Draft Recommendation Y.FNid

Framework of identifiers in future networks (Y.FNid)

Summary

This Recommendation first presents a review analysis of identifiers being used in the current networks and FN-related projects. It then presents the framework and general requirements of identifiers to be used in the future networks.

Table of Content

1. Scope

The scope of this Recommendation includes the following items:

- Specification of important objects requiring new identifiers in future networks (FNs);
- Analysis of the identifiers being used in existing networks and FNs projects;
- Framework and generic requirements for identifiers in FNs.

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.ipv6split] Recommendation Draft ITU-T Y.ipv6split (2011), *Framework of ID/locator split in IPv6-based NGN.*

Editor's Note: More references will be added as the draft matures.

3. Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

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.

Identifier [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).

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

Service node (SN) [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.

User [ITU-T Y.2701]: A user includes end user, person, subscriber, system, equipment, terminal (e.g. FAX, PC), (functional) entity, process, application, provider, or corporate network.

Editor's note: The final list will be sorted in alphabetical order and a subsection number will be assigned to each definition.

3.2 Terms defined in this document

Editor's Note: More definitions will be added as the draft matures.

4. Abbreviation and acronyms

This Recommendation uses the following abbreviations and acronyms:

FN	Future Network
ID	Identifier/Identity
DNS	Domain Name System
URL	Uniform Resource Locator
URI	Uniform Resource Identifier
NAI	Network Access Identifier
MAC	Media Access Control
NAP	Network Attachment Point
IMSI	International Mobile Subscriber Identity
IMEI	International Mobile Equipment Identity
SAE	System Architecture Evolution

Editor's Note: Additional abbreviations can be added as demanded by the document content. Once the list is complete, it will be sorted in alphabetical order.

5. Considerations on new identifiers in FNs

Editor's Note: This section will specify objects requiring identification.

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. So, this Recommendation specifies a new framework of identifiers in FNs.

The objects involved in a communication network are users, data or contents, end nodes (or hosts), network nodes, 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 which were designed about 40 years ago were dependent on only one type of identifier, called IP addresses. An IP address identifies both a host as well as the location of the host on the network topology. The Internet also uses domain names for identifying a realm of administrative autonomy domain of the network. However, the domain name is mapped to a specific IP address belonging to a host. Therefore, the domain name conventionally identifies the specific host, and that also only in the application layer. IP addresses are used in the application, transport and network layer protocols. 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 natively [ITU-T Y.2015]. Therefore, the creation of new identifiers for identifying hosts, communication sessions or services in the upper layer protocols is must for FNs. Although [ITU-T Y.2022] and [ITU-T Y.ipv6split] are specifying the functional architecture for the introduction of ID/locator split functions in NGN, they do not mention about the architecture of host IDs and their configuration methods.

Similarly, the present-day Internet lacks identifiers for universally representing data units or contents, which are the basic requirements for realizing content-centric or named data networking. The named data networks are considered to scale in a better manner as they can serve end 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 IDs, the future network also needs user IDs, service IDs, and location IDs. Moreover, the future network also needs new mapping or resolution systems for storing and proving dynamic relationship 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 longer time for updating its records, thus not suitable for storing dynamic ID mappings. The following clauses give an overview of existing identifiers and then describe the framework and generic requirements of the IDs and their mappings in FNs.

6. Analysis of existing identifiers

6.1 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 a data packet from a service node, the client node must discover the following three objects (also shown in Figure 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 other 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).

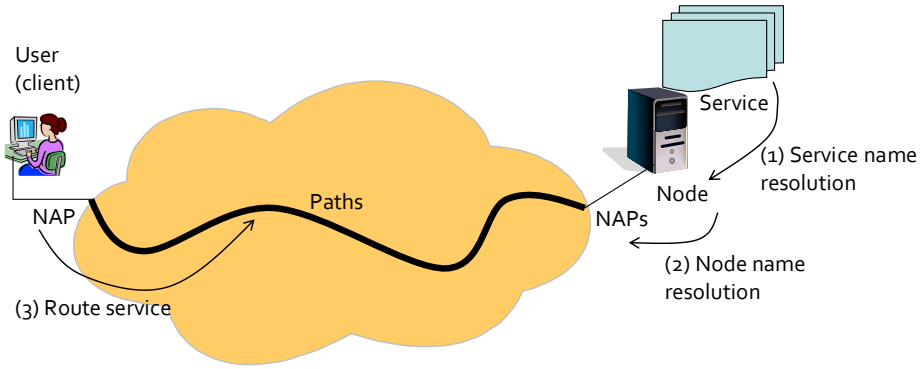

Figure 1. Four types of objects and three bindings in the Internet

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.

6.2 ITU-T Next Generation Network

The Recommendations [ITU-T Y.2001] [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 2) that need to be identified in the network.

- User: to represent in user/service mobility domain
- Device: to represent in device mobility domain
- Location: to represent in the point of attachment

Figure 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.

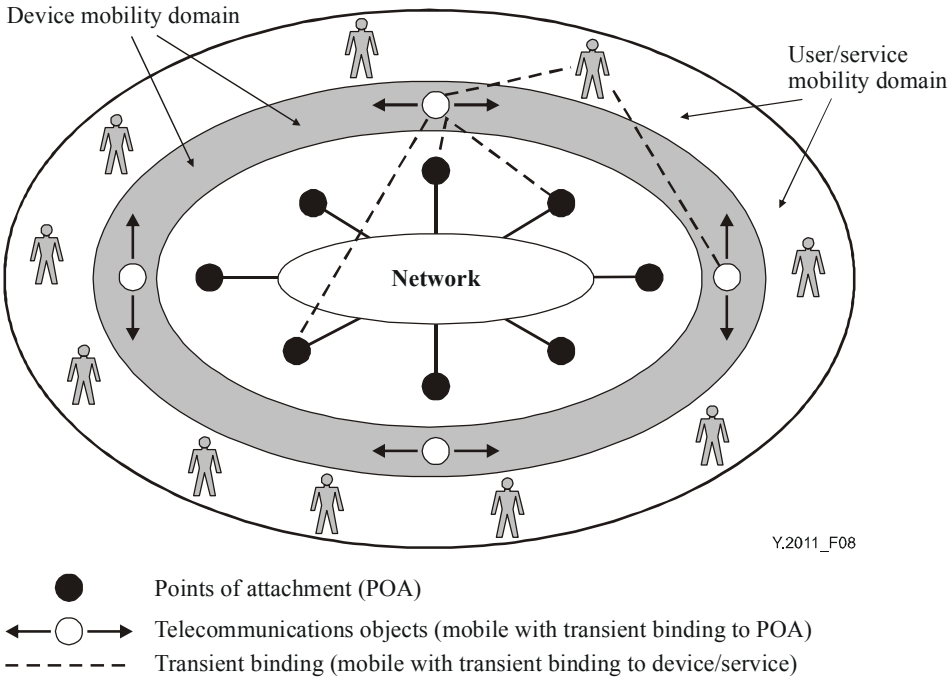

Figure 2. Relationships among users, devices, and locations [referenced from ITU-T Y.2011]

Recommendation [ITU-T Y.2015] has defined the node ID 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. Thus, FN should include new mapping functions and registries to support ID/LOC separation [ITU-T Y.2022].

Editor's Note: The objective of Clause 6 is to analyze current identification systems and find their limitations or problems. Current text in 6.2 lacks such analysis. Contributions are solicited.

6.3 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. 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 allocated 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 VLR when a mobile 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.

This means 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.

6.4 Observations from the perspective of FNs

If we review the identifiers for the four objects discussed in Clause 6.1, these identifiers can be summarized as follows:

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

In the above list, IP address seems a common identifier for most objects and 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 host files 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 node'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 the future network 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 network because of the following reasons:

1) In the Internet design, it was assumed that nodes were static whose NAPs would usually not change. As the mobility environment got popular recently, support for the mobile nodes has been considered as a special case in the Internet. In contrast, a paradigm shift is required in the future network as it has to encompass 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 frequently change 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., persistent node ID mapped to temporary NAP).

3) Multiple interfaces are common in mobile environments as we can see in wireless overlay networks consisting of wireless coverage of different scale 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) Mobile environment is more vulnerable to attack so higher security in the ID structure is required.

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

The above list is not complete; there could be many other issues to be resolved in the future network for efficiently working over mobile environments. Nonetheless, the above discussion provides the background information for why ITU-T should develop new ID standards for the future network.

Editor's note: this sub-clause may also include some explanation of DNS and its limitations for FN.

Editor's Note: A new sub-clause of the review of identifiers being used/considered in FN-related projects need to be added here.

7. Framework of identifiers in FNs

This clause specifies different types of IDs and their relationships in FNs.

7.1 General architecture

The various IDs are required to be handled and maintained in FNs. Figure 7.1 shows a general layout of various kinds of IDs and ID mapping registries that would be used in FNs. These IDs are user IDs, data or content IDs, service IDs, node IDs, and location ID (NAP ID or locators). There may be additional IDs, but for the sake of brevity in explanation, only these IDs are considered in this document. 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 network protocols. The ID mappings are utilized to achieve seamless services over heterogeneous physical networks, such as IP version 6, IP version 4 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.

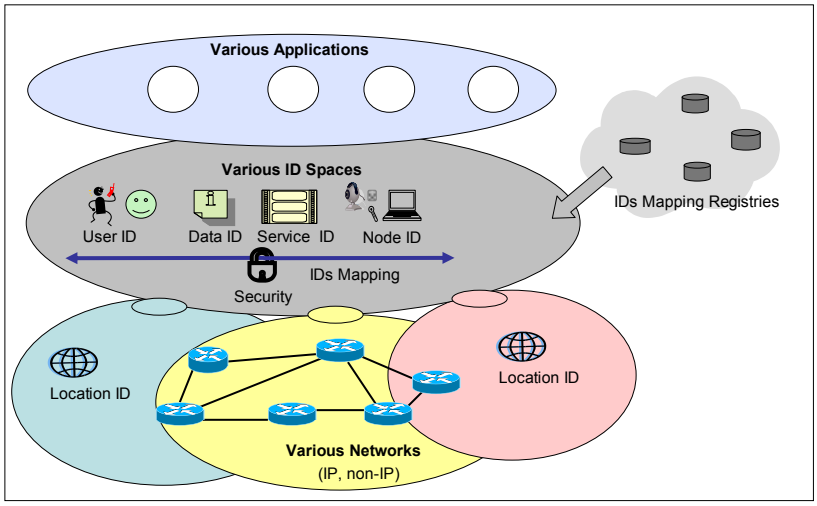

Figure 3. Various IDs in FNs.

7.2 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, 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 identifiers 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.
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.

7.3 IDs mapping management

As mentioned earlier, various types IDs are used in different layers of communication protocols. 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, IDs mapping functions and registries are required to store the relationship between IDs of different categories and scopes. 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 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 transport layer while IP addresses as used as locators to locate hosts 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 host to another, it should not use node IDs, but to use user IDs or service IDs in the transport and application session identification process.

8. Generic requirements for identifiers

The following are the generic requirements for identifiers of FNs.

1) The identifier must 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 must be unambiguous. That is, the identifier must be able to clearly represent an object of the given category. It is recommended that the identifier structure be defined in such a way that the object category may be embedded in the identifier value.
3) The identifiers can be persistent or temporary. A persistent ID may associate with the same object for ever or a longer time, while a temporary ID may associate with the object only for a short time and may be dissociate 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 possess values (or fields) that facilitate mapping an identifier of one category into identifiers of other categories. For example, a service identifier should contain a value that facilitates selecting appropriate locators associated with the most suitable communication method such as broadcast, unicast or anycast, for providing the given service to the user.
5) The mapping between identifiers of one category to the identifiers of another category can be either static or dynamic. The static mapping relationship should not change as time passes, while dynamic mapping should allow the relationship between identifiers change according to time or place.
6) The identifier should 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 IDs mapping functions must be accompanied by security functions for ensuring reliability in network operations and communication services.
8) The identifier of entities that do not exist anymore need to be removed from the ID mapping registries.

Editor's Note: Additional generic requirements will be added later. Contributions are solicited.

Appendix

Future actions for standardization

Editor's Note: This section was useful when this document was progressing as the FGFN document. But now this document has become an ITU-T Recommendation draft and may not need this section. For the time being it has been moved to Appendix (later it may be deleted).

Since the scope of this Recommendation is to specify the general framework and basic requirements of identifiers to be used in the future networks, it does not specify how these identifiers are configured and mapped to one another.

Therefore, new recommendations need to be created to specify the following items:

1. Methods for configuring identifiers of different categories;
2. Methods for mapping identifiers of one category into identifiers of other categories;
3. Methods for assigning identifiers to communication objects; and
4. Methods for administration of identifier distribution to different organizations;

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.

_____