Draft Recommendation ITU-T Y.3031 (ex-Y.FNid)

Identification Framework in Future Networks

Summary

This Recommendation deals with potential identifiers pertinent to networks envisioned in ITU-T Recommendation Y.3001. It presents a review analysis of user, data, service, node, and location identifiers being used in the current networks and FN-related projects. (Details of the review are in the appendix.) It then specifies the identification framework and general requirements of these identifiers in the Future Networks.

Keywords

Identifier, Identification Framework, Future Network

Table of Content

Draft Recommendation ITU-T Y.3031 (ex-Y.FNid)

Identification Framework in Future Networks

1. Scope

This Recommendation deals with potential identifiers pertinent to networks envisioned in ITU-T Recommendation Y.3001. Identifiers in the Recommendation cover nodes in the network and their locations, data to be exchanged across the nodes, services and their users. The Recommendation describes key components and their capabilities for identifier handling as a framework. High-level requirements are also given for the succeeding specifications on future networks.

2. References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is published regularly. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T Y.3001] Recommendation ITU-T Y.3001 (2011), *Future Networks: Objectives and Design Goals.*

[ITU-T Y.2015] Recommendation ITU-T Y.2015 (2009): *General requirements of ID/locator separation in NGN.*

[ITU-T Y.2022] Recommendation ITU-T Y.2022 (2011), *Functional architecture for the support of host-based ID/locator separation in NGN.*

[ITU-T Y.2057] Recommendation ITU-T Y.2057 (2012), *Framework of identifiers and locators separation in IPv6-based next generation networks.*

[ITU-T Y.2720] Recommendation ITU-T Y.2720 (2009), *NGN identity management framework*.

[ITU-T Y.3011] Recommendation ITU-T Y.3011 (2012), *Framework of network virtualization for future networks*.

3. Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 Future Network (FN) [ITU-T Y.3001]: A network able to provide services, capabilities, and facilities difficult to provide using existing network technologies. A Future Network is either:

a) A new component network or an enhanced version of an existing one, or

b) A heterogeneous collection of new component networks or of new and existing component networks that is operated as a single network.

3.1.2 Identifier [b-ITU-T Y.2091]: An identifier is a series of digits, characters and symbols or any other form of data used to identify subscriber(s), user(s), network element(s), function(s), network entity(ies) providing services/applications, or other entities (e.g., physical or logical objects).

3.1.3 Service [b-ITU-T Z.100 Sup.1]: A set of functions and facilities offered to a user by a provider.

3.1.4 Service node (SN) [b-ITU-T G.902]: Network element that provides access to various switched and/or permanent telecommunication services. In the case of switched services, the SN provides access call and connection control signaling and access connection and resource handling.

Note: The above definition is applicable to the "network" service node. This Recommendation uses "service node" also to refer to the "content" service node.

3.2 Terms defined in this document

None.

4. Abbreviation and acronyms

This Recommendation uses the following abbreviations and acronyms:

BAN	Body Area Networks
DNS	Domain Name System
FN	Future Network
FQDN	Fully Qualified Domain Name
GUID	Globally Unique Identifier
ID	Identifier
LAN	Local Area Network
LINP	Logically Isolated Network Partition
MAC	Media Access Control
MAN	Metropolitan Area Network
NAI	Network Access Identifier
NAP	Network Attachment Point
NDN	Named Data Networking
PAN	Personal Area Network
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network
WAN	Wide Area Network

5. Conventions

None.

6. Considerations on new identifiers in FNs

According to [ITU-T Y.3001], FNs are recommended to provide a new identification framework that can be helpful for intrinsic mobility support and optimal data access. FNs have a major goal of specifying a new architecture considering emerging networks that embrace various innovative communication paradigms. Therefore, it is required to specify an identification framework, defining new identifiers that would identify communication objects, which efficiently supports the new communication paradigms in FNs.

The objects involved in a communication network are users, data or contents, nodes (host or device, both physical and virtual), links, communication sessions, etc. A communication service is created by a functional interaction among these objects. These objects need to be uniquely identified in order to make it possible to select the proper combination of the functions provided by them. The current Internet's base functions designed in 1970s were dependent on only one type of identifier, called IP addresses. An IP address identifies both a node as well as the location of the node on the network topology. The Internet also uses IP addresses for identifying a realm of administrative autonomy domain of the network through mapping of domain names to IP addresses. IP addresses are often implicitly used in the application layer, e.g., through mapping between the IP address and FQDN of a mail server. The use of IP addresses as both identifiers, to identify hosts in the application and transport layers, and locators in the network layer is the root cause of the Internet not being able to support mobility in a native manner [ITU-T Y.2015]. Although [ITU-T Y.2022] and [ITU-T Y.2057] are specifying the functional architecture for the introduction of ID/locator split functions in NGN, they do not describe the architecture of IDs and their configuration methods. Therefore, new identifiers are needed for identifying nodes, data, communication sessions or services in the upper layer protocols in FNs.

Similarly, the present-day Internet's base functions lack identifiers for universally representing data or contents, which are the basic requirements for realizing content-centric or data-aware networking. The data-aware networks are considered to scale in a better manner as they can serve users with required data from the nearest points in the network. Therefore, new identifiers for data or contents should be defined so that a large volume of data can be efficiently accessed regardless of their locations.

Besides new node IDs and data or content IDs, FNs also need user IDs, service IDs, and location IDs. They also need new mapping or resolution systems for storing and providing dynamic relationships between different types of IDs. The current Domain Name System (DNS) stores the mappings between domain names and other parameters such as IP addresses. However, the DNS takes more time than acceptable for updating its records, thus not suitable for storing dynamic ID mappings.

7. Analysis of existing identifiers from the FN prospective

This clause presents an analysis of identifiers used in the current networks and FN related projects. The details are found in Appendix I "Overview of identifiers used in existing networks and FN-related projects".

7.1 Analysis of identifiers used in the Internet

The identifiers used in the Internet can be summarized as follows:

- Service and users: URI or URL, email address, IP address, NAI, etc.
- Node: IP address
- Network Access Point (NAP): IP address and/or MAC address
- Path: IP prefix

In the above list, IP addresses are the common identifiers for most objects and in multiple protocol layers.

The bindings between these objects in the current Internet could be summarized as follows:

- Service/user to node: the bindings are maintained in the DNS servers and are mostly static.
- Node to NAP: the bindings are fixed as an IP address identifies both the node and its NAP.

- NAP to Path: the bindings are maintained in the routing table by the use of the prefix of the NAP's IP address.

From the above observation, it can be said that the current Internet supports only static bindings between these objects, mostly by using static IP addresses.

Mobility will be a dominant feature of FNs as the number of network-capable mobile devices such as laptop computers and smart phones has already exceeded the number of fixed computers connected to the Internet. The current Internet identifier structure may cause some problems or be insufficient in the future because of the following reasons:

1) The Internet was designed with static nodes. NAPs were not built for change. As a result, with the mobility environment becoming widespread, the Internet now faces substantial challenges to support mobile nodes: A paradigm shift is required in FNs to realize mobile nodes as a major and integral component of the network.

2) It was assumed that IP addresses could be common identifiers for both nodes and their NAPs as the static nodes would remain attached to the same NAPs. However, for a mobile node, the NAP does change frequently while the node moves. Therefore, the node ID and NAP ID should be separated so that the node can retain its ID while changing its NAP ID. It means that we need a dynamic binding between them (e.g., a persistent node ID mapped to a temporary NAP).

3) Multiple interfaces are common in mobile environments as we can see in wireless overlay networks consisting of wireless coverage of different scales such as body area networks (BAN), personal area networks (PAN), local area networks (LAN), and wide or metropolitan area networks (MAN/WAN). However, in the current Internet, a node with a single NAP is the basic assumption. Therefore, the future network should consider a node with multiple interfaces that could be connected to multiple networks through multiple NAPs. In this case, a single node ID would be mapped to multiple NAP IDs.

4) There is no independent ID namespace for nodes in the Internet. As IP addresses are meant for node's NAP, we need a new node ID namespace.

5) The location of services/users will be very likely to change frequently in the future network environment, but the current DNS bindings are very static. Therefore, we need more dynamic bindings among node names, IDs, locations, and services/users.

The above list is not exhaustive. There could be many other issues to be resolved in the FNs for efficiently working in mobile environments. Nonetheless, the above text provides background information for the development of a new identification framework for FNs.

7.2 Analysis of identifiers considered in FN-related projects

Based on the overview given in Appendix I.4, the identifiers being proposed for future networks can be categorized based on their readability and hierarchy. The examples of these identifiers are given in Appendix I.4.

(1) human readable IDs and non-readable IDs (e.g., public key-based IDs)
(2) hierarchical IDs and flat IDs

Human readable IDs (such as content IDs) are composed of alphanumeric characters. These IDs would be beneficial when a human user has to read IDs for searching, processing or evaluating the objects represented by the IDs. On the other hand, public key-based IDs are not human readable, but would be useful for incorporating some security features into the IDs themselves. These IDs are self-certifiable.

Hierarchical IDs are better for creating a managed ID space. These are also helpful to assure the global uniqueness of IDs and to create a scalable hierarchical name resolution system. Human

readable IDs are usually hierarchical IDs, while the public key-based IDs are flat. Flat IDs may be better for assuring privacy, but may be difficult to assure their global uniqueness.

The length of IDs is also an important issue when IDs have to be included in the header of data packets. Public key-based IDs are long and may incur huge overhead when included in each packet. Therefore, the length of IDs should be optimal when they are included in packet headers. Hashing longer IDs (such as public keys) to create shorter tags to be included in packet headers may an approach to reducing the possible overhead, but the tags may loose the global uniqueness property. To avoid this problem, a globally unique ID may be created by attaching a global prefix to the hash value generated from the hostname or public key.

8. Identification framework in FNs

8.1 General architecture

The identification framework supports the unique ID space, maintains relationship between some of the IDs which represent objects, and provides the relationship information between among IDs when requested. It also supports searching for IDs of target objects for communication. The rectangle in Figure 1 shows the identification framework that consists of four components. The identification framework connects various communication objects and physical networks. The first component is the ID discovery service, which discovers various types of IDs related to communication objects. The second component is the ID spaces, which define and manage various kinds of IDs. The third component is ID mapping registries, which maintain mapping relationships between various kinds of IDs. The last component is the ID mapping service, which performs mappings of IDs of one category with the IDs of other categories.

In the ID spaces, there are user IDs, data or content IDs, service IDs, node IDs, and location IDs (NAP IDs or locators). There may be additional IDs, but for the sake of brevity in explanation, only these IDs are considered in this Recommendation. Various applications are realized through functional interactions of these IDs. The relationships between IDs are maintained in the ID mapping registries, which store and update mappings between IDs and provide such mappings to the ID mapping services. The ID mapping services utilize the ID mappings obtained from the ID mapping registries to achieve seamless services over heterogeneous physical networks, such as IP version 6 (IPv6), IP version 4 (IPv4) or non-IP networks that may use different protocols for forwarding data packets. These networks may use different locators to locate a node on the network topology and forward packets toward the node by the routing system. Moreover, data ID-based forwarding networks may not need the ID mapping service to map data IDs to locators, since these networks can forward data packets using the data IDs themselves.

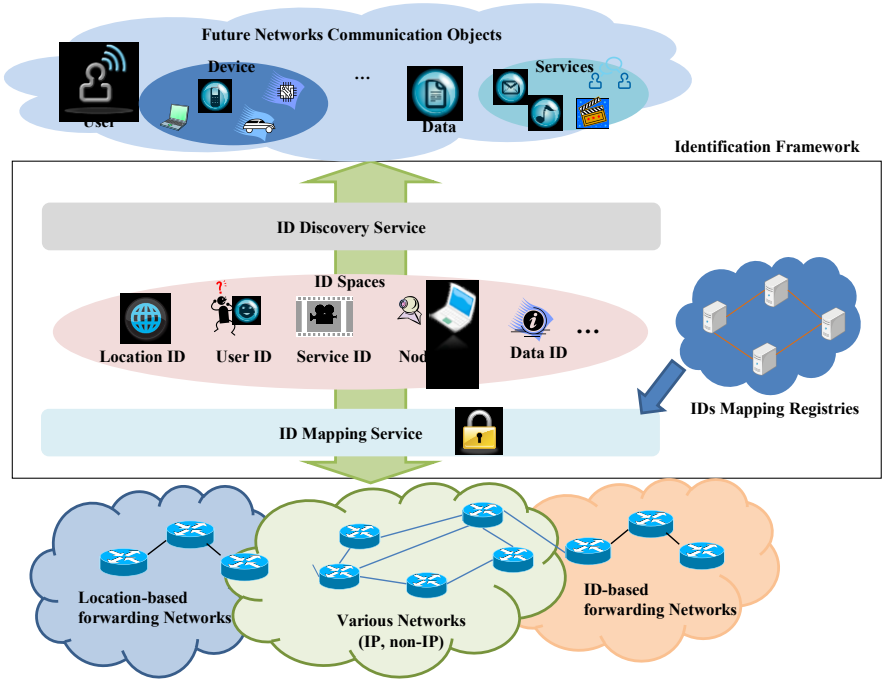


Figure 1. Identification framework in FNs.

8.2 ID spaces

An identifier uniquely identifies an object of a category in a particular scope. Here category means the type of object represented by the given ID. The category can be user, data or content, service, node, location, etc. Similarly, the scope represents the region in which the ID is valid. The scope can be local or global. The local scoped IDs are valid only in the local networking space, while the global IDs are valid globally. The scope may also be an administrative domain representing an autonomous network. The different categories of IDs included in the identifiers framework are overviewed below:

a. User ID

A user ID is assigned to a user to uniquely identify the user in the network. User IDs are used to search, authenticate, authorize and bill the user for a service.

b. Data/Content ID

A data/content ID is assigned to a data or content to uniquely identify it independent of its location or owner. The availability of data/content IDs would be helpful to create a new network architecture based on an information-centric paradigm. It would enhance data security without requiring the trust relationship establishment with the node possessing, offering, or delivering the content. This feature is helpful for content mobility and caching in the different locations in the network.

c. Service ID

Service IDs can further be divided into two subcategories: content service ID and network service ID. A content service ID specifies an application service and associates with service related attributes, such as the security keys, sequence numbers, and states. The content service IDs would be mainly used by server and client nodes to identify the services. A network service ID will specify a data forwarding service provided by the network nodes. It may specify a logically isolated network partition (LINP) in network virtualization [ITU-T Y.3011], a virtual local area network (VLAN), or a particular protocol used for handling data packets (e.g. forwarding, queuing, QoS supporting) in the network.

d. Node ID

A node ID is assigned to a physical or virtual device to uniquely identify it independent of its location in the network. The node ID would be used for access control of mobile nodes, trust establishment between nodes, and, optionally, to identify communication sessions existing between the nodes.

e. Location ID

A location ID or locator is assigned to a device or node to locate it in the network topology. The locator is used by the routing infrastructure to locate the node uniquely in the network topology. Locator formats are dependent on the network layer protocols or routing protocols which are used to locate the destination node and forward data towards it through the network.

The identifiers in general have the following features.

1. Identifiers can be of fixed length or variable length; they can be composed of bits or alphanumeric characters.
2. Different types of identifiers can represent the same object. Alternatively, an identifier can represent many objects of a given category or scope.
3. Identifiers can have hierarchical or flat structures. Hierarchical identifiers may be easier to search from ID mapping registries than flat identifiers. The hierarchical structure also helps in proliferation or generation of globally unique identifiers. On the other hand, the flat IDs provide benefits in terms of flexibility, persistency and privacy.
4. The relationship between identifiers can be static or dynamic. The static relationship persists for longer time while the dynamic relationship may be ephemeral.

The common understanding in the formats and configuration methods of these IDs would greatly help FNs to efficiently deal with the current and future new communication challenges. It would be also possible to leverage the approach used to configure the ID space of one category in the configuration of ID spaces of other categories. For example, if an approach to creating self-certifiable node IDs by using the hash value of the owner's public key is standardized, the same approach can be leveraged to configure self-certifiable data IDs.

8.3 ID mapping services

As mentioned earlier, various types IDs are used in different layers of communication protocols. In general, the location IDs or locators are mainly used in the network layer by the routing and addressing system, while the other IDs are used by the application and transport layers to identify various objects.

Thus, ID mapping services are required to store the ID mappings in the ID registries as well as to maintain the relationship between IDs of different categories and scopes. They also perform mappings of different types of IDs with their own specific networks. The ID mapping can be one-to-one, one-to-many or many-to-one. For example, if a user possesses two or more devices, one user ID will be associated (or mapped) with many node IDs. The mapping relationship can be of persistent or temporary, depending on how long the user holds the device in her possession. The mapping relationship can be either horizontal or vertical, depending on if two IDs that are mapped to each other are used in the same layer or in the different layers. For example, the mapping between a data/content ID and a service ID would be horizontal whereas the mapping between a user ID and a location ID would be vertical. A single ID or a combination of various IDs of different categories is used in an identification function of protocols. For example, in an ID/locator split network architecture [ITU-T Y.2015], node IDs are used to identify a session in the transport layer while IP addresses are used as locators to locate nodes and forward packets in the network layer. However, if FNs should also provide a service mobility capability by allowing a service to

move from one node to another, rather than using node IDs, FNs should use user IDs or service IDs in the session identification process.

The ID mapping services may not be needed sometimes. For example, data ID to locator mappings would not be needed in data-aware networking where data can be routed using their data IDs.

9. High-level requirements for identifiers

The followings are the high-level requirements for identifiers in FNs.

1) The identifier is required to be unique in the given scope. The scope of an identifier can be either local or global. It is recommended that the identifier structure be defined in such a way that the scope may be embedded in the value of the identifier.
2) The identifier is required to be able to clearly represent an object or a group of objects of the given category and scope.
3) The identifiers can be persistent or temporary. A persistent ID may be associated with the same object forever or for a specific time span, while a temporary ID may be associated with the object for a short time and may be dissociated from the object at any time. It is recommended that the identifier structure be defined in such a way that the persistent or temporary nature of an identifier may be embedded in the identifier value.
4) The identifiers are recommended to have features to facilitate their mapping to other identifiers of appropriate categories.
5) The mapping between identifiers of one category to the identifiers of another category can be either static or dynamic. The static mapping relationship are recommended not to change as time passes, while dynamic mapping are recommended to allow the relationship between identifiers change according to time or place.
6) The identifier is recommended to have a flexible structure so that it would have enough space for further refinement and modification as new requirements on identifiers emerge in the future.
7) The ID mapping functions are required to be accompanied by security functions for ensuring reliability in network operations and communication services.

10. Environmental considerations

The ID structure affects the design, implementation, operation and maintenance of networks and implicitly affects environmental impact of networks, but the relationship is vague and needs further study. The details of the environmental impacts are recommended to be discussed at the future Recommendations that would describe specific IDs.

11. Security considerations

Identification is the basis of identifying various objects. If there are any mistakes or malfunctions in assigning an identifier to an object, in mapping, or in any part of handling of identifiers, they may cause various incidents such as system fault, security attacks like replay, or leakage of privacy. Appropriate security considerations and countermeasures such as Identity Management [ITU-T Y.2720] are therefore recommended to consider in designing, operating, and maintaining the identifiers. For example, it is recommended to introduce appropriate authentication mechanisms when allocating identifiers, or mapping of identifiers, and for important identifiers, it is recommended to issue certificates, or make identifiers self-certifiable by using Public Key Infrastructure (PKI), and make it possible to verify the legitimacy of identifiers whenever and wherever necessary.

Appendix I

Overview of identifiers used in existing networks and FN-related projects

I.1 Node ID in the Internet

RFC 1498 [b-RFC1498] analyzes the naming and binding issue of the current Internet. It specifies the following four types of communication objects that should be distinguished from one another using names or identifiers:

1) Service and users: Services are the functions that one uses to obtain requested data, and users are the clients that use services. Examples of services are one that tells the time of day, one that performs accounting, or one that forwards packets. Examples of clients are desktop or laptop computers and smart phones.
2) Nodes: These are computers that can run services or user programs. Some nodes are clients that use services of the network, while other nodes implement the network services such as data forwarding services.
3) Network attachment points (NAPs): These are the ports or points of a network, where a node is attached. In many discussions about data communication networks, the term "address" is an identifier of a network attachment point.
4) Paths: These run between network attachment points, traversing forwarding nodes and communication links.

The observation about the four types of network objects listed above is that most of the naming requirements in a network can simply and concisely be described in terms of bindings and changes of bindings among these objects.

1) A given service may run at one or more nodes, and may need to move from one node to another without losing its identity as a service.
2) A given node may be connected to one or more network attachment points, and may need to move from one attachment point to another without losing its identity as a node.
3) A given pair of network attachment points may be connected by one or more paths, and those paths may need to change with time without affecting the identity of the attachment points.

In principle, to obtain data from a service node, the client node must discover the following three objects (also shown in Figure I.1):

1) A service node on which the required service operates,
2) A network attachment point to which that service node is connected,
3) A path from the service node’s network attachment point to the client node’s network attachment point. Actually this task is performed not by the client node, but by the network service nodes that provide data forwarding services in the network.

There are, in turn, three conceptually distinct binding services that the network needs to provide:

1) Service name resolution: to identify the nodes running the service.
2) Node name resolution: to identify attachment points that reach the nodes found in (1).
3) Route service: to identify the paths that lead from the requestor's attachment point to the ones found in (2).

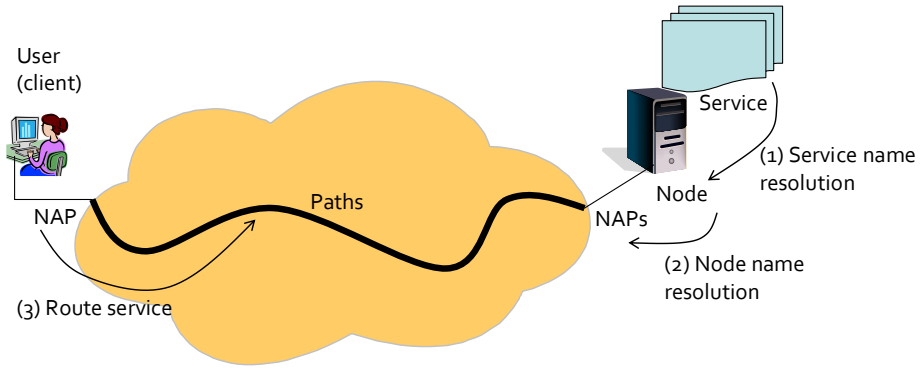


Figure I.1. Four types of objects and three bindings in the Internet

At each level of binding, there can be several alternatives, so a choice of which service node, which attachment point, and which path must be made.

I.2 User, device, and location IDs in ITU-T Next Generation Network

Recommendations [b-ITU-T Y.2001] [b-ITU-T Y.2011] specifying the general overview of NGN emphasize identifying issues to handle the advent of mobility services, different technologies and their interworking.

In the context of mobility services, number portability, etc., NGN refers the following objects (also depicted in Figure I.2) that need to be identified in the network.

1) User: to represent in user/service mobility domain
2) Device: to represent in device mobility domain
3) Location: to represent in the point of attachment

Figure I.2 shows that there is not necessarily any permanent relationship between the identities of objects involved in the network. Generally, NGN is required to establish transient relationship between the telecommunication objects and their locations. The user/device identities can be resolved into location identities or locators representing the NAPs.

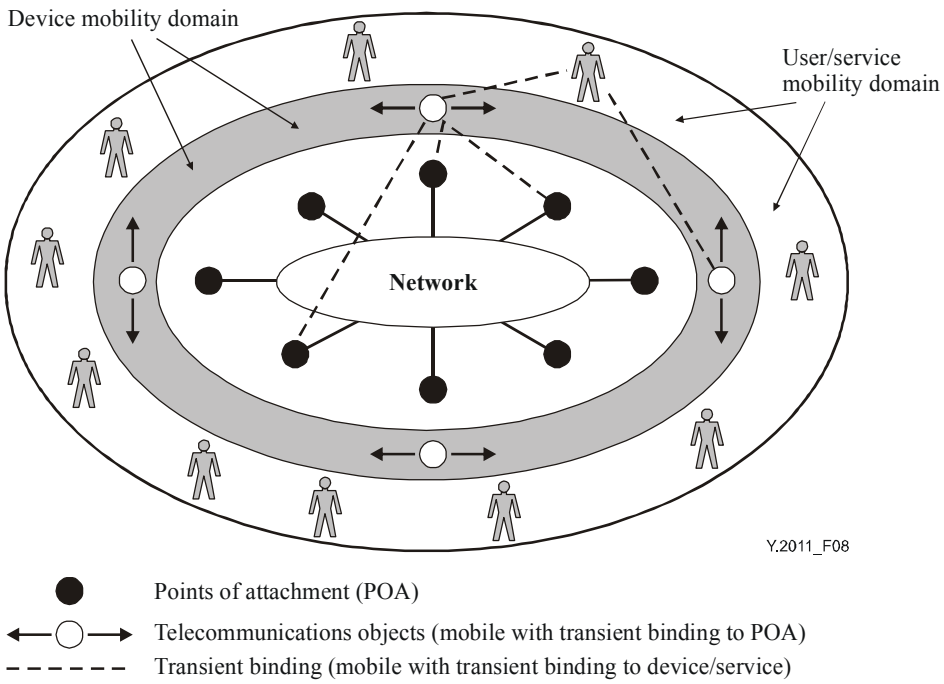


Figure I.2/Y.2011. Relationships among users, devices, and locations

The basic NGN architecture does not define different identifiers to denote a user and a device; both are represented by a URI or URL, or by an IP address. Lately, Recommendation [ITU-T Y.2015] has introduced the node ID in NGN to represent a communication node in the transport and higher layers for the purpose of introducing ID/locator separation in NGN. The node ID is independent of the node location as well as the network to which the node is attached so that the node ID is not required to change even when the node changes its NAP by physically moving or simply activating another interface. This looks reasonable, and FNs should include new mapping functions and registries to support ID/LOC separation such as ones specified in [ITU-T Y.2022] [ITU-T Y.2057].

I.3 Node ID in 3GPP System Architecture Evolution

The 3GPP System Architecture Evolution (SAE) is an all-IP architecture that uses IP protocols and functions to transport both voice and data packets through the Evolved Packet Core (EPC) network. The SAE is evolved from the GSM/3G architecture, which uses the following three types of identifiers assigned to user equipments (UE) [b-TS 23.003]:

1) Mobile Subscriber Integrated Service Digital Network (MSISDN) Number
2) International Mobile Subscriber Identity (IMSI)
3) International Mobile Equipment Identity (IMEI)

An MSISDN is the phone number assigned to a user. It is in the hierarchical structure as specified in E.164 [b-ITU-T E.164]. This is mainly used by a user (i.e. calling party) to setup a call with another user (i.e. called party). Using the MSISDN number, the call request is forwarded to the called party's the Home Subscriber Server (HSS), where the MSISDN number is mapped to the IMSI to find the current location of the called party in the EPC.

The IMSI is mainly used by the network to identify and authenticate a subscriber. It is stored in the HSS and MME (Mobility Management Entity) as an index value associated with the subscriber context. It is represented by a 15 digits number, arranged in a hierarchical structure, consisting of mobile country code (MMC), mobile network code (MNC) and mobile subscription identification number (MSIN). It, along with the MSISDN, is embedded in the SIM (Subscriber Identity Module).

The UE uses its IMSI to authenticate itself when it attaches to a network, which then allocates a random number called Temporary Mobile Subscriber Identity (TMSI) to the UE. For subsequent identification of the UE by the network, the TMSI is used, thus avoiding eavesdroppers from identifying and tracking the subscriber on the radio interface. The TMSI is randomly assigned by the Visitor Location Register (VLR) when the mobile UE is switched on. It is 32-bit long, represented in full hex digits, and locally valid within the geographic area of the VLR coverage for some fixed time.

The IMEI number is used by the network to identify valid devices and therefore can be used for stopping a stolen phone from accessing the network in that country. The IMEI is only used for identifying the device and has no permanent or semi-permanent relation to the subscriber. Moreover, it has no usage in the data communication process.

When a UE attaches with the network by sending an attach request to the MME, the latter requests the Packet Data Network Gateway (PGW) to allocate an IP address to the UE. As in the Internet, the IP address is used by the UE to identify the data communication session with a peer device.

From the above discussion it is observed that although the UE has different types of identifiers, these identifiers have no direct role in data communication. These are mainly used by the control plane for the UE identification, authentication, paging, billing, etc. These control and management functions are also relevant to the FN. Therefore, similar type of identifiers may be useful in the FN. Besides these control plane IDs, the FN may need to define new IDs for identifying UEs and data in the data plane as well. The protocols that handle data packets in the network may use those IDs to optimally transport data in mobile and multihomed FNs.

I.4 Identifiers considered in FN-related projects

This section overviews the different types of identifiers being proposed or considered in various FN related projects. It mainly summaries the identifiers considered in some representative future Internet architecture projects carried out in the USA, Europe, and Asia. MobilityFirst and Named Data Networking have been chosen from the USA projects [b-NSF-FIA], 4WARD [b-4WARD] from European projects, and AKARI [b-AKARI] and MOFI [b-MOFI] from Asian projects.

1) The MobilityFirst (MF) project

MF proposes a common framework of globally unique IDs (GUID) that can be used to name users, devices, contents, contexts and so on. It proposes public key GUID to form a basis for ensuring accountability of traffic, privacy, ubiquitous access-control, and secure routing by protecting infrastructure from address hijacking. Every packet includes GUID in its header so that network nodes can offer GUID based redirection or late binding to network addresses.

2) Named Data Networking (NDN) project

NDN proposes to assign a name to every data or content. It assumes hierarchically structured names, e.g., a video produced by PARC may have the name */parc/videos/WidgetA.mpg*, where '/' indicates a boundary between name components. Names do not need to be globally unique, although retrieving data globally requires a degree of global uniqueness. Names are opaque to the network, that is, routers do not need to understand the meaning of a name. This network-independent naming architecture allows applications to choose the naming schemes that meet their needs and allows the naming schemes to evolve independently from the network.

3) 4WARD project

European Future Internet Project 4WARD has proposed a network of information (NetInf) architecture based on an information-centric paradigm. It emphasizes making the information security functions independent of host-authentication. The NetInf naming framework has been

designed to securely name any kind of content, including Web pages, multimedia files, and real-time streams. In addition, it can be used to securely name services, people, and real-world objects. It uses a general term Information Object (IO) to refer to a piece of content or information. An IO has a globally unique identifier (ID), together with the IO's data and metadata. Thus, an IO is (ID, Data, Metadata). Data contains the information content of IO. Metadata contains attributes associated with the IO, e.g., public keys, content hashes, signatures, and certificates.

The ID is structured in the format as shown below.

Type	Authentication = Hash (PK)	Label = {Identifier Tags}

The type field is used to allow the NetInfo architecture flexibly and extensively adopt different naming schemes. It may specify the type of the content, hash function, ownership, security levels, or the variable format and structure of Labels and assist in interpreting this structure by the name resolution system.

The authentication field binds the ID to a public key (PK) through the use of a one-way, collision-resistant hash function. The PK may associate with every single IO as well as with the whole class of equivalent IOs. The owner of an IO is defined as any entity who knows secret key (SK) used to sign the data of the IO.

The Label field contains a number of arbitrary identifier tags associated with an IO, with a fixed or variable structure as specified by the Type field. These tags, which are related with the data content and/or owner, can be serial or random numbers. The Label field is optional, but the pair of authentication and label fields has to be globally unique.

4) AKARI project

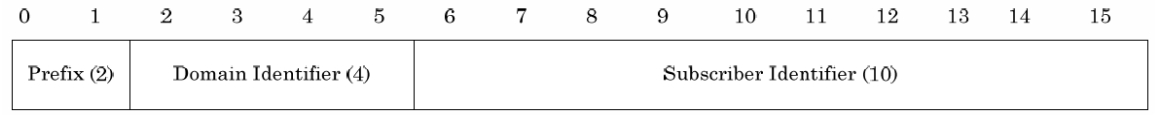
AKARI [b-AKARI] has proposed to assign a unique name (human readable alphanumeric characters) and ID (bit-string) to each host in the design of a new generation network based on ID/locator split. The hostname has two parts, local and global. The global part is the domain name in which the host is associated with, e.g., *mypc#domain1.com* has *mypc* as the local part and *domain1.com* as the domain name. The local hostname is clearly separated from the domain name by using '#' sign to facilitate faster resolution of hostnames into host IDs and locators as well as to efficiently update hostnames to IDs and locators mappings in the servers.

Similarly, AKARI proposes hierarchical host IDs, consisting both locally unique and globally unique parts. That is, a host ID consists of a globally unique prefix assigned by an ID assigning organization and locally unique suffix generated by hashing the hostname and a parameter. The host ID also has the scope and version fields, which are inserted between the prefix and local suffix parts.

5) MOFI project

In MOFI, a host ID (HID) can be represented in two kinds of formats according to types of communications. The first type is hierarchical HID for host based communications such as client-server, and the second type is flat HID for general communications including information (or contents) centric communications.

Firstly, a HID can be represented by a hierarchical format to provide the scalable inter-domain mobility control, in which the domain ID of HID is referred to by a specific mapping system. The current format of 128-bit (16-byte) HID contains the Autonomous System (AS) number as the domain identifier.



Secondly, a HID can be represented by a flat format to address all kinds of communication entities including contents (or information) and services as well as hosts. The flat ID is a self-certifying ID that helps in security enhancement. However, the flat IDs require another set of identifiers in order to manage a huge amount of flat IDs in a scalable manner. This new ID is authoritative domain (AD) ID so that all the flat IDs can be managed separately in their own registered AD. Both the HID and ADID have the same format as shown below.

Crypto type	Public key hash	signature

Bibliography

[b-RFC1498] IETF RFC 1498 (1993), *On the Naming and Binding of Network Destination*.

[b-TS 23.003] 3GPP TS 23.003 (2009), *Numbering, addressing and identification*.

[b-NSF-FIA] NSF Future Internet Architecture Project, http://www.nets-fia.net/

[b-4WARD] FP7-ICT-2007-1-216041-4WARD/D6.2, Second NetInf Architecture Description, January 2010.

[b-AKARI] V.P. Kafle, et al., *An ID/locator split architecture for future networks*, IEEE Communications Magazine, Vol. 48, No. 2, pp. 138-144, February 2010.

[b-MOFI] H. Jung, et al., *HINLO: An ID/LOC split scheme for mobile oriented future Internet*, Future Network & Mobile Summit 2011, June 2011.

[b-ITU-T E.164] Recommendation ITU-T E.164 (2005), *The international public telecommunication numbering plan*.

[b-ITU-T Y.2001] Recommendation ITU-T Y.2001 (2004), *General overview of NGN*.

[b-ITU-T Y.2011] Recommendation ITU-T Y.2011 (2004), *General principles and general reference model for Next Generation Networks*.

[b-ITU-T G.902] Recommendation ITU-T G.902 (1995), *Framework Recommendation on functional access networks (AN) - Architecture and functions, access types, management and service node aspects*.

[b-ITU-T Y.2091] Recommendation ITU-T Y.2091 (2008), *Terms, definitions and high-level terminological framework for Next Generation Networks*.

[b-ITU-T Z.100 Supp.1] Recommendation ITU-T Z.100 Supp.1 (1997), *SDL+ methodology: Use of MSC and SDL (with ASN.1)*.