Draft Recommendation ITU-T Y.2015 (Y.ipsplit)

General requirements for ID/locator separation in NGN

Summary

This Recommendation begins with showing the limitations of the conventional IP architecture, which uses IP addresses as both node identifiers (IDs) and locators, on supporting mobility, multihoming, fast endpoint renumbering, traffic engineering, and scalable routing. It then shows that ID/locator separation, i.e., the use of distinct sets of values as node IDs and locators, helps to overcome these limitations. This Recommendation provides general requirements for introducing ID/locator separation in NGN.

Table of Contents

1. Scope

This Recommendation begins by showing the limitations of the conventional IP architecture, which uses IP addresses as both node identifiers (IDs) and node locators, for supporting mobility and multihoming and mentions how such limitations would be overcome by ID/locator separation, i.e., by using distinct sets of values for node IDs and locators.

It then defines general requirements for ID/locator separation to efficiently support mobility, multihoming and host renumbering in NGN. Through ID/locator separation, it is recommended to have network topology-independent node IDs and topology-dependent locators, and maintain a mapping between NGN identifiers, Node IDs and locators.

It outlines a general architecture of ID/locator separation in NGN and provides general requirements of the architectural components. It also outlines security requirements of the architecture that are specific to ID/locator separation.

2. References

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

[ITU-T Y.2011]   Recommendation ITU-T Y.2011 (2004), *General principles and general reference model for next generation networks.*

[ITU-T Y.1251]   Recommendation ITU-T Y.1251 (2002), *General architectural model for interworking.*

[ITU-T Y.2012]   Recommendation ITU-T Y.2012 (2006), *Functional requirements and architecture of the NGN.*

[ITU-T Y.2201]   ITU-T Recommandation Y.2201 (2006), *NGN release 1 requirements.*

[ITU-T Y.2091]   Recommendation ITU-T Y.2091 (2006), *Terms and definitions for Next Generation Network.*

[ITU-T Y.1241]   Recommendation ITU-T Y.1241 (2001), *Support of IP-based services using IP transfer capabilities.*

[ITU-T E.164]   Recommendation ITU-T E.164 (1997), *The international public telecommunication numbering plan.*

[ITU-T Y.2052]   Recommendation ITU-T Y.2052 (2008), *Framework of Multi-homing in IPv6-based NGN*

[ITU-T H.323]   Recommendation ITU-T H.323 (2003), *Packet-based multimedia communication systems.*

[ITU-T Y.2801]   Recommendation ITU-T Y.2801 (2006), *Mobility management requirements for NGN.*

[IETF RFC 3261]   IETF RFC 3261 (2002), *SIP: Session Initiation Protocol.*

3. Definitions

3.1. Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1. access border gateway [ITU-T Y.2091]

A packet gateway between an access network and a core network.

3.1.2. address [ITU-T Y.2091]

An address is the identifier for a specific termination point and is used for routing to this termination point.

Note: This Recommendation only uses the term "address" in the case where it does not specifically refer to a locator or an identifier.

3.1.3. 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). Identifiers can be used for registration or authorization. They can be either public to all networks, shared between a limited number of networks or private to a specific network (private IDs are normally not disclosed to third parties).

Note: In this Recommendation, this identifier is referred to as "NGN identifier." We define a new term "Node ID" that would be used in transport and upper layers in the ID/locator separation architecture.

3.1.4. seamless service [ITU-T Y.2801]

The service that will prevent users experiencing any service disruptions while changing point of attachment.

3.1.5. service continuity [ITU-T Y.2801]

The ability for a mobile object user to maintain an ongoing service, including current states, such as user's network environment and session for a service.

3.1.6. session [ITU-T Y.2091]

A temporary telecommunications relationship among a group of objects in the service stratum that are assigned to collectively fulfill a task for a period of time. A session has a state that may change during its lifetime. Session-based telecommunications may be, but need not be, assisted by intermediaries (see mediated services). Session-based telecommunications can be one-to-one, one-to-many, many-to-one, or many-to-many.

3.2. Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1. locator (LOC)

A locator is the network layer topological name for an interface or a set of interfaces. LOCs are carried in the IP address fields as packets traverse the network.

Note: IP addresses can gradually become pure LOCs. However, on the contrary, it cannot be said that a LOC is an IP address. An IP address may associate with the IP layer as well as upper layer

protocols (such as TCP and HTTP), whereas a LOC will associate with only the IP layer and be used in IP address fields.

3.2.2. ID/LOC separation

ID/LOC separation is decoupling the semantic of IP address into the semantics of node IDs and LOCs. Distinct namespaces are used for node IDs and LOCs so that they can evolve independently. LOCs are associated with the IP layer whereas node IDs are associated with upper layers in such a way that ongoing communication sessions or services shall not be broken by changing LOCs due to mobility and multihoming.

Note: In the context of this Recommendation, a completely new namespace for node IDs can optionally be created that would leave the IP address space more or less intact for LOCs, allowing routing technologies to be developed independently of end-host mobility and end-host multihoming implications.

3.2.3. ID/LOC mapping

ID/LOC mapping is an association between a node ID and one or more LOCs.

Note 1: A single node ID or several node IDs can be associated with many LOCs associated with a single terminal. The node ID to LOC mapping can have the one-to-one, one-to-many, or many-to-one relationship.

Note 2: ID/LOC mapping is also called ID/LOC binding.

3.2.4. ID/LOC mapping storage function

An ID/LOC mapping storage function stores the mapping of NGN identifiers, Node IDs and LOCs. This function also updates mapping information, as well as provides mapping information to other functions on request. The mapping storage function can be physically located in an NGN terminal or with other NGN components.

3.2.5. ID/LOC mapping function

An ID/LOC mapping function gets mapping information from an ID/LOC mapping storage function and uses the corresponding node ID and/or LOC in packet headers. The ID/LOC mapping function works in a close correlation with the transport user profile associated with the transport control function.

Note: ID/LOC mapping functions can be physically located in an NGN terminal, an access border gateway, or any other NGN components.

3.2.6. node

A node is defined as a connection point that may be a network device, a user terminal or a process where data can be transmitted, received or forwarded. In general, a node is identified by its NGN identifier by the user, and by its node ID by the protocol stack.

3.2.7. node ID

A node ID is an identifier used at the transport and higher layers to identify the node as well as the endpoint of a communication session. A 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 network connectivity by physically moving or simply activating another interface. The node IDs should be used at the transport and higher layers for replacing the conventional use of IP addresses at these layers. A node may have more than one node ID in use.

Note: Unless otherwise specified, the term "ID" used in this Recommendation represents a node ID, not an NGN identifier specified in this or any other Recommendations.

4. Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API   Application Programming Interface

CPN   Customer Premises Network

DNS   Domain Name System

FE   Functional Entity

GERAN   GSM EDGE Radio Access Network

ID   Identifier

IP   Internet Protocol

ISP   Internet Service Provider

LAN   Local Area Network

LOC   Locator

NGN   Next Generation Network

SIP   Session Initiation Protocol

TCP   Transmission Control Protocol

URI   Uniform Resource Identifier

URL   Uniform Resource Locator

UTRAN   UMTS Terrestrial Radio Access Network

WiMAX   Worldwide Interoperability for Microwave Access

WLAN   Wireless Local Area Network

5. General overview of ID and LOC separation

This clause provides background information to assist the development of the Recommendation. The following subclauses describe a general reference model for ID/LOC separation.

5.1. General environment under IP based network

According to the definition of NGN [ITU-T Y.2001], the NGN framework is expected to support advanced architectural objectives over a unified IP network. NGN Release 1 assumes IPv4 or IPv6 networking at packet interconnection points and packet network interfaces [ITU-T Y.2201]. NGN is an IP based network and keeps all features of the IP protocol, although some features are counterproductive to the NGN objectives.

Figure 1 presents the reference framework of an IP based network, illustrating IP-based services and IP transfer capabilities [ITU-T Y.1241]. An IP based service is a set of functions and facilities that utilize IP transfer capabilities offered by NGN to a user. The IP transfer capability is a set of network capabilities provided by the IP layer. NGN decouples IP-based services and transport, allowing them to be offered separately and evolve independently [ITU-T Y.2001].

We assume that an IP based service is provided to end users or nodes. In the current IP network, even if the service is started between end nodes through their NGN identifiers such as E.164 [ITU-T

E.164], SIP ID [IETF RFC 3261], or URL, these nodes' IP addresses, which are obtained by translating the NGN identifiers from a mapping function storage such as DNS, are directly used for establishing a communication session and transferring data between the end nodes. The IP address not only describes the location of the end node or user within the IP based network topology but also uniquely identifies the end node in the transport and higher layers.
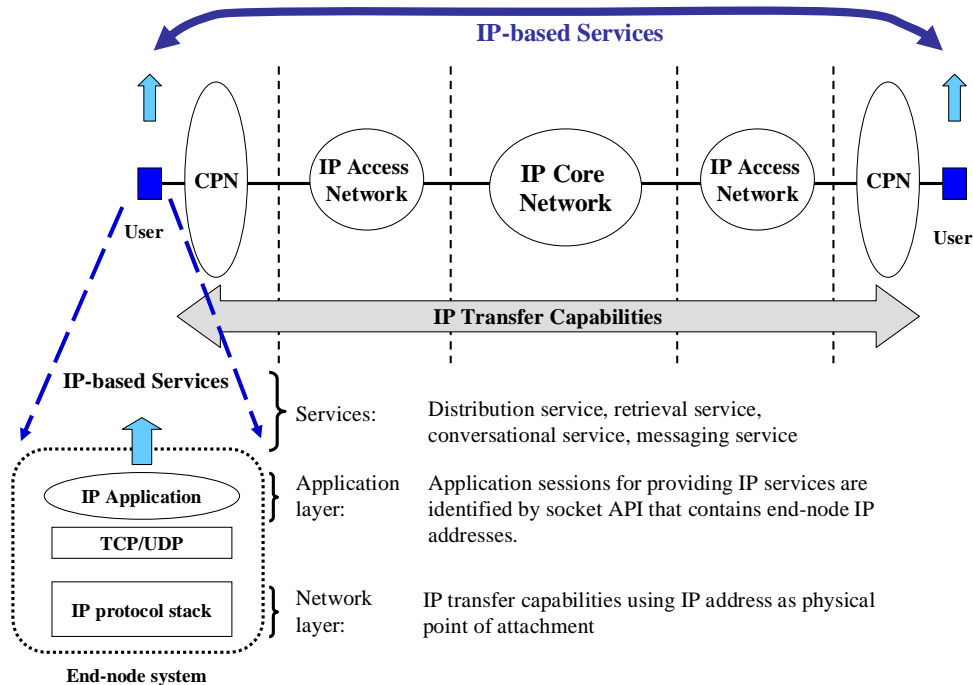
CPN: Customer Premises Network

Figure 1 – General architecture of IP based network [ITU-T Y.1241]

5.2. General concept of ID/LOC separation

An IP address assigned to a node has overloaded semantics in the conventional IP-based network. It is a node ID that uniquely identifies the node; it is a locator that uniquely locates the node in the network topology; and it also can be used for determining path to reach the node. Thus the IP address provides or helps provide answers to the following three questions about the node: who the node is, where the node is, and how to get to the node. These semantics embedded into every IP address are causing serious problems in supporting seamless services in a mobile or multihomed networking environment, where a node is allowed to change its locator while maintaining the same node ID. Thus, separating the role played by the conventional IP addresses into the roles of node IDs and LOCs solves these problems.

5.2.1. ID/LOC separation in IP based network

ID/LOC separation is a mechanism which decouples the transport and higher layers from the network layer so that an end-to-end communication session is not bound to IP addresses as it conventionally is as shown in Figure 2.A. The new architecture with ID/LOC separation distinguishes a node ID, which is a semantic name to recognize the endpoint of a communication session, from a LOC, which is a semantic name of an IP address, through a binding between the ID and LOC as shown in Figure 2.B. By doing so, IP addresses no longer directly associate with the communication session, but only with the network layer.
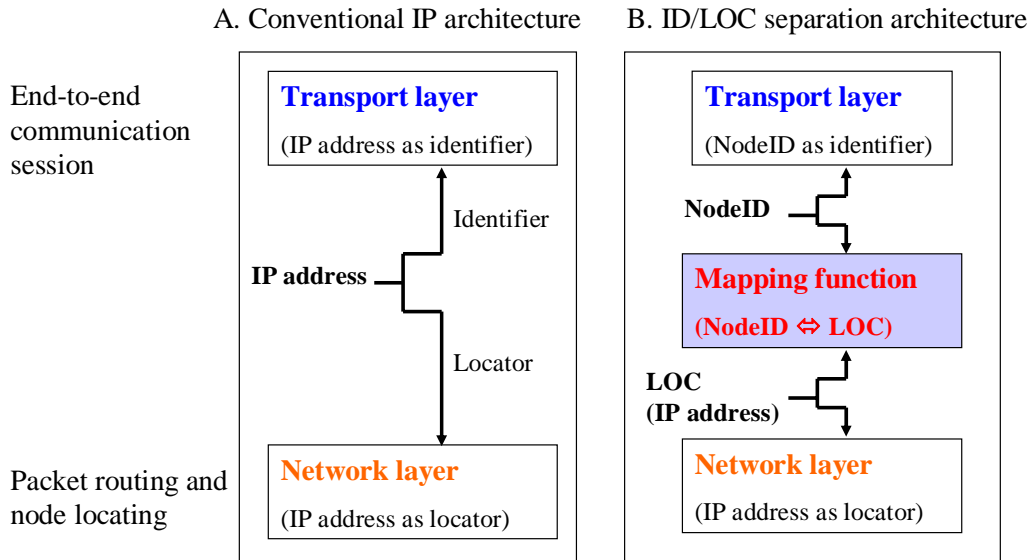
A. Conventional IP architecture   B. ID/LOC separation architecture

Figure 2 – Comparison between conventional IP architecture and new ID/LOC separation architecture

5.2.2. ID/LOC separation in NGN

5.2.2.1. Identification and location in NGN

NGN has the fundamental characteristic of supporting a variety of identification schemes. The followings are the examples of identification schemes [ITU-T Y.2001].

- E.164 [ITU-T E.164] numbering scheme;
- Unified Resource Locator (URL) scheme;
- Unique name system;
- Other naming conventions such as H.323 [ITU-T H.323], SIP [IETF RFC 3261], telephone and mail uniform resource identifier (URI).

The location of a telecommunication object (i.e., user or device) can be represented by the physical point of attachment (POA) where the object may be reached or found [ITU-T Y.2011]. The location in the IP-based transport network is represented by an IP address.

When a user or device initiates a communication session with another one, one of the above-mentioned identifiers is translated into a routable IP address through a network internal database or an external database such as the Domain Name System (DNS).

5.2.2.2. Architectural model

The advent of mobility, multihoming, and their interworking has increased network complexity and challenges to maintain service and session continuity when end nodes change their locations or network associations [ITU-T Y.2012]. For instance, an NGN terminal with dual interfaces can attach to two different points of the same access network or of different access networks, such as GERAN/UTRAN and WiMAX/WLAN, simultaneously. In this case, the terminal or end node is permitted to have two IP addresses (i.e., locators) belonging to the same access network or two different access networks as shown in Figure 3. In such a multihoming case, there should be no fixed relationship between the node ID and locator in order to enable the end node to change its locator when it changes the association point in the access network while keeping the same node ID. Thus new transient relationships between node IDs and LOCs are required to be supplemented in NGN.

ID/LOC mapping information can be stored in one or more ID/LOC mapping storage function located anywhere in the NGN core, access network, or end node. The mapping is updated by end nodes or access networks when they detect changes in ID/LOC relationships. Since the ID/LOC binding changes that occur due to end node mobility or multihoming are primarily detected by the end nodes or by the access network, it is recommended that the end nodes or access networks implement ID/locator mapping functions to format and process data packets by utilizing the ID/LOC binding information. Therefore, for faster adaptation to the changes, it can be beneficial to keep the scope of the mapping function local to the end node or the access network as shown in Figure 3. Data packets are transmitted through the core network by using LOCs only, i.e., IP addresses. A LOC used by the end node in packet headers is allowed to be replaced with another LOC by the access network for traffic engineering or other purposes.

The advantages of the ID/LOC separation architecture are as follows.

- Allow node IDs to be used in the long-term security and trust relationship.

- Allow LOCs to reflect the network topology and facilitate topological aggregation.

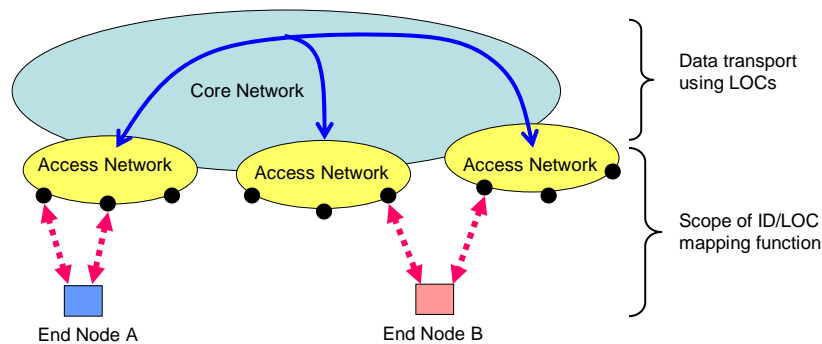- Allow node IDs to be persistent even when LOCs change due to mobility or multihoming.

Figure 3 – General concept of ID/LOC separation in NGN

6.   General requirements for ID/LOC separation

The NGN access transport functions are required to be capable of providing IP connectivity. The IP protocol may be carried over various underlying transport technologies in the IP access and core portions of the transport stratum [ITU-T Y.2201]. That is, IP is a key feature to support NGN services. However, the conventional IP architecture has some problems to support NGN services efficiently as mentioned in clause 5.

This clause provides general requirements related to ID/LOC separation.

6.1. Requirements for survivability

Survivability is provided by many functions that are necessary to realize highly reliable networks. NGN is required to support switching protection, rerouting, and service resiliency for survivability [ITU-T Y.2201]. However, the ID/LOC separation specific survivability mainly focuses on communication session continuity.

The following are general requirements for survivability related to ID/LOC separation.

- Upper layer sessions identified by node IDs are required to survive when switching the lower layer transport between different LOCs.

- ID/LOC separation is recommended to provide the capability that can immediately detect a link or end-to-end path failure.

- ID/LOC separation is recommended to provide the capability that can change data transport to an alternative link or end-to-end path within an acceptable time to recover from a failure.

- After recovery from link failure or quality degradation, ID/LOC separation is recommended to have the capability to switch data transport to the previous path by considering the network performance or quality of service.

- ID/LOC separation is recommended to provide the capability that can detect an imminent link or path failure and avoid communication session discontinuity by moving the traffic load to other less-loaded link or path.

6.2. Requirements for node ID persistency

ID/LOC separation is required to provide the capability to manage node ID persistency in such a way that a node ID used to identify the endpoint of a communication session remains unchanged during a service or application operation.

The following are general requirements for node ID persistency related to ID/LOC separation.

- The transport and higher layers are required to use the same node ID for a particular application service or transport session.

- The node ID is required to facilitate the continuation of an application service or transport session regardless of LOC changes.

- The node ID is required to be long-lived, i.e., it is required that the node ID used for a session not have to be replaced before the session terminates. However, the node ID may or may not be permanent. Its lifetime may depend on the user's willingness, network support, or privacy and security requirements.

6.3. Requirements for multihoming

NGN terminals are allowed to have two or more network connections through the same or different access networks with multiple network interfaces and multiple addresses [ITU-T Y.2052]. NGN is required to have the capability to allow terminals to choose one of the network providers or change network providers without incurring service and/or session discontinuity. Therefore, the architecture is required to support multihoming when one or both of two peer nodes are multihomed.

The following are general requirements for multihoming capability related to ID/LOC separation.

- An NGN terminal is required to have the capability to associate one node ID with multiple network interfaces or locators at the same time.

- An NGN terminal is required to have the capability to associate one node ID with different locators without incurring service and/or session discontinuity.

- An NGN terminal, even when it is single homed, can optionally choose network providers if the access network's policy allows.

- An NGN terminal can continuously maintain application services and communication sessions without any extra efforts while the access network changes or switches between upstream links to the core network.

6.4. Requirements for mobility

Generalized mobility means providing the ability to use different access technologies at different locations while the user and/or the terminal equipment itself may be in movement allowing users to use and manage consistently their applications/customer services across existing network boundaries [ITU-T Y.2001]. However, the ID/LOC separation specific mobility is only concerned

with service and session continuity, not with seamless mobility or seamless services as specified in [ITU-T Y.2801].

The following are general requirements for mobility related to ID/LOC separation.

–   An NGN terminal is required to maintain transport layer connectivity continuously while moving within the same access network.

–   An NGN terminal is required to maintain transport layer connectivity continuously while moving across heterogeneous wireless and/or wired access networks.

–   An NGN terminal is required to maintain transport layer connectivity continuously even when the access network or customer premises network is moving.

6.5.   Requirements for locator renumbering

Basically, an NGN terminal in the conventional NGN (i.e., where ID/LOC split has not been yet implemented) is assigned with one or more IP addresses from the access network. If the network's IP address block is changed, all terminals connected to the provider's network also have to change their IP addresses to the new ones belonging to the new IP address block. In this environment, ID/LOC separation is required to provide the capability that changes in the network's locator block do not influence communication session continuity.

The following are general requirements for network address renumbering related to ID/LOC separation.

–   A customer premises network can optionally be associated with different access networks.

–   A customer premises network can optionally change the access network without affecting communication session continuity.

–   An access network can optionally associate with different core networks.

–   An access network can optionally change the core network without affecting communication session continuity.

–   The network locator renumbering is required to be efficient so that it does not take much time and effort of the administrator.

6.6.   Requirements for traffic engineering

Traffic engineering provides the ability to direct traffic along non-default links. Multihoming is a prerequisite for traffic engineering. Corresponding to multihoming, either one or both of end host-based traffic engineering and site-based traffic engineering are required to be supported by ID/locator separation.

The following are general requirements for traffic engineering related to ID/LOC separation.

-   Either the terminal or the access network is allowed to monitor the traffic status of multiple available upstream links for latency, throughput, and service charge, in order to switch links intelligently.

-   Either the terminal or the access network is required to be permitted to change the transmission path for load balancing, load sharing, failure avoidance or recovery by allowing the use of alternate LOCs from the available ones.

-   An NGN terminal can optionally choose an appropriate LOC by dynamically monitoring the network condition in order to change the transmission path.

-   An NGN terminal can optionally change its LOC for traffic engineering without discontinuing communication sessions.

7.   Functional requirements for ID/LOC separation

This clause describes functional requirements for the ID/LOC separation organizational components, without intending to describe the functional requirements for general NGN components.

The aim of ID/LOC separation is to eliminate the overloaded semantics of IP address from the NGN architecture. Node IDs are used in the transport and higher layers while IP addresses are used for forwarding data packets through underlying transport technologies in access and core portions of the transport stratum. Therefore, the functional entities related to ID/LOC separation may handle some operations of the NGN transport stratum to exclude using IP addresses as node ID in communication sessions.

7.1.   Requirements for node ID

NGN is intended to provide an efficient, secure, and trustworthy identity like numbering, naming, and addressing for end users, network providers, and service providers [ITU-T Y.2201]. Basically, the identity has some capabilities for user identification, in order for network providers and service providers to authenticate and authorize users for NGN services.

In the ID/LOC separation architecture, the meaning of node ID is somewhat different from the identity mentioned above. In this Recommendation, the newly defined node ID is used at the transport and higher layers to identify the end node or endpoint of communication sessions.

The followings are general requirements for node ID capabilities.

- The node ID namespace is required to fully decouple the network layer from the higher layers. That is, the node ID is required to replace all occurrences of IP addresses within the transport and higher layers.

- The node ID is required to uniquely identify the endpoint of a communication session from the aspects of transport and higher layer protocols.

- During a communication session, the node ID is required not to change due to changes in LOCs.

- The node ID is required to be associated with one or more LOCs. The association may change without disconnecting an ongoing communication service.

- The node ID can optionally have a hierarchical structure for scalability of mapping systems.

- A terminal is required to have one or more node IDs. The node ID is allowed to be long-lived until the user, terminal, or network decides to replace it. Node IDs can have a local or global scope.

- A node ID can optionally be assigned permanently to an NGN terminal or be generated by the terminal itself or assigned by some other entity on demand.

- The node ID namespace is required to be authenticateable. A node ID may be generated from the public key of an asymmetric key pair or from an NGN identifier, which may self-assert or get authentication from a third-party.

7.2.   Requirements for LOC

The LOC of an NGN terminal represents the physical point of attachment of the terminal in the NGN access network. The LOC is used to find/reach the terminal.

At the transport stratum, NGN is required to support IPv4, IPv6, or both, so the LOC may take the form of an IPv4 address or an IPv6 address.

The followings are general requirements for LOC capabilities.

- – LOCs must be globally or locally routable.

- – LOCs can optionally represent a strict network topology. That is, LOCs can optionally be typically assigned based on the structure of the network provider. LOCs can optionally be allocated by using an addressing scheme specific to the access network.

- – LOCs can optionally have an aggregatable structure for scalability.

- – LOCs are recommended to be globally unique in order to represent a unique location in the global network topology. LOC collisions are required to be strictly forbidden within the scope of the LOC namespace.

- – LOCs are required to be assigned or authorized by the access network.

- – LOCs can optionally be resolved into corresponding node IDs or NGN IDs by the ID/LOC mapping storage function.

- – Different LOCs are can optionally be used for different communication sessions between two terminals in a multihoming environment.

7.3.   Basic functionalities

Conventionally, an NGN identifier such as an URL or a SIP identifier is translated into an IP address when starting an application service. The IP address is then used as an identifier in the transport and higher layers to identify the endpoint of the communication session and as a locator in the network layer to locate the endpoint and route packets in the network topology. However, in mobility and multihoming environments, it is not necessary that there exists a permanent relationship between the NGN identifier and IP address.

In Figure 4, to eliminate the permanent relationship, the conventional mapping function of the NGN that maps between NGN identifiers to IP addresses is augmented with an additional function to map from NGN identifiers to node ID, Node IDs to Locators. As usual, the end user starts an end-to-end communication service using its NGN identifier. The mapping function residing in the user terminal translates the NGN identifier into the node ID, which is used at the transport stratum to uniquely identify the endpoint of the communication session. The mapping function, residing either in the end user terminal or in the network, would translate the NGN identifier or node ID into LOCs, which are used for media transport. Alternatively, the mapping between NGN identifiers to node IDs as well as to LOCs may take place in a single operation of the ID/LOC mapping function. The introduction of the new mapping function separates transport functions, which are composed of IP access as well as IP core transport functions, from services and applications for supporting end-to-end transparency. The end-to-end communication session does not break even when the user terminal changes its LOCs.
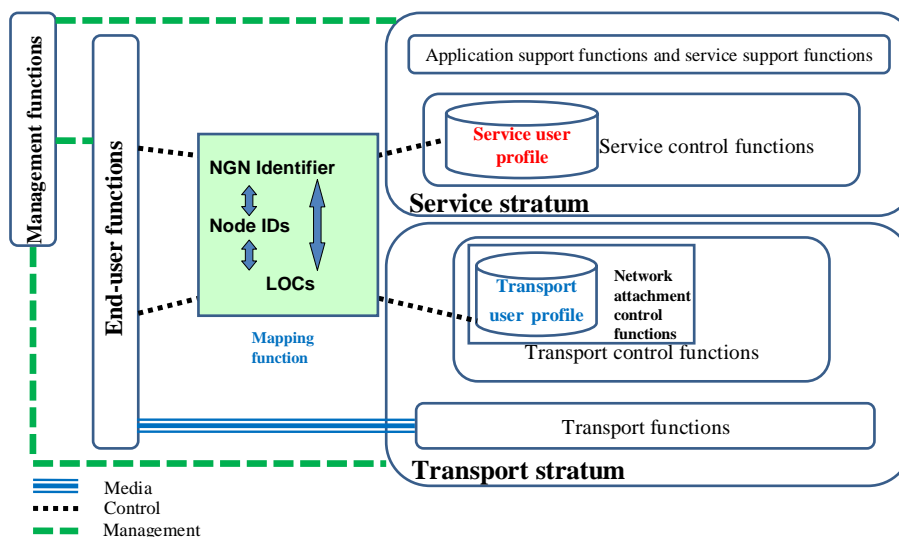
Figure 4 – Overview of functionalities for ID/LOC separation in NGN

NOTE 1 – The figure represents an abstract view of the NGN architecture referenced from [ITU-T Y.2012].

NOTE 2 – To implement ID/LOC separation, the mapping function depicted by the shaded box is added in the conventional NGN architecture to introduce node IDs between NGN identifiers and IP addresses (i.e., locators).

NOTE 3 – The mapping from an NGN identifier to a LOC may take place in two stages, i.e., from the NGN identifier to a node ID in the first stage and from the node ID to the LOC in the second stage. In an alternative approach, it may be possible to map the NGN identifier to the node ID as well as to the LOC in a single stage. Or mapping may not be required at all if the NGN identifier is routable as a LOC.

NOTE 4 – The mapping can involve functional components, such as the ID/LOC mapping storage function and the ID/LOC mapping function, as given Section 8. However, specific descriptions of these functions are outside the scope of this Recommendation.

NOTE 5 – The mapping function works in close correlation with the service user profile and the transport user profile.

## 8. General architecture for ID/LOC separation in NGN

General architectural functions for ID/LOC separation and their allocation to different functional components are covered in this clause. The basic requirements for the general architecture are also outlined here.

8.1. General considerations of ID/LOC separation

The objective of the architecture for ID/LOC separation is to support efficient multihoming and mobility management by separating the role played by IP addresses in the current IP architecture into the roles of node IDs and LOCs.

The IDs, in general, should be location-independent and valid for a long time. On the other hand, LOCs are considered to be location-dependent, i.e., associated with the network, and are allowed to change frequently to support mobility or multihoming. A node ID is required to associate with more than one LOC at any instant to support multihoming or with different LOCs at different instants as

the end node moves to different networks. The ID/LOC mapping data is assumed to be stored in an ID/LOC mapping storage function.
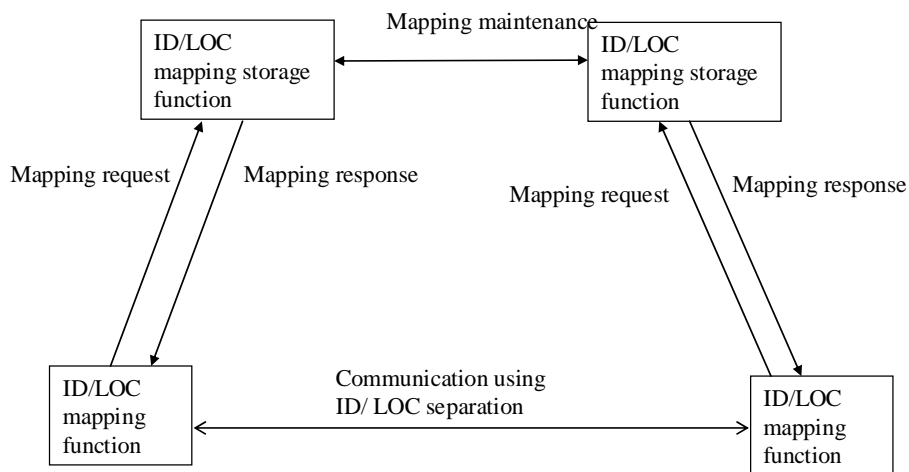
Figure 5 – ID/ LOC separation architectural components in NGN

8.2. Architectural components

The components involved in the ID/LOC separation architecture are shown in Figure 5. Note that although the ID/LOC mapping storage function and ID/LOC mapping functions are shown separately in the figure, they can physically be collocated in an NGN terminal or a border access gateway. ID/LOC mapping storage functions and ID/LOC mapping functions are the main components of the architecture. The ID/LOC mapping storage functions maintain ID/LOC mapping data. The ID/LOC mapping functions communicate with each other to distribute, update and retrieve mapping information. The ID/LOC mapping storage functions are also recommended to communicate with other network elements that originate/update ID/LOC mapping information (not shown in the figure).

The ID/LOC mapping function requests the ID/LOC mapping storage function to get mapping information corresponding to a node ID. The ID/LOC mapping storage function searches its database for the requested node ID. If it is found, the ID/LOC mapping storage function responds to the ID/LOC mapping function with the mapping information. Otherwise, it forwards the request to other ID/LOC mapping storage functions. This process is repeated until the mapping is found in the system. The ID/LOC mapping function uses the mapping information to implement mapping functions and communicate with other ID/LOC mapping functions. In between two ID/LOC mapping functions there can be additional ID/LOC mapping functions to support multi-level mapping for routing data through better paths in terms of security, reliability, QoS, etc.

8.3. Architectural requirements

This subclause presents requirements for maintaining ID/LOC mapping storage function, implementing ID/LOC mapping functions, detecting mapping changes and recovering from failures.

The following are the requirements for maintaining the ID/LOC mapping storage function.

- Mapping information is required to be kept distributed in the system to avoid any bottleneck and single point of failure at the ID/LOC mapping storage function.

- The overhead in maintaining mapping databases is required to be low.

- Mapping updates are required to propagate to ID/LOC mapping storage functions in a due course of time, while keeping the update frequency within some limit so that the network does not get congested by the mapping information.

- The mapping information retrieval time is required not to exceed the given limit of connection setup time.

- Mapping information stored at different ID/LOC mapping storage functions is required to be consistent.

- Security mechanisms are required to prevent a malicious entity from corrupting the mapping database.

- Irrespective of their location in the access network or the core network, ID/LOC mapping storage functions are required to be accessible from any other locations in NGN.

- It is required that mapping information take account of user and device location privacy issues.

The following are the requirements for the ID/LOC mapping function.

- The ID/LOC mapping function is required to use an appropriate security mechanism while retrieving mapping information from the ID/LOC mapping storage function.

- The ID/LOC mapping function is recommended not to use the same mapping information for ever. The ID/LOC mapping function is required to refresh mapping information from ID/LOC mapping storage functions after a certain period of time.

- An end node supporting the ID/LOC mapping function is also required to be able to communicate with other nodes that do not support the ID/LOC mapping function.

- An end node is required not to use the ID/LOC mapping function if the peer node does not support the function.

The following are the requirements for failure detection and recovery from ID/LOC mapping changes.

- Mapping changes are required to be propagated to concerned ID/LOC mapping functions and ID/LOC mapping storage functions in a due course of time such that ongoing communication services and sessions are not disconnected by the changes.

- ID/LOC mapping functions or any other network components are required to implement a mechanism for recovering from the ID/LOC mapping failure.

9. Capability from ID/LOC separation

The application of ID/LOC separation in the NGN architecture provides the following capabilities to end users, network providers, and service providers.

a) End user capabilities:

   i. An end user becomes able to support services seamlessly even when the terminal changes its point of attachment within the same access network or across various access networks.

   ii. The ID/LOC separation allows end users to change network providers easily.

b) Network provider capabilities:

   i. Since node IDs have the characteristic of being location-independent, and since LOCs are used to specify the topological location in the network, network providers can focus on

providing scalable routing using the topologically aggregatable LOCs and can establish the better routing policy for traffic engineering and reliability.

  ii. ID/LOC separation can play a role in supporting load sharing.

 iii. ID/LOC separation can play a role in making network renumbering easier.

c)   Service provider capabilities:

  i. An NGN service provider becomes able to deliver application services continuously even when the user terminal changes its point of attachment to the network.

  ii. The process of session management for supporting uninterrupted connectivity in a mobility or multihoming environment becomes simpler.

10. Security consideration

ID/LOC separation is expected to deal with dynamic conditions where LOCs are allowed to change frequently due to mobility or multihoming. In such cases, the secured and authenticated mapping between node IDs and LOCs is highly required to prevent any malicious entity from corrupting mapping information and diverting traffic to some unwanted places.

Mainly the following entities/tasks are required to be secured.

a) ID/LOC mapping storage function: The ID/LOC mapping database is required to be secured.

b) ID/LOC update mechanism: Only authenticated entities are recommended to update the mapping database. That is, an NGN terminal or ID/LOC mapping storage function is required to accept an ID/LOC update only when it comes from an authenticated ID/LOC mapping storage function or terminal.

c) ID/LOC retrieve mechanism: An NGN terminal is required to use secured mechanisms to retrieve ID/LOC mapping data from authenticated ID/LOC storage functions. No any entities in the middle are allowed to alter mapping data.

d) NGN terminal cache: In case an NGN terminal uses ID/LOC mapping stored in its cache while initializing communication sessions, the cache is required to be secured enough against the possible alteration by software bugs or virus.

No new security implications are introduced in data transport or routing because locators provide a subset of the functions of IP addresses in the current NGN architecture.

___***___