/EAP authentication phase. The client MAC address is likely locally administered (second bit of first octet set), although this condition is not necessary for support of the SMI attribute. This information is visible to the NAS (in the client source address) and possibly to the RADIUS server (in the Calling-Station-ID). The RADIUS validates the user identity, but cannot validate the machine identity, as no stable machine identifier is available at this point. After the RADIUS server returns an Access-Accept, keying material is built on the client and on the NAS.

Once authentication is completed and a protected link has been established between the client machine and the access network infrastructure (acting as NAS), the client machine exchanges with the infrastructure a stable identifier. In one scenario, the client provides a stable identifier to the AP/WLC. In another scenario, the client requests a stable identifier from the AP/WLC.

In cases where the client generates the stable identifier, the NAS records the identifier and uses it as SMI. Some implementations may choose to let the NAS generate a SMI in all cases, and simply map the NAS SMI to the stable identifier returned by the client.

2.1.1. General Use Cases

In all cases, the RADIUS server received during the 802.1X/EAP phase the client RCM as the Calling-Station-Id value. When the client rotates its MAC address, the RADIUS server receives the new MAC Address as the Calling-Station-Id, and has no mechanism to know that the same client machine is initiating a new session with a new MAC address. This can cause database inflation on the RADIUS server, keeping cached a set of policies for a client that may never come back (as the client is already back with a different MAC address), or causing possible confusion when RCM collision happens. If the wireless infrastructure (NAS) receives a stable machine identifier information from the client, after authentication with the client first MAC address, then the NAS SHOULD share this identifier with the

RADIUS server via the following process.

After the NAS has received a stable identifier representation from the client machine, the NAS SHOULD send a new access-request message to the RADIUS server. The access-request includes the NAS-IP-address or the NAS-Identifier, the Calling-Station-ID, the State attribute and the SMI. The SMI attribute SHOULD be added with the value determined by the NAS from the identifier sent by the client machine. The Calling-Station-ID is the current RCM MAC address. The 48-bit value of all zeros is special, and indicates that the client is requesting a SMI.

The RADIUS server supporting the SMI attribute considers the authentication as already validated and SHOULD return an Access-Accept message containing the SMI attribute. At this point, the RADIUS records the SMI value for that client if it was in the Access-Request message and associates it with the client entry matching the Calling-Station-ID specified in the Access-Request.

If the NAS request had the SMI AVP set to the special all-zero value and the RADIUS server did not uniquely identify the client machine, then the RADIUS server SHOULD return an Access-Accept message with

the SMI AVP set to the special all-zero value. The NAS then generates a local SMI for the client, and sends it to the client machine over a protected frame on one hand, and to the RADIUS server on the other hand. The communication to the RADIUS server takes the form of the Access-Request, Access-Accept exchange described above.

Later, the client rotates its MAC address. If neither the wireless infrastructure or the RADIUS server is forewarned about the change, then a new session is started and the process above repeats. Alternatively, several implementations allow the client machine to forewarn the wireless infrastructure about the upcoming RCM change, and for the AP to know in advance the value of the next MAC address for that client. In that case, the infrastructure recognizes the same machine in the new MAC address. However, the MAC address has changed from the RADIUS viewpoint (new Calling-Station-ID) and most implementations will require a new authentication. As the client initiates a new authentication request to the RADIUS server, the Calling-Station-ID is the new MAC address, and the RADIUS server sees the client as a new machine.

Thus as above, at the end of the re-authentication phase, the NAS SHOULD send to the RADIUS server a new Access-Request message mentioning both the new Calling-Station-ID and the SMI. The RADIUS server records the unicity of the machine across both MAC addresses. This information can be used to flush the older entry, provide continuation of policies (posture) or other purposes.

If the SMI was included in an Access-Request packet, the NAS MUST ensure that the SMI appears in subsequent Accounting-Request (Start, Interim and Stop) for the same client.

The RCM MAC address MUST NOT change when the client use session resumption for EAP. A change at that time would indicate resumption data exchanged with a different client, and thus would be interpreted as a security breach. A client changing its MAC address MUST NOT use any cached session resumption information, and MUST start a new authentication, unless it has first been identified as a single client.

Later and at any time, the source of the SMI (the client or the NAS) may update the SMI value. At that time, the NAS SHOULD send to the RADIUS server the updated SMI as per above. In all these cases, the

SMI is a new attribute to the session identity that the RADIUS server is tracking.

[2.1.2.](#) Special scenarios

The infrastructure can opt to represent to other infrastructure systems (including RADIUS) the client directly as the RCM (case 1), the stable identifier provided by the client (case 2), or another stable identifier generated by the infrastructure (case 3). In case 1, the RADIUS server receives the RCM as the Calling-Station-Id and the provisions from 2.1.1 apply directly. In cases 2 and 3, when the client changes its MAC address and the infrastructure immediately recognizes the new MAC address as representing the same machine as before, no client MAC address change occurs from the perspective of the other infrastructure systems. In this context, RCM management is only occurring within the infrastructure system acting as the NAS, and no new SMI exchange is needed with the RADIUS server. The SMI is expected to be stable, and thus to remain the same as the client changes its MAC address. However, it may happen that the client may decide to provide a new SMI during an active session. It may also happen that the infrastructure decides to change the SMI for a given client. It is only when a new stable machine identifier is shared between the NAS the other infrastructure elements that a new SMI exchange is needed between the NAS and the RADIUS server.

In some cases, the AP and the client establish a secure link, but the client does not immediately exchange with the infrastructure on a unique identifier. In that case, the NAS is initially unable to establish a unique identifier for the client machine, but does not know if the RADIUS server may have such value. Thus, after a secure link has been established with the client, the NAS SHOULD send an Access-Request message to the RADIUS server following the format described in the previous section, with the SMI AVP and its value set

to the special all-zero value. The RADIUS server supporting the SMI attribute but that has not established a unique identifier for the client machine SHOULD respond with an Access-Accept message following the format described in the previous section and the SMI attribute with value set to the special all-zero value. Just as above, the NAS then records that the RADIUS server does not have a stable identifier for the client. Later, the client machine and the NAS exchange on a stable identifier. After this exchange completes, the NAS SHOULD

send a new Access-Request to the RADIUS server as described in the previous section, with the SMI value set. The process then continues as in 2.1.1.

[2.1.3.](#) Failure Handling

Clients not supporting stable identifiers exchanges with the wireless infrastructure will neither provide a stable identifier to the AP/WLC nor request one. As the NAS is unable to determine if the client has exchanged a stable identifier with the RADIUS server, the NAS SHOULD initiate an Access-Request with the SMI value set to the special all-zero value even in that case.

The RADIUS server not supporting the SMI is unable to process the request and SHOULD respond with an Access-Reject message. The NAS SHOULD then consider that the RADIUS server is unable to exchange SMI values for that client, and SHOULD stop sending Access-Requests with SMI values pertaining to that client to that RADIUS server. In this configuration, it is likely that a solid implementation will record this non-support, and stop sending SMIs for later clients as well.

[2.2.](#) Stable RADIUS machine identifier

Some methods use RADIUS to authenticate the client machine itself, irrespective of the user authentication. In that case, the RADIUS server receives a stable identifier for the machine, even when the MAC address and the associated Calling Station-Id are changing.

In this case, the client initially attaches to the network in a constrained state and proceeds through the 802.1X/EAP authentication phase. The client MAC address is likely locally administered. During the authentication phase, the RADIUS server validates the machine identity, or validates the user identity with an identifier also unique for the particular machine.

[2.2.1.](#) General Use cases

After the NAS and the client machine have established a secure connection, no stable identifier exchange occurs between the client and the NAS. Thus the NAS SHOULD send to the RADIUS server an Access-Request for the Calling-Station-ID with the SMI AVP as specified in 2.1.1, but with a payload set to the special all-zero value.

As the RADIUS server uniquely identifies the machine, the RADIUS SHOULD interpret the special all-zero value as 1. the NAS supports the SMI AVP, 2. the NAS does not have an SMI yet for this client and 3. the NAS requests the SMI for the client, if available.

The RADIUS server having established a unique identifier for the client machine SHOULD respond with an Access-Accept response formatted as described in 2.1.1, that includes the SMI AVP and value. It should be clear that in cases where the client uses its real MAC address (locally-significant bit set to 0), the SMI may contain the client Calling-ID value (machine MAC address), or another identifier determined by the RADIUS server and which value is implementation-specific.

In cases where the RADIUS Access-Accept message included a valid (non-zero) SMI value, the NAS records this identifier as a stable value for the client machine.

Later, client MAC rotation occurs and the client does not provide a stable identifier to the NAS during that phase. The NAS thus considers the new MAC address as a new client and initiates 802.1X authentication.

At the end of the authentication, the RADIUS server and the NAS operate as above: the NAS SHOULD send an Access-Request message as described in [section 2.1.1](#) with the SMI AVP, set to the special all-zero value. The RADIUS server has identified the client machine and SHOULD respond with an Access-Accept message, as described in [section 2.1.1](#), containing the SMI AVP and value.

The NAS uses this value to recognize that the new MAC is the same client as the previous MAC. the NAS can then use this awareness to facilitate network operations (e.g. flush previous MAC address cached keys, ensure IP address continuity [DHCP proxy], inform upstream devices [gratuitous ARPs] or others).

If the SMI was included in an Access-Request packet, the NAS MUST ensure that the SMI appears in subsequent Accounting-Request (Start, Interim and Stop) for the same client.

Later and at any time, the source of the SMI (the client or the NAS) may update the SMI value. At that time, the NAS SHOULD send to the RADIUS server the updated SMI as per above. In all these cases, the SMI is a new attribute to the session identity that the RADIUS server is tracking.

[2.2.2.](#) Special scenarios

In some cases, the RADIUS server supports the SMI AVP, receives the Access-Request message with the SMI value set to the special all-zero from the NAS, but the RADIUS server did not uniquely authenticate the machine (e.g. user authentication). The RADIUS server SHOULD then return an Access-Accept message, with the SMI AVP, which payload value is set to the special all-zero value. The NAS records in that case that no SMI is available on the RADIUS server for this client.

[2.2.3.](#) Failure Handling

As in 2.1, RADIUS servers that do not support SMI SHOULD return an Access-Reject message. RADIUS servers that do not receive an Access-Request message with the SMI value from the NAS SHOULD NOT send an unsolicited SMI attribute and value to the NAS.

[2.3.](#) Stable NAS and stable RADIUS machine identifiers

In this scenario, both the NAS and the RADIUS server are able to establish a stable identity for the client, from their respective exchanges with the client. The client first attaches to the network in a constrained state and proceeds through the 802.1X/EAP authentication phase. The client MAC address is likely locally administered. As in 2.2, the server RADIUS uniquely identifies the machine. Additionally, once a protected link has been established between the client and the AP/WLC, as in 2.1, the client requests from the NAS a stable identifier or provides to the NAS a stable identifier. This identifier may be different from that established by the RADIUS server.

[2.3.1.](#) General cases

After keying material is exchanged between the NAS and the client machine, scenario 2.1 occurs. The NAS SHOULD send an Access-Request message to the RADIUS server formatted as described in [section 2.2.1](#), with the SMI AVP. The AVP value is the client identifier determined by the NAS. The RADIUS server compares the value to its own SMI value for that Calling-Station-ID value. Several possibilities arise: * Some RADIUS implementations may decide to replace the RADIUS

SMI with the SMI forwarded by the NAS. In that case, the RADIUS server SHOULD return to the NAS an Access-Accept formatted as

described in 2.1.1, optionally with the SMI AVP, which value is the one sent by the NAS. The NAS records the Access-Accept to signify that the SMI was successfully recorded by the supporting RADIUS server. * Some implementations may decide to replace the NAS SMI with the SMI determined by the RADIUS server. In that case, the RADIUS server SHOULD return to the NAS an Access-Accept message formatted as described in 2.1.1, with the SMI AVP, which value is the one determined by the RADIUS server. The NAS records the Access-Accept and the SMI returned by the RADIUS server. Some NAS implementations may decide to conserve both values, some others may decide to replace the NAS SMI with the SMI returned by the RADIUS server.

If the SMI was included in an Access-Request packet, the NAS MUST ensure that the SMI appears in subsequent Accounting-Request (Start, Interim and Stop) for the same client.

Later and at any time, the source of the SMI (the client or the NAS) may update the SMI value. At that time, the NAS SHOULD send to the RADIUS server the updated SMI as per above. In all these cases, the SMI is a new attribute to the session identity that the RADIUS server is tracking.

2.3.2. Special scenarios

As in 2.1, RADIUS servers that do not support SMI SHOULD return an Access-Reject message. In some cases, the AP and the client establish a secure link, but the client does not immediately exchange with the infrastructure on a unique identifier. In that case, the NAS is initially unable to establish a unique identifier for the client machine, but does not know if the RADIUS server may have such value. Thus, after a secure link has been established with the client, the NAS SHOULD send an Access-Request message to the RADIUS server with the SMI AVP and its value set to the special all-zero value. The RADIUS server supporting the SMI attribute that has established a unique identifier for the client machine SHOULD respond with an Access-Accept message and the SMI attribute and its value as described in [section 2.1.1](#). Just as in 2.2, the NAS then records the RADIUS server SMI value for the client.

Later, the client machine and the NAS exchange on a stable identifier. After this exchange completes, the NAS SHOULD send a new Access-Request to the RADIUS server, formatted as described in 2.1.1, with the SMI value set. The process then continues as in 2.3.1.

[2.3.3.](#) Failure Handling

As in 2.1, RADIUS servers that do not support SMI SHOULD return an Access-Reject message. RADIUS servers that do not receive an Access-Request message with the SMI value from the NAS SHOULD NOT send an unsolicited SMI attribute and value to the NAS.

[3.](#) Stable-Machine-Identifier

The Stable-Machine-Identifier attribute conveys the SMI. A summary of the RADIUS SMI attribute is shown below. The fields are transmitted from left to right. The assignment rules follow [RFC 6929 section 10.3](#)

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	
+-----+-----+		+-----+-----+	
		Extended-Type Value ...	
+-----+-----+		+-----+-----+	

Type:

This field is identical to the Type field of the Attribute format defined in [\[RFC2865\] Section 5](#). The code is 241.

Length

The Length field is one octet and indicates the length of this Attribute, including the Type, Length, and "Value" fields. This field is identical to the Type field of the Attribute format defined in [\[RFC2865\] Section 5](#).

Extended-Type The Extended type field is one octet, and follows the definition of [\[RFC6929\] section 2.1](#). The code is 12.

Value The Value represents the Stable Machine Identifier. The format and content of the value is implementation-specific. Implementations might choose to store the SMI as a 48 bit-value, to match the length of a MAC-address. However, it is RECOMMENDED to use a longer value for better atomicity, for example 256 bits.

[4.](#) Attribute table

The following table provides a guide to which attribute(s) may be found in which kinds of packets, and in what quantity.

Henry & Cam-Winget Expires 13 October 2022 [Page 11]

Internet-Draft RADIUS SMI TLV April 2022

Request	Accept	Reject	Challenge	Accounting # Request	Attribute
0-1	0-1	0	0	0-1	241.12 Stable Machine Identifier

[5.](#) Diameter Consideration

Diameter needs to define an identical attribute with the same Type value. The SMI should be available as part of the NASREQ application [\[RFC4005\]](#).

[6.](#) Security & Privacy Considerations

It is strongly recommended that the SMI format used is such that neither the machine globally unique MAC address nor the machine user identity are revealed. As such, the SMI should not be either of these values, or derived from these values using a simple and reversible algorithm.

The RADIUS entities (RADIUS proxies and clients) outside the home network MUST NOT modify the SMI or insert a SMI in an Access-Accept. However, there is no way to detect or prevent this.

Attempting theft of service, a man-in-the-middle may try to insert, modify, or remove the SMI in the Access-Accept packets and Accounting packets. This risk is common to RADIUS packets and thus also applies

to SMI exchanges. However, RADIUS Access-Accept and Accounting packets already provide integrity protection.

If the NAS includes SMI in an Access-Request packet, a man-in-the-middle may remove it. This will cause the issues that the SMI was designed to solve. To prevent such an attack, and as specified in [RFC 5080](#), the NAS SHOULD include a Message-Authenticator(80) attribute within Access-Request packets containing a SMI attribute.

[7.](#) IANA Considerations

This document requests a new RADIUS Extension Attribute to be defined as: ~~~~ Value: TBD Description: Stable Machine Identifier Data Type: string Reference: this document ~~~~

[8.](#) References

[8.1.](#) 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>>.

- [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/info/rfc2865>>.
- [RFC4005] Calhoun, P., Zorn, G., Spence, D., and D. Mitton, "Diameter Network Access Server Application", [RFC 4005](#), DOI 10.17487/RFC4005, August 2005, <<https://www.rfc-editor.org/info/rfc4005>>.
- [RFC6929] DeKok, A. and A. Lior, "Remote Authentication Dial In User Service (RADIUS) Protocol Extensions", [RFC 6929](#), DOI 10.17487/RFC6929, April 2013, <<https://www.rfc-editor.org/info/rfc6929>>.
- [RFC6973] Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Hansen, M., and R. Smith, "Privacy Considerations for Internet Protocols", [RFC 6973](#),

8.2. Informative References

- [ESNI] Rescorla, E., Oku, K., Sullivan, N., and C. A. Wood, "Encrypted Server Name Indication for TLS 1.3", Work in Progress, Internet-Draft, [draft-ietf-tls-esni-05](#), 4 November 2019, <<https://www.ietf.org/archive/id/draft-ietf-tls-esni-05.txt>>.
- [SEC_IMPACT] Durumeric, Z., Ma, Z., Springall, D., Barnes, R., Sullivan, N., Bursztein, E., Bailey, M., Halderman, J.A., and V. Paxson, "The Security Impact of HTTPS Interception", 26 February 2017, <<https://jhalderm.com/pub/papers/interception-ndss17.pdf>>.
- [TLS_PROXY] Wang, E., Ossipov, A., and R. DuToit, "TLS Proxy Best Practice", Work in Progress, Internet-Draft, [draft-wang-tls-proxy-best-practice-01](#), 4 March 2020, <<https://www.ietf.org/archive/id/draft-wang-tls-proxy-best-practice-01.txt>>.
- [ZUNIGA] Zuniga, J. C., Bernardos, C. J., and A. Andersdotter, "MAC address randomization", Work in Progress, Internet-Draft, [draft-ietf-madinas-mac-address-randomization-01](#), 7 March 2022, <<https://www.ietf.org/archive/id/draft-ietf-madinas-mac-address-randomization-01.txt>>.

Acknowledgments

Authors' Addresses

Jerome Henry
Cisco Systems, Inc.
Email: jerhenry@cisco.com

Nancy Cam-Winget
Cisco Systems, Inc.

Email: ncamwing@cisco.com