Access-Network-Identifier Option in DHCP
draft-bhandari-dhc-access-network-identifier-04

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 of a network device has a range of
   application. For e.g. 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 v4
   (DHCPv4) [RFC2131] and Dynamic Host Configuration Protocol v6
   (DHCPv6) [RFC3315] options for access network identification that is
   added by Client or Relay agent in the DHCPv4 or DHCPv6 messages
   towards the Server.

   Dynamic Host Configuration Protocol (DHCP) client or 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 type 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 client or 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) inserts access network identifiers in DHCP
messages. 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.com
        +--+ DHCP
        |AP|-------.                        {Access Specific Policies)
        +--+       |          _-----_              |
              +-----+       _(       )_        +-----+
              | MAG |-=====(    PMIPv6  )======-| LMA |-
              +-----+       (_ Tunnel_)        +-----+
        +--+ DHCP   |          '-----'
        |AP|-------'
        +--+
        SSID: IETF-2
        Operator-Id: provider2.example.com
```

                 Access Networks attached to MAG

3. Terminology

All the DHCP related terms used in this document to be interpreted as
defined in the Dynamic Host Configuration Protocol v4 (DHCPv4)
[RFC2131] and Dynamic Host Configuration Protocol v6 (DHCPv6)
[RFC3315] specifications. DHCP refers to both DHCPv4 and DHCPv6
messages and entities 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 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

Access network identifier option carries information to identify the
access network to which the client is attached to. This information
includes access technology type, network identifier and access
network operator identifiers.

The format of the DHCPv4 Access-Network-Identifier option is shown
below.


```
    Code    Len           ANI Sub-options
   +------+------+------+------+------+--   --+-----+
   | code | len  |  s1  |  s2  |  s2  | ...   |  sn |
   +------+------+------+------+------+--   --+-----+
```

code: 8-bit code carrying Access Network Identifier sub-options,
      If added by relay agent: Relay Agent Information Option (82)
      If added by client: OPTION_ACCESS_NETWORK_ID (TBD1)

len: 8 bit indicating total length of the included suboptions.

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

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

  ANI Sub-options are defined in following sections.

4.1. DHCPv4 Access-Network-Identifier Sub-options

Access network identifier information will be defined in multiple
sub-options. The initial assignment of DHCP access network
identifier Sub-options is as follows:

```
          Sub-option Code              Sub-Option Description
          ---------------              ----------------------
              TBD7                     Access-Network-Type Sub-option
              TBD8                     Network-Name Sub-option
              TBD9                     AP-Name Sub-option
              TBD10                    Operator-Identifier Sub-option
              TBD11                    Operator-Realm Sub-option
```

5. DHCPv6 Access-Network-Identifier options

   The Access Network Identifier option defined here will be added by
   DHCPv6 client in upstream DHCPv6 messages or by the Relay in Relay-
   forward messages.

```
          Option Code            Descrption
          ---------------        ----------------------
              TBD2               OPTION_ANI_ATT
              TBD3               OPTION_ANI_NETWORK_NAME
              TBD4               OPTION_ANI_AP_NAME
              TBD5               OPTION_ANI_OPERATOR_ID
              TBD6               OPTION_ANI_OPERATOR_REALM
```

6. DHCPv4 and DHCPv6 Access-Network-Identifier Options

   This section defines DHCPv4 suboption and DHCPv6 options for access
   network identification.

6.1. Access-Network-Type option

   This option is used for exchanging the type of the access technology
   the client is attached to the network. There can only be a single
   instance of this specific option in any DHCPv6 message or single
   instance of this specific sub-option in DHCPv4
   OPTION_ACCESS_NETWORK_ID or Relay Agent information option. Its
   format is as follows:

DHCPv4:
```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| suboption-code|   Length      |            ATT                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

 suboption-code: 8-bit code, it should be set to value of (TBD7),
                  indicating that its a Access-Network-Type sub-option

 Length: 8-bit unsigned integer indicating the length of this suboption
     in octets, excluding the suboption-code and length fields.
     This field MUST be set to 2.

DHCPv6:
```
 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 Code (TBD2)       |            OptLen             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      ATT                                      +
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

option-code: 16-bit code OPTION_ANI_ATT (TBD2)
option-length: 16-bit unsigned integer indicating length
                   in octets of this option

Common format applicable to DHCPv4 and DHCPv6:
Access Technology Type (ATT)

     An 16-bit field that specifies the access technology through
     which the client is connected to the access link.

     The values is as populated from the IANA name space
     Access Technology Type Option type values as requested in [RFC5213]

     0: Reserved   ("Reserved")
     1: Virtual   ("Logical Network Interface")
     2: PPP   ("Point-to-Point Protocol")
     3: IEEE 802.3   ("Ethernet")
     4: IEEE 802.11a/b/g ("Wireless LAN")
     5: IEEE 802.16e   ("WIMAX")

6.2. **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. There can only be a single instance
   of each of these options in any DHCPv6 message or single instance of
   each of these sub-options in DHCPv4 OPTION_ACCESS_NETWORK_ID or Relay
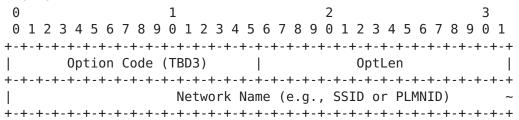   Agent information option. The format of these options is defined
   below.

   DHCPv4:

```
    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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |suboption code |   Length      |                             ~
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                  Network Name (e.g., SSID or PLMNID)       ~
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

   suboption code: 8-bit code, it should be set to value of (TBD8),
                    indicating that its a Network-Name sub-option

   Length: 8-bit indicating Total length of this sub option,
            excluding the suboption code and length fields.
            The value can be in the range of 2 to 32 octets.

   DHCPv6:
```
    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 Code (TBD3)      |            OptLen             |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                  Network Name (e.g., SSID or PLMNID)       ~
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

   option-code: 16-bit code OPTION_ANI_NETWORK_NAME (TBD3)
   option-length: 16-bit unsigned integer indicating length
                       in octets of this option.The value can be in the
                       range of 2 to 32 octets.

   Common format applicable to DHCPv4 and DHCPv6:

   Network Name: The name of the access network to which the mobile
      node is attached. The type of the Network Name is dependent on
      the access technology to which the mobile node is attached. If it
      is 802.11 access, the Network Name MUST be the SSID of the
      network. If the access network is 3GPP access, the Network Name
      is the PLMN Identifier of the network. If the access network is
      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'. Encoding MUST be UTF-8.

   DHCPv4:

    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
   +-+
   |suboption code | Length | ~
   +-+
   | Access-Point Name   ~
   +-+

   suboption code: 8-bit code, it should be set to value of (TBD9),
                   indicating that its a Network-AP-Name sub-option

   Length: 8-bit indicating Total length of this sub option,
            excluding the suboption code and length fields.
            The value can be in the range of 2 to 32 octets.

   DHCPv6:

    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 Code (TBD3) | OptLen |
   +-+
   | Access-Point Name   ~
   +-+

   option-code: 16-bit code OPTION_ANI_AP_NAME (TBD4)
   option-length: 16-bit unsigned integer indicating length
                      in octets of this option.The value can be in the
                      range of 2 to 32 octets.

   Common format applicable to DHCPv4 and DHCPv6:

   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 Media Access
      Control (MAC) address 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 string is carried in UTF-8
      representation.

6.3. 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.There can only be a single instance of each of these options
   in any DHCPv6 message or single instance of each of these sub-options
   in DHCPv4 OPTION_ACCESS_NETWORK_ID or Relay Agent information option.
   The format of these options is defined below.

DHCPv4:

```
  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
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 | suboptioncode |    Length     |                             ~
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 ~      Operator Enterprise ID    |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

   suboption code: 8 bit code, It should be set to value of (TBD10),
                 indicating that it is Operator-Identifier sub-option

   Length: Total length of this sub option, excluding the suboption code
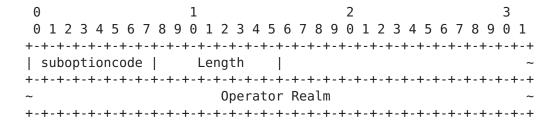   and length fields.

DHCPv6:
```
  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 Code (TBD4)       |             OptLen            |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                 Operator Enterprise ID                        |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

   option-code: 16-bit code OPTION_ANI_OPERATOR_ID (TBD5)
   option-length: 16-bit unsigned integer indicating length
                      in octets of this option.

 Common format applicable to DHCPv4 and DHCPv6:

   Operator Enterprise ID: Vendor ID as a four octet
                       Private Enterprise Number [SMI].

DHCPv4:

```
     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
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    | suboptioncode |     Length    |                             ~
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    ~                      Operator Realm                          ~
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

   suboption code: 8 bit code, It should be set to value of (TBD11),
                indicating that it is Operator-Realm sub-option

   Length: Total length of this sub option, excluding the suboption
      code and length fields.

DHCPv6:

```
     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 Code (TBD4)        |            OptLen             |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    ~                      Operator Realm                          ~
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

   option-code: 16-bit code OPTION_ANI_OPERATOR_REALM (TBD6)
   option-length: 16-bit unsigned integer indicating length
                      in octets of this option.

   Common format applicable to DHCPv4 and DHCPv6:

   Operator Realm: Realm of the operator. 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].Up to 253 octets of the operator realm.

7. Client Behavior

   All hosts or clients MAY include access network identifier options in
   all the upstream DHCP messages to inform the receiver about the
   access network it is attached to.

8. Relay Agent Behavior

   DHCP Relay Agents MAY include these options before forwarding the
   DHCP message to provide information about the access network over
   which DHCP messages from the client is received.

9. Server Behavior

   If DHCP Server is unable to understand this option it MUST be
   ignored. There is no requirement that a server return this option
   and its data in a downstream DHCP message. If DHCP Server is able to
   process these options it MAY use it for address pool selection policy
   decisions if configured. It MAY store this information along with
   the lease for logging and audit purpose.

10. IANA Considerations

   This document defines DHCPv4 Access Network Identifier option which
   requires assignment of DHCPv4 option code TBD1 assigned from "Bootp
   and DHCP options" registry (http://www.iana.org/assignments/
   bootp-dhcp-parameters/bootp-dhcp-parameters.xml), as specified in
   [RFC2939].

   IANA is requested to assign Sub-option codes for the following DHCPv4
   Sub-options from the "DHCP Relay Agent Sub-Option Codes"

           Sub-option Code   Sub-Option Description
           ---------------   ----------------------
               TBD7   Access-Network-Type Sub-option
               TBD8   Network-Name Sub-option
               TBD9   AP-Name Sub-option
               TBD10   Operator-Identifier Sub-option
               TBD11   Operator-Realm Sub-option

   IANA is requested to assign option codes for the following DHCPv6
   options from the "DHCPv6 and DHCPv6 options" registry (http://
   www.iana.org/assignments/dhcpv6-parameters/dhcpv6-parameters.xml).

```
        Option Code              Descrption
        ---------------      -----------------------
            TBD2                OPTION_ANI_ATT
            TBD3                OPTION_ANI_NETWORK_NAME
            TBD4                OPTION_ANI_AP_NAME
            TBD5                OPTION_ANI_OPERATOR_ID
            TBD6                OPTION_ANI_OPERATOR_REALM
```

11. Security Considerations

Since there is no privacy protection for DHCP messages, an
eavesdropper who can monitor the link between the DHCP server, relay
agent and client 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].

12. Acknowledgements

The authors would like to thank Kim Kinnear, Ted Lemon, Gaurav
Halwasia, Bernie Volz for their valuable inputs.

13. Change log

Changes from 00 - 01

o Modified v4 top level option to be either option 82 if added by
   relay or a new top level option if added by client

o Removed DHCPv6 container option

o Reorganized the options to converge v4 and v6 option descriptions

Changes from 01-02

o Modified v4 DHCP option format to align with the 1 byte code, len

o Corrected typos

Changes from 02-03

o No change

Changes from 03-04

o split network name and ap name into separate options, removed E
   bit allowing different encoding

o corrected the option code, type alignment to match the boundary

o split operater id into enterprise id and realm as separate options

[14](). Normative 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.

[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.

[RFC2434]   Narten, T. and H. Alvestrand, "Guidelines for Writing an
            IANA Considerations Section in RFCs", BCP 26, RFC 2434,
            October 1998.

[RFC2939]   Droms, R., "Procedures and IANA Guidelines for Definition
            of New DHCP Options and Message Types", BCP 43, RFC 2939,
            September 2000.

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

[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.

   [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

   Jouni Korhonen
   Renesas Mobile
   Linnoitustie 6
   FIN-02600 Espoo,
   Finland

   Phone:
   Email: jouni.nospam@gmail.com

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

Email: mgrayson@cisco.com