                  Access Network Identifier Option in DHCP
                  draft-ietf-dhc-access-network-identifier-07

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.

Requirements Language

   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].

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

   Access network identification (ANI) of a network device has a range
   of applications. For example the local mobility anchor in a Proxy
   Mobile IPv6 domain is able to provide access network and access
   operator specific handling or policing of the mobile node traffic
   using information about the access network to which the mobile node
   is attached.

   This document specifies Dynamic Host Configuration Protocol for IPv4
   (DHCPv4) [RFC2131] and Dynamic Host Configuration Protocol for IPv6
   (DHCPv6) [RFC3315] options for access network identification that is
   added by Relay agent in the DHCPv4 or DHCPv6 messages towards the
   Server.

   Dynamic Host Configuration Protocol (DHCP) relay agent aware of the
   access network and access operator add 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

   Proxy mobile IPv6 [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
   Proxy Mobile IPv6 is a component of the overall architecture. Some
   of these architectures require the ability of the local mobility
   anchor (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 PCC [TS23203] and ANDSF [TS23402] in 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 a
   access network owned by the home operator than when owned by a
   roaming partner. The service treatment can also be different based
   on the configured Service Set Identifiers (SSID) in case of IEEE
   802.11 based access networks. 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 Mobile
   Access Gateway (MAG) to LMA. MAG can learn this information from
   DHCP options as inserted by DHCP Relay agent before MAG. If MAG
   relays DHCP messages to LMA as specified in [RFC5844] this

information can be inserted by MAG towards LMA in the forwarded DHCP
messages.

Figure 1 illustrates an example Proxy Mobile IPv6 deployment where
Access Points (AP) acting as a DHCP relay agent inserts access
network identifiers in DHCP messages relayed from the connected
clients. The mobile access gateway learns this information over DHCP
and delivers the information elements related to the access network
to the local mobility anchor over Proxy Mobile IPv6 signaling
messages. In this example, the additional information could comprise
the SSID of the used IEEE 802.11 network and the identities of the
operators running the IEEE 802.11 access network infrastructure.
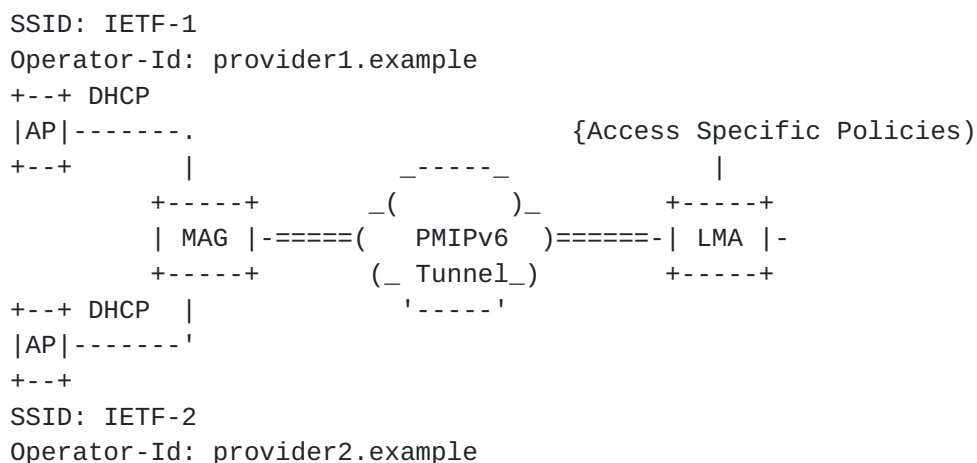
```
      SSID: IETF-1
      Operator-Id: provider1.example
      +--+ DHCP
      |AP|-------.                       {Access Specific Policies)
      +--+       |            _-----_            |
           +-----+        _(       )_        +-----+
           | MAG |-=====(   PMIPv6  )======-| LMA |-
           +-----+        (_ Tunnel_)        +-----+
      +--+ DHCP   |            '-----'
      |AP|-------'
      +--+
      SSID: IETF-2
      Operator-Id: provider2.example

              Access Networks attached to MAG
```

3. Terminology

All the DHCP related terms used in this document are to be
interpreted as defined in the Dynamic Host Configuration Protocol
(DHCPv4) [RFC2131] and Dynamic Host Configuration Protocol for IPv6
(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 Proxy Mobile IPv6 specifications
[RFC5213] and [RFC5844]. Additionally, this document uses the
following abbreviations:

Service Set Identifier (SSID)

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

   Vendor ID

      The Vendor ID is the SMI Network Management Private Enterprise
      Code of the IANA-maintained Private Enterprise Numbers registry
      [SMI].

4. DHCPv4 Access-Network-Identifier Option

   The Access Network Identifier carries information to identify 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 Access Network Identifier 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.

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

```
    SubOpt  Len      Sub-option Data
   +------+------+------+------+------+------+--...-+------+
   | code |  N   | s1   | s2   | s3   | s4   |      | sN   |
   +------+------+------+------+------+------+--...-+------+
```

   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 DHCP access network identifier sub-options
   is as follows:

```
+================+=====================================+
| SUB-OPTION CODE |      SUB-OPTION DESCRIPTION         |
+================+=====================================+
|    <IANA-1>     | Access Technology Type Sub-option   |
+========================================================+
|    <IANA-2>     | Access Network Name Sub-option      |
+========================================================+
|    <IANA-3>     | Access Point Name Sub-option        |
+========================================================+
|    <IANA-4>     | Access Point BSSID Sub-option       |
+========================================================+
|    <IANA-5>     | Operator-Identifier Sub-option      |
+========================================================+
|    <IANA-6>     | 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:

```
   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
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  | Subopt Code  |    Length    |   Reserved   |     ATT      |
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Subopt Code
   <IANA-1>.

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 value 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., a SSID in case of IEEE 802.11 Access Network, or PLMN
   Identifier [TS23003] in case of 3GPP access) and Access Point name to
   which the client is attached. The format of these sub-options is
   defined the following sections.

4.3.1. **DHCPv4 Network Name Sub-option**

```
    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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |  Subopt Code  |    Length     |                               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+                               |
   .                                                               .
   .                   Network Name (e.g., SSID or PLMNID)         .
   .                                                               .
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

   Subopt Code
      <IANA-2>.

   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 IEEE 802.11 based
      networks, the network name will be the SSID of the network. For
      3GPP access based it is the PLMN Identifier of the access network
      and for 3GPP2 access, the Network Name is the Access Network
      Identifier[ANI].

      When encoding the PLMN Identifier, both the Mobile Network Code
      (MNC) [TS23003] and Mobile Country Code (MCC) [TS23003] MUST be 3
      digits. If the MNC in use only has 2 digits, then it MUST be
      preceded with a '0'.

4.3.2. **DHCPv4 Access-Point Name Sub-option**

```
    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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |  Subopt Code  |     Length      |                             |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+                             |
   .                                                              .
   .                       Access-Point Name                      .
   .                                                              .
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Subopt Code
   <IANA-3>.

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 Network Name (e.g., SSID)
   identifies the operator's access network, 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 as specified in [RFC6991] mac-address string
   type of the device 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

```
    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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |  Subopt Code  |     Length      |                             |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+                             |
   |                        Access-Point BSSID                     |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Subopt Code
   <IANA-4>.

Length
   6.

Access-Point BSSID

The 48-bit Basic Service Set Identification (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 identifier of the access network to which the client is
attached. The format of these sub-options is defined below.

4.4.1. DHCPv4 Operator Enterprise ID Sub-option

```
     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
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |   Subopt Code  |     Length     |                             .
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    .       Operator Enterprise ID    |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Subopt Code <IANA-5>.

Length
   4.

Operator Enterprise ID
   The operator's Vendor ID (as described in Section 3) is Private
   Enterprise Number (PEN) [SMI].

4.4.2. DHCPv4 Operator Realm Sub-option

```
     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
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |   Subopt Code  |     Length     |                             |
    |-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+                             |
    .                                                               .
    .                         Operator Realm                       .
    .                                                               .
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Subopt Code
   <IANA-6>.

Length
   The length of the Operator Realm field.

Operator Realm

Realm of the operator (Ex: EXAMPLE.COM). A (home) realm is the
administrative domain with which the user or system maintains an
account relationship. Realm names are required to be unique, and
are piggybacked on the administration of the DNS namespace.
Realms are encoded using a domain name encoding defined in
[RFC1035].

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            |
+================+======================================+
|   <IANA-7>     | OPTION_ANI_ATT                       |
+========================================================+
|   <IANA-8>     | OPTION_ANI_NETWORK_NAME              |
+========================================================+
|   <IANA-9>     | OPTION_ANI_AP_NAME                   |
+========================================================+
|   <IANA-10>    | OPTION_ANI_AP_BSSID                  |
+========================================================+
|   <IANA-11>    | OPTION_ANI_OPERATOR_ID               |
+========================================================+
|   <IANA-12>    | OPTION_ANI_OPERATOR_REALM            |
+========================================================+
```

5.1. DHCPv6 Access-Technology-Type Option

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

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         OPTION_ANI_ATT         |             Option-Len        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Reserved     |      ATT      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Option-Code
   OPTION_ANI_ATT (<IANA-7>).

Option-Len
   2.

Reserved

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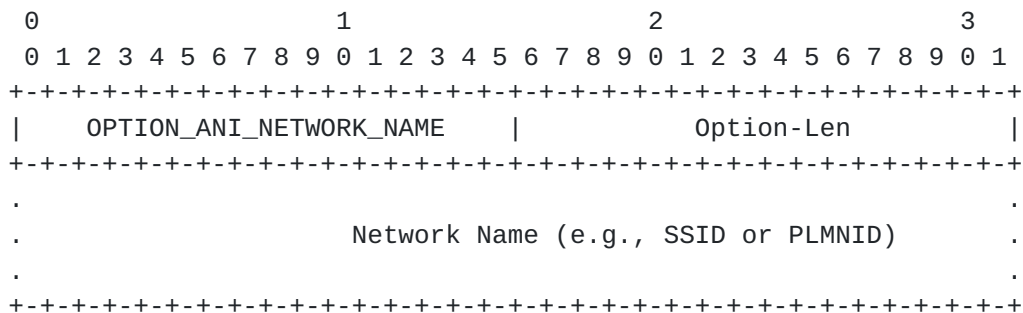initialized to 0 by the sender and MUST be ignored by the
receiver.

Access Technology Type (ATT):
The contents of this field is 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., a SSID in case of IEEE 802.11 Access Network, or PLMN
Identifier [TS23003] in case of 3GPP access) and Access Point name to
which the client is attached. The format of these options is defined
below.

5.2.1. DHCPv6 Network Name Option

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     OPTION_ANI_NETWORK_NAME    |          Option-Len           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
.                                                               .
.                  Network Name (e.g., SSID or PLMNID)          .
.                                                               .
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Option-Code
OPTION_ANI_NETWORK_NAME (<IANA-8>).
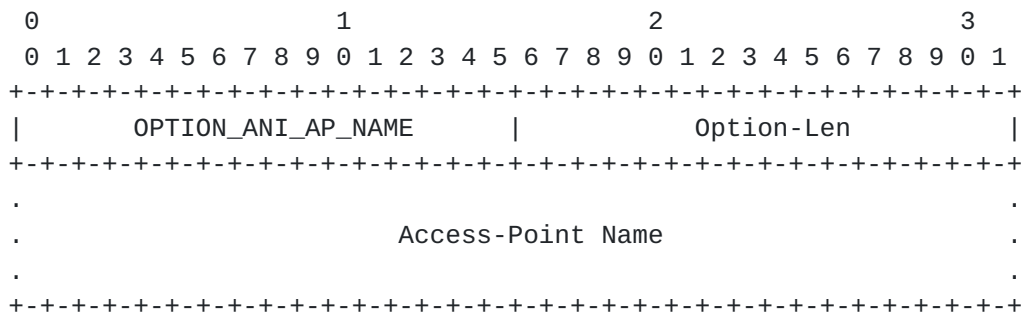
Option-Len
The length of the Network Name field.

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

5.2.2. DHCPv6 Access-Point Name Option

```
       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
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |        OPTION_ANI_AP_NAME       |            Option-Len       |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      .                                                               .
      .                        Access-Point Name                     .
      .                                                               .
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

   Option-Code
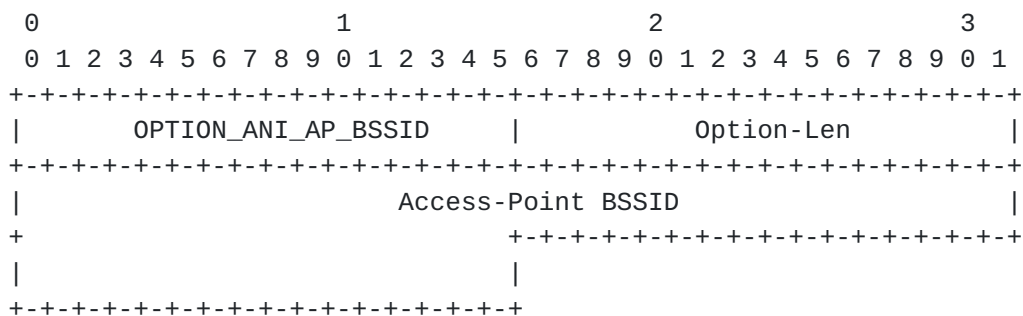   OPTION_ANI_AP_NAME (<IANA-9>).

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

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

5.2.3. DHCPv6 Access-Point BSSID Option

```
       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
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |        OPTION_ANI_AP_BSSID      |            Option-Len       |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |                         Access-Point BSSID                    |
      +                           +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |                           |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

   Option-Code
      OPTION_ANI_AP_BSSID (<IANA-10>).

   Option-Len
      6.

   Access-Point BSSID
      The contents of this field is 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 Enterprise ID Option

```
    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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |     OPTION_ANI_OPERATOR_ID    |            Option-Len          |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                      Operator Enterprise ID                    |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Option-Code
   OPTION_ANI_OPERATOR_ID (<IANA-11>).

Option-Len
   4.

Operator Enterprise ID
   The operator's Vendor ID (as described in Section 3) is Private
   Enterprise Number (PEN) [SMI].

5.3.2. DHCPv6 Operator Realm Option

```
    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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |   OPTION_ANI_OPERATOR_REALM   |            Option-Len          |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   .                                                               .
   .                        Operator Realm                         .
   .                                                               .
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Option-Code
   OPTION_ANI_OPERATOR_REALM (<IANA-12>).

Option-Len
   The length of the Operator Realm field.

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

6. Relay Agent Behavior

DHCPv4 Relay Agents MAY include sub-options defined in section 4.2
through 4.4 in the Relay Agent Information option as defined in
[RFC3046] before forwarding the DHCP message to provide information

about the access network over which DHCP messages from the client is received.

DHCPv6 Relay Agents MAY include options defined in Section 5 in 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 is received.

7. Server Behavior

If DHCPv4 server does not understand the option defined in Section 4 it must ignore the DHCPv4 Access Network Identifier option received. If the DHCPv4 server does not understand the received sub-option defined in sections 4.1 through 4.4 in the DHCPv4 Relay Agent Information option (82) it must ignore those sub-options only. If DHCPv4 Server is able to process the DHCPv4 Access Network Identifier sub-options defined in sections 4.1 through 4.4 received in DHCPv4 Relay Agent Information option, it MAY use this information for address pool selection policy decisions as per its configured policy. The DHCPv4 server MAY store this information along with the lease for logging and audit purpose. The DHCPv4 server MAY use the sub-options defined in sections 4.1 through section 4.4 inserted by the DHCPv4 relay agent in the Relay Agent Information option based on its configured policy. When generating a response, the server echoes back Relay Agent Information options with all received sub-options in it, as specified in Section 2.2 of [RFC3046].

If the DHCPv6 server receives the options defined in Section 5 and is configured to store or 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.

8. IANA Considerations

IANA is requested to assign 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/bootp-dhcp-parameters.xml>:

```
+=================+=========================================+
|  SUB-OPTION CODE |        SUB-OPTION DESCRIPTION           |
+=================+=========================================+
|     <IANA-1>     | Access Technology Type Sub-option      |
+=================+=========================================+
|     <IANA-2>     | Access Network Name Sub-option         |
+=================+=========================================+
|     <IANA-3>     | Access Point Name Sub-option           |
+=================+=========================================+
|     <IANA-4>     | Access Point BSSID Sub-option          |
+=================+=========================================+
|     <IANA-5>     | Operator-Identifier Sub-option         |
+=================+=========================================+
|     <IANA-6>     | Operator-Realm Sub-option              |
+=================+=========================================+
```

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

```
+=================+=========================================+
|   OPTION CODE    |        OPTION DESCRIPTION              |
+=================+=========================================+
|     <IANA-7>     | OPTION_ANI_ATT                         |
+=================+=========================================+
|     <IANA-8>     | OPTION_ANI_NETWORK_NAME                |
+=================+=========================================+
|     <IANA-9>     | OPTION_ANI_AP_NAME                     |
+=================+=========================================+
|    <IANA-10>     | OPTION_ANI_AP_BSSID                    |
+=================+=========================================+
|    <IANA-11>     | OPTION_ANI_OPERATOR_ID                 |
+=================+=========================================+
|    <IANA-12>     | 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.

To minimize the unintended exposure of this information, this option
SHOULD be included by DHCP entities only when it is configured.
Where critical decisions might be based on the value of this option,
DHCP authentication as defined in "Authentication for DHCP Messages"
[RFC3118] and "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)"

[RFC3315] SHOULD be used to protect the integrity of the DHCP
options. Link-layer confidentiality and integrity protection may
also be employed to reduce the risk of disclosure and tampering.

Security issues related DHCPv6 are described in section 23 of
[RFC3315].

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 DHCPv4 relay agent information option
[RFC4030] SHOULD be deployed as well. DHCP server administrators are
strongly advised to configure DHCP servers that use this option to
communicate with their relay agents using IPsec, as described in
Section 21.1 of [RFC3315].

10. Acknowledgements

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

11. References

11.1. Normative References

   [RFC2119]   Bradner, S., "Key words for use in RFCs to Indicate
               Requirement Levels", BCP 14, RFC 2119, March 1997.

   [RFC2131]   Droms, R., "Dynamic Host Configuration Protocol", RFC
               2131, March 1997.

   [RFC3046]   Patrick, M., "DHCP Relay Agent Information Option", RFC
               3046, January 2001.

   [RFC3315]   Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C.,
               and M. Carney, "Dynamic Host Configuration Protocol for
               IPv6 (DHCPv6)", RFC 3315, July 2003.

11.2. Informative References

   [ANI]   "Interoperability Specification (IOS) for High Rate Packet
               Data (HRPD) Radio Access Network Interfaces with Session
               Control in the Access Network, A.S0008-A v3.0", October
               2008.

   [RFC1035]   Mockapetris, P., "Domain names - implementation and
               specification", STD 13, RFC 1035, November 1987.

   [RFC3118]   Droms, R. and W. Arbaugh, "Authentication for DHCP
               Messages", RFC 3118, June 2001.

   [RFC3629]   Yergeau, F., "UTF-8, a transformation format of ISO
               10646", STD 63, RFC 3629, November 2003.

   [RFC4030]   Stapp, M. and T. Lemon, "The Authentication Suboption for
               the Dynamic Host Configuration Protocol (DHCP) Relay Agent
               Option", RFC 4030, March 2005.

   [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.

   [RFC6991]   Schoenwaelder, J., "Common YANG Data Types", RFC 6991,
               July 2013.

   [SMI]   "PRIVATE ENTERPRISE NUMBERS, SMI Network Management
               Private Enterprise Codes", February 2011.

   [TS23003]   "Numbering, addressing and identification", 2011.

   [TS23203]   "Policy and Charging Control Architecture", 2012.

   [TS23402]   "Architecture enhancements for non-3GPP accesses", 2012.

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
USA

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
USA

Email: volz@cisco.com

Jouni Korhonen
Broadcom Communications
Porkkalankatu 24
FIN-00180 Helsinki
Finland

Email: jouni.nospam@gmail.com