**ITU-T Recommendation Y.ipv6split**

# Framework of ID/LOC separation in IPv6-based NGN

***Justification of this Recommendation [Extracted by Y. 2015]:***

- *NGN supports several types of access networks such as fixed wired/optical networks, wireless LANs, and cellular networks. Hence, NGN terminals shall have the ability to use different access technologies and connect to multiple Internet Service Providers (ISPs) with multiple interfaces and addresses.*
- *NGN is required to support mobility and multihoming. To support this, an NGN terminal should have an identifier which is independent of the location of the terminal as well as the network(s) to which it is connected.*

*Through separating the role played by IP addresses into the roles of identifiers and locators, it could be much easier to support seamless communication, especially in mobility and multihoming environments.*

*Editor's Note: we will start the ID/Locator separation (Y.ipv6split) related works at Q7/13 simultaneously with Q5/13. The work of Q7/13 mainly focuses on how to deploy the IPv6 network or to use IPv6 addresses. For example, we will consider using IPv6 addresses as Node ID and also as Locator. The IPv6 addresses as Node ID have not a global routable feature such as IPv6 addresses in RFC4291, which title is IP Version 6 Addressing Architecture. The IPv6 addresses as Locator have a global routable feature. It means that the IPv6 addresses as Locator are normal IPv6 addresses, which are already allocated and used in current Internet. Therefore, we don't have any overlap between Q7/13 and Q5/13's works in viewpoint of the ID/LOC separation related works because the work of the Q7/13 is not making a new architecture or technology.*


## Summary

This Recommendation describes a framework of IPv6 separation into identifier and locator in IPv6-based NGN. This recommendation identifies the architecture, functional procedure and applications of IPv6 separation in IPv6-based NGN (NGNv6).



## Keywords

*[TBD]*

**Table of Contents**

**ITU-T Recommendation Y.ipv6split**

**Framework of ID/LOC Separation in IPv6-based NGN**

## 1 Scope

According to the definition of NGN [ITU-T Y.2001], the Y.2051 is expected to support advanced architectural objectives of NGN using IPv6 protocols and mechanisms. It also defines new term "IPv6-based NGN" to provide packet-based services with the help of underlying transport and access technologies. On the other hand, Y.2015 defines general requirements for ID/LOC separation to efficiently support mobility, multihoming and host renumbering in NGN.

Aligning with Y.2015 and Y.2051, the IPv6-based NGN is required to use Node IDs and locators in order to overcome the limitations of the conventional IP architecture.

The scope of this Recommendation includes:

- IPv6 addressing schemes for ID/LOC separation
- Mapping Functions and Procedures for ID/LOC separation in IPv6-based NGN
- Deployment Scenarios for ID/LOC separation in IPv6-based NGN

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

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

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

[ITU-T Y. 2015] ITU-T Draft Recommendation Y.2015, *Separation of IP into identifier and locator in NGN*

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

[ITU-T Y.2051] ITU-T Recommendation Y.2051 (2008), *General Overview of IPv6-based NGN.*

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

[ITU-T Y.2201] ITU-T Recommendation Y.2201 (2006), *NGN Release 1 Requirements.*

[IETF RFC4193] IETF RFC 4193 (2005), *RFC4193, Unique Local IPv6 Unicast Addresses.*

# 3 Definitions

## 3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

### 3.1.1 Address [ITU-T Y.2091] [ITU-T Y.2015]

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.

### 3.1.2 Identifier [ITU-T Y.2091] [ITU-T Y.2015]

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.

### 3.1.3 Locator (LOC) [ITU-T Y.2015]

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.

### 3.1.4 ID/LOC separation [ITU-T Y.2015]

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.

### 3.1.5 Node [ITU-T Y.2015]

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.

### 3.1.6 Node ID [ITU-T Y.2015]

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.

### 3.1.7 IPv6-based NGN [ITU-T Y.2051]

This refers to NGN that supports addressing, routing protocols, and services associated with IPv6. An IPv6-based NGN shall recognize and process the IPv6 headers and options, operating over various underlying transport technologies in the transport stratum.

Note: In this Recommendation, this term is abbreviated to "NGNv6."

## 3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

*Editor's note: this draft Recommendation is developing some new terms such as node IDv6, node IDv4 and so on. So the joint meeting with idM group is needed to clarify these terms at the next meeting.*

### 3.2.1 ID/locator mapping record

ID/locator mapping record contains the relationship between a node IDv6 and a locator. ID/locator mapping record pertaining to a UE contains the node IDv6 and locator the UE possesses. The UE should possess at least one node IDv6 and one locator at any time. When the UE possesses many locators (e.g., when it is multihomed), its node IDv6 may relate to many locators at the same time.

### 3.2.2 ID/locator Mapping Function – Functional Entity (ILMF-FE)

An ID/locator mapping function – functional entity (ILMF-FE) is the major component of the ID/locator separation architecture in NGNv6. It obtains ID/locator mapping record from an ID/locator mapping storage and uses the node IDv6 and locator in communication protocols. The ILMF-FE uses node IDv6 in the transport and upper layer protocols and locators in the network layer protocol and packet header. Using the node IDv6 as a reference value, the ILMF-FE can dynamically change locators in the network layer protocol and packet header, while continuously using the same node IDv6 in the transport and upper layers. The ILMF-FE thus hides the effect of locator changes from the transport and upper layer services.

Note: This definition is the refined version of the same term defined in ITU-T Y.2015.

### 3.2.3 ID/Locator Mapping Storage – Functional Entity (ILMS-FE)

An ID/locator mapping storage – functional entity (ILMS-FE) stores and updates ID/locator mapping record. It accepts an ID/locator mapping record lookup request from the ILMF-FE, searches the corresponding mapping record in its record, and forwards the mapping record to the ILMF-FE. It also accepts an ID/locator mapping record update request from authorized functional

entities such as ILMF-FE, NACF, UE, and border access gateways, and carries out corresponding updates.

Note: The ILMS-FE is similar to the ID/LOC mapping storage function defined in ITU-T Y.2015.

### 3.2.4 Namespace

A collection of names, identified by an IPv6 address, that allows the Node ID and Locator to use within an IPv6 address space. That is, the node ID and LOCs are selected and used in only IPv6 address space.

### 3.2.5 node IDv6

A node IDv6 is a node ID used in the ID/LOC separation architecture of NGNv6. Similar to an IPv6 address, the node IDv6 is recommended to have a hierarchical representation consisting of prefix, scope, version and other fields.

### 3.2.6 node IDv4

A node IDv4 is a node ID used in the ID/LOC separation architecture of NGNv4. Similar to an IPv4 address, the node IDv4 is allowed to have a hierarchical representation consisting of prefix, scope, version and other fields.

## 4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

| | |
|---|---|
| DHCPv6 | Dynamic Host Configuration Protocol for IPv6 |
| DHT | Distributed Hash Table |
| DNS | Domain Name Service |
| ILMF-FEs | ID/Locator Mapping Function – Functional Entity(ies) |
| ILMS-FEs | ID/Locator Mapping Storage – Functional Entity(ies) |
| NGNv6 | IPv6-based NGN |
| NGNv4 | IPv4-based NGN |
| ORCHID | Overlay Routable Cryptographic Hash Identifiers |
| SIP | Session Initiation Protocol |

**URL Uniform Resource Locator5 Conventions**

*[TBD]*

## 6 IPv6 addressing schemes for ID/LOC separation

*Editor's Note: This clause will suggest the IPv6 addressing architecture to support ID/LOC separation. It means that IPv6 addresses are used as the node ID and LOC in the same time.*

*Editors' note: Since this clause is concerned with developing a framework for ID/LOC separation in IPv6-based NGN, it is better not to talk about IPv4 addressing space. That is, this clause is focused on IPv6 Addresses. The IPv4 to IPv6 migration or coexistence scenarios and applications may be considered in other clauses.*

In the conventional IP based network, an IPv6 address assigned to an end node has two meanings node ID and locator. The node ID uniquely identifies the end node while locator uniquely locates the end node in the network topology. The locator also provides information for determining a path to reach the end node. Thus the separation rules of IPv6 addresses should be required in order to apply the ID/LOC separation.

### 6.1 IPv6 address space

Figure 1 shows the node ID and locator namespaces in the IPv6 address space. The node ID and locator namespace may overlap. Namely, some IPv6 addresses are allowed to be used as node IDs as well as locators. In these cases, ID/LOC separation schemes are required to distinguish the node ID from the Locator.

Editor's Note: to define the ID/LOC separation schemes is out of scope. In clause 6.3 "IPv6 address configuration," we propose the special schemes just as an example.

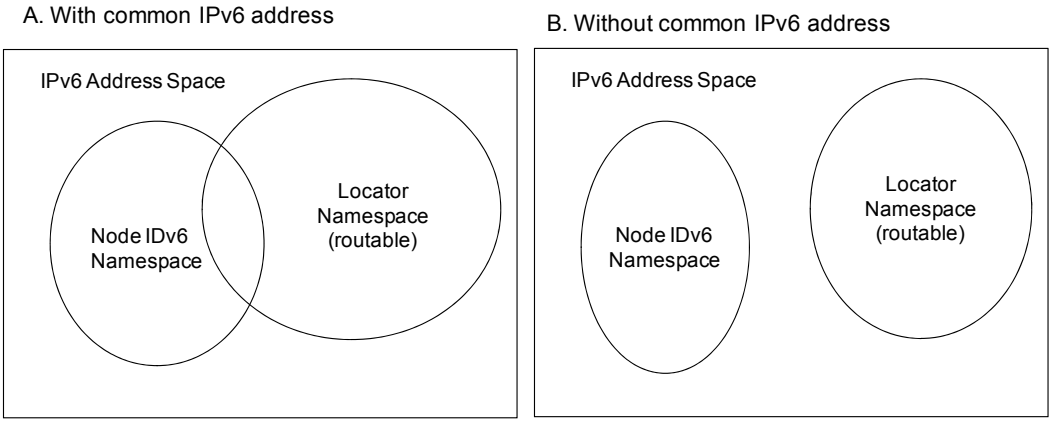


**Figure 1- Node ID and locator namespaces in IPv6 address space**

### 6.2 Separation of IPv6 address space

ID/LOC separation is a mechanism which decouples the transport layer from the network layer so that an end-to-end communication session is not bound to IPv6 addresses. The IPv6 addresses with ID/LOC separation distinguish a node ID, from a LOC through a binding between the ID and LOC as shown in Figure 2.B.

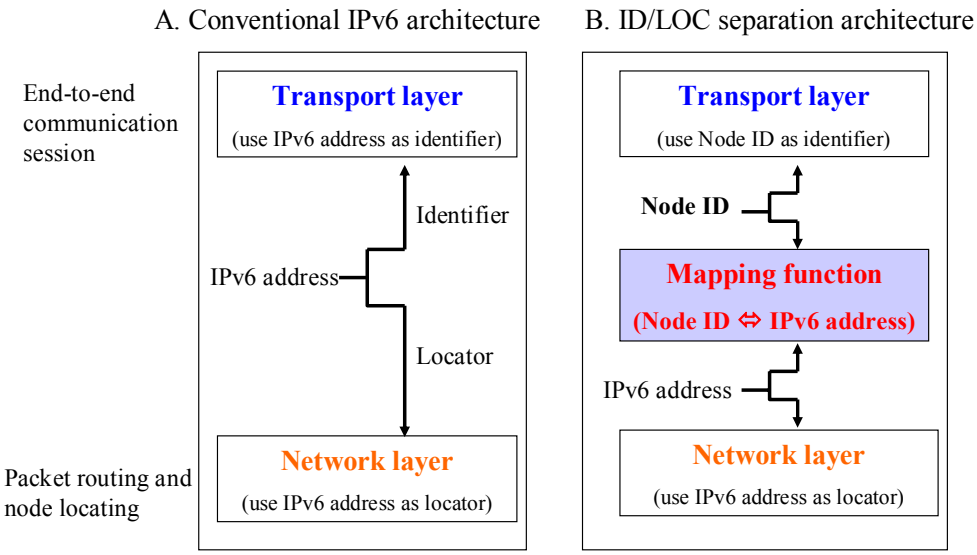


**Figure 2 – Comparison between conventional IPv6 architecture and ID/LOC separation IPv6 architecture [copied from Y.2015 with sight modification]**

In figure 2.B, a node ID is s semantic name to recognize the endpoint of a communication session. A locator is a semantic name of an IPv6 address. By doing so, IPv6 addresses as the locator no longer directly associate with the communication session, but only with the network layer [ITU-T Y.2015]. In here, IPv6 addresses should not be used only as locator. Because IPv6 addresses have addressing hierarchy and scopes, it is required to use IPv6 address space to configure node ID. Therefore, the separation scheme of IPv6 address space is required with the support of mapping functions.

### 6.2.1 Host based IPv6 address separation

The separation schemes of IPv6 address space should be supported with the help of mapping function in host as shown in Figure 3.

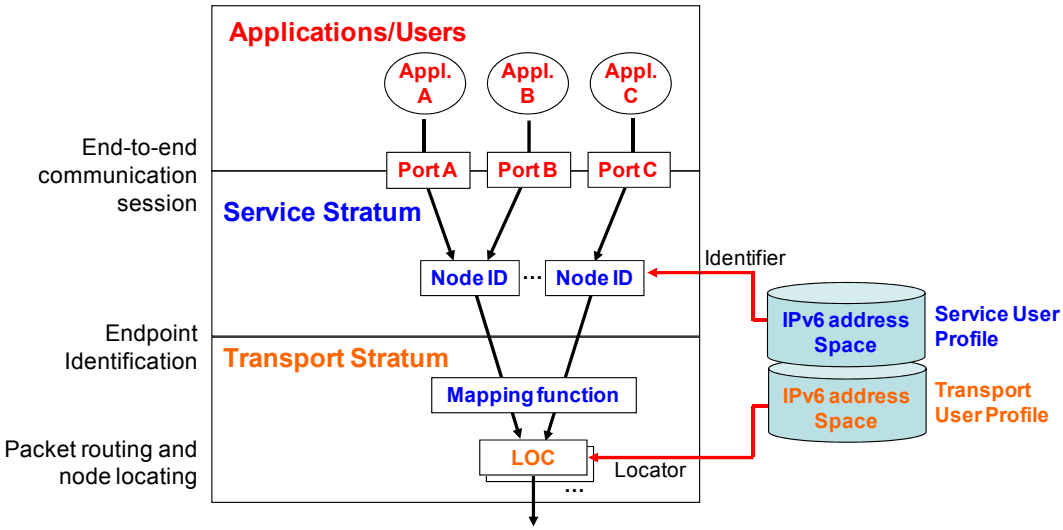


**Figure 3 – Host based IPv6 address separation**

### 6.2.2 Network based IPv6 address separation

The separation schemes of IPv6 address space should be supported with the help of mapping function over NGNv6 network as shown in Figure 4.

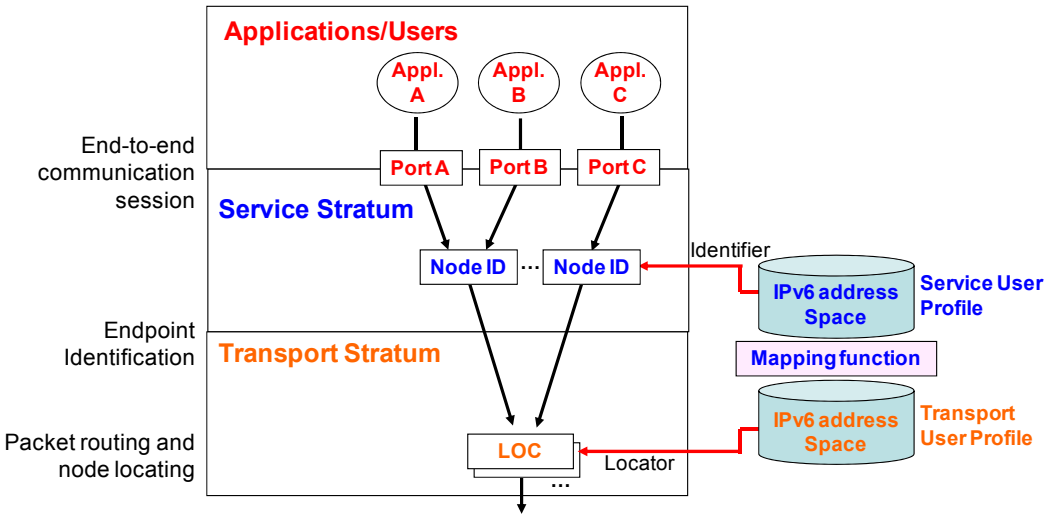


**Figure 4 – Network based IPv6 address separation**

## 6.3 IPv6 address configuration

### 6.3.1 Node ID configuration

Node IDs can be configured from the IPv6 address space using one of the following methods.

- Persistent IPv6 address as node ID: A persistent IPv6 address can be used as a node ID in separate namespace from locator. That is, there are the reserved blocks of global IPv6 address spaces as node ID. This is the role of authority of IPv6 address allocation. The persistent IP address can continuously be used by the transport and upper layers protocols as a node ID even when the network layer protocols configure a new IPv6 address when the node moves to a new network. The persistent IPv6 address is routable and can be used as both node ID and locator. The persistent IPv6 address is routable. The mobile node can use the persistent IPv6 address as its locator if the node is located in the home network. Otherwise, the mobile node will use the persistent IPv6 address only as the node ID and use another temporary address as the locator.
- IPv6 address with specific prefix as node ID: To distinctly separate node ID and locator namespaces from each other, specific prefixes are used for configuring node IDs. One example of such prefix is Overlay Routable Cryptographic Hash Identifiers (ORCHID) [b-IETF RFC 4843]. Such node IDs are not routable in the IPv6 address space. Other example is "unique local IPv6 unicast addresses" [b-IETF RFC 4193].
- IPv6 address with specific values in type and scope fields as node ID

### 6.3.2 Locator configuration

Locators are configured from IPv6 address space according to any address configuration method available in the access network. Such methods may be DHCPv6 [b-IETF RFC 3315] [b-IETF RFC 3646] [b-IETF RFC 3736], auto configuration [b-IETF RFC 2462] any other methods specific to NGN.

# 7 Mapping Procedures for ID/LOC separation in NGNv6

## 7.1 Mapping Functions for ID/LOC separation in NGNv6

An NGN identifier such as an URL or a SIP identifier is translated into a Node ID or an IP address when starting an application service. The Node ID is then used as an identifier in the transport and higher layers to identify the endpoint of the communication session. The IP address is used 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, Node IDs and IP addresses [ITU-T Y.2015]. This Recommendation follows these functionalities of Figure 5 in the viewpoint of NGNv6.

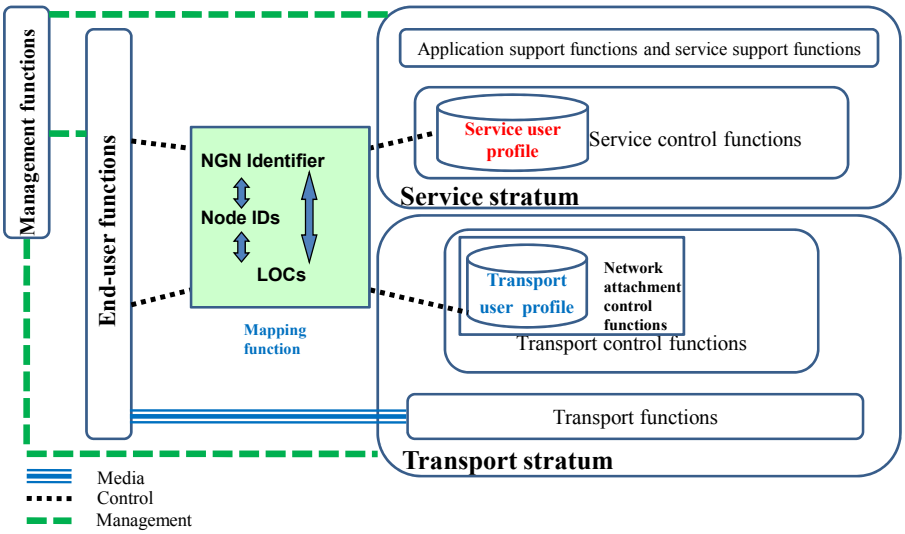


**Figure 5 – Overview of functionalities for ID/LOC separation in NGN [ITU-T Y.2015]**

NGNv6 is defined as a NGN which supports addressing, routing, protocols and services associated with IPv6. This applies not only to transport function in access and core networks but also to other functions such as end user, transport control and application/service support functions in ITU-T Recommendation Y.2011 and Y.2012 [ITU-T Y.2501]. As shown in Figure 6, there are three relationships among the NGN functions and FEs in order to describe the ID/LOC separation rules in NGNv6.

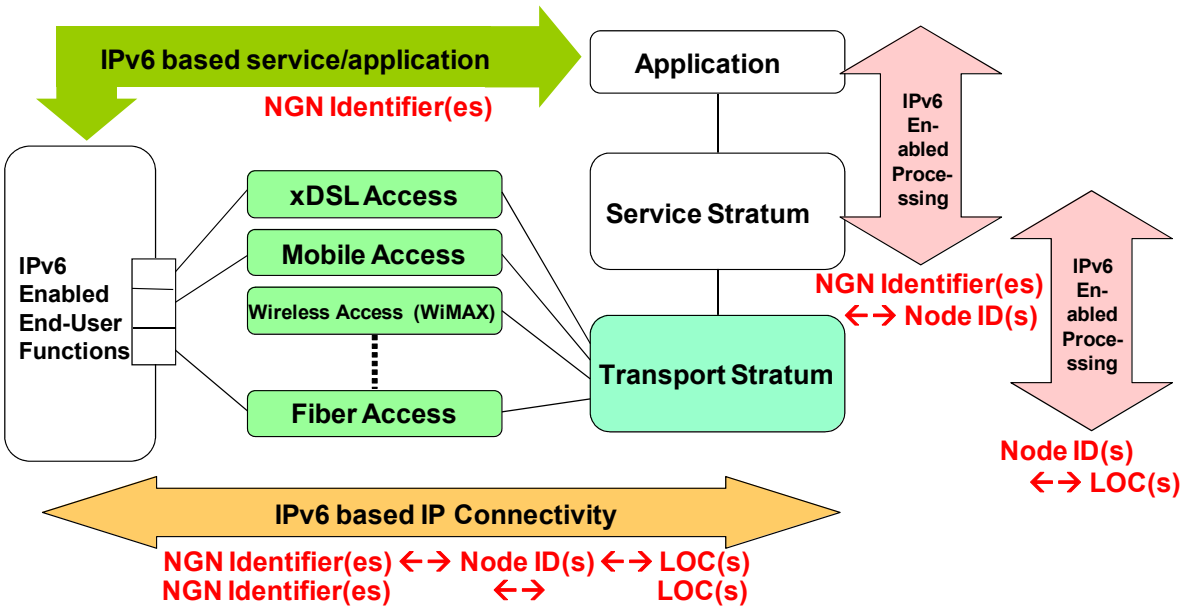


**Figure 6 – Extension of IPv6-based NGN to support ID/LOC separation**

## 7.2 Mapping Procedures for ID/LOC separation in NGNv6

*Editor's Note: we will develop the following items: How to maintain ID/LOC mapping, How to organize mapping database and mapping services, How to perform mapping and How to detect and recover from mapping changes.*

The mapping procedure for ID/LOC separation involves two major components: ID/LOC mapping function and ID/LOC mapping storage function [ITU-T Y.2015]. These components are shown in Figure 6. Note that although the ID/LOC mapping storage and ID/LOC mapping functions are shown separately in the figure 7, they can physically be collocated in a UE or end node, or border access gateway.

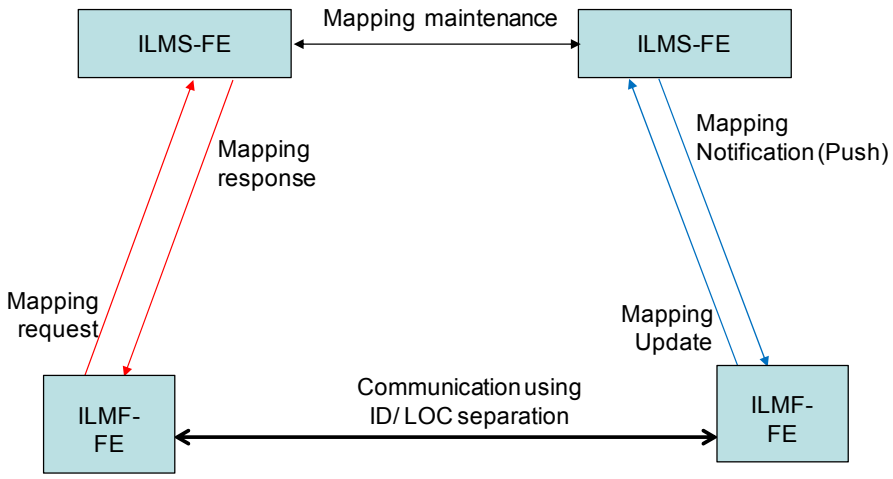


**Figure 7 – ID/ LOC separation architectural components in NGN**

### 7.2.1 Maintaining the Mapping Records among ILMS-FE

The ID/LOC mapping storage – functional entities (ILMS-FEs) maintain ID/LOC mapping record. That is, the ILMS-FE collects ID/LOC mapping record either from UEs or from border access

gateways, distributes the mapping record among the storages, and provides the mapping record to UEs and border access gateways when requested. The ILMS-FEs can be connected to each other in different configurations so that they can efficiently collect, store and distribute up-to-date ID/LOC mapping record. The ILMS-FEs can be connected in a hierarchical structure, or in a flat structure, or in a hybrid structure.

A hierarchical structure like the DNS [b-IETF RFC 1035] may work well for the ILMS-FE because the node IDv6 also has hierarchical representation as domain names [b-IETF RFC 1034]. The DNS like hierarchical ILMS-FE system that maintains multiple cached copies of mapping record in different locations of the system is scalable for faster lookup of ID/LOC mapping record by end nodes. However, such system is suitable only for maintaining static mapping record (i.e., that do not change frequently) because the existence of multiple cached copies makes it difficult to globally update the mapping record in a short time. Avoiding caching the mapping data in distributed manner or storing mapping record for a particular node IDv6 prefix only in an authoritative storage [b-IETF RFC 1035] will help in correctly updating the mapping record when changes occur. However, this will increase the mapping record lookup time for UEs as well as the communication load at the authoritative storage.

A flat structure of ILMS-FE can be suitable for updating mapping record frequently. In a mobile environment where the access network topology changes frequently, ID/LOC mapping record associated to an end node also change frequently. To maintain such dynamic mapping record, the flat structure of ILMS-FEs can be organized into a DHT-based P2P network. The DHT-based ILMS-FE system will facilitate faster updates and lookups.

To utilize the benefits of both the hierarchical and flat structures, ILMS-FEs may be organized in a hybrid structure, where the leaf nodes (i.e., authoritative registries) of the hierarchical structure have additional P2P connections. The hierarchical structure will be used for finding ID/LOC mapping record by utilizing the hierarchical notation of node IDv6, whereas the flat structure of authoritative storages are recommended to be used for faster updating ID/LOC mapping record.

The ILMS-FE gets ID/locator mapping record of a UE either from the NACF, UE, or border gateways when the UE is attached to the network. That is, when the NACF accepts a connection request of the UE, it assigns an IPv6 address as the locator to the UE. NACF then informs the ILMS-FE about the ID/locator mapping record of the UE. Alternatively, when the UE gets its new locator (either by configuring the locator by itself using the advertized network parameters or by obtaining the locator by some other means like DHCP), it may send an update request to the ILMS-FE. Or, in case a border access gateway assigns a new locator to the UE or detects the locator change by some other means (e.g., intercepting DHCP signaling), it may send the update request to the ILMS-FE system. Thus, different ways are possible to register or update ID/locator mapping record stored in the ILMS-FE.

### 7.2.2 Requesting and Responsing the Mapping Records between ILMF-FE and ILMS-FE

The ILMF-FE performs ID to locator mapping for data communication. The ILMF-FE sends a lookup query to the ILMS-FE to obtain the ID/locator mapping record of a peer UE. The ILMF-FE provides the node IDv6 to the transport and upper layer protocols and corresponding locators to the network layer protocol. The ILMF-FE can dynamically change locators in the network layer protocol, while using the same node IDv6 in the transport and upper layer protocols for a communication session. Thus, the ILMF-FE hides the locator changes due to the network layer mobility or multihoming from the transport and upper layer protocols.

The ILMF-FE resides either in a UE or in a border access gateway, or in both. The ILMF-FE residing in the UE can perform host-based mobility and multihoming management. In case of mobility, when the UE moves from one network to another, it obtains a new locator. The ILMF-FE stops using the old locator and starts using the new locator in the network layer protocols, while hiding the impact of locator change from the transport and application layer protocols. Similarly, in case of multihoming, the ILMF-FE will switch locators in the network layer protocols based on the dynamically changing characteristics of the available networks.

The ILMF-FE residing in the border gateway can provide network-based mobility and multihoming management. In case of network-based mobility, the UE is not required to possess the capability to execute mobility management functions. Instead, the ILMF-FE of the border access gateway traces the mobile UE and manages its mobility by changing locators in the outgoing and incoming data packets. To change locators in the packet headers, the border access gateway uses node IDs as the reference value. Similarly, the ILMF-FE of a multihomed border gateway can change the destination locator of outgoing packets to route them through a preferred path. It can also change the source locator of outgoing data packets in order to receive incoming acknowledgement or response packets through a preferred path. Thus, the ILMF-FE in the border access gateway may support traffic engineering by forwarding and receiving packets through preferred paths.

In addition to supporting mobility, multihoming and traffic engineering, the ILMF-FE changes locators in the border gateway for enabling the use of different locator spaces in the access and core networks and making the routing functions scale in the core network [b-IETF LISP]. To change the routing locators present in the network layer header of packets, the border access gateway may employ one of the following mechanisms: translation and tunneling. In case of the translation, the border gateway replaces the locators used in the access network with another set of locators that are used in the core network. On the other hand, in the case of tunneling, the border gateway encapsulates the packet with an additional network layer header containing the new set of locators. The locators included in the outer header will be used to route the packets in the core network. In the border gateway located in the access network of the peer UE, the translation and tunneling processes are reversed. That is, in the case of translation, the border gateway replaces the locators used in the core network with the locators of the access networks, and in the case of tunneling, the outer network layer header is simply removed from the packets.

#### 7.2.3. Detecting Mapping Record Changes and Recovery from Failure

Since a node IDv6 persists for a longer time, the ID/locator mapping record changes only when the UE changes its locator. The UE changes its locator when it physically moves from one network to another or simply activates a new interface. One of challenges of ID/locator separation based NGNv6 is to timely detect the mapping record change by the concerned functional entities. For example, when a mobile UE changes its locator while having communication sessions with a peer UE, the peer UE should be able to detect the locator change of the mobile UE in a short time. The peer UE can detect the mapping record change in several ways. It may get a mapping record change notification either from the mobile UE or from the border gateway located closer to the mobile UE. The ILMS-FE can also push the mapping record change notification to the peer UE.

The UEs or border gateways can recover from the failure caused by mapping changes. As soon as a mapping change is detected, the ILMF-FE of the UE or border gateway may cache and retransmit data packets or may employ other techniques to avoid an adverse impact on the transport and application layer sessions. Moreover, the NACF and RACF may be used for mapping change detection and failure recovery.

## 8 Deployment Scenarios for ID/LOC separation in NGNv6

*Editors' note: Main purpose of this clause is giving IPv6 only deployment scenarios through ID/LOC separation in NGNv6. Therefore, using IPv4 addresses is excluded. That is, the IPv4 to IPv6 migration or coexistence scenarios may be not considered in this clause.*

This clause provides the scenarios to deploy IPv6 through ID/LOC separation in NGNv6. In these scenarios, the node ID and LOCs are used in only IPv6 address space. The scenario assumes under the growth of IPv6 deploying network conditions where most of access networks are IPv6 capable and also core network is recommended to be transported through IPv6 Protocol.

**Case 1: Node ID namespace is not overlapped with locator namespace**

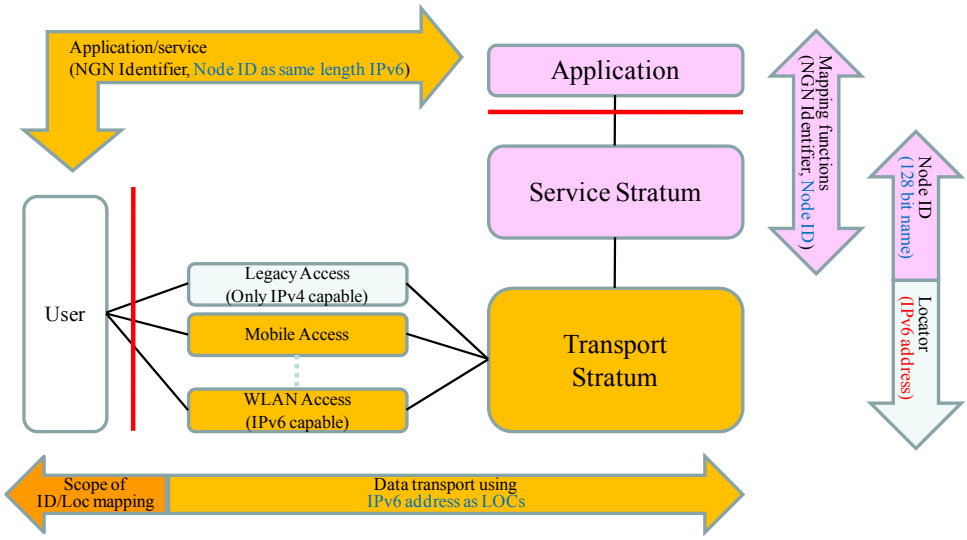


**Figure 8 – General ID/LOC separation architecture – node ID as same length of IPv6 and LOC as IPv6 address**

Node ID namespace is defined in IPv6 address space as shown in Figure 1. But the common part of namespaces in Figure 1.A is not existed in this case. In this scenario, only mapping function is required, because non-routable IPv6 address as node ID is required to be mapped to routable IPv6 address as locator.

The node ID just have a same form of IPv6 address, it is recommended to be allocated to the user equipments by authority organization or domain provider. As a result the node ID cannot be used for routing any more. In this case, the node ID and Locator will be completely separated, so that the ID/LOC mapping function will be covered between an end user and access network and core network to bind node ID to LOCs as shown in Figure 8.

In this case, regarding IPv6 deployment and the node ID and locator separation architecture, it is possible to make scenario as a long-term approach. First of all, the node ID is recommended to be newly defined by representing new concept, which means that new node ID can appeared like as contents ID, public key, or virtual ID. But regarding deployment issue, it is feasible to have same ID length as IPv6 128bit. For example, the node ID can be assigned to 128bits hash value to enhance security.

Regarding the ID/LOC mapping function, all of node IDs are required to be mapped to LOCs and the function is recommended to support dynamic update relationship between IDs and LOCs. Therefore the mapping function has more important functionalities to support communication

network in NGN, so that many concerning issues will be raised and should be release that, such as security, privacy, manageability, and etc. These are out of scope.

**Case 2: Node ID namespace is overlapped with locator namespace**

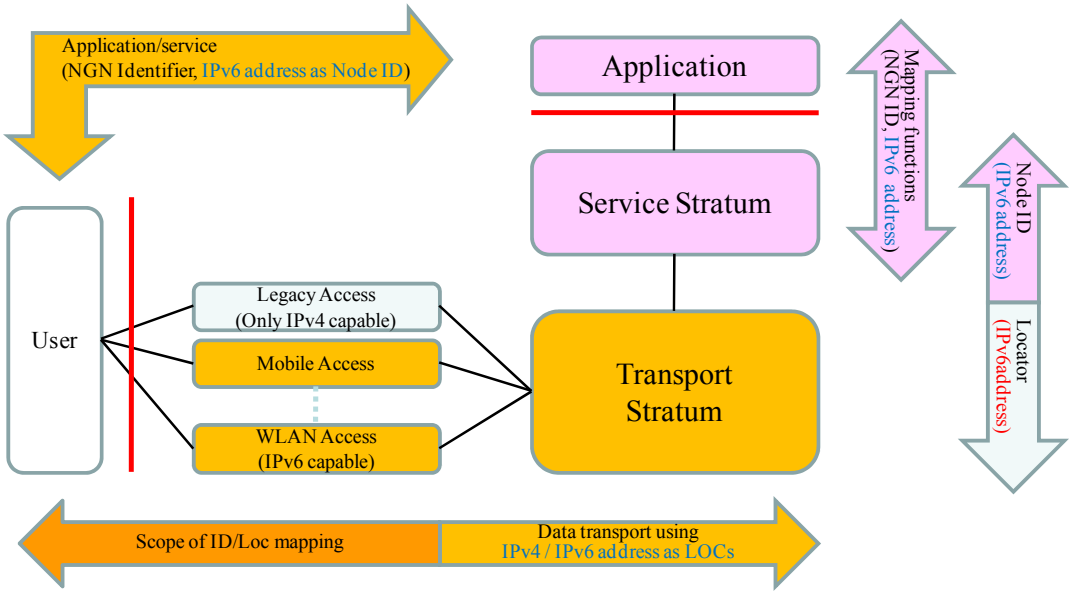


**Figure 9 – General ID/LOC separation architecture – node ID as IPv6 address and LOC as IPv6 address**

Node ID namespace is defined in IPv6 address space as shown in Figure 1. In this scenario, the routable IPv6 address is recommended to be used as node ID and locator at the same time. Therefore, the rule of overlapping exclusion is required in align with the ID/LOC mapping function as shown in Figure 9.

The node ID as IPv6 address may be used for routing and may not be used for routing. The former case can pass over the ID/LOC mapping function. On the other hand, the latter case should be needed to ID/LOC mapping procedure. As a result routable IPv6 address should be allocated to the UE in order to communicate with IPv6 access network and IPv6 core network.

In this case, regarding IPv6 deployment and the node ID and locator separation architecture, it is possible to make scenario as a short-term approach, so that the ID/LOC separation architecture can be incrementally adopted. The node ID and Locator may be separated logically. For example, all of IPv6 capable end user can be communicated with NGN core by using assigned routable IPv6 address as node ID.

Regarding the ID/LOC mapping function, it may not be needed as long as supporting DNS like resolution system. However the ID/LOC mapping function is recommended to be incrementally deployed to achieve completely separation architecture like as case 1.

## 9 Security considerations

*[TBD]*

# Appendix I

## Two-tier ID/LOC mapping

(This appendix does not form an integral part of this Recommendation)

Regarding the IPv6 based ID/LOC separation in NGNv6, there are couple of positions of the ID/LOC mapping components to support IPv6 node ID under the current IPv4 network as shown in Figure I.1.

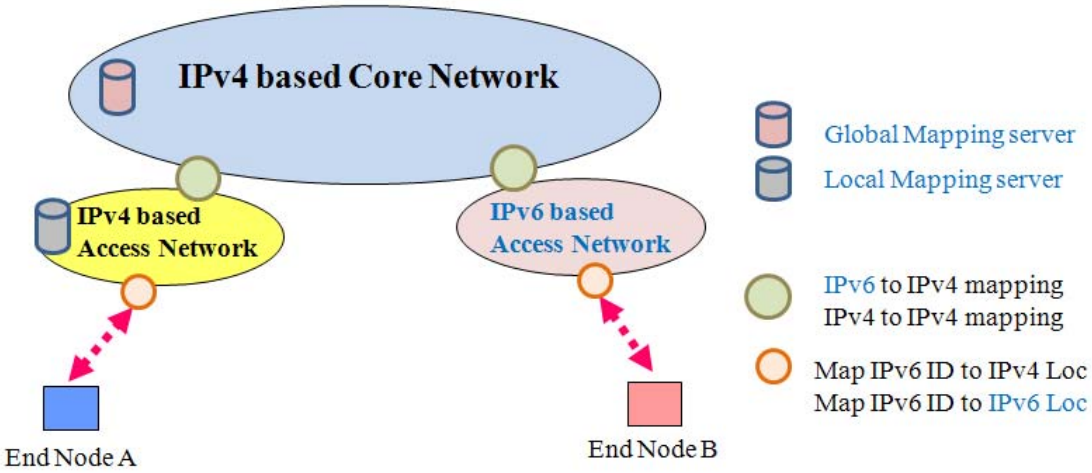


**Figure I.1 – ID/LOC mapping server position and architecture**

The first position exists between end node and access network. In this Recommendation node ID could be an IPv6 address so that we encourage usage of IPv6 application and service to achieve IPv6 deployment. But most of access networks are IPv4 based network as well as IPv4 core network. Therefore an IPv6 node ID shall be resolved to IPv4 Locator to transport data packet through the IPv4 access network. On the other hand, there are few IPv6 based access network in NGN, so that an IPv6 node ID could be resolved to IPv6 Locator. So an ID/LOC mapper located in the first position request IPv4 Locator or IPv6 Locator to a local Mapping server. The Local Mapping server could store ID/LOC mapping information. If a local mapper does not obtained a Locator mapped to Node ID, the mapper should request resolution to global ID/LOC mapping server.

The second position exists between access network and core network. A mapper located in the second position request IPv4 or IPv6 locator to a global Mapping server. The two-tier Mapping architecture could have benefits for mobility support. One of major objective of the ID/LOC separation architecture is to support efficient mobility management. Regarding the mobility support, LOCs aligned with a node ID could be changed frequently according to the end host movement. So the ID/LOC mapping information should be prohibited to reflect frequent changing of Locator information to the global scale mapping server in core network.

In addition, the volume of mapping information that mapping databases contain is huge. The robustness of the database and efficiency in the mapping resolution process are highly required for the scalable architecture of NGN. So the two-tier ID/LOC Mapping server could also achieve scalable and robust mapping service as shown in Figure 2.

If an end node A wants to communicate with end node B, firstly an ID/LOC mapper performs transition from node ID to LOC. In this procedure, the mapper requirs to get the ID/LOC mapping record from a local ID/LOC mapping server within access network. And also a border gateway shall perform the same procedure to get a mapping data from a global mapping server within core network.

## Appendix II

# Scenarios in IPv6 and IPv4 address space coexistence

(This appendix does not form an integral part of this Recommendation)

This appendix provides the scenarios to deploy IPv6 through ID/LOC separation in NGNv6 and NGNv4. In these scenarios, a Node IDs and LOCs are IPv6 and/or IPv4 address. The Figure II.1 shows just one case of them.

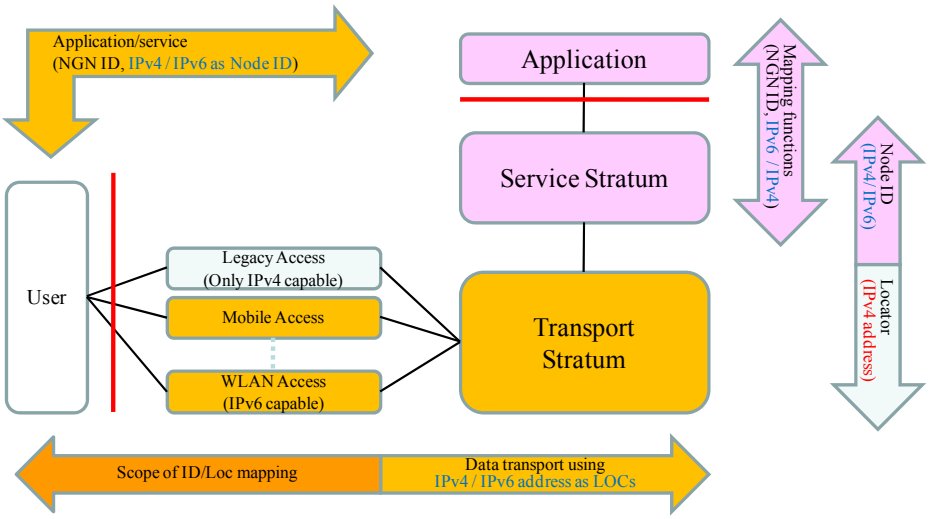


**Figure II.1 – General ID/LOC separation architecture – IPv6 node ID and IPv4 LOC**

### II.1 Communication scenarios between hosts in the same node ID namespaces

**Case 1: Node ID namespace exists in IPv6 address space and Locator namespace exists in IPv4 address space**

The scenario assumes under the current IP network conditions where the most part of access networks are only IPv4 capable networks and core network can be transporting by only IPv4 data. Therefore the node ID is IPv6 address, and the locator is IPv4 address.

In this scenario, an IPv6 capable access network should have connectivity with IPv4 core network, in addition to start with application and service using IPv6 address as node ID under the only IPv4 access network shown in Figure II.1.

If a Node ID can be used in IPv6 address, all of user equipments would have capable to start with service and application using IPv6 address as node ID. For instance, current applications and services established communication sessions by using 32 bit IPv4 addresses, but on the other hand, the most of applications and services will be able to establish by using 128 bit IPv6 addresses. As a result, IPv6 capable applications and services will be developed plentifully.

In order to transport IPv6 data packets to IPv4 network, a transition mechanism should be needed. But the ID/LOC separation can be translated from IPv6 address as node ID to IPv4 address, which can be used in real locator using the ID/LOC mapping function without considering transition mechanism. Therefore the transition from IPv6 to IPv4 will be achieved naturally, so that data packets should be transported to core network using IPv4 address.

Regarding the IPv6 capable access network's interoperability, the ID/LOC mapping function can be located and activated between access network and core network, so that the translation from IPv6 address to IPv4 address should be accomplished.

**Case 2: Node ID namespace exists in IPv4 address space and Locator namespace exists in IPv6 address space**

IPv6 deployment was already achieved up to a certain point, where the core network is IPv6 capable network. Therefore, we only should consider legacy IPv4 access network to support connectivity to IPv6 core network.

Regarding interoperability with IPv4 legacy access network and IPv6 core network, the ID/LOC mapping function can be performed in twice; one is for the translation from IPv6 address as node ID to IPv4 address as locator within legacy access network, the other is for the translation from IPv4 address to IPv6 address as locator in core network. For instance, in the mapping between user equipments and access network, binding from IPv6 address as node ID to IPv4 address as locator can be accomplished firstly. And then also transition from IPv4 address to IPv6 address should be achieved to transport data packet.

## II.2 Interworking scenarios between hosts in different node ID namespaces

According to Y.2015 [ITU-T Y.2015], a node ID should be used at the transport and higher layers for replacing the conventional use of IP addresses at these layers to prevent direct binding between NGN identifier and LOCs. So we can think about that IPv4 address could be used as the node ID. The scenario that IPv4 address could be node ID comes under the adoption of ID/Loc separation in NGNv4. To encourage IPv6 deployment, the Recommendation shall use IPv6 address as Node ID, so that we do not concern the case of node IDv4. However there are some capabilities of coexisting node IDv4 and node IDv6, a interworking scenario shall be considered for interoperability between end nodes.

Regarding the IPv6 deployment, the scenarios do not assume the only NGNv6. That is, both of the NGNv4 and NGNv6 should be coexisted for a long time. Therefore end nodes using node IDv4 shall have capability to interwork with an end node using node IDv6.

In this interworking scenario, Locator used in the core network does not care about that IPv4 addresses are used as LOCs or IPv6 addresses are used as LOCs, because ID/LOC separation can take account of transition from IPv6 to IPv4 and vice versa to transport data packet through core network.

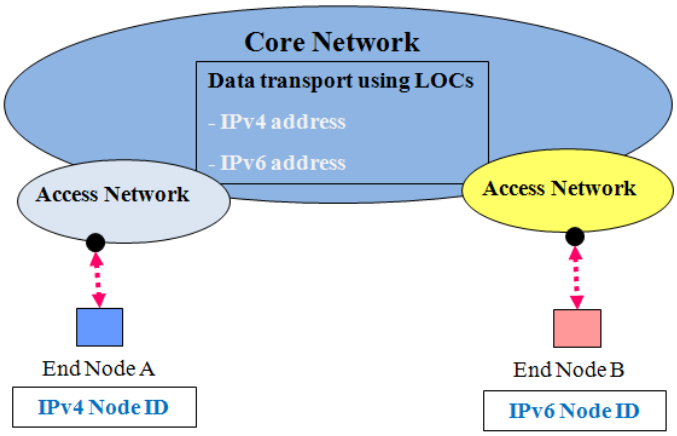


**Figure II.2 – IPv4 Node ID and IPv6 Node ID**

The figure II.2 depicts a end node A as used in node IDv4 attach the access network in NGNv6, on the other side an end node B as used in node IDv6 also attach the access network. The black circle shows a point of ID/LOC mapping occurrence. The figure also shows that the core network could be an IPv4 based network or IPv6 based network.

If a node ID can be used in IPv6 address, all of user equipments would have capable to start with service and application using IPv6 address by 128 bits form. So application developers shall choose IPv6 capable APIs to make IPv6 based service or application. But a correspondent end host B use node IDv6, so that the ID/LOC mapping architecture takes account of mapping IPv4 node ID to locator as well as mapping node IDv6 to locator. To achieve interworking between IPv4 and node IDv6 mapping under the coexisted scenario, IPv6 to IPv4 transition mechanisms could be adopted to ID/LOC separation architecture in NGNv6. Especially address translator from IPv6 to IPv4 and vice versa could be adopt to the architecture between end node and access network.

If a end node A as used in node IDv4 want to communicate with a end node B as used in IPv6 node ID, address translator such as NAT-PT takes a node ID and change a node IDv4 to IPv6 address form and vice versa. This translator process has not related with ID/LOC mapping procedure, so that translated IPv4 or IPv6 form also required to map locator.

**Case 3: Node ID namespace exists in IPv4/IPv6 address space and Locator namespace exists in IPv4 address space**

The scenario assumes under the IP network where the most part of access networks are only IPv4 capable networks and core network can be transporting by only IPv4 data. Therefore the node ID is IPv4 address or IPv6 address. The locator is IPv4 address. In case of communication peer with different type of node ID, interworking schemes using different node IDs should be required.

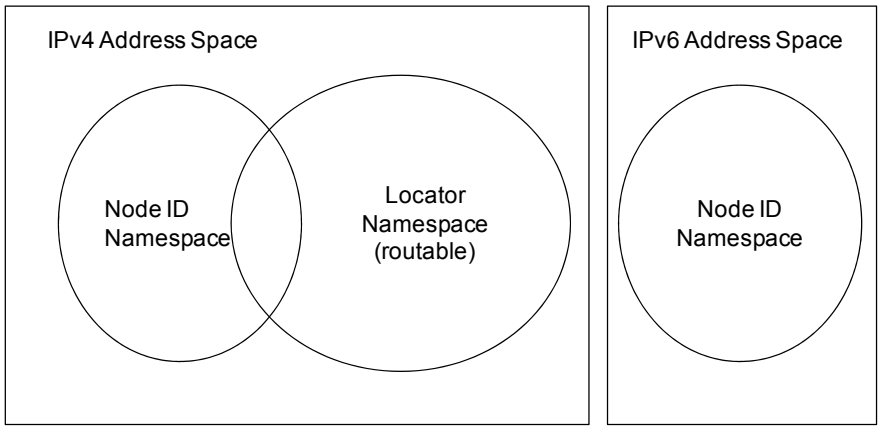


**Figure II.3 – Node ID namespaces in IPv6/IPv4 address space and locator namespace in IPv4 address space**

**Case 4: Node ID namespace exists in IPv4/IPv6 address space and Locator namespace exists in IPv6 address space**

The scenario assumes under the future IP network conditions where the most part of access networks are only IPv6 capable networks and core network can be transporting by only IPv6 data. The majority of the node ID is IPv6 address, but IPv4 address is still used as node ID. In here, the locator is IPv6 address. In case, interworking schemes using different node IDs should be considered.

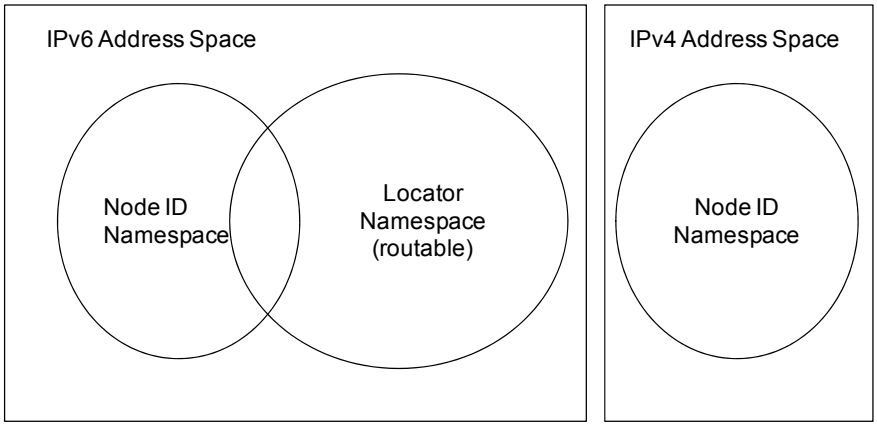


**Figure II.4 – Node ID namespaces in IPv6/IPv4 address space and locator namespace in IPv4 address space**

## Bibliography

[b-IETF RFC 1034] IETF RFC 1034 (1987), *Domain names - concepts and facilities*.

[b-IETF RFC 1035] IETF RFC 1035 (1987), *Domain names - implementation and specification*.

[b-IETF RFC 2260] IETF RFC 2260 (1998), *Scalable Support for Multi-homed Multi-provider Connectivity.*

[b-IETF RFC 2462] IETF RFC 2462(1998), *IPv6 Stateless Address Autoconfiguration*.

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

[b-IETF RFC 3315] IETF RFC 3315(2003), *Dynamic Host Configuration Protocol for IPv6 (DHCPv6).*

[b-IETF RFC 3582] IETF RFC 3582 (2003), *Goals for IPv6 Site-Multihoming Architectures.*

[b-IETF RFC 3646] IETF RFC 3646(2003), *DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6).*

[b-IETF RFC 3736] IETF RFC 3736(2004), *Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6.*

[b-IETF RFC 4177] IETF RFC 4177(2005), *Architectural Approaches to Multi-Homing for IPv6.*

[b-IETF RFC 4193] IETF RFC 4193(2005), *Unique Local IPv6 Unicast Addresses*.

[b-IETF RFC 4423] IETF RFC 4423, *Host Identify protocol (HIP) Architecture*

[b-IETF RFC 4843] IETF RFC 4843(2007), *An IPv6 Prefix for Overlay Routable Cryptographic Hash Identifiers (ORCHID)*.

[b-IETF draft L3shim] IETF Internet Draft, *Level 3 Multihoming shim protocol*

[b-IETF draft GSE] IETF Internet Draft, *GSE - An Alternate Addressing Architecture for IPv6*

[b-IETF LISP] *Locator ID separation protocol (LISP)*, draft-ietf-lisp-03.txt, July 2009.

_____