ETSI GR NGP 004 V1.1.1 (2018-01)

Next Generation Protocol (NGP); Evolved Architecture for mobility using Identity Oriented Networks

Disclaimer

The present document has been produced and approved by the Next Generation Protocols (NGP) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference
DGR/NGP-004

Keywords
GRIDS, identity, ION, IoT, mapping system, mobility

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Group Report (GR) has been produced by ETSI Industry Specification Group (ISG) Next Generation Protocols (NGP).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Executive summary

This work item focuses on using Identity Oriented Networks (ION) for next generation architectures toward 5G and beyond. The basic concept and goal behind ION is to dissociate the identifier and temporal location information for an entity. Ideally, this goal should endeavour for deployment to support current architectures while also enabling more optimal future architectures. The work aims to examine and propose recommendations to improve and simplify the network infrastructure to support mobility natively by adopting ION. In addition, the work item may require the development of new protocols and/or modification of existing protocols.

Introduction

The Internet is seminal for communication technologies and is a powerful enabler for modern applications with connectivity needs. However, when the Internet was designed the requirements were wildly different from the applications to be enabled by 5G infrastructure. Forty years ago, no one expected the user behaviour to evolve from text based fixed Internet access to streaming 4K quality media over a mobile device with session continuity. Mobility support is today the norm and new solutions should be examined for the network to support these new capabilities. As the Internet is pervasive and therefore these solutions should still interoperate with the current architecture.

Today the user's expectation and experience is at the forefront driving the requirements of applications such as session continuity, augmented reality, virtual reality or high definition video. Most importantly perhaps, the future deployment of 5G gives a unique opportunity to examine how core technologies may be modified, enhanced or replaced for a more secure, robust and optimized architecture for the future mobile networks.

With this in focus, the present document reviews the current state-of-art of Identity-oriented solutions (ION), and provides recommendations toward new protocols and/or modification of existing ones in the context of ION.

1 Scope

The present document provides an overview of existing identity oriented protocols, mapping systems and proposes next generation mobility with a generic and resilient identity services infrastructure.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] Number of Mobile-Only Internet Users Now Exceeds Desktop-Only in the U.S.

NOTE: Available at https://www.comscore.com/Insights/Blog/Number-of-Mobile-Only-Internet-Users-Now-Exceeds-Desktop-Only-in-the-U.S.

[i.2] Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016-2021 White Paper.

NOTE: Available at http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html.

[i.3] M. Hoefling, M. Menth, and M. Hartmann: "A Survey of Mapping Systems for Locator/Identifier Split Internet Routing", IEEE Communications Surveys & Tutorials, vol. 15, n. 4, Fourth Quarter 2013.

[i.4] International roaming explained.

NOTE: Available at http://www.gsma.com/publicpolicy/wp-content/uploads/2012/09/Africa-International-roaming-explained-English.pdf.

[i.5] IETF draft-herbert-nvo3-ila: "Identifier-locator addressing for network virtualization", T. Herbert.

NOTE: Available at https://tools.ietf.org/html/draft-herbert-nvo3-ila-00.

[i.6] IETF draft-padma-ideas-problem-statement: "Problem Statement for Identity Enabled Networks", P. Pillay-Esnault, M. Boucadair, C. Jacquenet, G. Fioccola, A. Nennker.

NOTE: Available at https://datatracker.ietf.org/doc/draft-padma-ideas-problem-statement-01.

[i.7] ETSI GS NGP 001: "Next Generation Protocol (NGP); Scenario Definitions".

[i.8] IETF RFC 6301 (July 2011): "A Survey of Mobility Support in the Internet", Z. Zhu, R. Wakikawa, and L. Zhang.

[i.9] IETF RFC 3753 (June 2004): "Mobility Related Terminology", J. Manner, and M. Kojo.

[i.10] ETSI TS 124 301: "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS) (3GPP TS 24.301)".

[i.11] ETSI TS 136 300: "Access Network (E-UTRAN); Overall description; Stage 2 (3GPP TS 36.300)".

[i.12] ETSI TS 123 060: "Access General Packet Radio Service (GPRS); Service description (3GPP TS 23.060)".

[i.13] ETSI TS 129 060: "General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp Interface (3GPP TS 29.060)".

[i.14] IETF RFC 6275 (July 2011): "Mobility Support in IPv6", C. Perkins, D. Johnson, and J. Arkko.

[i.15] IETF RFC 5213 (August 2008): "Proxy Mobile IPv6", S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury and B. Patil.

[i.16] IETF RFC 5949 (September 2010): "Fast Handovers for Proxy Mobile IPv6", H. Yokota, K Chowdhury, R. Koodli, B. Patil, and F. Xia.

[i.17] IETF RFC 6740 (November 2012): "Identifier-Locator Network Protocol (ILNP) Architectural Description", Atkinson, RJ. and SN. Bhatti.

[i.18] IETF RFC 6830 (January 2013): "The Locator/ID Separation Protocol (LISP)", D. Farinacci, V. Fuller, D. Meyer and D. Lewis.

[i.19] IETF RFC 7401 (April 2015): "Host Identity Protocol Version 2 (HIPv2)", R. Moskowitz, T. Heer, P. Jokela and T. Henderson.

[i.20] 3GPP TS 22.261: "Service requirements for next generation new services and markets".

[i.21] IETF draft-ietf-lisp-predictive-RLOCs: "LISP Predictive RLOCs", D. Farinacci, P. Pillay-Esnault.

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

binding: process of binding an identifier to its associated LOC(s), based on a lookup/query of the NMS

entity: device or node or a process, which needs to be identified in a network

Identifier (IDf): name that can be used to identify an entity unambiguously within a scope

Identity(IDy): identity of an entity used to securely access the mapping system and to enhance anonymity and privacy

locator: routable address in a network

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

3GPP	3rd Generation Partnership Project
5G	Fifth Generation Mobile Networks
BGP	Border Gateway Protocol
DHT	Distributed Hash Table
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
EMM	EPC Mobility Management
EPC	Evolved Packet Core

GMM	GPRS Mobility Management
GPRS	General Packet Radio Service
GRIDS	Generic Resilient Identity Services
HLR	Home Location Register
IDf	Identifier
IDMS	Integrated Database Management System
IDy	device identity
ION	Identity Oriented Network
IoT	Internet of Things
IP	Internet Protocol
ISP	Internet Service Provider
LTE	Long Term Evolution
MIP	Mobile IP
NMS	Network Mapping System
NMSFK	Network Mapping System with Full Knowledge
NMSPK-LL	Network Mapping System with Partial Knowledge using Local Lookup
NMSPK-SRL	Network Mapping System with Partial Knowledge using Single Remote Lookup
NMSPK-IRL	Network Mapping System with Partial Knowledge using Iterative Remote Lookup
NMSPK-HSO	Network Mapping System with Partial Knowledge with Hierarchically Structured Overlay
NMSPK-DHT	Network Mapping System with Partial Knowledge with Distributed Hash Table
NMSPK-MCO	Network Mapping System with Partial Knowledge with Multicast Overlay
PKI	Public Key Infrastructure
UE	User Equipment
VLR	Visitor Location Register
VPN	Virtual Private Network

4 Identity Oriented Networks (IONs): Architecture Overview

4.1 Introduction

The current Internet architecture, which has been built with and on top of the Internet Protocol (IP), was designed for a very different environment from modern networks. Early versions of the Internet Protocol were designed in the 1970's. The Internet protocol architecture has evolved over time since then, largely as a result of the Internet Engineering Task Force (IETF) organization. However, the landscape of networks has changed dramatically and many of the initial Internet architecture tenets have changed too.

As an example of one of these dramatic Internet architectural changes, today many Internet references cite that 70 % of the access sessions setup towards it are originated on a mobile device. However, at the start of the Internet design, the notion of mobility was not even considered.

Today, mobility is a major Internet requirement, and the number of users operating mobile devices has exploded, overtaking the number of fixed PC connections in 2014 [i.1]. According to reference [i.2], the projected growth of mobile devices is 1,5 per person, reaching a staggering total number of 11,6 billion connections by 2020. To cement a more near-term understanding of this trend, that global mobile data traffic has increased by 74 % in 2015 (according to reference [i.2]). Indeed, ubiquitous mobility is the norm and here to stay.

It is also very important to highlight that both the definition of mobility and its correlated requirements in the networks have drastically changed over time. For instance, in order to transit from LTE to 5G, the network requirements have become more stringent with respect to KPIs for latency, reliability, throughput, etc. [i.20]. This increase, in conjunction with evolving user behaviour, presents many technical challenges in the current Internet architecture in order to meet the requirements of future networks. Furthermore, due to the huge success of the Internet, there are many other non-technical issues that impact the Internet architecture: for instance those related to economical, or user behaviour. All of these technical and non-technical aspects need to be taken into account in the future solutions for any Internet architecture and protocol evolution (as detailed in ETSI GS NGP 001 [i.7]). In order to meet the aforementioned challenges of the current architecture based on IP, the present document introduces Identity Oriented Networks (IONs) as a candidate solution and provides a novel framework for next generation networks using a holistic approach. Furthermore, the present document extends some of the recommendations provided in ETSI GS NGP 001 [i.7] with respect to IONs.

4.2 Key Aspects of the Architecture

4.2.1 Identifier and Location Decoupling

This clause, introduces the key aspects of the ION architecture focusing on the fundamental importance of separating:

i) identifier; and

ii) location for each Entity within the network.

Furthermore, it provides an overview of the possible Entity identifier binding approaches and listing the pro and cons for each solution.

A mobile entity that intends to operate mobility needs three basic components (see references [i.7] to [i.11]):

a) An identifier, which univocally identifies an entity in the network. This is a static mobile entity identifier, in the context of the mobility system it wants to use.

b) A locator, which provides information regarding the current location of an entity. This is typically the static address of the Access Point that the mobile entity wants to connect to or be reachable from.

c) A network mapping system that creates a temporal binding of the identifier and the locator.

Additionally, new optional services can be possible with an Identity (IDy) (see reference [i.6]) for identifiers associated with it. These services namely access control, authorization of who can resolve location of an identifier use policy and metadata tied to Identity.

In a fixed network, an IP address has an overloaded semantic and it represents both the identifier and location of an entity. In the Internet Protocols, these two components were effectively bound, co-located, and somewhat immutable. As the network evolved, new breeds of devices have been introduced, which are increasingly highly mobile, and there has been an increased need to individually distinguish a multitude of applications that run on a device. However, the traditional methodologies, which use well-known ports and data forwarding, such as in mobile IP (MIP), [i.8] and [i.14] to [i.16] or 3GPP EPC mobility management (EMM) and GPRS mobility management (GMM) [i.12], solve the problem inefficiently. MIP binds a temporary IP address to a static IP address while in 3GPP (EMM and GMM) a temporary IP address to 3GPP Base Station IP address and Mobile Identifier. In 3GPP, the mobility structured Hierarchy of Identifiers is as follows:

1) Cells;

2) Tracking Areas;

3) Networks; and

4) Countries.

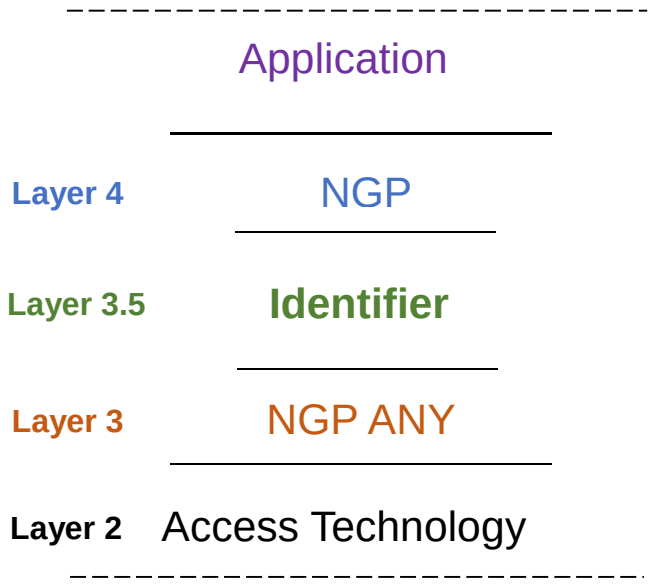
In order to maintain session continuity, the mobile device needs to retain some identifier that allows the communication to be seamless. In fact, when a device moves, the only component that changes is its location or its access point and not its identifier, however, today's overloaded semantic of an IP address for identifier and locator make them indistinguishable, therefore the only solution is to retain the IP address. However, holding on to an IP address during mobility requires solutions such as anchoring or reforwarding that introduce delays.

In order to overcome these issues, the ION architecture proposes to separate the identifier and location components. In ION the following components are present:

1) Entity identifier - identifies unambiguously entities within a scope.

2) Locator address -provides a location that is decoupled from the entity identifier.

This proposal does not intend to change the IP infrastructure, and proposes to work in a backward compatible manner with the current Internet, since the concept behind ION is applicable to any underlying network infrastructure. The basic idea beyond our proposal is to insert a naming/identifier sub-layer in the protocol stack, generally as an over-layer of IP stack as shown in figure 1. The Identity oriented architecture relies on defining the identifier of the entity and a mapping or binding to the location of the entity in order to forward traffic. The identifier namespace comprises the whole IPv4 and IPv6 address space to enable it to interoperate with traditional applications, while newer applications can use the newly defined identifier, which may not be necessarily IP address namespace. In alternative, the Identity oriented architecture may also reside directly on the L2 level in this case the mapping is between the identifier and the L2 layer. The evolved architecture using Identity oriented networks aims at using the IP addressing, but inserting an Identifier layer and gives new possibilities to change the upper layer by having identifier aware applications above the identifier layer.



NOTE: In reality the Identifier layer can be mapped to any layer used for forwarding or route locators.

Figure 1: Proposed stack

It is possible to have multiple locations for an identifier in case an entity is multi-homed. This case brings lot of complexity in today's IP networks because of the already overloaded semantics of identifier and location with IP. However the decoupling will give greater flexibility for multi homing cases.

An important characteristic of the identifier format is that it needs to satisfy or facilitate several requirements, which are both technical and non-technical. One approach is to have a "dumb" identifier, which only serves the purpose of identifying an entity, and nothing more. Another alternative is format the identifier by conferring to it some properties inherently. Table 1 captures the main pros and cons of some of the characteristics the format could have. While table 1 is not exhaustive, it provides an idea of the number of parameters, which are potentially connected to the identifier infrastructure.

Table 1: Characteristics of an identifier format: Pros and Cons

Identifier format characteristics	Pros	Cons
Large name space	Need to account for billions of devices, scalable	Very large space - Might become hard to manage in the long run, and likely to reduce performance
Unique Global Identifier	It facilitates the creation of a unique mapping service. Requires access to a mapping service, an entity can be easily identified through its identifier. Efficiency depends on latency of mapping in hardware or forwarding path	It leads to possible lack of privacy, and security risks. Robo Calls once your phone number is known, One mitigation is the use of ephemeral identifier and change it often
Multiple Identifiers	It allows multiple identifiers, which may have multiple classes of services. Preserve privacy by allowing some identities to be ephemeral	Complexity
Easily mapped /Translatable to IP	It provides backward compatibility with existing apps. It is cost effective, since no changes are required for the base infrastructure	Mappings need to be fast. In mobile technology this is done in the firmware for RAN and SW in for core but it is expensive
Variable Length	It provides backward compatibility with existing apps It is cost effective. It also can work with both IPv4 and ipv6 as well as non-IP solutions	It leads to high implementation costs
Non-Encrypted	Ease of use and troubleshooting	Security Risk
Encrypted	It increases the level of security	It is not human readable. It is hard to use, and troubleshoot
Human Readable	Human Manageable. Ease to use	Security Risk
Hierarchical	Easy to look up. Easy assignment	Need Identifier with structure. Lack of privacy and security risks as the root has access to all
Non-Structured	Need to ensure no collision. Can use crypto-keys. Complete freedom	Might be harder to manage look-up scale
Range or scope	Easier to have hierarchy in mapping systems. Administrative Domain control easier. Lawful interception	Confidentiality
Geographical awareness	Easier for incremental deployment Administrative control per AS or ISP. Policy possible per administrative domain	Privacy, confidentiality, tracking
Provider Dependency		Locked in, Migration
Structured	Under this solution, it is easier to have orthogonal distributed systems, where each of them identifies a different type of devices (i.e. mobiles, IoT ephemeral, etc.), apps/processes, and slices. It is possible to classify the entities and customize behaviours, services and apps. The name identifies type of objects (e.g. a fridge is not mobile, and will not belong to smart home)	Masquerading, Misconfiguration, Maliciously Misrepresenting
Context-aware	It allows to perform instantiation. It allows customize behaviours, services and applications based on Identifier awareness billing	Privacy, Net Neutrality

4.2.2 Identifier Allocation

Ideally, identifiers should be unique and have an easy allocation scheme with minimal overhead for the administrators. It would be desirable to support public and private identifiers for various use case requirements. Public identifiers may be visible to the external world or not. Private identifiers should still be unique in order to avoid issues during merges. The method of allocation of identifiers may be automatically or administratively by configuration. It is also possible for an entity to select its identifiers and register with provider. However the user selected identifiers should be checked for uniqueness at the provider or in the mapping infrastructure storing the identifiers-location pairs.

4.2.3 Identifier Groups, Range and Scope

If some entities have similar properties such as mobility scope, it may be desirable to allocate and manage them as a group, e.g. from the same "identifier block" to enable aggregation. Grouping of identifiers sharing the same context, such as on a train or plane should also be possible. These identifier groups may also be used for policy controls eventually or the controls could also be delegated at the time of mapping binding and requests.

4.2.4 Identifier Structure and Life Span

The identifier should be unique in order to facilitate interoperability and simplify the implementation of some use cases. More precisely, the format may be different as long as there sufficient information for the encapsulation decode. A collision detection mechanism such as already in place in several solutions should be put in place in case of automatic allocation.

Finally, it is possible to have ranges for automatic allocation and for manual allocation or it should be possible to at least have private or public instances.

4.3 Mapping and Generic Identity Services Infrastructure (GRIDS)

This clause provides an overview of mapping infrastructures, which is one of the central services of a GeneRic Identity Service (GRIDS) used for mobility, and the current available solutions.

The main functionality of a mapping service provided by GRIDS is to map or bind the identifier associated to an entity within a network with its physical location. An overview of several mapping options for Identity oriented networks is given in [i.3], and the classification and table is expanded and provided here for reference. The network mapping systems are classified into seven groups:

a) Network mapping system with full knowledge (NMSFK)- it is composed by a centralized network mapping system, composed by a single mapping server that contains full knowledge on how to map identifiers to LOCs.

b) Network mapping system with partial knowledge using local lookup (NMSPK-LL) - it is composed by a distributed network mapping system, composed by a plurality of mapping servers. The information related to which mapping server needs to be accessed in order to retrieve mapping for a specific identifier is contained into local lookup tables.

c) Network mapping system with partial knowledge using single remote lookup (NMSPK-SRL) - it is composed by a distributed network mapping system, composed by a plurality of mapping servers. In this case the lookup table that contains information related to which mapping server needs to be accessed in order to retrieve mapping for a specific identifier is contained into a global lookup table.

d) Network mapping system with partial knowledge using iterative remote lookup (NMSPK-IRL) - it is composed by a distributed network mapping system, composed by a plurality of mapping servers. In this case in order to find the network mapping server that contains the information queried, an iterative process is established: the request is directed initially to the highest authoritative server, which if not in possess of the requested information, provides feedback referral to a lower level authoritative server. If this new server does not have the requested mapping information, it refers to a lower authoritative server. This process continues until mapping server with the wanted mapping information is discovered.

e) Network mapping system with partial knowledge with hierarchically structured overlay (NMSPK-HSO) - it is composed by a distributed network mapping system, composed by a plurality of mapping servers. In this case the mapping servers are ordered in a hierarchical manner and the mapping information are retrieved following this overlay structure.

f) Network mapping system with partial knowledge with distributed hash table (NMSPK-DHT) - it is composed by a distributed network mapping system, composed by a plurality of mapping servers. In this case the mapping servers are clustered in distributed hash tables (DHTs), and the mapping information are retrieved through referrals among DHTs.

g) Network mapping system with partial knowledge with multicast overlay (NMSPK-MCO) - it is composed by a distributed network mapping system, composed by a plurality of mapping servers. In this case the mapping servers are grouped in multicast groups, and the query is sent in multicast.

Table 2 provides a thorough summary of the currently available network mapping systems for ION solutions.

Table 2: Summary of available or already proposed network mapping systems for ION

Name	Structure	Scalability	Resilience	Security	Relaying
LISP-NERD (NMSFK)	Hierarchical	MSs store partition of mappings and ingress tunnel routers (ITRs) assemble complete mapping table.	Replication of MSs	X.509 certificates	Yes
APT (NMSFK)	Hierarchical	Default mappers (DMs) know all mapping information.	Replication of DMs	Digital signatures	Yes
FIRMS (NMBPK-LL)	Flat and hierarchical	ITRs/MSs know global table.	Replication all components	X.509, PKI	Yes
"HiiMap"(NMSPK-SRL)	Flat and hierarchical	One regional prefix per EID, large storage requirements.	Replication, DHTs	PKI	No
ILA (NMSPK-SRL)	Flat		Relies on DNS	DNSSEC	No
One-Phase Lookup Using Reverse DNS/ DNSMAP(NMSPK-IRL)	Flat	Uses DNS infrastructure.	Relies on DNS	DNSSEC	No
Two-Phase Lookup Using Reverse DNS (NMBPK-IRL)	Flat	Uses DNS infrastructure.	Relies on DNS	DNSSEC	No
ILNP-DNS (NMSPK-IRL)	Flat	Uses DNS infrastructure.	Relies on DNS	DNSSEC	No
Use of DNS for HIT-to-IP Lookup in HIP (NMBPK-IRL)	Flat	Uses DNS infrastructure.	Relies on DNS	DNSSEC	No
LISP-TREE (NMSPK-IRL)	Flat and hierarchical	Uses DNS infrastructure, optionally own physical infrastructure based on DNS software.	Relies on DNS	DNSSEC	No
LISP-DDT (NMSPK-IRL)	Flat and hierarchical	Based on DNS software.	Similar to DNS	Similar to DNSSEC	No
IVIP DRTM (NMSPK-IRL)	Hierarchical	Aggregation of mapping information, load balancing between components.	Replication of all components	None	No
IDMS (NMSPK-IRL)	Flat and hierarchical	Uses DNS infrastructure, IDMS implementation.	DNS, replication of MS.	PKI, digital signatures	No
"MobilityFirst" (NMSPK-IRL)	Flat	GUID's mapping with late binding.	Replication of MSs	None	No
LISP+ALT (NMSPK-HSO)	Hierarchical	BGP aggregation and limitations, complex configuration.	Replication of all components	BGP security	Optionally
LISP-CONS (NMSPK-HSO)	Hierarchical	Strict aggregation hierarchy.	Replication of all components, redundant topology	Similar to BGP and DNSSEC	Yes
LISP-HMS (NMSPK-HSO)	Hierarchical	Strong aggregation of mapping information, DHT.	Replication of all components	BGP security	No
ID/Locator Distributed Mapping Server (NMSPK-HSO)	Hierarchical	BGP and DHT, aggregation.	DHTs	None	No
IRON (NMSPK-HSO)	Hierarchical	Aggregation.	Replication of all components	Mutual authentication between components	Yes
RZBS (NMSPK-HSO)	Hierarchical	Similar to DNS.	Replication of all components	Trust relationships between sub realms	No
LISP-DHT (NMSPK-DHT)	Hierarchical	DHT.	Replication of all components	X.509 certificates	No

Name	Structure	Scalability	Resilience	Security	Relaying
ER+MO (NMSPK-DHT)	Hierarchical	BGP and DHT, aggregation.	Replication of all components	BGP security, Kademlia security	Yes
DHT-MAP (NMSPK-DHT)	Flat	DHT.	Replication of all components	Digital signatures	No
HIP-DHT (NMSPK-DHT)	Flat	DHT.	DHTs	None	No
RANGI (NMSPK-DHT)	Hierarchical	DHT.	DHTs	Digital signatures	No
CoDoNS (NMSPK-DHT)	Flat	DHT.	Replication of all components	None	No
MDHT (NMSPK-DHT)	Flat	Multilevel DHT.	Replication of all components	None	Yes
LISP-SHDHT (NMSPK-DHT)	Flat and hierarchical	DHT.	Replication of all components	None	No
EMACS-LISP (NMBPK-MCO)	Hierarchical	Number of multicast groups, unnecessary multicast traffic.	Replication of MSs	None	No
GTP/ EMM	Hierarchical (2 level)	Difficult to scale and costly to support Tunnel Mappings providing IoN like capability. Proven to scales within network to 400Million simultaneously connected subscribers. Scalability between countries is not ideal often involving "tromboning" back to home network as cheaper and less complex to do this, although there is a capability to do path re-direction when roaming in 3GPP.	Provides full cellular support from mobility over IP Supports 'Flex' capability - good R&A	Control is built into Cellular GTP network signalling: AS security and NAS security	Yes
M2CNP	Flat and hierarchical				

While it is desirable to have different forwarding mechanisms as described in the next clause, there is a case for a common control plane across all Identifier-aware protocols. While many identifier-enabled data plane mechanisms serve fundamentally different objectives and do not need to interoperate there is a potential benefit in providing them a common mapping interface. A common mapping system infrastructure may facilitate cross-platform synergy.

4.4 Mapping Service Responsibility

The responsibility for the mapping may reside with the owner of the identifier or the owner of the locator. Both approaches exist today.

In the DNS, authoritative servers belong to the owner of the DNS namespace. In case of mobility, DNS names may be mapped to IP numbers of foreign networks. In cellular communication systems, mobile phone user may roam into the area of another provider where its phone number is registered by the foreign mobile communication provider in the Visitor Location Register (VLR), i.e. the owner of the infrastructure takes care of the mapping. In case of a phone call, an entry in the Home Location Register (HLR) of the mobile communication provider refers to the foreign mobile communication provider.

Today, ISPs, mobile, wireless and fixed networks and VPNs operate geographical boundaries [i.4] or areas of administration for physical and logical networks and these administrative areas form natural boundaries for some of the mapping server capabilities required to operate network addressing and mobility. If the majority of things in one of these areas of administration communicate with each other in a geographical zone then it makes sense to keep the mapping server as close (in terms of physical proximity) as is possible.

There are not many options to effect binding and few of the above schemes take advantage of geographical location implications (GTP and M2CNP do).

To facilitate scalability, mapping systems may be organized hierarchically, e.g. in terms of identifier space or locator space that may reflect AS boundaries. The responsibility for the mapping may be assigned to an appropriated hierarchy level. It would be possible to imagine a tree of GRIDS with a distributed root system that would link the different network mapping servers for companies. If the look up is beyond the administrative domain of the company then go one level up. The root mapping server for a company A will have the default and linkage to other mapping servers if needed.

For example, a sensors network may be part of a private domain and within limited scope and these devices would only communicate through a specialized application interface or gateway to the internet. In this case, it would be beneficial to have an allocation authority to manage them locally.

4.5 Mapping System design principles

4.5.1 Distribution and Redundancy

The mapping system design and architecture should avoid being single points of failure and should enforce resiliency. This methodology is used already in many systems today and relies on spreading the load across multiple systems.

4.5.2 Scale and Performance

A future mapping system will serve multiple applications requiring a vast number of entries and requires massive scalability. Distribution, hierarchy, aggregation as well as caching management techniques (such as time to live or stale management) may help to achieve these goals. However, fast query resolution is also an important objective to cope with the need for low latency. Therefore, the resolution mechanisms should be very efficient. Furthermore, mobility support requires that updates can be made simply, fast, and as needed. Last but not least, identifier formats may be considered for aggregation in order to scale, but the system should be flexible enough to disaggregate them if needed.

4.5.3 Performance Optimization

For massive scale and high performance, it is imperative that the number of entries in any mobility database is minimized. In addition, in order to support scale and dynamism for a next generation network, the identifier-locator mapping system should provide efficient queries and updates. Furthermore, aggregation of similar entities that have similar behaviours may result in more effective mapping systems. Entities may register to mapping nodes based on proximity and system intelligence should be good enough to determine where and how appropriate information should be updated for reachability. This scheme may have advantage of eliminating the need for any configuration other than a system that operated DNS entry to find the appropriate mapping node. For any mapping system to be successful, it will need to be robust, distributed and provide redundancy. The mapping system design and architecture should support distribution to avoid any single point of failure in supporting mobility as a fundamental modern networking capability.

4.5.4 Flexible, Open and Efficient Mapping System Interfaces

Newer identifier-aware applications or identifier-based protocols may define their own identifier allocation scheme and mapping if they do not need compatibility or operability with today's systems. Therefore, a flexible and extensible mapping system towards novel identifier and mapping types would be useful beyond the scenarios covered here. Furthermore, mapping resolution should be fast to support low delay requirements of future communication.

4.6 Forwarding Infrastructure

This clause provides an overview on forwarding infrastructures.

The main functionality of a forwarding infrastructure is to ensure that packets being are routed to their correct locations destinations, which may change due to host mobility. The IP was originally designed for the fixed access networks and was not designed for mobile devices. Therefore mobility protocols have been proposed by different SDOs, such as 3GPP, IETF, to support host mobility, e.g. GTP [i.13], PMIP [i.15], MIP [i.14], LISP [i.18], HIP [i.19], ILA [i.5], and ILNP [i.17]. Those mobility protocols are mainly developed for the IP-based hosts, since they have been widely deployed in the current Internet. However, considering the increasingly numbers of simple hosts for Internet of Thing (IoT) services, e.g. no IP stack supported, the next generation forwarding infrastructure should be a general solution (available capable for supporting all kinds of packets, i.e. not only IP packets).

Also, simple hosts will have limited power capabilities, so the next generation forwarding infrastructure should be able to decrease the signalling between the network and user hosts and decrease the size of packets transferred in through the radio interface.

With the identifier- locator separation concept, the next generation network will be designed as follows:

Option 1:

1) The host will communicate with peer node via its identifier.
2) The edge equipment will perform a lookup on the mapping system or map caches for the binding identifier-locator.
3) Edge equipment will encapsulate (or translate or tunnel) a locator layer for packet forwarding.
4) Routers in the network will forward packets based on the locator.
5) Peer edge equipment will remove the locator layer of packets and send them to the peer node.

Option 2:

1) The host will communicate with peer node via its identifier.
2) The host will perform a lookup on the mapping system or map caches for the binding identifier-locator.
3) The host will then either encapsulate (or translate or tunnel) a locator layer for packet forwarding.
4) Router in the network will forward packets based on locator.
5) The peer host will then receive the packets.

5 Next Generation ION Network Architecture

5.1 ION Network Architecture

The network architecture consists of GRIDS system and various edge networks. The architecture is shown in figure 2.

The GRIDS system provides out of many services, the basic identifier-Locator mapping relationship management function for the communication process: It is responsible for maintaining the mapping relationship between identifiers and Locators and providing identifier-Locator mapping information to the user plane functional entities that need to obtain the identifier-Locator mapping relationship in the network.

The mapping system can be classified into two types: Local GRIDS system and Global GRIDS system. The Local GRIDS system provides a mapping service only for the edge network where the mapping service is located; the mapping service is not visible to other edge networks. The Global GRIDS system can provide mapping services between the edge networks.

The inter-grids communication can support selective leaking of identifier-locator bindings for cases involving roaming.

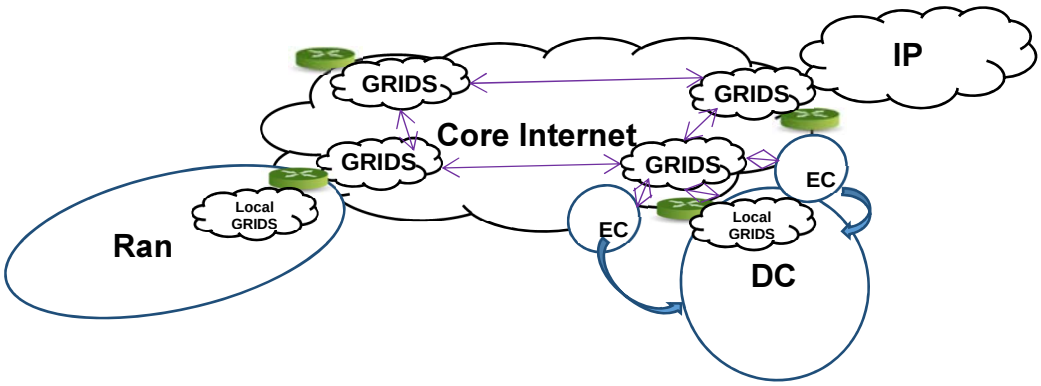


Figure 2: Architecture for ION network

Option 1: The mapping system is integrated as one part of a 5G network, as shown in figure 3. In this option, a new network function named GRIDS is attached to the service bus in the 5G network control plane.

Especially, the architecture of ION in a Mobile Network is shown as following.

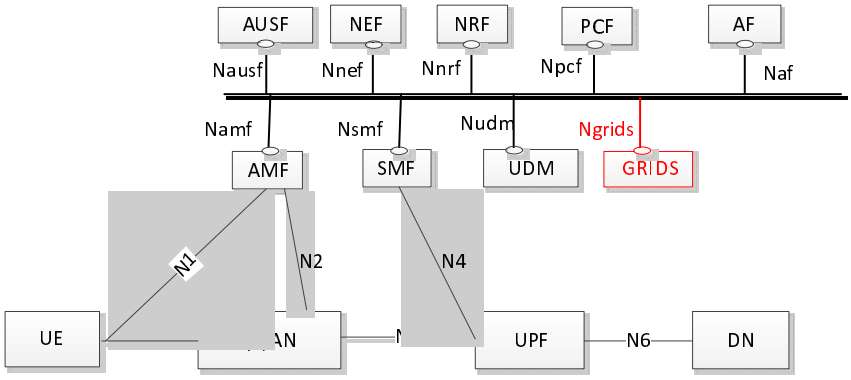


Figure 3: Architecture of ION in mobile network (Option 1)

The main functions of GRIDS are:

- maintaining identifier-Locator mapping relations and related auxiliary information;
- interacting with other network function such as AMF, SMF, etc. through the service bus and providing a mapping service;
- interacting with GRIDS in other network(s) to retrieve, update or synchronize the mapping information dependent on the mapping infrastructure described in the previous clause.

The functional description of these network functions in 5G network is specified as follows:

- Access and Mobility Management Function (AMF).
- Session Management Function (SMF).
- Unified Data Management (UDM).
- Policy Control function (PCF).
- User Plane Function (UPF).
- User Equipment (UE).
- (Radio) Access Network ((R)AN).
- Data Network (DN), e.g. operator services, Internet access or 3rd party services.

- Authentication Server Function (AUSF).
- Network Exposure Function (NEF).
- NF Repository Function (NRF).

Especially, AMF is in charge of Registration management, Reachability management, Mobility Management. It needs to be enhanced to interact with GRIDS for location info updating.

SMF is in charge of session management and UPF management, it needs to be enhanced to support the allocation of the Locator and interact with GRIDS to register the mapping information.

Option 2: The GRIDS system is deployed separately from the 5G network, and the 5G network functions access GRIDS through some kind of interface such as the N6 interface.

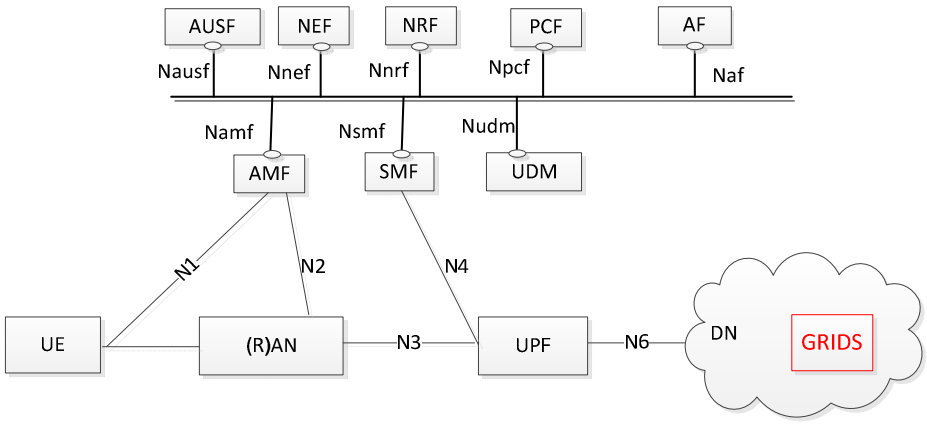


Figure 4: Architecture of ION in mobile network (Option 2)

In this option, the GRIDS can be a common mapping system infrastructure and does not interact with the 5G network control plane network functions directly. So these network functions do not need to be modified. The UE can interact with the GRIDS directly.

5.2 Future Control Plane

The GRIDS (Generic Resilient Identity Services) is a distributed control platform, which consist of the core GRIDS-IS (Identity Services), GRIDS-MS (Mapping/Location Services). In the future, new services can be added to this modular system.

Figure 5: Component of GRIDS

The UE communicates with GRIDS through AMF for the registration, location update, etc., via the N1 interface.

The UPF communicates with GRIDS through SMF for the locator allocation, locator lookup, etc., via the N4 interface.

The Control plane protocol stack is shown as following:

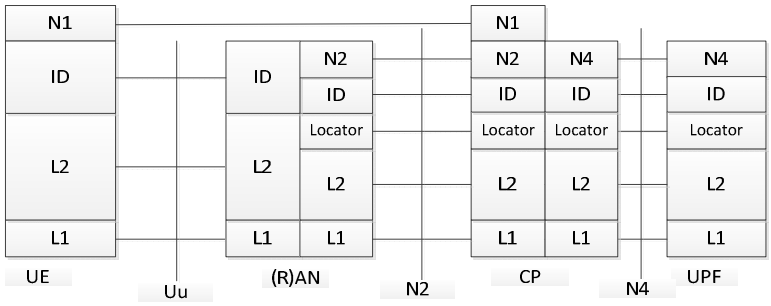


Figure 6: Control plane

5.3 Future User Plane

There are two options for User plane protocol stack.

Option 1:

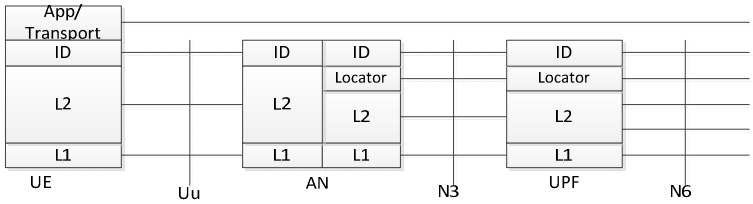


Figure 7: User plane (Option 1)

Option 2: Encapsulation

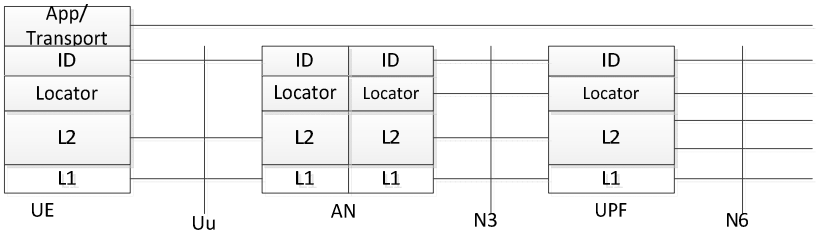


Figure 8: User plane (Option 2)

The difference between these options is whether the UE has a Locator in its protocol stack or not.

User packets forwarding between UE and (R)AN is based on L2 or the identifier layer, which depends on specific access technologies. Between (R)AN and UPF there is a locator routing network, which consist of routers supporting capable to route packets according to locator. Locators on (R)AN and UPF are allocated by the mapping system.

It is to be noted that the data payload and even the identifier can be encrypted so as to improve privacy. The identifier here is not the IMEI, and there are several methods to protect the identifier and its privacy.

5.4 Data Plane Agnostic Solution

The ION architecture advocates for a common control plane that is agnostic to the different data plane forwarding. The control plane with the GRIDS functionality is common across multiple data plane solutions namely ION Data plane, LISP, HIP, ILA and ILNP etc. that may adopt different techniques for forwarding such as encapsulation or translation.

6 Functionalities Supported

6.1 Registration and reachability management

6.1.1 Registration management

A UE needs to register with the network to get authorized to receive services, to enable mobility tracking and to enable reachability. When the UE first accesses to the network, the registration procedure is performed. During the registration, the GRIDS performs the authentication procedure, which is diverse from network to network; also the locator is allocated and the mapping information is registered to the mapping system.

The registration procedure is as in figure 9.

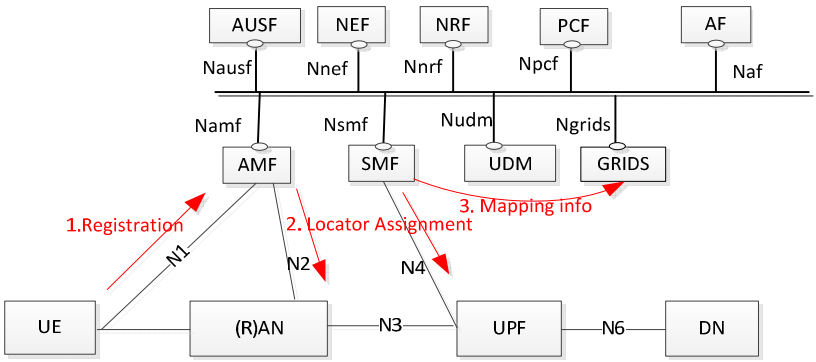


Figure 9: Registration procedure

Firstly, the UE performs L2 access procedure, the details depend on the access technology. Then, the UE sends a Registration message to the AMF, which includes its identifier and registration area. If the UE is authenticated successfully, (R)AN and UPF locators will then be allocated. The locator allocation should be based on the location of the UE and ensure that the packet will be routed to the correct (R)AN and UPF. The identifier and Locators mapping information will be sent to GRIDS. GRIDS will store and manage such mapping information. Mapping information can be synchronized between different GRIDS dependent on the implemented mechanism. (R)AN and UPF may also store the context information (including identifiers and locators).

After registration, the UE can send data to peers. Source identifier and destination identifier will be included in the Packet. (R)AN will retrieve the context and find the (R)AN Locator and UPF Locator for this UE. (R)AN will send this packet to UPF with the locator header. The UPF will retrieve the destination Locator by sending a Mapping Query to GRIDS. GRIDS will retrieve the destination Locator by the destination identifier and send back to the UPF. The UPF will send the packet to the peer with the destination Locator information.

6.1.2 Reachability management

Reachability management is used to find the UE location in Mobile Terminated data. Paging procedures are used when the UE is in IDLE mode. UE reachable area can be managed by LocatorList as shown in figure 10. The UE reachable area is the area registered during registration procedures. The Registration procedure will be invoked when this area changes.

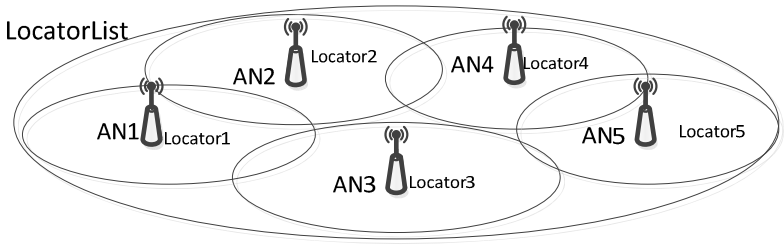


Figure 10: LocatorList based UE reachable area

In MT data procedure, the UPF will send Data notifications to the SMF with the UE identifier. The SMF will retrieve query GRIDS for the Locators information of the UE. If UE is in IDLE mode, a LocatorList will be returned. AMF will invoke the paging procedure based on the LocatorList. After the UE responses the paging request, the mapping information will be updated.

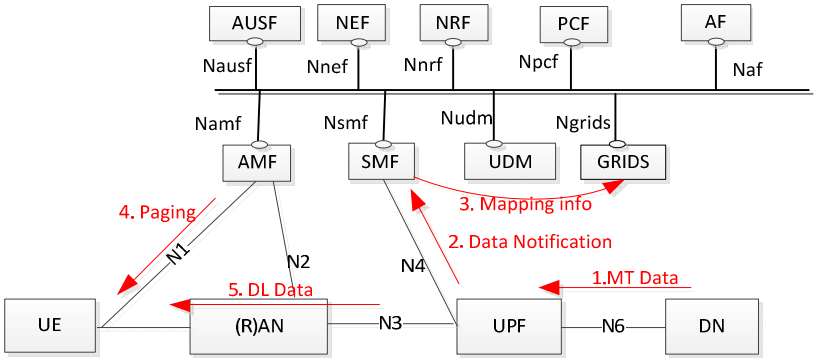


Figure 11: MT data procedure

6.2 Mobility management

6.2.1 Mobility changes

When the UE moves out of its current service area, the UE will be served by a new network entity. In this case, the UE needs to perform a mobility procedure.

There are two kinds of mobility procedures:

- Mobility without UPF change:
  - It has good mobility performance since there is therefore no need to notify the peer about the locator changing.
  - It can cause triangular routing.
- Mobility with UPF change:
  - To avoid triangular routing, the UPF can be changed to ensure an efficient path.

6.2.2 Mobility without UPF change

Normally, the UPF only serves a specific scope, which depends on the network topology. When the UE moves between (R)ANs without causing a UPF change, the following procedure is performed.

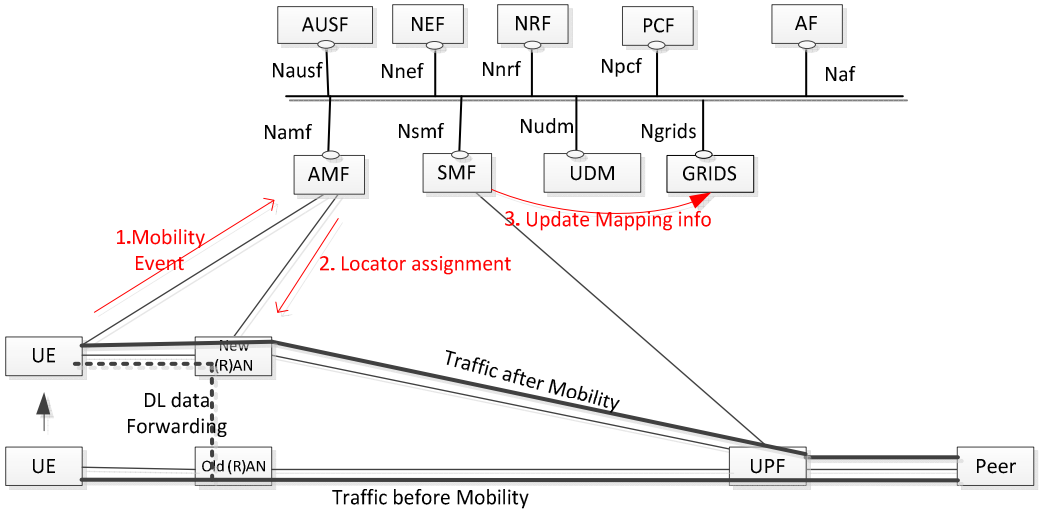


Figure 12: Mobility without UPF change

When the UE moves from the old (R)AN to the new (R)AN, the UE notifies the AMF about the mobility event. Then a New Locator may be allocated to the new (R)AN. This new mapping information will be updated to GRIDS. The Old (R)AN starts to forward the DL data after the AMF notified the new Locator to the old (R)AN. The SMF sends the new (R)AN Locator to the UPF. The traffic will be sent through the new (R)AN.

6.2.3 Mobility with UPF change

When the UE moves between UPFs, the following procedure is performed.

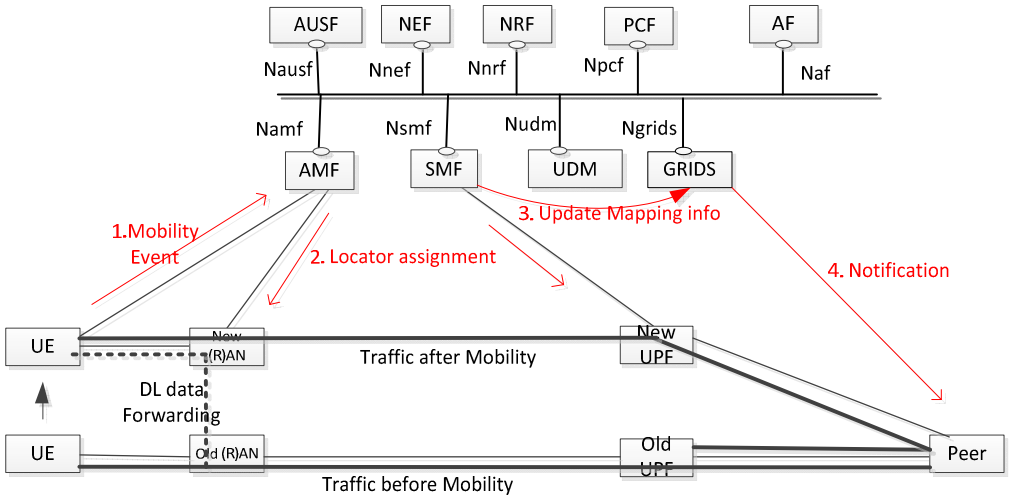


Figure 13: Mobility with UPF change

When the UE moves from the old (R)AN to the new (R)AN, the UE notifies the AMF about the mobility event. Then a New Locator will be allocated to the new (R)AN and the new UPF. This new mapping information will be updated to GRIDS. The Old (R)AN starts to forward the DL data after the AMF notified the new Locator to the old (R)AN. The new UPF will send the notify message with new UPF locator to the peer. The traffic will be sent through the new UPF and (R)AN. Session continuity is achieved as sockets at hosts are based on the identifiers rather than the IP locators.

6.2.4 Mobility with Predictive movement

The two above scenarios show the data plane today. With Identity Oriented networks, it is possible in some cases to have the UE register for a specific route when the mobility pattern is known in advance. This technique is detailed in [i.21]. In this case, the Peer may send traffic ahead of the UE movement. In this case the packets are already buffered by the time the UE completes its movement.

6.3 Confidentiality and Security

6.3.1 Privacy

The privacy issues need to be considered in the use of identifier and mapping systems.

For example, by looking up an entity's identifier in the mapping system, one can get its up-to-date locators and other meta-data that identifies the entity. Thus, access control needs to be implemented in the mapping system, so that the private information is open only to authorized requesters.

If an entity uses an identity, attackers can do cross-site analysis to associate information from different sites together. For example, if someone accesses a site and makes some purchase and then another site using the same entity identity, the attacker can then do cross-site analysis and reject the insurance application, even if the attacker does not know who is behind that identity. The identifier allocation mechanism may need to allow temporary Identifiers, different cryptographic identifiers for different purposes, or the main identifiers to spawn child identifiers that cannot be associated in theory.

6.3.2 Verification

Since identity is used to authenticate an entity (e.g. device, user, service, etc.), one may want to verify the validity of identity in some scenarios, such as identity based access control and mapping update. The format of an identity may be in the form of a public key or some meaningless string or number to an outside observer. Although an identity also uniquely refers to an entity temporally, it does not serve the same purpose as an identifier. The identity lifecycle is not necessarily tied to that of the identifier.

There are a couple of approaches, which may relate with the identity design, allocation and trust models.

One approach is self-verifiable identities. In recent future Internet architecture proposals, self-verifiable identities designs are popular since it they do not require a centralized allocation authority or a root of trust. Hence identity verification is fast due to independence of third parties like PKI. However, the main problem is that it cannot deal with identity collision (although there is a low chance for collisions to happen).

Another more traditional approach relies on PKI to assign an entity a certificate. The one who wants to prove it is the holder of an identity who just provides a signature, and the peer can verify it by just querying the certificate and uses the public key to verify the signature. The drawback of this approach is that it relies on a (usually off-line) PKI, and the latency to query the certificate is long.

A more modern approach, which combines the advantages of the above two approaches, is identity- based signature (IBS), where part of the identity by itself is a public key (indeed, one can calculate the public key from a third party's master key), so that the latency for querying certificates is eliminated.

Finally, ION can also use non-cryptographic approaches for identifier verification. For example, one can trust its provider, and its provider trusts another provider, which maintains the authoritative information of the identifier holder. Using this "trust-chain", one can trust the identifier ownership. However, this approach often relies heavily on offline procedures.

In addition of the techniques proposed above, the identities or keys may be changed across sessions for greater privacy and security.

6.3.3 Security

By introducing identifier as a new Internet architecture layer and mapping system as a new Internet infrastructure component, ION may introduce new attack vectors, because verification of identity and mapping consumes significant resources, including network, computation and storage. The design of ION should avoid DDoS attacks against the new layer and the new infrastructure component.

DDoS prevention is always difficult due to the open-access nature of the Internet. However, there are practical techniques available, including resources over-provision, rate-limiting, access control, back-pressure, and accounting. The detailed design of the prevention techniques may be related to the identity design and mapping system designs.

6.3.4 Mapping and Services System Security

The secure mapping system should be robust enough to withstand direct and indirect attacks. The expectation is that if one area of the system is attacked, it can be gracefully taken out or otherwise the propagation of the attack is prevented so as not to bring down the entire system.

The access to the mapping system itself should be governed by policy, secured and authenticated. Any mapping added to the mapping system should be cryptographically signed by the registering entity and verifiable. Requesters of information should also be authenticated. Any exchange of information should be protected against spoofing. The methodology used is usually ECDH key exchanges.

The indirect attacks should be also considered by rate-limiting the number of messages. Much of this can be done by heuristics such as on popular websites, which increase the capacity elastically in case of greater demand. Access control should not use traditional granular-based access lists since they do not scale and are hard to manage.

One example of scalable access control is through the use of authentication keys to determine whether the devices have the right credentials. Use of metadata to describe a device may also be used to describe the category of the device and assign it credentials or restrictions (example cameras should not initiate communication with sensors, however sensors may trigger a camera for live streaming).

6.4 Heterogeneous Multi-Access Support

UEs can be simultaneously connected to heterogeneous multi-access networks, including 3GPP access, WLAN and Fixed network, etc. The system should be able to take advantage of these multiple accesses to improve the user experience, such as providing high-data-rate services, etc.

The system should support multi-access networks with a common AN - CN interface (access-agnostic). It also needs to provide the access traffic steering, access traffic switching and access traffic splitting functions when the UE connects via a multi-access networks.

ION can provide a common AN-CN interface to support access agnostic function. Multi-access can be supported well by one identifier mapping with multi-Locators. When UEs connect multi-access networks, each access network can allocate a separated locator. The mapping system will maintain those mapping info between locators and UE identifier. Traffic can be steered, switched and split to different locators according to the traffic policy.

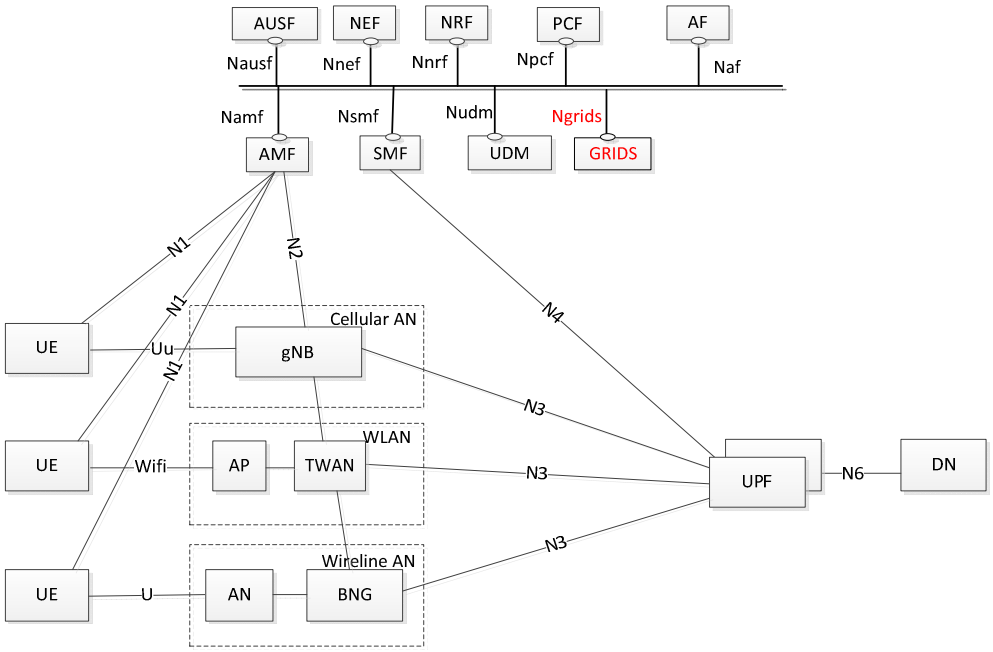


Figure 14: Multi-Access

6.5 Edge computing

Edge computing enables the service provider close to the UE to reduce end-to-end latency, promote the QoE by the efficient service delivery. The 5G core network selects a UPF close to the UE and executes the traffic steering functions from the UPF to the local Data Network. The service continuity may be required due to user or application mobility.

In ION, the traffic can be routed to the application server in local data network on the Locator. Service continuity can be achieved by the unchanged identifier of application between the application servers.

There are two steps for mobility in Edge computing. Firstly, the UE mobility will be invoked as the mobility procedure in previous clause. Then, the UE will connect to the old Local UPF and old application servers. Finally, the application mobility will be invoked. The application mobility can be realized through VM/Container migration and the identifier of application instance will be kept the same during the migration. The Locator will be changed to the new Local UPF and the traffic will be routed to the new application server.

For this edge computing scheme in 5G scenario, to be compatible with the existing 5G architecture, the UE's IP address can be used as the UE's identifier for the UE side. When the UE accesses the edge computing service, the network uses the selected original local UPF to establish an original PDU session connecting to the local edge computing server for the UE. After the UE moves, the UE needs to change the used UPF for accessing the edge computing server. On the basis of maintaining the original UPF, the network selects a target UPF for the UE at the current location to establish the target PDU session for the UE to access the current edge computing server. The target PDU session uses the same UE IP address as the original PDU session, that is, the UE IP remains unchanged although the Locator changes. During the establishment of the target PDU session, the original PDU session is retained which is used for in transit data transmission.

Here is an example of how this scheme could be implemented in 5G.When UE moves to a new location, the SMF chooses a target UPF for UE, and sends a request to UE to establish a target PDU session that associated with the original PDU session indicated by PDU session identifier contained in the request message, at the same time the original PDU session is still maintained. UE sends a response to SMF to accept the establishment of the target PDU session and trigger the start of establishment of target PDU session, the original PDU session identifier and a new PDU session identifier for target PDU session are included in the response to correlate the two PDU sessions. The target PDU session uses the new UPF connecting to the new edge computing server that hosts the application instance after migration, and share the same IP address with original PDU session. After the application instance migration to the new edge computing server complete, the UE can communicate with application instance using the target PDU session and release the original PDU session.

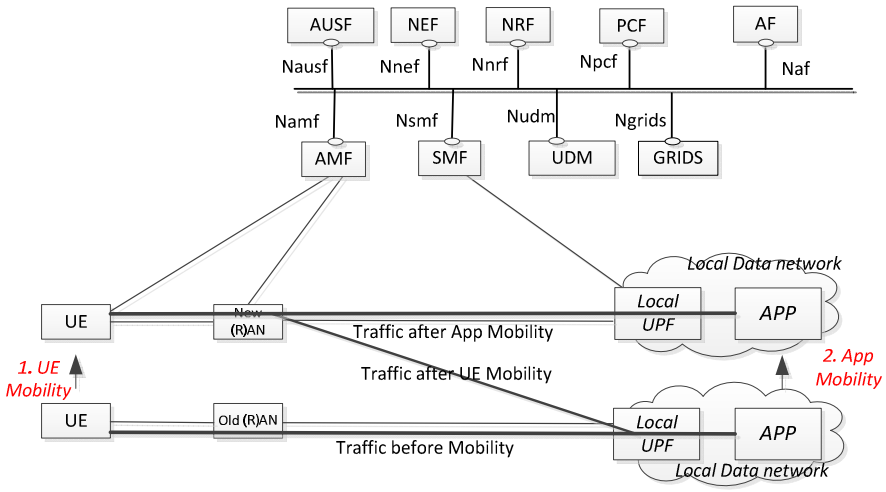


Figure 15: Edge Computing

6.6 IoT Support

In 5G research, eMBB, URLLC and IoT are three basic scenarios that are to be covered by 5G network, and AS. As one of the basic scenarios, the IoT scenario has its own communication characteristics, such as large number of devices, small data transmission or, very low communication frequency.

Introduced by IoT's communication characteristic requirements, 5G network should be designed to provide an optimized method for IoT traffic transmission to increasing network resource utilization, so the signalling and the network contexts should be reduce to save network resources for data transmission. ION could be as a candidate for 5G IoT transmissions.

UE is preconfigured with UE identifier and Application Server identifier before attaches to the network, so there is no need for IP address configuration procedures. The UE identifier and Application Server identifier are used to uniquely identify the UE and the AS in the specific scope.

The packets sent between UE and AS include an identifier header and an AuthCode, the identifier header contains UE identifier and Application Server identifier; the AuthCode contains the authentication information of the packet.

RAN and UPF maintain identifier routing table for each AS, an Application Server identifier indexes each entry in the identifier routing table. For those UE that communicate with the same AS, they should share the same identifier routing entry so as to avoid maintaining the network context for each UE. The basic information of the identifier routing table entry consists of Application Server identifier field and next hop filed, the Application Server identifier field is used to identify the AS and the next hop field contains next hop information corresponding to the identifier routing table. In addition, identifier routing table can also contain traffic mode, QoS information, and security authentication related information, the traffic mode is used to indicate whether downlink data exist; QoS information is used by RAN and UPF to provide QoS service for the packet.

The identifier routing table could be preconfigured in RAN and UPF or dynamically configured through signalling process.

When receiving a packet, RAN and UPF find entry in identifier routing table that matching the Application Server identifier in the packet, and then forward packet based on the routing table entry; after packet arrives UPF, UPF also implements security check using AuthCode in packet. This is shown in figure 16.

RAN and UPF get traffic mode for specific Application Server identifier from their own identifier routing table, if the traffic mode indicates downlink data exists, the RAN and UPF will create or update temporary context for UE for downlink traffic transmission of the UE. The temporary context includes UE identifier and the corresponding next hop information, on RAN the next hop information means the cell information from which the UE sends data packet; on UPF the next hop information means the RAN information from which the UE sends data packet. For downlink transmission, based on the temporary context whose UE identifier matches the UE identifier in packet identifier header, UPF will forward packet to RAN, and RAN will forward packet to UE.

All the UEs' packets that are sent to the same AS use the same identifier routing table entry in RAN and UPF for the specific AS, so the network does not need to implement signalling procedures for each UE to establish a transmission path, also the network does not need to maintain context for each UE.

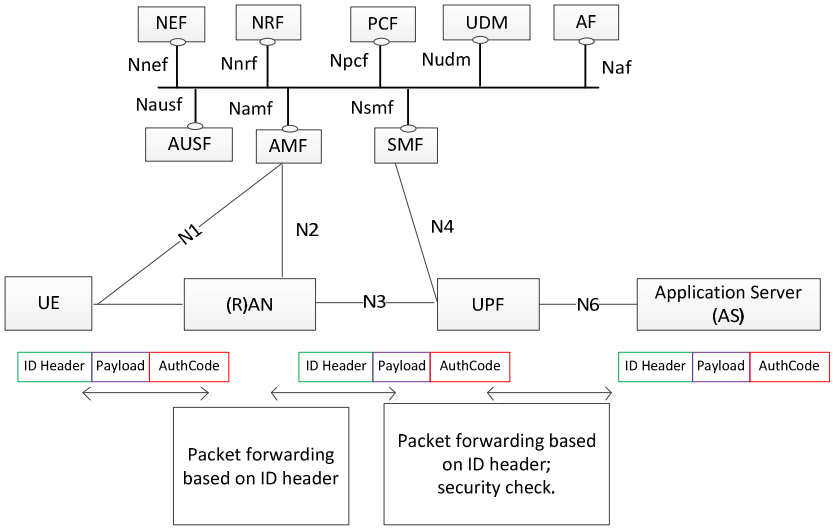


Figure 16: 5G IoT

6.7 Automatic Bootstrapping

Automatic bootstrapping is required in advanced communication because the diversity of communication will be so massive that a user cannot be expected to cope with the configuration of each and every application. 5G, IoT, and machine-to-machine (M2M) communication are just emerging examples. In the future, it is highly desirable that there should be minimal or Zero Touch Provisioning (ZTP) on new devices coming online. Automatic bootstrapping is particularly pertinent for the industrial Internet where M2M is expected to be functional with minimum human intervention.

7 Summary

Identity Oriented Network as described in the present document claims several benefits over existing systems (that conflate identifiers and addresses) for 5G and beyond. Furthermore, the Generic Identity Services (GRIDS) infrastructure is an enabler for a host of new services as well as network management. Lastly, the Identity Oriented Network solutions can seamlessly interoperate with the current architecture and yet be flexible enough to interoperate with future forwarding infrastructures as well.

Annex A:
Authors & contributors

The following people have contributed to the present document:

Rapporteur:

Padma Pillay-Esnault Huawei Technologies, padma@huawei.com

Other contributors:

Gerry Foster University of Surrey, Surrey, g.foster@surrey.ac.uk

Eduard Grasa i2Cat, Barcelona, eduard.grasa@i2cat.net

Kevin Smith Vodafone, UK, kevin.smith@vodafone.com

Uma Chunduri Huawei Technologies, uma.chunduri@huawei.com

Yangfei Huawei Technologies, yangfei15@huawei.com

Liubingyang (Bryan) Huawei Technologies, liubingyang@huawei.com

Weixinpeng (Jackie) Huawei Technologies, weixinpeng@huawei.com

History

Document history		
V1.1.1	January 2018	Publication