Internet Engineering Task Force (IETF)
Request for Comments: 7839
Category: Standards Track
ISSN: 2070-1721

S. Bhandari
S. Gundavelli
M. Grayson
B. Volz
Cisco Systems
J. Korhonen
Broadcom Limited

June 2016

Access-Network-Identifier Option in DHCP

Abstract

This document specifies the format and mechanism that is to be used for encoding Access-Network Identifiers in DHCPv4 and DHCPv6 messages by defining new Access-Network-Identifier options and sub-options.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc7839.

Table of Contents

1. Introduction

Access-network identification of a network device has a range of applications. For example, the Local Mobility Anchor (LMA) in a Proxy Mobile IPv6 (PMIPv6) domain is able to provide service treatment for the mobile node's traffic based on the access network to which the mobile node is attached.

This document specifies the Dynamic Host Configuration Protocol for IPv4 (DHCPv4) [RFC2131] and the Dynamic Host Configuration Protocol for IPv6 (DHCPv6) [RFC3315] options for access-network identification that is added by the relay agent in the DHCPv4 or DHCPv6 messages sent towards the server. The scope of applicability for this option is between a DHCP relay agent and a mobile access gateway where the same operator typically operates both these functions

A DHCP relay agent that is aware of the access network and access operator adds this information in the DHCP messages. This information can be used to provide differentiated services and policing of traffic based on the access network to which a client is attached. Examples of how this information can be used in mobile networks can be found in [RFC6757].

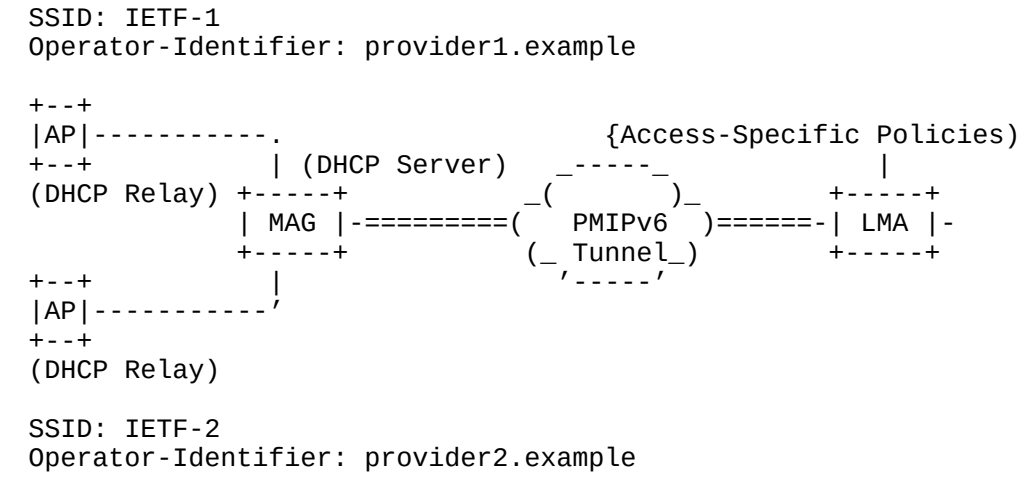
2. Motivation

PMIPv6 [RFC5213] can be used for supporting network-based mobility management in various types of network deployments. The network architectures, such as service provider Wi-Fi access aggregation or WLAN integrated mobile packet core, are examples where PMIPv6 is a component of the overall architecture. Some of these architectures require the ability of the LMA [RFC5213] to provide differentiated services and policing of traffic to the mobile nodes based on the access network to which they are attached. Policy systems in mobility architectures, such as Policy and Charging Control (PCC) [TS23203] and Access Network Discovery and Selection Function (ANDSF) [TS23402] in the 3GPP system, allow configuration of policy rules with conditions based on the access-network information. For example, the service treatment for the mobile node's traffic may be different when they are attached to an access network owned by the home operator than when owned by a roaming partner. In the case of access networks based on IEEE 802.11, the service treatment can also be different based on the configured Service Set Identifiers (SSIDs). Other examples of services include the operator's ability to apply tariff based on the location.

The PMIPv6 extension as specified in [RFC6757] defines PMIPv6 options to carry Access-Network Identifiers in PMIPv6 signaling from the Mobile Access Gateway (MAG) to the LMA. The MAG can learn this

information from the DHCP options as inserted by the DHCP relay agent in the access network. If the MAG relays the DHCP messages to the LMA as specified in [RFC5844], this information can be inserted by the MAG towards the LMA in the forwarded DHCP messages.

Figure 1 illustrates an example of PMIPv6 deployment. In this example, the access network is based on IEEE 802.11 technology, the DHCP relay agent function is located on the Access Point (AP), and the DHCP server function is located on the MAG. The MAG delivers the information elements related to the access network to the LMA over PMIPv6 signaling messages. The MAG obtains these information elements from the DHCP relay agent as per this specification. The information elements related to the access network include the SSID of the used IEEE 802.11 network, the geo-location of the access network to which the mobile node is attached, and the identity of the operator running the IEEE 802.11 access-network infrastructure.



Access Networks Attached to MAG

3. Terminology

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 [RFC2119].

All the DHCP-related terms used in this document are to be interpreted as defined in DHCPv4 [RFC2131] and DHCPv6 [RFC3315] specifications. "DHCP message" refers to both DHCPv4 and DHCPv6 messages throughout this document.

All the mobility-related terms used in this document are to be interpreted as defined in the PMIPv6 specifications [RFC5213] and [RFC5844]. Additionally, this document uses the following abbreviations:

Service Set Identifier (SSID)

The Service Set Identifier (SSID) identifies the name of the IEEE 802.11 network. The SSID differentiates from one network to the other.

Operator-Identifier

The Operator-Identifier is the Structure of Management Information (SMI) Network Management Private Enterprise Code of the IANA-maintained "Private Enterprise Numbers" registry [SMI]. It identifies the operator running the access network where the client is attached.

4. DHCPv4 Access-Network-Identifier Option

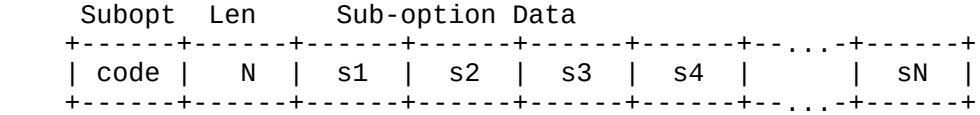
The Access-Network Identifier (ANI) carries information related to the identity of the access network to which the client is attached. This information includes access-technology type, network identifier, and access network operator identifiers.

Relay agents that include ANI information include one or more sub-options (see Section 4.1) in the Relay Agent Information option [RFC3046].

4.1. DHCPv4 Access-Network-Identifier Sub-options

The Access-Network-Identifier information will be defined in multiple sub-options allocated from the "DHCP Relay Agent Sub-Option Codes" registry.

ANI Sub-options: The ANI sub-options consist of a sequence of Sub-Option Code, Length, and Value tuples for each sub-option, encoded in the following manner:



Subopt code
The 1-octet code for the sub-options defined in the following sections.

Len
An unsigned 8-bit integer giving the length of the Sub-option Data field in this sub-option in octets.

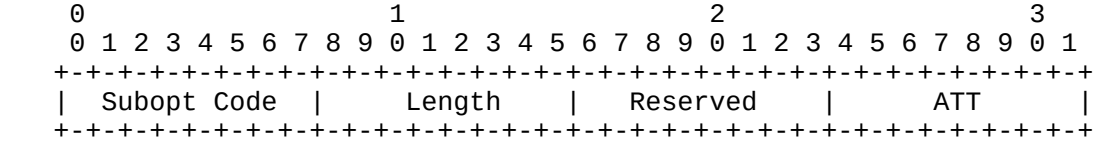
Sub-option Data (s1 to sN)
The data area for the sub-option.

The initial assignment of the DHCP Access-Network-Identifier sub-options is as follows:

SUB-OPTION CODE	SUB-OPTION DESCRIPTION
13	Access-Technology-Type Sub-option
14	Access-Network-Name Sub-option
15	Access-Point-Name Sub-option
16	Access-Point-BSSID Sub-option
17	Operator-Identifier Sub-option
18	Operator-Realm Sub-option

4.2. DHCPv4 Access-Technology-Type Sub-option

This sub-option is used for exchanging the type of the access technology of the network to which the client is attached. Its format is as follows:



Subopt Code
13

Length
2

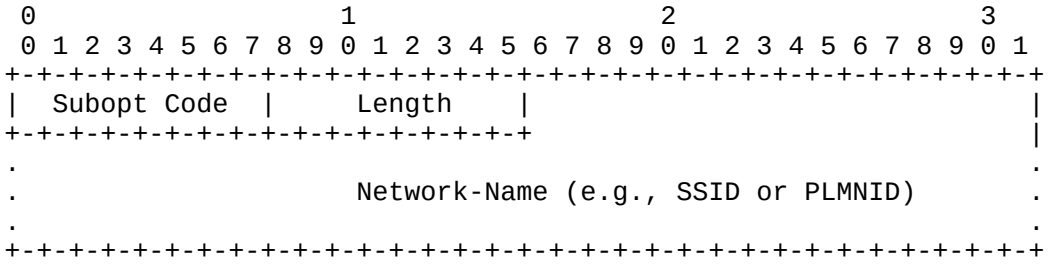
Reserved
An 8-bit field that is unused for now. The value MUST be initialized to 0 by the sender and MUST be ignored by the receiver.

Access-Technology-Type (ATT)
An 8-bit field that specifies the access technology through which the client is connected to the access link from the IANA name space "Access Technology Type Option type values" registry defined in [RFC5213].

4.3. DHCPv4 Network-Identifier Sub-options

These sub-options are used for carrying the name of the access network (e.g., an SSID in the case of an IEEE 802.11 access network or a Public Land-based Mobile Network (PLMN) Identifier [TS23003] in the case of a 3GPP access network) and the Access-Point Name to which the client is attached. The format of these sub-options is defined in the following sections. The Network-Identifier sub-options are only for the currently known access-technology types.

4.3.1. DHCPv4 Network-Name Sub-option



Subopt Code
14

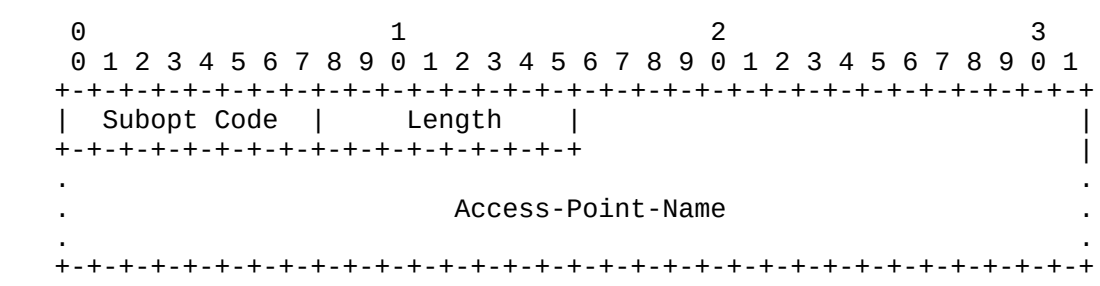
Length
The length of the Network-Name field.

Network-Name
The name of the access network to which the mobile node is attached. The encoding MUST be UTF-8 as described in [RFC3629].

The type of the Network-Name is dependent on the access technology to which the mobile node is attached. For networks based on IEEE 802.11, the Network-Name will be the SSID of the network. For 3GPP access-based networks, it is the PLMN Identifier of the access network, and for 3GPP2 access, the Network-Name is the ANI [ANI].

When encoding the PLMN Identifier, both the Mobile Network Code (MNC) [TS23003] and Mobile Country Code (MCC) [TS23003] MUST be three digits. If the MNC in use only has two digits, then it MUST be preceded with a '0'.

4.3.2. DHCPv4 Access-Point-Name Sub-option

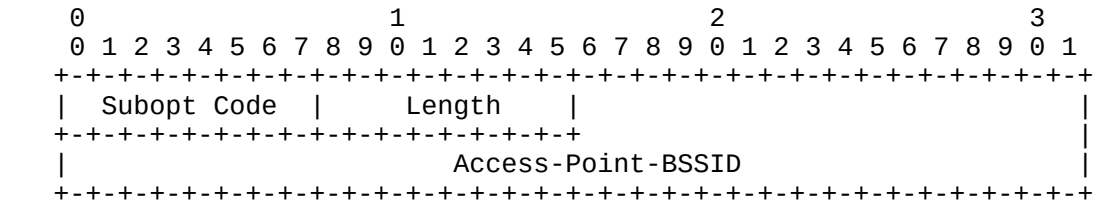


Subopt Code
15

Length
The length of the Access-Point-Name field.

Access-Point-Name
The name of the access point (physical device name) to which the mobile node is attached. This is the identifier that uniquely identifies the access point. While the Network-Name (e.g., SSID) identifies the operator's access network, the Access-Point-Name identifies a specific network device in the network to which the mobile node is attached. In some deployments, the Access-Point-Name can be set to the string representation of the Media Access Control (MAC) address of the device as specified in [RFC6991] (see mac-address typedef) or some unique identifier that can be used by the policy systems in the operator network to unambiguously identify the device. The encoding MUST be UTF-8 as described in [RFC3629].

4.3.3. DHCPv4 Access-Point-BSSID Sub-option



Subopt Code
16

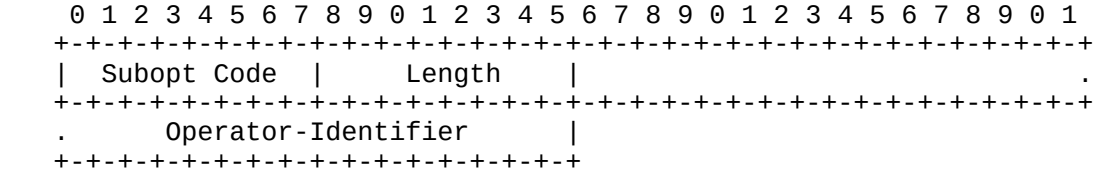
Length
6

Access-Point-BSSID
The 48-bit Basic SSSID (BSSID) of the access point to which the mobile node is attached.

4.4. DHCPv4 Operator-Identifier Sub-options

The Operator-Identifier sub-options can be used for carrying the Operator-Identifiers of the access network to which the client is attached. The format of these sub-options is defined below.

4.4.1. DHCPv4 Operator-Identifier Sub-option

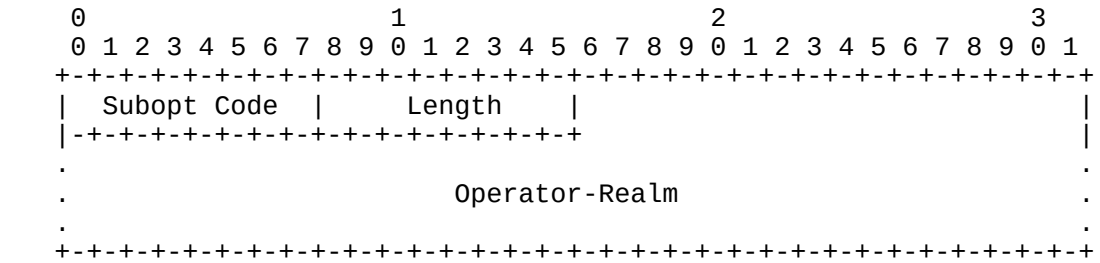


Subopt Code
17

Length
4

Operator-Identifier
The Operator-Identifier is a variable-length Private Enterprise Number (PEN) [SMI] encoded in a network byte order. Please refer to Section 3.1.3 of [RFC6757] for additional details.

4.4.2. DHCPv4 Operator-Realm Sub-option



Subopt Code
18

Length
The length of the Operator-Realm field.

Operator-Realm
Realm of the operator (e.g., EXAMPLE.COM). Please refer to Section 3.1.3 of [RFC6757] for additional details.

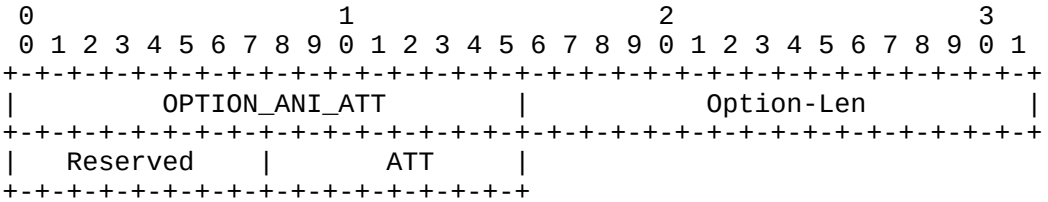
5. DHCPv6 Access-Network-Identifier Options

The Access-Network-Identifier options defined here may be added by the DHCPv6 relay agent in Relay-forward messages.

OPTION CODE	OPTION DESCRIPTION
105	OPTION_ANI_ATT
106	OPTION_ANI_NETWORK_NAME
107	OPTION_ANI_AP_NAME
108	OPTION_ANI_AP_BSSID
109	OPTION_ANI_OPERATOR_ID
110	OPTION_ANI_OPERATOR_REALM

5.1. DHCPv6 Access-Technology-Type Option

This option is used for exchanging the type of access technology the client uses to attach to the network. Its format is as follows:



Option-Code
OPTION_ANI_ATT (105)

Option-Len
2

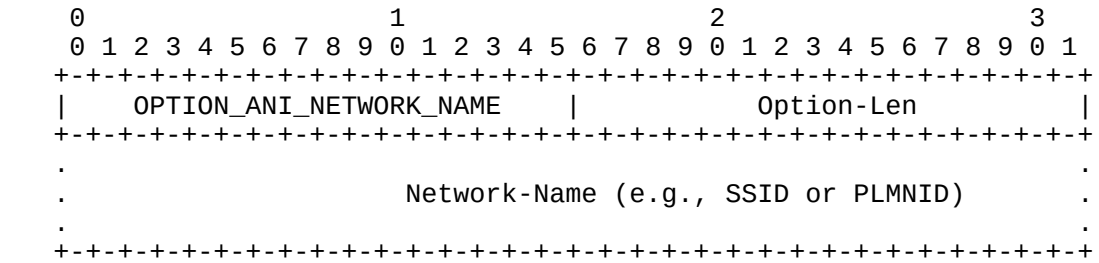
Reserved
An 8-bit field that is unused for now. The value MUST be initialized to 0 by the sender and MUST be ignored by the receiver.

Access-Technology-Type (ATT):
The contents of this field are the same as the ATT field described in Section 4.2.

5.2. DHCPv6 Network-Identifier Options

These options can be used for carrying the name of the access network (e.g., an SSID in the case of an IEEE 802.11 access network or a PLMN Identifier [TS23003] in the case of a 3GPP access network) and an Access-Point Name to which the client is attached. The format of these options is defined below.

5.2.1. DHCPv6 Network-Name Option

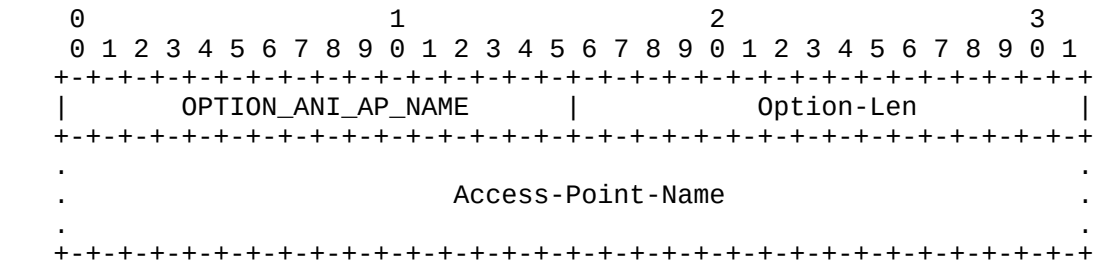


Option-Code
OPTION_ANI_NETWORK_NAME (106)

Option-Len
The length of the Network-Name field.

Network-Name
The contents of this field are the same as the Network-Name field described in Section 4.3.1.

5.2.2. DHCPv6 Access-Point-Name Option

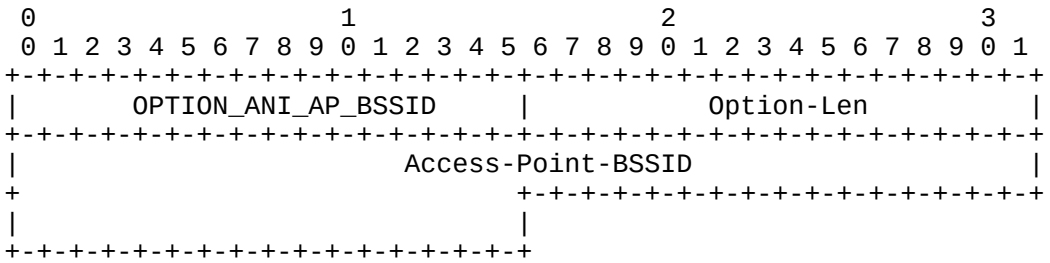


Option-Code
OPTION_ANI_AP_NAME (107)

Option-Len
The length of the Access-Point-Name field.

Access-Point-Name
The contents of this field are the same as the Access-Point-Name field described in Section 4.3.2.

5.2.3. DHCPv6 Access-Point-BSSID Option



Option-Code
OPTION_ANI_AP_BSSID (108)

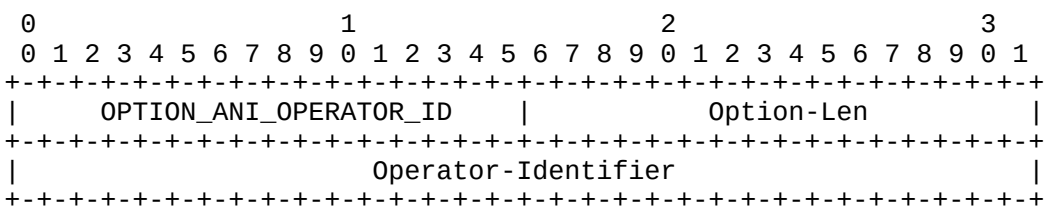
Option-Len
6

Access-Point-BSSID
The contents of this field are the same as the Access-Point-BSSID field described in Section 4.3.3.

5.3. DHCPv6 Operator-Identifier Options

The Operator-Identifier options can be used for carrying the Operator-Identifier of the access network to which the client is attached. The format of these options is defined below.

5.3.1. DHCPv6 Operator-Identifier Option

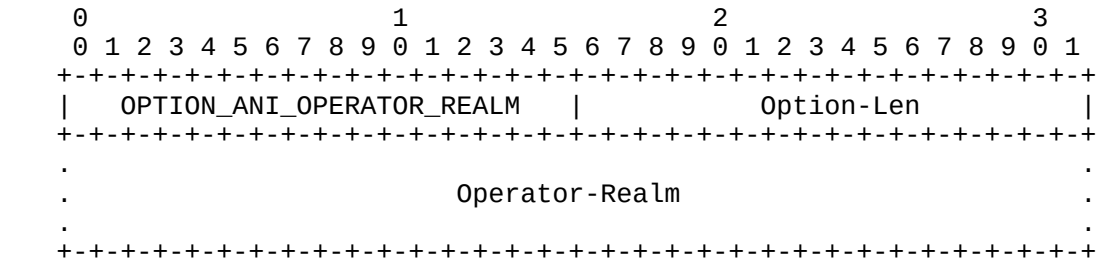


Option-Code
OPTION_ANI_OPERATOR_ID (109)

Option-Len
4

Operator-Identifier
The contents of this field are the same as the DHCPv4 Operator-Identifier Sub-option field described in Section 4.4.1.

5.3.2. DHCPv6 Operator-Realm Option



Option-Code
OPTION_ANI_OPERATOR_REALM (110)

Option-Len
The length of the Operator-Realm field.

Operator-Realm
The contents of this field are the same as the Operator-Realm field described in Section 4.4.2.

6. Relay Agent Behavior

DHCPv4 relay agents MAY include sub-options as defined in Section 4.2 through 4.4 of [RFC3046] in the Relay Agent Information option for providing information about the access network over which DHCP messages from the client are received.

The DHCPv4 relay agent MUST include the DHCPv4 Access-Technology-Type Sub-option (Section 4.2) when including any of these sub-options in the DHCP message: DHCPv4 Network-Name Sub-option (Section 4.3.1), DHCPv4 Access-Point-Name Sub-option (Section 4.3.2), and DHCPv4 Access-Point-BSSID Sub-option (Section 4.3.3).

DHCPv6 Relay Agents MAY include options (defined in Section 5) in the Relay-forward message when forwarding any DHCPv6 message type from clients to the servers to provide information about the access network over which DHCPv6 messages from the client are received.

The DHCPv6 relay agent MUST include the DHCPv6 Access-Technology-Type Option (Section 5.1) when including any of these options in the DHCP message: DHCPv6 Network-Name Option (Section 5.2.1), DHCPv6 Access-Point-Name Option (Section 5.2.2), and DHCPv6 Access-Point-BSSID Option (Section 5.2.3).

7. Server Behavior

The DHCPv4 base specification [RFC2131] requires that the DHCPv4 server ignore the DHCPv4 Access-Network-Identifier Option if it does not understand the option.

If the DHCPv4 server does not understand the received sub-option defined in Sections 4.1 through 4.4 of [RFC3046], the DHCPv4 Relay-Agent-Information Option, it MUST ignore those sub-options only. If the DHCPv4 server is able to process the DHCPv4 Access-Network-Identifier sub-options defined in Sections 4.1 through 4.4 of [RFC3046], the DHCPv4 Relay-Agent-Information Option, it MAY use this information obtained from the sub-option for address pool selection or for policy decisions as per its configured policy. This information obtained from the sub-option SHOULD NOT be stored unless it is absolutely needed. However, if it is stored, the information MUST be deleted as quickly as possible to eliminate any possibility of the information getting exposed to an intruder.

The DHCPv4 server MUST ignore the received DHCPv4 Access-Network-Identifier Option and process the rest of the message as per the base DHCPv4 specifications if the received DHCPv4 message does not include the DHCPv4 Access-Technology-Type Sub-option (Section 4.2) but does include any one of these other options: DHCPv4 Network Name Sub-option (Section 4.3.1), DHCPv4 Access-Point-Name Sub-option (Section 4.3.2), or DHCPv4 Access-Point-BSSID Sub-option (Section 4.3.3).

DHCPv6 base specification [RFC3315] requires that the DHCPv6 server ignore the DHCPv6 Access-Network-Identifier Option if it does not understand the option.

If the DHCPv6 server receives the options defined in Section 5 and is configured to use the options defined in Section 5, it SHOULD look for the DHCPv6 Access-Network-Identifier options in the Relay-forward message of the DHCPv6 relay agent(s) based on its configured policy. The server MAY use received ANI options for its address pool selection policy decisions as per its configured policy. This information obtained from the options SHOULD NOT be stored unless it is absolutely needed. However, if it is stored, the information MUST be deleted as quickly as possible to eliminate any possibility of the information getting exposed to an intruder.

The DHCPv6 server MUST ignore the received DHCPv6 Access-Network-Identifier Option and process the rest of the message as per the base DHCPv6 specifications if the received DHCPv6 message does not include the DHCPv6 Access-Technology-Type Option (Section 5.1) but it does includes any one of these other options: DHCPv6 Network-Name Option

(Section 5.2.1), DHCPv6 Access-Point-Name Option (Section 5.2.2), or DHCPv6 Access-Point-BSSID Option (Section 5.2.3).

8. IANA Considerations

IANA has assigned sub-option codes for the following DHCPv4 sub-options from the "DHCP Relay Agent Sub-Option Codes" registry, <http://www.iana.org/assignments/bootp-dhcp-parameters>:

SUB-OPTION CODE	SUB-OPTION DESCRIPTION
13	Access-Technology-Type Sub-option
14	Access-Network-Name Sub-option
15	Access-Point-Name Sub-option
16	Access-Point-BSSID Sub-option
17	Operator-Identifier Sub-option
18	Operator-Realm Sub-option

IANA has assigned option codes for the following DHCPv6 options from the "Option Codes" registry for DHCPv6, <http://www.iana.org/assignments/dhcpv6-parameters>, as specified in [RFC3315]:

OPTION CODE	OPTION DESCRIPTION
105	OPTION_ANI_ATT
106	OPTION_ANI_NETWORK_NAME
107	OPTION_ANI_AP_NAME
108	OPTION_ANI_AP_BSSID
109	OPTION_ANI_OPERATOR_ID
110	OPTION_ANI_OPERATOR_REALM

9. Security Considerations

Since there is no privacy protection for DHCP messages, an eavesdropper who can monitor the link between the DHCP server and relay agent can discover access-network information.

[RFC3118] and [RFC3315] describe many of the threats in using DHCP. [RFC3118] and [RFC3315] each provide a solution; the Authentication Option for DHCPv4 and DHCPv6 (respectively). However, neither of these options are in active use and therefore are not a viable mitigation option. DHCP itself is inherently insecure and thus link-layer confidentiality and integrity protection SHOULD be employed to reduce the risk of disclosure and tampering.

It is possible for a rogue DHCP relay agent to insert or overwrite with incorrect Access-Network-Identifier options for malicious purposes. A DHCP client can also pose as a rogue DHCP relay agent by sending incorrect Access-Network-Identifier options. While the introduction of fraudulent DHCP relay agent information options can be prevented by a perimeter defense that blocks these options unless the DHCP relay agent is trusted, a deeper defense using the authentication sub-option for the DHCPv4 Relay-Agent-Information Option [RFC4030] SHOULD be deployed as well. Administrators SHOULD configure DHCP servers that use this option to communicate with their relay agents using IPsec, as described in Section 21.1 of [RFC3315].

The information elements that this document is exposing are the client’s access-network information. These pertain to the access network to which the client is attached, such as Access-Technology Type (e.g., WLAN, Ethernet, etc.), Access-Point Identity (Name, BSSID), and Operator-Identifier and Operator-Realm. In deployments where this information cannot be secured using IPsec [RFC4301] or other security protocols, administrators SHOULD disable the capability specified in this document on the DHCP entities.

10. References

10.1. 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, <http://www.rfc-editor.org/info/rfc2119>.

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, DOI 10.17487/RFC2131, March 1997, <http://www.rfc-editor.org/info/rfc2131>.

[RFC3046] Patrick, M., "DHCP Relay Agent Information Option", RFC 3046, DOI 10.17487/RFC3046, January 2001, <http://www.rfc-editor.org/info/rfc3046>.

[RFC3315] Droms, R., Ed., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, DOI 10.17487/RFC3315, July 2003, <http://www.rfc-editor.org/info/rfc3315>.

10.2. Informative References

[ANI] "Interoperability Specification (IOS) for High Rate Packet Data (HRPD) Radio Access Network Interfaces with Session Control in the Access Network", 3GPP2 A.S0008-C v4.0, April 2011.

[RFC3118] Droms, R., Ed. and W. Arbaugh, Ed., "Authentication for DHCP Messages", RFC 3118, DOI 10.17487/RFC3118, June 2001, <http://www.rfc-editor.org/info/rfc3118>.

[RFC3629] Yergeau, F., "UTF-8, a transformation format of ISO 10646", STD 63, RFC 3629, DOI 10.17487/RFC3629, November 2003, <http://www.rfc-editor.org/info/rfc3629>.

[RFC4030] Stapp, M. and T. Lemon, "The Authentication Suboption for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Option", RFC 4030, DOI 10.17487/RFC4030, March 2005, <http://www.rfc-editor.org/info/rfc4030>.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, DOI 10.17487/RFC4301, December 2005, <http://www.rfc-editor.org/info/rfc4301>.

[RFC5213] Gundavelli, S., Ed., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, DOI 10.17487/RFC5213, August 2008, <http://www.rfc-editor.org/info/rfc5213>.

[RFC5844] Wakikawa, R. and S. Gundavelli, "IPv4 Support for Proxy Mobile IPv6", RFC 5844, DOI 10.17487/RFC5844, May 2010, <http://www.rfc-editor.org/info/rfc5844>.

[RFC6757] Gundavelli, S., Ed., Korhonen, J., Ed., Grayson, M., Leung, K., and R. Pazhyannur, "Access Network Identifier (ANI) Option for Proxy Mobile IPv6", RFC 6757, DOI 10.17487/RFC6757, October 2012, <http://www.rfc-editor.org/info/rfc6757>.

[RFC6991] Schoenwaelder, J., Ed., "Common YANG Data Types", RFC 6991, DOI 10.17487/RFC6991, July 2013, <http://www.rfc-editor.org/info/rfc6991>.

[SMI] IANA, "PRIVATE ENTERPRISE NUMBERS, SMI Network Management Private Enterprise Codes", March 2016, <https://www.iana.org/assignments/enterprise-numbers>.

[TS23003] 3GPP, "Numbering, addressing and identification", 3GPP TS 23.003 13.4.0, December 2015.

[TS23203] 3GPP, "Policy and charging control architecture", 3GPP TS 23.203 13.6.0, December 2015.

[TS23402] 3GPP, "Architecture enhancements for non-3GPP accesses", 3GPP TS 23.402 13.4.0, December 2015.

Acknowledgements

The authors would like to thank Kim Kinnear, Ted Lemon, Gaurav Halwasia, Hidetoshi Yokota, Sheng Jiang, and Francis Dupont for their valuable input. Also, thank you to Tomek Mrugalski for a thorough review of the document.

Authors' Addresses

Shwetha Bhandari
Cisco Systems
Cessna Business Park, Sarjapura Marathalli Outer Ring Road
Bangalore, KARNATAKA 560 087
India

Phone: +91 80 4426 0474
Email: shwethab@cisco.com

Sri Gundavelli
Cisco Systems
170 West Tasman Drive
San Jose, CA 95134
United States

Email: sgundave@cisco.com

Mark Grayson
Cisco Systems
11 New Square Park
Bedfont Lakes, FELTHAM TW14 8HA
England

Email: mgrayson@cisco.com

Bernie Volz
Cisco Systems
1414 Massachusetts Ave
Boxborough, MA 01719
United States

Email: volz@cisco.com

Jouni Korhonen
Broadcom Limited
3151 Zanker Rd
San Jose, CA 95134
United States

Email: jouni.nospam@gmail.com