Netext
Internet-Draft
Intended status: Informational
Expires: December 12, 2014

Ravi. Valmikam
Unaffiliated
Rajeev. Koodli
Intel

June 10, 2014

EAP Attributes for WiFi - EPC Integration
draft-ietf-netext-wifi-epc-eap-attributes-08

Abstract

With WiFi emerging as a trusted access network for service providers, it has become important to provide functions commonly available in 3G and 4G networks in WiFi access networks as well. Such functions include Access Point Name (APN) Selection, multiple Packet Data Network (PDN) connections and seamless mobility between WiFi and 3G/4G networks.

The EAP/AKA (and EAP/AKA') protocol is required for mobile devices to access the mobile Evolved Packet Core (EPC) via trusted WiFi networks. This document defines a few new EAP attributes to enable the above-mentioned functions in trusted WiFi access networks.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

WiFi has emerged as a trusted access technology for mobile service providers. It has become important to provide certain functions in WiFi which are commonly supported in licensed-spectrum networks such as 3G and 4G networks. This draft specifies a few new EAP attributes for a Mobile Node (MN) to interact with the network to support some of the functions (see below). These new attributes serve as a trigger for network nodes to undertake the relevant mobility operations. For instance, when the Mobile Node indicates and the network agrees for a new IP session (i.e., a new Access Point Name or APN in 3GPP), the corresponding attribute (defined below) can act as

a trigger for the Mobile Anchor Gateway (MAG) to initiate a new mobility session with the Local Mobility Anchor (LMA). This document refers to [RFC6459] for the basic definitions of mobile network terminology (such as APN) used here.

The 3rd Generation Partnership Project (3GPP) networks support many functions that are not commonly implemented in a WiFi network. This document defines EAP attributes that enable the following functions in trusted WiFi access networks using EAP-AKA' [RFC5448] and EAP-AKA [RFC4187]:

- APN Selection
- Multiple APN Connectivity
- WiFi to 3G/4G (UTRAN/EUTRAN) mobility

Since the attributes defined here share the same IANA registry, the methods are applicable to EAP-AKA', EAP-AKA and EAP-SIM [RFC4186] and, with appropriate extensions, are possibly applicable for other EAP methods as well. In addition to the trusted WiFi access networks, the attributes are applicable to any trusted "non-3GPP" access network that uses the EAP methods and provides connectivity to the mobile EPC (which provides connectivity for 3G, 4G and other non-3GPP access networks).

1.1. APN Selection

The 3GPP networks support the concept of an APN (Access Point Name). This is defined in [GPRS]. Each APN is an independent IP network with it's own set of IP services. When the MN attaches to the network, it may select a specific APN to receive desired services. For example, to receive generic internet services, user device may select APN "Internet" and to receive IMS voice services, it may select APN "IMSvoice".

In a WiFi access scenario, a MN needs a way of sending the desired APN name to the network. This draft specifies a new attributes to propagate the APN information via EAP.

1.2. Multiple APN Connectivity

As an extension of APN Selection, a MN may choose to connect to multiple IP networks simultaneously. 3GPP provides this feature via Additional Packet Data Protocol (PDP) contexts or Additional Packet Data Network (PDN) connections, and defines the corresponding set of signaling procedures. In a trusted WiFi network, a MN connects to the first APN via DHCPv4 or IPv6 Router Solicitation. This document

specifies an attribute that indicates the MN's capability to support multiple APN connectivity.

1.3. WiFi to E-UTRAN mobility

When operating in a multi-access network, a MN may want to gracefully handover it's IP attachment from one access to another. For instance, a MN connected to 3GPP E-UTRAN network may choose to move its connectivity to a trusted WiFi network. Alternatively, the MN may choose to connect from both the access technologies simultaneously, and maintain two independent IP attachments. To implement these scenarios, the MN needs a way to correlate the UTRAN/ E-UTRAN session with the new WiFi session. This draft specifies an attribute to propagate E-UTRAN session identification to the network via EAP. This helps the network to correlate the sessions between the two RAN technologies and thus helps the overall handover process.

2. Reference Architecture and 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].

3. Protocol Overview

3.1. Brief Introduction to EAP

EAP is defined as a generic protocol in [RFC3748]. EAP, combined with one of the payload protocols such as EAP-AKA' [RFC5448] can accomplish several things in a network:

- Establish identity of the user (MN) to the network.

- Authenticate the user during the first attach with the help of an authentication center that securely maintains the user credentials. This process is called EAP Authentication.

- Re-authenticate the user periodically, but without the overhead of a round-trip to the authentication center. This process is called EAP Fast Re-Authentication.

This draft makes use of the EAP Authentication procedure. The use of EAP Fast Re-Authentication procedure is for further study. Both the EAP Authentication and EAP Fast Re-Authentication procedures are specified for trusted access network use in 3GPP. [TS-33.402]

3.2. IEEE 802.11 Authentication using EAP over 802.1X

In a WiFi network, EAP is carried over the IEEE 802.1X Authentication protocol. The IEEE 802.1X Authentication is a transparent, payload-unaware mechanism to carry the authentication messages between the MN and the WiFi network elements.

EAP, on the other hand, has multiple purposes. Apart from it's core functions of communicating MN's identity to the network and proving MN's credentials, it also allows the MN to send arbitrary information elements to help establish the MN's IP session in the network. The following figure shows an example end-to-end EAP flow in the context of an IEEE 802.11 WiFi network.

```
 MN                        WAP                        WAC          IPCN
                                                     (MAG)         (LMA)
 1)|<----------Beacon--------|                         |             |
 2)|<----------Probe-------->|                         |             |
   |                         |                         |             |
   |              802.11 Auth| (Open System)           |             |
 3)|<----------------------->|<----------------------->|             |
   |                         |                         |             |
   |                  802.11 | Association             |             |
 4)|<----------------------->|<----------------------->|             |
   |                         |                         |             |
   |           (802.1X)      |        (CAPWAP/802.1X)  |             |
 5)|<----EAP Req/Identity----|<----EAP Req/Identity----|             |
   |                         |                         |             |
 6)|----EAP Resp/Identity--->|----EAP Resp/Identity--->|             |
   |                         |                         |             |
 7)|<-EAP Req/AKA-Challenge--|<-EAP Req/AKA-Challenge--|             |
   |                         |                         |             |
 8)|-EAP Resp/AKA-Challenge->|-EAP Resp/AKA-Challenge->|             |
   |                         |                         |             |
 9)|<-----EAP Success--------|<-----EAP Success--------|             |
   |                         |                         |             |
10)|<====== 802.11 Data ====>|<=== CAPWAP(802.3 Data)=>|<=Tunnel to=>|
   |                         |                         | core network|
   |                         |                         |             |
```

Figure 1: Example EAP Deployment

Legend:

o MN: Mobile Node

o WAP: WiFi Access Point

- WAC: WiFi Access Controller. In a PMIPv6 [RFC5213] network, hosts the MAG functionality or is assumed to have a suitable interface to the MAG. In the following, we simply use "WAC" notation. The MAG functionality within the WAC (or within the WiFi access network), or a suitable interface to MAG is assumed for PMIPv6 deployments.

- IPCN: IP Core Network. This includes the LMA function. It generically also includes the AAA server function.

-

- NOTE: The figure shows separate WiFi Access Point and WiFi Access Controller, following the split-MAC model of CAPWAP [RFC5415]. A particular deployment may have the two functions within a single node.

Call Flow Description:

1. MN detects a beacon from a WAP in the vicinity

2. MN probes the WAP to determine suitability to attach (Verify SSID list, authentication type and so on)

3. MN initiates the IEEE 802.11 Authentication with the WiFi network. In WPA/WPA2 mode, this is an open authentication without any security credential verification.

4. MN initiates 802.11 Association with the WiFi network.

5. WiFi network initiates 802.1X/EAP Authentication procedures by sending EAP Request/Identity

6. MN responds with it's permanent or temporary identity

7. WiFi network challenges the MN to prove it's credentials by sending EAP Request/AKA-Challenge

8. MN calculates the security digest and responds with EAP Response/AKA-Challenge

9. If authentication is successful, WiFi network responds to MN with EAP Success.

10. End-to-End data path is available for MN to start IP level activity (DHCPv4, IPv6 Router Solicitation etc.,)

4. New EAP Attributes

The following sections define the new EAP attributes and their usage.

4.1. APN Selection

In a WiFi network, a MN includes AT_VIRTUAL_NETWORK_ID attribute in EAP-Response/AKA-Challenge to indicate the desired APN identity for the first PDN connection.

If the MN does not include AT_VIRTUAL_NETWORK_ID attribute in EAP-Response/AKA-Challenge, the network may select an APN by other means. This selection mechanism is outside the scope of this document.

4.2. WiFi to UTRAN/E-UTRAN Mobility

When a multi-access MN enters a WiFi network, if MN intends to continue the IP session previously attached via UTRAN/E-UTRAN, it shall include the following parameters in the EAP-Response/AKA-Challenge.

- AT_HANDOVER_INDICATION : This attribute indicates to the network that MN intends to continue the IP session from UTRAN/E-UTRAN. If a previous session can be located, network shall honor this request by connecting the WiFi access to the existing IP session.

- AT_HANDOVER_SESSION_ID: MN may use this attribute to identify the session on UTRAN/E-UTRAN. If used, this attribute shall contain P-TMSI (Packet Temporary Mobile Subscriber Identity) if the previous session was on UTRAN or shall contain M-TMSI (Mobile Temporary Mobile Subscriber Identity) if the previous session was on E-UTRAN. This attribute helps the network correlate the WiFi session to an existing UTRAN/E-UTRAN session.

4.3. Connectivity Type

A Mobile Node indicates its preference for connectivity using the AT_CONNECTIVITY_TYPE attribute in the EAP-Response/AKA-Challenge message. The preference indicates whether the MN wishes connectivity to the Evolved Packet Core (so-called "EPC PDN connectivity") or Internet Offload (termed as "Non-Seamless Wireless Offload").

The network makes its decision and replies with the same attribute in the EAP Success message.

5. Attribute Extensions

The format for the new attributes follows that in [RFC4187]. Note that the Length field value is inclusive of first two bytes.

5.1. AT_VIRTUAL_NETWORK_ID

The AT_VIRTUAL_NETWORK_ID attribute identifies the virtual IP network that the MN intends to attach to. The implementation of the virtual network on the core network side is technology specific. For instance, in a 3GPP network, the virtual network is implemented based on the 3GPP APN primitive.

This attribute SHOULD be included in the EAP-Response/AKA-Challenge message.

```
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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|AT_VIRTUAL     | Length        | Virtual Network Id            |
|  _NETWORK_ID  |               |                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Virtual Network Id                           |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 2: AT_VIRTUAL_NETWORK_ID EAP Attribute

Virtual Network Id:

An arbitrary octet string that identifies a virtual network in the access technology MN is attaching to. For instance, in 3GPP E-UTRAN, this could be an APN. See [TS-23.003] for encoding of the field.

5.2. AT_VIRTUAL_NETWORK_REQ

When MN intends to connect an APN, MN shall use this attribute to indicate different capabilities to the network. In turn, the network provides what is supported.

From the MN, this attribute can be included only in EAP-Response/Identity. From the network, it SHOULD be included in the EAP Request/AKA-Challenge message. In the MN-to-network direction, the Type field (below) indicates MN's request. In the network-to-MN direction, the Type field indicates network's willingness to support the request; a present Type field indicates the network support for that Type.

```
    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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |AT_VIRTUAL_    |     Length    |  Virt-Net-Req | Virt-Net-Req  |
   |NETWORK_REQ    |               |     Type      |   Sub-type    |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 3: AT_VIRTUAL_NETWORK_REQ EAP Attribute

Virt-Net-Req Type:

Type shall have one of the following values:

- TBA IANA: Reserved

- TBA IANA: Single PDN connection

- TBA IANA : Multiple PDN connection. Can request Non-Seamless WiFi Offload or EPC connectivity (see Connectivity Type attribute below)

Virt-Net-Req Sub-type:

Sub-type shall have one of the following values:

- TBA IANA : Reserved

- TBA IANA : PDN Type: IPv4

- TBA IANA : PDN Type: IPv6

- TBA IANA : PDN Type: IPv4v6

5.3. AT_CONNECTIVITY_TYPE

A Mobile Node uses this attribute to indicate whether it wishes the connectivity type to be Non-Seamless WLAN Offload or EPC. This attribute is applicable for multiple PDN connections only.

From the MN, this attribute can be included only in EAP-Response/ Identity. From the network, it SHOULD be included in the EAP Request/AKA-Challenge message.

```
    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
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |AT_CONNECTIVITY|     Length    | Connectivity  | Reserved      |
    |_TYPE          |               | Type          |               |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 4: AT_CONNECTIVITY_TYPE EAP Attribute

Connectivity Type:

Connectivity Type shall have one of the following values:

- TBA IANA : Reserved

- TBA IANA : Non-Seamless WLAN Offload (NSWO)

- TBA IANA : EPC PDN connectivity

5.4. AT_HANDOVER_INDICATION

This attribute indicates a MN's handover intention of an existing IP attachment.

This attribute SHOULD be included in the EAP-Response/AKA-Challenge message.

```
    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
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |AT_HANDOVER_IND| Length = 1 +  | Handover      |   Pad         |
    |               | Session Id Len| Type          |               |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 5: AT_HANDOVER_INDICATION EAP Attribute

Handover Type:

- 0 - MN has no intention of handing over an existing IP session, i.e., MN is requesting an independent IP session with the WiFi network without disrupting the IP session with the UTRAN/E-UTRAN. In this case, no Session Id (Section 5.5) may be included.

- 1 - MN intends to handover an existing IP session. In this case, MN may include a Session Id (Section 5.5) to correlate this WiFi session with a UTRAN/E-UTRAN session.

5.5. AT_HANDOVER_SESSION_ID

When MN intends to handover an earlier IP session to the current access network, it may propagate identity that can help identify the previous session from UTRAN/E-UTRAN that MN intends to handover. This attribute is defined as a generic octet string. MN may include E-UTRAN GUTI if the previous session was a E-UTRAN session. If the previous session was a UTRAN session, MN may include UTRAN Global RNC ID (MCC, MNC, RNC Id) and P-TMSI concatenated as an octet string.

This attribute SHOULD be included in the EAP-Response/AKA-Challenge message.

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|AT_HANDOVER_   |   Length      |  Access       |  Reserved     |
|  SESSION_ID   |               |  Technology   |               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           Session Id                          |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 6: AT_HANDOVER_SESSION_ID EAP Attribute

Access Technology:

This field represents the RAN technology from which the MN is undergoing a handover.

- TBA IANA: Reserved

- TBA IANA: UTRAN

- TBA IANA: E-UTRAN

Session Id:

An arbitrary octet string that identifies the session in the source access technology. As defined at the begining of this section, the actual value is RAN technology dependent. For E-UTRAN, the value is GUTI. For UTRAN, the value is Global RNC Id (6 bytes) followed by P-TMSI (4 bytes).See [TS-23.003] for encoding of the field.

5.6. AT_MN_SERIAL_ID

This attribute defines the MN's machine serial number. Examples are International Mobile Equipment Identity (IMEI) and International Mobile Equipment Identity Software Version (IMEISV). Other formats may be defined in the future.

This attribute SHOULD be included in the EAP-Response/AKA-Challenge message.

```
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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|AT_MN_         |   Length      |  Serial ID    |  Reserved     |
|  SERIAL_ID    |               |    Type       |               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           MN Serial Id                        |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 7: AT_MN_SERIAL_ID EAP Attribute

Serial ID Type:

This field identifies the type of the MN Identifier. New values may be defined in the future.

o TBA IANA: Reserved

o TBA IANA: IMEI

o TBA IANA: IMEISV

MN Serial Id

An arbitrary octet string that identifies the MN's machine serial number. The actual value is device-specific. See [TS-23.003] for encoding of the field.

6. Security Considerations

This document defines new EAP attributes to extend the capability of EAP-AKA protocol as specified in Section 8.2 of RFC 4187 [RFC4187]. The attributes are passed from the MN to the AAA server. The document does not specify any new messages or options to the EAP-AKA protocol.

The attributes defined here are fields which are used in existing trusted 3G and 4G networks, where they are exchanged (in protocols specific to 3G and 4G networks) subsequent to the mobile network authentication (e.g., using the UMTS-AKA mechanism). The exact model is followed here with the EAP-AKA (or EAP-AKA', EAP-SIM) authentication; the new attributes specified MUST be processed only after a successful EAP authentication. In doing so, the new attribute processing, security-wise, is no worse than that in existing 3G and 4G mobile networks.

7. IANA Considerations

This document defines the following new skippable EAP-AKA attributes. These attributes need assignments from the "EAP-AKA and EAP-SIM Parameters" registry at https://www.iana.org/assignments/eapsimaka-numbers/eapsimaka-numbers.xhtml

o AT_VIRTUAL_NETWORK_ID (Section 5.1) - TBA by IANA

o AT_VIRTUAL_NETWORK_REQ (Section 5.2) - TBA by IANA

o AT_CONNECTIVITY_TYPE (Section 5.3) - TBA IANA

o AT_HANDOVER_INDICATION (Section 5.4) - TBA by IANA

o AT_HANDOVER_SESSION_ID (Section 5.5) - TBA by IANA

o AT_MN_SERIAL_ID (Section 5.6) - TBA by IANA

This document requests a new IANA registry "Trusted non-3GPP Access EAP Parameters", and requests assignments for the following fields:

o Virt-Net-Req Type (Section 5.2) - TBA by IANA

o Virt-Net-Req Sub type (Section 5.2) - TBA by IANA

o Connectivity Type (Section 5.3) - TBA IANA

o Access Technology (Section 5.5) - TBA by IANA

o Serial ID Type (Section 5.6) - TBA by IANA

8. Acknowledgment

Thanks to Sebastian Speicher for the review and suggesting improvements. Thanks to Mark Grayson for proposing the MN Serial ID attribute. And, thanks to Brian Haberman for suggesting a new registry.

9. Informative References

[EPC] "General Packet Radio Service (GPRS);enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access", 3GPP TS 23.401 8.8.0, December 2009.", , <http://www.3gpp.org/ftp/Specs/html-info/23401.htm>.

[GPRS] "General Packet Radio Service (GPRS); Service description; Stage 2, 3GPP TS 23.060, December 2006", , <http://www.3gpp.org/ftp/Specs/html-info/23060.htm>.

[RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, Ed., "Extensible Authentication Protocol (EAP)", RFC3748, June 2004, <http://www.ietf.org/rfc/rfc3748.txt>.

[RFC4186] Haverinen, H. and J. Salowey, "Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)", RFC 4186, January 2006.

[RFC4187] Arkko, J. and H. Haverinen, "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)", RFC4187, January 2006, <http://tools.ietf.org/html/rfc4187>.

[RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.

[RFC5415] Calhoun, P., Montemurro, M., and D. Stanley, "Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification", RFC5415, January 2009, <http://www.ietf.org/rfc/rfc5415.txt>.

[RFC5448] Arkko, J., Lehtovirta, V., and P. Eronen, "Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')", RFC 5448, May 2009.

[RFC6459] Korhonen, J., Soininen, J., Patil, B., Savolainen, T., Bajko, G., and K. Iisakkila, "IPv6 in 3rd Generation Partnership Project (3GPP) Evolved Packet System (EPS)", RFC 6459, January 2012.

[TS-23.003] "3rd Generation Partnership Project: Numbering, Addrssing and Identification, 3GPP TS 23.003 12.2.0, March 2014.", , <http://www.3gpp.org/ftp/Specs/html-info/23003.htm>.

[TS-33.402]
"3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses, 3GPP TS 33.402 8.6.0, December 2009.", , <http://www.3gpp.org/ftp/Specs/html-info/33402.htm>.

Appendix A. Change Log

o: Initial Draft

o: v01: status to Informational, Updated References, Revised the Figure

o: No changes from 01 to 02

o: Per recent 3GPP updates, added the Connectivity Type attribute to allow indicating Non-Seamless WLAN Offload or EPC connectivity

o: version-04: Revised AT_VIRTUAL_NETWORK_REQ to include 1) single PDN vs Multiple PDN connections, 2) PDN Types, and referred to NSWO Connectivity Type attribute

o: version 05: Added AT_MN_SERIAL_ID. Revised the IANA Considerations section

o: version 06, 07: various edits

o: AD review revs

Authors' Addresses

Ravi Valmikam
Unaffiliated
USA

Email: valmikam@gmail.com

Rajeev Koodli
Intel
USA

Email: rajeev.koodli@intel.com