INTERNET-DRAFT J. Mueller
Intended Status: Informational AT&T Foundry
Expires: January 7, 2017 T. Herbert
Facebook
July 6, 2016

Mobility Management for 5G Network Architectures Using Identifier-locator Addressing

draft-mueller-ila-mobility-00

Abstract

This specification describes Mobility Management Architecture for 5G Networks Using Identifier-Locator Addressing in IPv6 for virtualized mobile telecommunication networks. Identifier-locator addressing differentiates between location and identity of a network node. The approach presented in this draft enables mobility management on Layer 3, and provides a simplified and more efficient architecture with less core network utilization compared to traditional architecture.

Table of Contents

1 Introduction and Problem Statement

Mobility has been a challenge for IP based network since the area of smartphones began. One challenge is to ensure seamless and transparent mobility for mobile devices among different locations and in between several Radio Access Technologies. More complexity has been added through Cloud computing and virtualization in which services might change their physical location within a virtualized architecture, too. In regards of current research and develpment on Mobile Edge Cloud and 5G, high availability, low delay and ultra high bandwidth requirements are required for a massive amount of communuicating instances ranging from cellulars, high-definition multimedia streaming, Internet-of-Things (IoT), critical infrastructures among others.

IP has been overloaded and used at teh same time for locator and identifier. requirements: efficient routing, scalability, mobility, security lead changesin the design principles on decoupling Locator-Identifier wihtin IP.

This specification describes Mobility Management Architecture for 5G Networks Using Identifier-Locator Addressing (ILA) ([nvo3]) in IPv6 for virtualized mobile telecommunication networks. Identifier-locator ([nvo3]) addressing differentiates between location and identity of a network node. The approach presented in this draft enables mobility management on Layer 3, provides a simplified and more efficient architecture, less core network utilization.

The concept of ILA extends the Identifier-Locator Network Protocol (ILNP) ([RFC6740], [RFC6741]) defines a protocol and operations model for identifier-locator addressing in IPv6.

1.1 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 RFC 2119 [RFC2119].

The following terminology will be referred to in the document.

* ILA ID or only ID: unique identifier in ILA terms - not used public and only used for GUTI creation for each new attachment. The International Mobile Subscriber Identity (IMSI) can be used for ID generation.

* ILA host: An end host that is capable of performing ILA translations for both sending and receiving. An ILA host uses the

ILA resolver protocol to get identifier to locator mappings for destinations in communication.

* ILA router: A network device that performs ILA translations. ILA routers participate in a mapping distribution protocol.

* Globally Unique Temporary UE Identity (GUTI): temporary address considered as a temporary ILA ID.

* ILA Locator (LOC): either International Mobile Equipment Identity (IMEI) or an IP address that has been assigned to a single UE.

* User Equipment (UE): device with identifier such as a mobile phone or IoT gateway.

* Access Point (AP): Base station, evolved-NodeB (eNB) in 4G.

* Gateway (GW): Gateway, e.g. Serving-Gateway (SWG) or Packet-Data-Network-Gateway (PGW) in 4G.

* Application Function (AF): refers to the 3GPP terminology and stands for any IP service.

2 Motivation There is increasing demand for improved connectivity for a growing number of devices including IoT, mobile phones, cars, etc. 5G

networking is intended to address access and core bottlenecks to provide for lower lower latency, higher throughput, and greater number of connected devices. There are several challenges in applying Mobile-Edge-Computing (MEC) concepts due to Layer 2 tunneling and signaling overhead. The following architecture is based on a layer 3 design that obviates the need for layer 2 tunneling and signaling overhead. The design decisions and call flow outline an approach using ILA for mobility management in 5G networks that overcomes challenges of legacy networks. A flatter network architecture as well as optimizations in the data and control path are presented, which result in a shorter communication path and therefore lower delay.

3 Related Work, Protocols and Concepts This section provides an overview on of the state-of-the-art on related Work, protocols and

concepts for mobility management on mobile networks. In particular the 4th Generation (4G) of mobile telecommunication networks has been taken into comparison for this draft.

3.1 Mobile IPv6 The IETF specified Mobile IPv6 to ensure connectivity and reachability in case of client mobilty within an IPv6 network.

Mobility is solved by assigning an additional IPv6 address - the Care-of-Address (CoA) - next to the current IPv6 address that as been assigned in the home network. Therefore a UE is equipped with a home address, plus primary CoA in case of foreign network attachment. IPv6 is classified as host-based mobility protocol, due to the fact, that the UE is in charge of announcing its mobility to the network. In particular it is the clientresponsibility for signalling binding update signaling to HA. In order to ensure reachability, the UE communicates its new assigned CoA to the Home Agent, which acts as a router and registrar for UEs. Connection requests are intercepted and re-routed in case CoA entries for a UE exists. A tunnel is established between the UE at the CoA and the HA for securely exchanging packets. Per default, the first packet is routed from the correspondent UE towards CoA of the UE via the HA. All consecutive packets will follow on the same path, which might include a detour, but hides the new location of the UE for privacy reasons. The feature of route optimization allows the UE to directly contact the correspondent UE, therefore cuts out the HA from the communication path and forwards packets on a shorter route. Security of the Mobile IPv6 is enhanced through IPSec for binding updates to avoid spoofing of CoA for a UE.

3.2 Proxy MobileIPv6 The IETF specified Proxy Mobile IPv6 provides network-based mobility management for UE and extends the Mobile IPv6 in the way, that host-based mobility management functionalities in Mobile IPv6 are excluded from the client into the network in Proxy Mobile IPv6. The Local Mobility Anchor (LMA) acts as topological anchor point and manages the UE's binding state. The Mobile Access Gateway (MAG) manages the mobility-related signaling on behalf of a UE at the access router. It is responsible for tracking the UE's movements to and from the access link for signaling the UE's local mobility anchor.

3.3 Host Identity Protocol (HIP) HIP ([hip]) is provising a secure solution for identifier/locator-split by adding a new host identity layer into protocol stack. A cryptographic namespace build upon a host identity as public key allows scalability and multi-homing within the network. An extensions of DNS supports rendezvous server functioanlity for secure host identity lookup. A secure channel is establishment over Diffie-Hellmann-key exchange between two communicating entities. The communication setup is considered as robust against DOS, due to a riddle solved at the requestor side. On the other side a high overheaed for the secure communication establishment due to key exchange has to be taken into consideration.

3.4 Locator/ID Separation Protocol (LISP)

https://tools.ietf.org/html/rfc6830 network-layer-based protocol that enables separation of IP addresses into two new numbering spaces: Endpoint Identifiers (EIDs) and Routing Locators (RLOCs) tunnel router encapsulates and decapsulates packets

3.5 ILNP

3.6 Identifier-Locator Addressing (ILA) * reduced header size * MN - Network Virtualization Edge * NVE creates and maintains local state

about each Virtual Network for which it is providing service on behalf of a Tenant System.

3.7 Comparison of ILA to alternative approaches

This section compares the ILA approach to some alternatives that have been discussed in 5gangip list.

3.7.1 ILNP

Identifier Locator Network Protocol (ILNP [RFCXXXX]) is an experimental protocol that splits and IPv6 address into a locator and identfier. ILA is fundamentally based on ILNP.

The key differences between ILA and ILNP are:

* ILNP requires changes to the transport layer. This limits ILNP to be used only on hosts and every transport protocol implementation would need to be modified to use ILNP. Presumably to overcome the limitation above, some sort of ILNP proxy could be defined to perform ILNP in a middlebox.

* ILA does not require changes to the transport layer.

* Checksum neutral translation means that transport layer does not need to be parsed to perform ILA. This also ensures that existing device offloads (like checksum offload) work seamlessly.

* ILNP employs IPv6 extension headers which are mostly considered non-deployable. ILA does not use these.

* Core support for ILA is in upstream Linux, to date there is no publically available source code for ILNP.

* ILNP involves DNS to distribute mapping information, ILA assumes mapping information is not part of naming.

3.7.2 LISP

Locator Identifier Separation Protocol (LISP [RFCXXXX) is an IP encapsulation protocol where the destination address in the outer IP header is a locator and the destination address in the inner header is an idnetifier.

The key differences between ILA and LISP are:

* ILA is not encpasulation so there is not associate encapsulaiton overhead. For instance IPv6/IPv6 in LISP would have 52 bytes of overhead whereas ILA translation has zero.

* LISP may not work with some network device offloads whereas ILA works with all stateless offloads (ILA is transparent to the network so that it would just see TCP/IP packets for instance).

* ILA has been accpeted into Linux, LISP has not been accepted.

* ILA can run either on end hosts (ILA hosts) or in the network (ILA routers). In ILA hosts the mapping database is a cache to optimize communications.

* ILA defines locators and identifiers to be 64 bits whereas LISP allows them to be full 128 bit address making for for memory needed in mapping table.

* ILA is not encpasulation so there is not associate encapsulaiton overhead. For instance IPv6/IPv6 in LISP would have fifty-six bytes of overhead whereas ILA translation has zero.

* The process of ILA translation is much more efficient than performing LISP. The translation path is:

  1) Parse IP header and extract the destination address

  2) Lookup destination in a hash table (obviated with cached route for ILA hosts)

  3) Write new destination address (16 byte copy)

  4) Forward to new destination (or receive at final destination).

  LISP processing is more involved. To do encapsulation an outer IP header, UDP header and LISP header need to be inserted. Tunnel fragmentation and MTU need to be considered [RFCXXXX] (i.e. increasing the size of a packet may exceed tunnel MTU). At the remote tunnel end point, the outer IP header must be

validated and aa lookup done on the destination address to see if it is a local address . A lookup must be done on the destination UDP port to find that it is a LISP port. If the UDP checksum is not zero that must also be validated. The LISP header must also be processed. Once the encapsulation is verfied, the headers are removed and the inner packet is either forwarded or received.

3.8 Taxonomy & Summary Comparing solutions above in a taxonomy and compare them using the following parameters:

* multi-homing? * multi-path? * IP-session continuity: all three * seamless handover or transparent handover? Attached with same or different interface * state - number and positions * overhead through tunneling or header extension * client mobility support and efficient update of location information in the network * number of functional elements in the architecture

4 Mobility Management Architectures for 5G Network Using ILA This section outlines the architecture supporting ILA in mobile

networks. The main functional blocks for connectivity, mobility support, security and charging are presented. Message flows for basic use cases executed by the mobile UE such as attachment, data transport with session handover and detachment are outlined.

4.1 Address format for ILA mobile

The address format is derived out of the ILA draft in ([nvo3]).

```
      /* IPv6 canonical address format */      |            64
bits              |             64 bits          |      +-------
-------------------------+-------------------------------+
|   IPv6 Unicast Routing Prefix  |      Interface Identifier
|      +---------------------------------+----------------------
--------+

      /* ILA for IPv6 */      |            64 bits
|3 bits|       61 bits          |      +------------------------
--------+-------------------------------+      |
Locator            | Type |     Identifier         |      +-----
-----------------------------------------------------------+
```

4.2 Architecture with functional elements and reference points

The presented architecture is aligned on the 3GPP Evolved Packet System ([23.401], [23.402]) following the separation of control plane and data plane. Whereas 3GPP EPS addresses mobility through Layer 2 tunneling with GTP, this approach provides a Layer 3 mobility approach utilizing the ILA concepts for mobility.

TODO: architecture bootstrapping: which entity assigns ILA address space for LOC and ID?

4.3 Functional Elements

* The User Equipment (UE) is the mobile device (cellular or laptop) executing services such as apps on the device, binding apps to the ID as communication endpoints, handling the bindings of all associated LOC/ID's and performing mobility as described below. The UE performs security related functions via its (Embedded) SIM handing at least one or multiple identifiers provisioned by one or multiple network operators. Security related functions include authentication of the UE towards the network (more specifically the AP) and certificate management for establishing secure transport connections. Either the UE supports IPv6 or ILA for handling locator and ID bindings and updates or the etwork is handling ILA functionality on behalf of the UE. Storage and management of multiple locators for multi-path and multi-homing is supported by the UE support.

* The Access Point (AP) is the first point of contact from the UE when attaching over radio to the network. Its main purpose is routing, gating and forwarding data and control packets. The Radio Access Technology (RAT) is independent of the proposed concept and therefore out of scope of this document. 3G, 4G, 5G or WiFi are applicable RATs. The AP is also capable of caching for Content-Centric-Networks (CCN) TODO:LINK like apps, in order to store content or host service instances close to the user at the edge of the network. Another aspect of the cache is to support transparent handovers, during which buffering of packets at the target AP is required. Therefore a X2-like connection between APs is required. The AP supports a support a policy enforcement function (PEF) as well as a Event Reporting Function (ERF) aligned on the 3GPP defined Policy Control and Charging (PCC) functionality for the EPS in ([23.203], [29.212]). Uplink QoS management is handled by the AP, too. In order to differentiate between multiple types of data traffic, signaling, high-priority, real-time and non-real-time connections can be

distinguished and the order of packet processing in the AP can be influenced for uplink. The same concept applies for downlink in the GW. Forward Error Correction (FEC), IP header compression, encryption of user data stream are supported by the AP, too.

* The Gateway (GW) encompasses management and policy enforcement functions as well. Its main purpose is routing, gating and forwarding data and control packets. Therefore functionalities such as downlink QoS enforcement, APN management and charging is performed by each GW.

* The Mobility Management Entity (MME) handles the initial authentication, authorization and mobility management of UE's over the control plane. The MME is responsible for tracking the UE's mobility and is in charge for updating the registries with near real-time status updates for LOC/ID mapping. ID and LOC assignment are performed by the MME.

* The Home Subscriber Server (HSS) stores and manages user profile information. These include the static information such as the assigned ID, security credentials as well as dynamic information LOC and the current Tracking Area.

* The Policy Charging Rules Function (PCRF) controls data flows in the network architecture according to pre-defined rules. Such rules can be created by the network operator such as an upper limited for the data rate or total bytes transferred given a time interval (e.g. 2GB per month data plane with unlimited speed and a reduction of bandwidth after reaching the limit of 2G). Other rules differentiate between class of services for various traffic flow types identified on their Traffic Flow Template (TFT) characteristics such as source, destination, port and protocol information. The PCRF is handling charging for traffic flows using online (pre-paid) and offline (post-paid) charging. Both charging modes include a charging based on metrics such as service invocations, online time, data transferred, or no-charging. Out of credit events may influence the current connectivity for online charging, whereas offline charging is accumulating charging records which are usually processed in a monthly period.

* The Access Network Discovery and Selection Function (ANDSF) is

a database used for mapping the user location with available access networks. With this information, the ANDSF is capable of signaling suggestions for handovers to UE's. A UE is therefore able to operate only on one interface at a time to save resources. In case of the availability of adjacent RAT and after reception of a handover suggestion from the ANDSF, the UE is able to enable the suggested interface, perform a scan and finally decide whether or not to attach to the new targeted RAT. The database can be filled using device monitoring/telemetry statistics signaled from the UE to the network or by active measurements of the environment.

TODO: OPEN - assignment to Functional Elements needed * filtering * gating * legal interception on the AP, to include the case, in which traffic re-routed only by the AP and is not traversing the GW.

4.4 Signaling and data flow

4.5.1 Provisioning A Subscriber Identity Module (SIM)-card is provisioned by the network operator with a unique ID, that is

comparable to the IMSI in 3GPP telco architectures (2G, 3G and 4G). This draft is no differentiating between a physical or an embedded SIM. The ID unambiguous identifies the UE within the global network, is used for identification, authentication, authorization and charging purposes. In addition, security credentials and preferred network identifier are provisioned for authentication as well as network selection are provisioned. The matching information to the SIM card is stored in the HSS.

4.5.2 Attachment After powering on the device, a scan for available networks is performed on the device, which selects the network

with the strongest signal and performs a network attachment procedure aligned with ([23.401], [23.401]) towards the Access Point (AP) using security parameters, ID, last MME associated with (GUMMEI) and last GUTI assigned by MME with ID GUMMEI - the Packet Temporary International Mobile Subscriber Identity (M-TSMI).

For each network attachment and due to privacy concerns for not revealing the identify of the UE towards the public, a creation of a Globally Unique Temporary UE Identity (GUTI) is performed.

The AP derives the last MME association out of the network attachment request sent by the UE and queries the last or a new

MME based on availability of information for UE authentication. The MME performs a lookup in the user database of the network operator, which is the Home Subscriber Server (HSS) and/or Home Location Register (HLR) and receives a profile in return.

In the following, the MME selects and configures the AP and GW according to the profile received and signals the profile including the GUTI towards the AP and GW.

The AP allocates a LOC for the UE, binds the GUTI-LOC combination locally in a cache, publishes its binding in the MME and signals the GUTI-LOC towards the client.

Quality of Service (QoS) and charging related policies are installed in the AP and GW. The AP handled uplink and the GW downlink related traffic shaping functions. Charging can be performed in both functional elements (AP or GW), whereas a centralized charging in case of multi-path streaming is preferred.

4.5.3 Communication scenarios for data transport for an End-to-End session After the successful attachment, a service can be

invoked. There are three main data path to be considered, to address all use cases. The use cases can be distinguished between a UE accessing a service in the AF. A UE is communicating with another UE. The example use cases below outline the details and point out the differences compared to today's networks.

TODO: Include schema as in nvo3 - 5.3 Reference network for scenarios

1) UE to AF through the complete network

Considering a communication scenario in which a UE queries a website ("http://about.att.com/innovation/foundry") in a browser. An ID is retrieved in return from the DNS.

UE[Task UE_T1] -> DNS // request ID for URL DNS -> UE[Task UE_T1] // ID for URI

The sequence for traversing the network looks as follows.

UE(GUTI/LOC):[Task UE_T1] <-> AP <-> GW <-> AF[Task AF_T1]

The request is forwards to the AP, which performs ILA router functionality and a lookup in a local lookup table. Depending on finding an entry in the local lookup table, the routing is influenced and the packet is redirected. Otherwise routing on the initial destination LOC/ID is fulfilled.

2) UE_1 to UE_2 attached to distinct APs

UE1[Task UE1_T1] <-> AP_1 <-> GW <-> AP_2 <-> UE2[Task UE2_T1]

Considering a communication scenario in which one mobile device (UE1) is contacting a second mobile device (UE2). ILA routing is done in the AP. TODO: Classic signaling and data flow similar to legacy networks.

3) UE_1 to UE_2 attached to the same AP

UE_1[Task UE1_Tx] <-> AP <-> UE_2[Task UE2_Ty]

Considering a communication scenario in which two communicating entities are attached to the same AP and therefore are in close proximity. The solution for routing traffic in todays network is the establishment of the datapath from the UE over the access network (e.g. eNB) into the core network (e.g. EPC) and back to the access network and finally to the UE. Charging needs to be performed in the AP for this data flow. This communication pattern creates a delay caused by the bearer concept of 3GPP network, which encapsulate and de-apsulate data in Layer 2 tunnels between the eNB and the PGW.

4) UE to Mobile Edge Cloud (MEC) UE[Task UE_T1] <-> DNS Considering a communication scenario in which a Virtual Reality (VR) application on a smartphone is accessing a low-delay service in the network e.g. an image recognition service. In order to provide a high quality of experience for the user, the delay between the mobile device and the service should be reduced.

Firstly, a DNS lookup resolves the URL into a ID to identify the closest service instance. The lookup process may be resolve to a service co-located at the AP or trigger the deployment of that service instance within a datacenter co-located or attached to the AP.

A request is created and addressed with the source LOC/ID and

targeted towards the destination LOC/ID.

The sequence for traversing the network looks as follows.

UE[Task UE_T1] <-> AP <-> AF[Task AF_T1]

5) Summarizing, the use of ILA for mobile reduces allows multiple improvements compared to legacy telecommunication networks. Firstly, the improved datapath has less hops to traverse between UE and AF or UE_1 and UE_2 due to the flatter architecture. Secondly, the less overhead is created due to the reduction of GTP tunnels between network elements. Thirdly, the more efficient routing reduces the core network traffic by routing traffic particularly locally and avoiding re-routing and traffic forwarding through the complete core network, even in scenarios, in which the communication partner are in close proximity and attached to the same AP. lower delay, which is one critical requirement for 5G networks.

4.5.4 Homogeneous Handover Client mobility using the same access network technology due to location changes is referred to as homogeneous handover. Triggers for homogeneous handover may be changes in signal strength at the UE or network based handover due to network policies such as load balancing.

The status information (the list of signals received from adjacent APs including their signal strength) signaled from the UE towards the AP indicates its position via triangulation as well as the alternative AP's to which the UE may connect to.

Reasons for handovers may be evacuation/preemption of resources on the AP due to emergency scenarios or higher priority calls, UE/AP/service load balancing or physical mobility of the UE among the network. The current resource utilization (e.g. data rates) of the UE or historical traffic pattern may influence the handover and the AP selection process.

The MME selects a new AP (AP_new) as target for the handover of the UE away from the current AP (AP_current). The decision is signaled to related AP's and the UE. AP_current starts de-allocating resource blocked by the UE and AP_new blocks resources required by the UE. Since most UE's are considered to have only a single RAT of each type (one WLAN or one LTE interface) an interruption in the connection while handover is to be expected. In order to avoid packet loss at the UE, buffering at the AP_new as well as packet forwarding from AP_current to AP_new are supported. Only after UE successfully

establishes connectivity at the AP_new, previously blocked resources at AP_current are freed up, which are used as handover role-back in case of failure. Finally the MME announces the new LOC(AP_new)/ID for the UE as an update at GW and in the DNS.

New incoming connections are forwards directly towards the UE over AP_new using the proclaimed LOC/ID.

4.5.5 Heterogeneous Handover Client mobility may involve various Radio Access Technologies (RAT), in which the client is handed off

from RAT_1 to RAT_2. The client is not required to move physically for heterogeneous mobility. Instead measurements on the UE or suggestion from the network over the ANDSF may trigger handovers even when the UE is physically not moving.

Heterogeneous handover may be motivated for optimizing connectivity between UE and a service to move a multimedia connection with high bandwidth requirements from cellular towards WLAN or a security sensitive bank transaction from WLAN towards cellular.

Heterogeneous (compared to homogenous) handovers may be performed seamless with establishing a second alternative connection in parallel to the existing and tearing down the old connection, after successfully establishing the new connection. In order to provide higher bandwidth over multi-path, both connections may be kept open in parallel. In this regard, the MME adds another LOC'/ID as update to the existing entry LOC/ID in the registry on the gateways and DNS.

4.5.6 Detachment A detachment from the network can happen gracefully by shutting down the phone and de-registering it from the AP or

suddenly due to a loss of connection. In both situations, a de-registration from the UE out of the list of active users attached to the AP is done directly or indirectly (after inactivity for a predefined timeframe). Resource reservations are freed up again after detachment.

4.6 TODO: Other cases idle mode, paging

Emergency call support

Connectivity between UE and AF

Connectivity between UE and other UE

Similar AP or TA

Distinct AP or TA

5. Discussion Backwards compatibility

IP address allocation split into locator and identifier part

loc at attachment via MME/GW

id at attachment via AP/MME

<Document text>

```
Definitions and code {
  line 1
  line 2
}
```

Special characters examples:

The characters , , ,
However, the characters \0, \&, \%, \" are displayed.

.ti 0 is displayed in text instead of used as a directive.
.\" is displayed in document instead of being treated as a comment

C:\dir\subdir\file.ext Shows inclusion of backslash "\".

3 Security Considerations

<Security considerations text>

4 IANA Considerations

<IANA considerations text>

5 References

5.1 Normative References

[KEYWORDS] 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>.

[RFC1776] Crocker, S., "The Address is the Message", RFC 1776, DOI 10.17487/RFC1776, April 1 1995, <http://www.rfc-editor.org/info/rfc1776>.

[TRUTHS] Callon, R., "The Twelve Networking Truths", RFC 1925, DOI 10.17487/RFC1925, April 1 1996, <http://www.rfc-editor.org/info/rfc1925>.

5.2 Informative References

[EVILBIT] Bellovin, S., "The Security Flag in the IPv4 Header", RFC 3514, DOI 10.17487/RFC3514, April 1 2003, <http://www.rfc-editor.org/info/rfc3514>.

[RFC5513] Farrel, A., "IANA Considerations for Three Letter Acronyms", RFC 5513, DOI 10.17487/RFC5513, April 1 2009, <http://www.rfc-editor.org/info/rfc5513>.

[RFC5514] Vyncke, E., "IPv6 over Social Networks", RFC 5514, DOI 10.17487/RFC5514, April 1 2009, <http://www.rfc-editor.org/info/rfc5514>.

Authors' Addresses

Dr.-Ing. Julius Mueller
260 Homer Ave

Palo Alto, CA 94301
US

EMail: jmu@att.com
and
Tom Herbert
Facebook
1 Hacker Way
Menlo Park, CA 94052
US

Email: tom@herbertland.com