Network Working Group
Internet-Draft
Intended status: Informational
Expires: July 10, 2018

D. von Hugo
Deutsche Telekom
B. Sarikaya
Huawei
S. Bhatti
University of St. Andrews
M. Liebsch
NEC
R. Schott
Deutsche Telekom
S. Seo
Korea Telekom

January 10, 2018

Access Technology Independent Connectivity and Mobility Control Problem Statement

draft-hsblss-attic-ps-01

Abstract

This document attempts to make the case for new work involving possibly a framework and protocols that need to be developed to be used among various virtualized functions and the end user which may be moving. First a set of functional requirements are developed and then these requirements are further elaborated in terms of potential engineering and design constraints. The need for the new work is described next.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on July 10, 2018.

Table of Contents

1. Introduction

Current networking infrastructure is moving towards a converged common core network serving wireline and wireless access networks to which the end users are connected (see e.g. [METIS]). Such a network if realized in terms of 5G projects being undertaken worldwide is expected to meet the stringent requirements discussed in [I-D.vonhugo-5gangip-ip-issues].

In this document a system architecture which is composed of modularised adaptable network functions of control plane and data plane and their interconnections is assumed. Much of this functionality is expected to be implemented as virtualized functions running in central and/or distributed computation environment (cloud) as well as traditional physical entities in parallel.

The system architecture we consider brings new set of functional requirements that need to be considered in developing new protocols as well as potential engineering and design constraints which we will elaborate in this document.

The protocol discussion is based on and builds upon existing documents on access technology independent connectivity and mobility handling. Identifier Locator Network Protocol (ILNP) is designed as a data plane protocol based on identifier locator separation principle for end user mobility with no tunneling [RFC6740]. ILNP has control plane components defined using DNS [RFC6742] and ICMPv6 [RFC6743].

Identifier Locator Addressing (ILA) protocol is designed as a data plane protocol for task communication and migration in L3 based data center networks [I-D.herbert-nvo3-ila]. ILA's applicability has been investigated in [I-D.mueller-ila-mobility] by attempting to apply it directly to 4G 3GPP Evolved Packet System (EPS).

2. 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. Converged Access-Agnostic Core Network

Key principles and concepts in next generation system architecture include separation of User Plane (UP) functions from the Control Plane (CP) functions, allowing independent scalability, evolution, and a flexible deployment at e.g. centralised location or distributed (remote) locations; the concept relies on a new definition of the network functions. Wherever applicable, procedures (i.e. the set of interactions between network functions) are defined as services, so that their re-use is possible. The principles include being access independent and allowing efficient multiple access. Each Network Function (NF) can interact with the other NF directly if required. The architecture does not preclude the use of an intermediate function to help route control plane messages. On the other hand, the architecture shall be flexible enough to allow for hassle-free introduction of newly specified network services.

Currently network infrastructure is being transformed into two-layer data center or cloud as Core Network (CN) and the Access Network (AN) which mainly accommodates wireless access network and wireline access network closer to the user.

Especially for new ultra low latency services offering vehicular communications a placement of both user data plane functions (e.g. caches or anchors) and corresponding control plane tasks (e.g. activating and monitoring them) near the points of attachment (e.g. road side radio antennas) may be required.

As major control plane functionalities in such a core network the handling of network access management including consideration of user mobility, measures for providing session continuity as well as accounting for security and authentication has been identified. Data plane functions for packet routing and forwarding accordingly have to be present also.

4. Functional Requirements

The new system architecture brings a set of functional requirements which will be set forward in this section.

- Harmonised and seamless capability, i.e. one protocol / protocol-suite that provides all the functionality listed below together, and without disruption to end-to-end connectivity.
- Mobility for hosts / end-systems.
- Mobility for networks / sites / routers.
- Multi-homing for hosts / end-systems, including support for multi-path transport.
- Multi-homing for networks / sites / routers.
- Support for network virtualisation / network partitioning.

5. Non-Functional Requirements

Next, we discuss non-functional requirements involving potential engineering design constraints. They arise mainly from the need to increase resource usage efficiency by reducing signalling overhead and allowing for traffic shaping according to capacity availability.

- No use of tunnels, either layer 2 or layer 3.
- No use of middle boxes, i.e. no proxies. Anchor points perform important duties such as policy, accounting etc. as well as mapping that cannot be ignored. In anchor-less mobility, without anchor points, UE is the only common device in the path to perform

these functions. When anchors are removed then it becomes a challenge to provide functions like security and trust. One option is to use the UE as the only remaining single anchor point to perform its own accounting and policy and other functions. Such an approach however may create further implications to network operators which to our knowledge have not yet been dealt with.

- Support for end-to-end privacy and security. There are secure execution environments/processors in UE's these days, where all the finger print recognition, password encryption etc. is done and perhaps it is possible to extend these to run secure network functions. However, a trusted federation between any UE and the corresponding/accessible network entities cannot be assumed without doubt in any case. In view of this, virtualizing and distributing anchor point functions, e.g. mapping identifiers to the most recent locators, security associations (SA), etc. so they can run in the network at the points of attachment close to the UE will need to be investigated.

- Flexible addressing / numbering, e.g. distinguishing between globalised addressing as well as localised addressing.

- An end-to-end model (in support to the above four requirements).

- Support for current IPv6 addressing, e.g. /64 prefix assignment.

- Support for Identifier-Locator separation, e.g. as discussed in [RFC6115].

- Ability to use for mapping between identifiers and addresses an existing name resolution system (e.g. DNS), but also to make use of new/future systems, e.g. Dynamic Hash Tables (DHT) [RFC7363].

- Backwards compatibility for existing applications, e.g. support of socket API so that binaries do not need to be recompiled.

- Incremental deployment, e.g. only need to update those hosts that require new capability (this implies mixed operation, possibly dual-stack, within a network).

The network path selection and user data distribution should work transparently. Access path selection should be independent for Uplink and Downlink. A common core network independent of the access networks should be accessible by the UE. Network path selection should be adaptive to the link quality implications to match with service specific performance requirements. Distribution and aggregation of user data across multiple network paths at the IP layer should be supported.

Transport protocol level independence is a strong requirement in identifier locator separation based mobility protocols. This means that UE can have a locator or address but it should not be used as connection end point. The identifier which may not be routable should be used as the connection end point instead. This enables that no modifications at the transport layer in the host stack are required. However, using current IPv6 addressing, it seems transport protocol level independence can not be achieved without possibly simple code modifications in widely used transport protocol software. In view of the required capability of incremental deployment this issue should be solvable.

Regarding incremental deployment, legacy nodes will exist in the network especially in terms of the server nodes. How to support such legacy nodes will need to be investigated.

6. IP Sessions

Network layer or IP session normally has two components: source IP address and destination IP address. In case identifier locator separation protocol is used IP session has four components, i.e. source locator, source identifier, destination locator and destination identifier. With transport layer independence IP session should be composed of source identifier and destination identifier only.

Session continuity in the case of UE mobility should be provided. In an anchorless system, UE mobility incurs changes to the locators. Session management should maintain the established sessions when the UE moves. This also involves informing the destinations of the locator change. This is done in the control plane.

Enabling the various mobility scenarios while minimizing any negative impact on the user experience investigating solutions to coordinate the relocation of user-plane flows with the relocation of applications (hosted close to the point of attachment of the UE) due to the mobility of users can be considered as the challenges.

7. Goals

From the requirements set forward above we will derive the goals that need to be achieved. The goals of the work will involve:

- Align with the identifier usage, e.g. 64-bit identifier for UE, e.g. International Mobile Subscriber Identity (IMSI) as well as IPv6 prefix usage, single or multiple unique /64 prefixes

- Propose solution approaches to deal with operational problems such as charging or policy and QoS enforcement in a framework not relying on tunneling and the information in tunnel headers

- Develop a framework involving mobility management without tunneling, IP sessions for session continuity, handoff improvements, support for virtual network identifiers to be used by virtualized network functions in data centers, and support for legacy servers

- Define a version of the protocol that supports data center execution for intercommunication among control plane virtualized network functions

- Define control plane improvements to enable fast intertechnology handoffs

- Define proxy node behavior to enable legacy nodes

8. IANA Considerations

None.

9. Security Considerations

Various white papers exist that discuss security considerations related to the next generation systems, e.g. [NGMN]. Due to the request for intrinsic realization of security, such aspects have to be considered by design for architecture and protocols.

Especially as a joint usage of resources and network functions by different virtual network functions seems to be inevitable in the framework of next generation systems outlined in this document the need for strong security measures in such an environment is a major challenge.

10. Privacy Considerations

Support of full privacy of the users (customers and tenants / end service providers) is a basic feature of the next generation trusted and reliable communications offering system. Such a high degree of ensured privacy shall be reflected in the proposed architecture and protocol solutions.

Especially as Identifiers and mapping of Locators to them are addressed some privacy concerns arise. Mobility solutions tend to expose unique identifiers. A solution inside the mobile network exposes these identifiers to the network operator, which is not a big

deal since the network operator already has information about the device's location. In contrast, an IP level solution exposes both the identifiers and the locations at the IP layer. That means that web sites, for example, can now track the device's successive locations by watching the IP address. Solutions such as transporting the identifiers not as part of the IP header should be considered, e.g. in the handling of legacy hosts.

11. Acknowledgements

This work has been partially performed in the framework of the cooperation Config. Contributions of the project partners are gratefully acknowledged. The project consortium is not liable for any use that may be made of any of the information contained therein.

Comments, constructive criticisms in general on this work (including previous versions) from Christian Huitema, Cameron Bynes, Lorenzo Colitti, Mikael Abrahamsson, David Lake, Samita Chakrabarti, Jouni Korhonen, Zhu Jing are respectfully acknowledged.

12. References

12.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

12.2. Informative References

[I-D.herbert-nvo3-ila]
Herbert, T. and P. Lapukhov, "Identifier-locator addressing for IPv6", draft-herbert-intarea-ila-00 (work in progress), October 2017.

[I-D.mueller-ila-mobility]
Mueller, J. and T. Herbert, "Mobility Management Using Identifier Locator Addressing", draft-mueller-ila-mobility-03 (work in progress), February 2017.

[I-D.vonhugo-5gangip-ip-issues]
Hugo, D. and B. Sarikaya, "Review on issues in discussion of next generation converged networks (5G) from an IP point of view", draft-vonhugo-5gangip-ip-issues-03 (work in progress), March 2017.

[M.2083] ITU-R, "Rec. ITU-R M.2083-0, IMT Vision-Framework and overall objectives of the future development of IMT for 2020 and beyond", September 2015.

[METIS] Elayoubi, S. and et al., "5G Service Requirements and Operational Use Cases: Analysis and METIS II Vision", Proc. euCNC, 2016.

[NGMN] NGMN Alliance, "NGMN White Paper", February 2015.

[RFC6115] Li, T., Ed., "Recommendation for a Routing Architecture", RFC 6115, DOI 10.17487/RFC6115, February 2011, <http://www.rfc-editor.org/info/rfc6115>.

[RFC6740] Atkinson, RJ. and SN. Bhatti, "Identifier-Locator Network Protocol (ILNP) Architectural Description", RFC 6740, DOI 10.17487/RFC6740, November 2012, <http://www.rfc-editor.org/info/rfc6740>.

[RFC6742] Atkinson, RJ., Bhatti, SN., and S. Rose, "DNS Resource Records for the Identifier-Locator Network Protocol (ILNP)", RFC 6742, DOI 10.17487/RFC6742, November 2012, <http://www.rfc-editor.org/info/rfc6742>.

[RFC6743] Atkinson, RJ. and SN. Bhatti, "ICMP Locator Update Message for the Identifier-Locator Network Protocol for IPv6 (ILNPv6)", RFC 6743, DOI 10.17487/RFC6743, November 2012, <http://www.rfc-editor.org/info/rfc6743>.

[RFC7363] Maenpaa, J. and G. Camarillo, "Self-Tuning Distributed Hash Table (DHT) for REsource LOcation And Discovery (RELOAD)", RFC 7363, DOI 10.17487/RFC7363, September 2014, <http://www.rfc-editor.org/info/rfc7363>.

Authors' Addresses

Dirk von Hugo
Deutsche Telekom
Deutsche-Telekom-Allee 7
D-64295 Darmstadt
Germany

Email: Dirk.von-Hugo@telekom.de

Behcet Sarikaya
Huawei
5340 Legacy Dr.
Plano, TX 75024

Email: sarikaya@ieee.org

Saleem Bhatti
University of St. Andrews

Email: saleem@st-andrews.ac.uk

Marco Liebsch
NEC

Email: marco.liebsch@neclab.eu

Roland Schott
Deutsche Telekom

Email: roland.schott@telekom.de

SungHoon Seo
Korea Telekom

Email: sh.seo@kt.com