

NETEXT WG
Internet-Draft
Intended status: Standards Track
Expires: March 12, 2015

R. Pazhyannur
S. Speicher
S. Gundavelli
Cisco
J. Korhonen
Broadcom
J. Kaippallimalil
Huawei
September 8, 2014

**Extensions to the PMIPv6 Access Network Identifier Option
draft-ietf-netext-ani-location-03.txt**

Abstract

Access Network Identifier (ANI) Mobility option was introduced in [RFC6757] enabling a MAG to convey identifiers like network identifier, geolocation, and operator identifier. This specification extends the Access Network Identifier mobility option with sub-options to carry civic location and MAG group Identifier. This specification also defines a ANI Update timer sub-option that determines when and how often the ANI will be updated.

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 <http://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 March 12, 2015.

Copyright Notice

Copyright (c) 2014 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

(<http://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 Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	2
2.	Conventions and Terminology	3
2.1.	Conventions	3
2.2.	Terminology	4
3.	Protocol Extension	4
3.1.	Civic location Sub-Option	4
3.2.	MAG group identifier Sub-Option	5
3.3.	ANI Update-Timer Sub-Option	5
4.	Protocol Considerations	6
4.1.	MAG Considerations	6
4.2.	LMA Considerations	7
5.	IANA Considerations	8
6.	Security Considerations	9
7.	Acknowledgements	10
8.	References	10
8.1.	Normative References	10
8.2.	Informative References	10
	Authors' Addresses	11

[1.](#) Introduction

[RFC6757] introduced the Access Network Identifier (ANI) mobility Option. This enabled a MAG to provide the Network Identifier, geolocation, and Operator-Identifier sub options. When the access network is WLAN, the Network Identifier sub option may contain SSID and BSSID of the Access Point (AP), the geolocation of the AP, and the Operator-Identifier may contain the realm of the operator managing the WLAN. The MAG sends the above information to the LMA. The LMA may use this information to determine access network specific policies (in terms of QoS, DPI, etc). Further, the LMA may make this information available to location based applications.

While the above mentioned sub-options provide a rich set of information, in this document we describe the need for extending the ANI sub options, especially for WLAN deployments. In WLAN deployments (especially indoor AP deployments), it is difficult to provide Geo-spatial coordinates of APs. At the same time, for many location based applications the civic location is sufficient. This

motivates the need for a ANI civic location sub-option. In many deployments, operators tend to create groups of APs into "AP-Groups". These groups have a group identifier. The group-identifier is used proxy for coarse location (such as floor of a building, or a small building). The group identifier may also be used to provide a common policy (e.g., QoS, charging, DPI) for all APs in that group. This specification provides a sub-option for the MAG to convey a group-identifier to the LMA. The provisioning of the group-identifier is outside the scope of this specification and is typically done via a configuration mechanism such as CLI (Command line Interface), CAPWAP ([RFC5415], [RFC5416]), etc. This document also provides a new sub-option that determines how often the MAG will update the ANI. In typical deployments, it is expected that the MAG will update the ANI as soon as it changes. This is certainly true when the MAG is co-located with the AP. When a client roams from one AP to another AP, the MAG on the roamed (or sometimes referred to as the target) AP will provide the new ANI (for example the network identifier and geolocation of the new AP). However, if the MAG is co-located with an Access Controller (also known as Wireless LAN Controller), then a client roaming from one AP to another AP does not necessarily perform an ANI update. This leads to stale ANI information at the LMA. To cover the cases where ANI is always fresh or potentially "stale", we introduce a new ANI Update Timer option. This enables the MAG to inform the LMA when and how often the MAG will update the ANI. The MAG sends an ANI update only if the ANI Update Timer has expired and the ANI values have changed since the last ANI update. Consequently, this enables the LMA to determine whether the ANI is stale or not and when to expect an update. The LMA can use ANI update Timer option to set the maximum frequency at which it wants to receive ANI updates. This may be particularly useful in environments where a MAG covers a large number of Wi-Fi APs and there is high client mobility between the APs for example in a stadium Wi-Fi deployment. For example, if a LMA does not want ANI updates any more often than 100 seconds, then it can propose 100 seconds as the value for ANI update timer.

[RFC6757] provides ANI sub-options to carry geolocation information. In this document we provide additional sub-options to carry civic location, and group identifier. This document also defines an ANI sub-option to enable a MAG to communicate how often the MAG will update the ANI information.

2. Conventions and Terminology

2.1. Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC 2119](#) [RFC2119].

2.2. Terminology

All the mobility related terms used in this document are to be interpreted as defined in [[RFC5213](#)] and [[RFC5844](#)].

3. Protocol Extension

3.1. Civic location Sub-Option

The civic location is a mobility sub-option carried in the Access Network Identifier option defined in [[RFC6757](#)]. This sub-option carries the civic location information of the mobile node as known to the MAG. The format of this option is defined below.

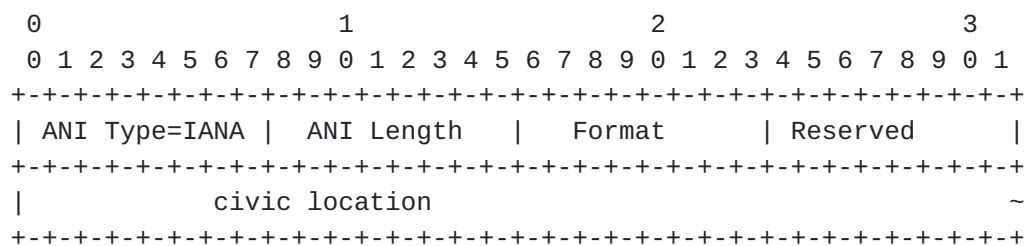


Figure 1: Network-Identifier Sub-option

ANI Type: <IANA-1>

ANI Length: Total length of this sub option in octets, excluding the ANI Type and ANI length fields.

Format: This specifies the encoding format of the civic location. Two values (0, and 1) are defined in this as specification as described below. The remaining values (2 through 255) are reserved.

0: This value denotes Binary Encoding. The location format is based on the encoding format defined in [Section 3.1 of \[RFC4776\]](#), whereby the first 3 octets are not put into the civic location field (i.e., the code for the DHCP option, the length of the DHCP option, and the 'what' element are not included).

1: This value denotes XML Encoding. [[RFC5139](#)] provides an XML format for representing the civic location. This is specified in the Presence Information Data Format Location Object.

civic location: This field will contain the civic location. The format (encoding) type is specified in the format field of this sub option. Note that the length shall not exceed 253 bytes.

3.2. MAG group identifier Sub-Option

The MAG group identifier is a mobility sub-option carried in the Access Network Identifier option defined in [RFC6757]. The MAG group identifier identifies the group affiliation of the MAG within that Proxy Mobile IPv6 domain. The group identifier is not assumed to be globally unique, across different network operators. However, group identifier should be unique within an operator network. In domains spanning multiple operators it is recommended that the operator identifier sub-option (defined in [RFC6757]) be used in addition to group identifier sub-option to ensure uniqueness. When the MAG is configured with a group identifier, the MAG should send its group identifier in the PBU. (The configuration of this identifier is outside the scope of this specification. The usage of the identifier by the LMA is left to implementation.) The format of this sub-option is defined below.

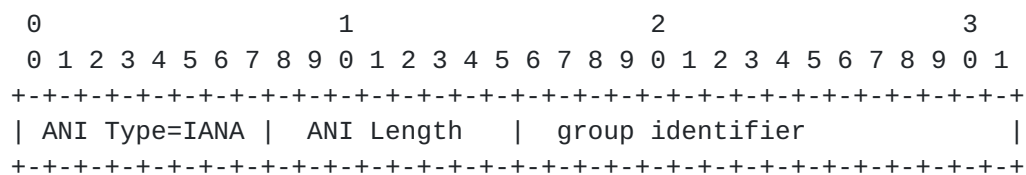


Figure 2: MAG group identifier Sub-option

ANI Type: <IANA-2>

ANI Length: Total length of this sub option in octets, excluding the ANI Type and ANI length fields. The value is always 2.

group identifier: This is a 2 octet unsigned integer value assigned to a group of MAGs.

3.3. ANI Update-Timer Sub-Option

The ANI Update Timer is a mobility sub-option carried in the ANI option defined in [RFC6757]. [Section 4](#) describes how the MAG and LMA use this sub option.

ANI sub-option(s) that the mobile access gateway is configured to carry in the Proxy Mobile IPv6 messages.

- o ANI Update Timer Considerations: The MAG sets the Update-timer based on a exchange of timer values with the LMA. When the Update-Timer Sub option is carried in a PBU, it is considered as a proposed value for the Update-timer. The LMA may change the value of the Update-timer received in the PBU. When the LMA provided value for the Update-timer is different than what is sent by the MAG, the MAG should use the LMA provided value. If the MAG does not receive an Update-timer sub option in PBA (in response to sending the sub-option in the PBU), then MAG behavior is in accordance to [\[RFC6757\]](#). When ANI parameters of a mobility session change, the MAG checks whether the update-timer has expired. If the update timer has expired, the MAG sends a PBU with the ANI option. The ANI option reflects the updated access network parameters for that mobility session. If the update timer has not expired, the MAG does not send a PBU. When the update-timer for a mobility session expires, the MAG checks whether the ANI parameters have changed. If the parameters have changed, the MAG sends a PBU with ANI option. If the parameters have not changed, the MAG does not send a PBU (and the update-timer remains expired). Note that the MAG may send a PBU even before the Update-Timer expires. This could be, for example, to initiate a QoS service request to the LMA (see [\[RFC7222\]](#)). In such cases, the MAG must reset the update timer when it sends a PBU.
- o If the mobile access gateway had any of the Access Network Information mobility options included the Proxy Binding Update sent to a local mobility anchor, then the Proxy Binding Acknowledgement received from the local mobility anchor SHOULD contain the Access Network Information mobility option with the specific sub-options. If the mobile access gateway receives a Proxy Binding Acknowledgement with a successful Status Value but without an Access Network Information mobility option, then the mobile access gateway SHOULD log the event and, based on its local policy, MAY proceed to terminate the mobility session. In this case, the mobile access gateway knows the local mobility anchor does not understand the Access Network Information mobility option and therefore MAY consider it as a misconfiguration of the Proxy Mobile IPv6 domain.

4.2. LMA Considerations

- o The conceptual Binding Cache entry data structure maintained by the local mobility anchor, described in [Section 5.1 of \[RFC5213\]](#), MUST be extended to store the access-network-related information

elements associated with the current session. Specifically, the following parameters MUST be defined:

- * civic location
 - * MAG group identifier
 - * ANI Update-Timer
- o On receiving a Proxy Binding Update message from a MAG with the ANI option, the LMA must process the option and update the corresponding fields in the Binding Cache entry. If the option is not understood by that LMA implementation, it will skip the option and process the PBU without these options.
 - o If the received Proxy Binding Update message does not include the Access Network Information option, then the mobility session associated with that Proxy Binding Update MUST be updated to remove any access network information elements.
 - o If the local mobility anchor understands/supports the Access Network Identifier mobility sub-options defined in this specification, then the local mobility anchor MUST echo the Access Network Identifier mobility option with the specific sub-option(s) that it accepted back to the mobile access gateway in a Proxy Binding Acknowledgement. The civic location and group identifier sub-options defined in this specification MUST NOT be altered by the local mobility anchor. The LMA may change the value of the Update-Timer sub option. It may choose to either echo the same value, or increase or decrease the timer value. For example, if the LMA does not want to receive frequent updates (as implied by the timer value) it may choose to increase the value. Similarly, if the LMA needs to receive ANI updates as soon as possible then it may set the value to zero (0) in the PBA.

5. IANA Considerations

This document requires the following IANA action.

- o Action-1: This specification defines a new Access Network Identifier sub-option called civic location Sub-option. This mobility sub-option is described in [Section 3.1](#) and this sub-option can be carried in Access Network Identifier mobility option. The type value <IANA-1> for this sub-option needs to be allocated from the registry "Access Network Information (ANI) Sub-Option Type Values". RFC Editor: Please replace <IANA-1> in [Section 3.1](#) with the assigned value, and update this section accordingly.

- o Action-2: This specification defines a new Access Network Identifier sub-option called MAG group identifier Sub-option. This mobility sub-option is described in [Section 3.2](#) and this sub-option can be carried in Access Network Identifier mobility option. The type value <IANA-2> for this sub-option needs to be allocated from the registry "Access Network Information (ANI) Sub-Option Type Values". RFC Editor: Please replace <IANA-2> in [Section 3.2](#) with the assigned value, and update this section accordingly.
- o Action-3: This specification defines a new Access Network Identifier sub-option called ANI-Update-Timer Sub-option. This sub-option is described in [Section 3.3](#) and this sub-option can be carried in Access Network Identifier mobility option. The type value <IANA-3> for this sub-option needs to be allocated from the registry "Access Network Information (ANI) Sub-Option Type Values". RFC Editor: Please replace <IANA-3> in [Section 3.3](#) with the assigned value, and update this section accordingly.

6. Security Considerations

The civic location sub-option defined in this specification is carried in the Access Network Identifier option defined in [[RFC6757](#)]. This sub-option is carried in Proxy Binding Update and Proxy Binding Acknowledgement messages. This sub-option is carried like any other Access Network Identifier sub-option as defined in [[RFC6757](#)]. Therefore, it inherits from [[RFC5213](#)] and [[RFC6757](#)], its security guidelines and does not require any additional security considerations.

The civic location sub-option carried in the Access Network Information option exposes the civic location of the network to which the mobile node is attached. This information is considered to be very sensitive, so care must be taken to secure the Proxy Mobile IPv6 signaling messages when carrying this sub-option. The base Proxy Mobile IPv6 specification [[RFC5213](#)] specifies the use of IPSec for securing the signaling messages, and those mechanisms can be enabled for protecting this information. Operators can potentially apply IPSec Encapsulating Security Payload (ESP) with confidentiality and integrity protection for protecting the location information.

Access-network-specific information elements that the mobile access gateway sends may have been dynamically learned over DHCP or using other protocols. If proper security mechanisms are not in place, the exchanged information between the MAG and LMA may be compromised. This situation may result in incorrect service policy enforcement at the local mobility anchor and impact to other services that depend on this access network information. This threat can be mitigated by

ensuring the communication path between the mobile access gateway and the access points is properly secured by the use of IPSec, Transport Layer Security (TLS), or other security protocols.

7. Acknowledgements

TBD

8. References

8.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC4776] Schulzrinne, H., "Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information", [RFC 4776](#), November 2006.
- [RFC5139] Thomson, M. and J. Winterbottom, "Revised Civic Location Format for Presence Information Data Format Location Object (PIDF-LO)", [RFC 5139](#), February 2008.
- [RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", [RFC 5213](#), August 2008.
- [RFC5844] Wakikawa, R. and S. Gundavelli, "IPv4 Support for Proxy Mobile IPv6", [RFC 5844](#), May 2010.
- [RFC6757] Gundavelli, S., Korhonen, J., Grayson, M., Leung, K., and R. Pazhyannur, "Access Network Identifier (ANI) Option for Proxy Mobile IPv6", [RFC 6757](#), October 2012.
- [RFC7222] Liebsch, M., Seite, P., Yokota, H., Korhonen, J., and S. Gundavelli, "Quality-of-Service Option for Proxy Mobile IPv6", [RFC 7222](#), May 2014.

8.2. Informative References

- [RFC5415] Calhoun, P., Montemurro, M., and D. Stanley, "Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification", [RFC 5415](#), March 2009.
- [RFC5416] Calhoun, P., Montemurro, M., and D. Stanley, "Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Binding for IEEE 802.11", [RFC 5416](#), March 2009.

Authors' Addresses

Rajesh S. Pazhyannur
Cisco
170 West Tasman Drive
San Jose, CA 95134
USA

Email: rpazhyan@cisco.com

Sebastian Speicher
Cisco
Richtistrasse 7
Wallisellen, Zurich 8304
Switzerland

Email: sespeich@cisco.com

Sri Gundavelli
Cisco
170 West Tasman Drive
San Jose, CA 95134
USA

Email: sgundave@cisco.com

Jouni Korhonen
Broadcom
Porkkalankatu 24
Helsinki FIN-00180
Finland

Email: jouni.nospam@gmail.com

John Kaippallimalil
Huawei
5340 Legacy Drive, Suite 175
Plano, Texas 75024
USA

Email: john.kaippallimalil@huawei.com

