International Telecommunication Union

ITU-T Y.2057

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(11/2011)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

Next Generation Networks – Frameworks and functional architecture models

Framework of node identifier and locator separation in IPv6-based next generation networks

Recommendation ITU-T Y.2057

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	**Y.2000–Y.2099**
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Numbering, naming and addressing	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Smart ubiquitous networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
Future networks	Y.3000–Y.3099

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Y.2057

Framework of node identifier and routing locator separation in IPv6-based next generation networks

Summary

Recommendation ITU-T Y.2057 describes a framework of node identifier and routing locator separation (also known as ID/LOC separation) in IPv6-based next generation networks (NGNs). It describes IPv6 address separation, mapping functions and procedures, and considerations for the deployment of identifier and locator separation in IPv6-based NGNs.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T Y.2057	2011-11-29	13

Keywords

ID/LOC separation, IPv6 address.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Y.2057

Framework of node identifier and routing locator separation in IPv6-based next generation networks

1 Scope

Recommendation ITU-T Y.2051 defines a new term, "IPv6-based NGN", to support advanced architectural objectives of the next generation network (NGN) by using IPv6 protocols and mechanisms. Recommendation ITU-T Y.2015 describes general requirements for identifier and locator separation (also known as ID/LOC separation) to efficiently support mobility, multihoming and host renumbering in the NGN.

In order to enrich the IPv6-based NGN with the benefits of ID/locator separation, this Recommendation describes a framework of ID/LOC separation in the IPv6-based NGN.

The scope of this Recommendation includes:

– IPv6 addressing schemes for ID/LOC separation

– mapping functions and procedures for ID/LOC separation in IPv6-based NGNs

– considerations of deployment for ID/LOC separation in IPv6-based NGNs.

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

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

[ITU-T Y.2022] Recommendation ITU-T Y.2022 (2011), *Functional architecture for the support of host-based separation of node identifiers and routing locators in next generation networks.*

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

[ITU-T Y.2701] Recommendation ITU-T Y.2701 (2006), *Security requirements for NGN release 1.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 address [b-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.

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

3.1.3 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 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 with no implications on end-host mobility or end-host multihoming.

3.1.4 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 as "NGNv6."

3.1.5 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 – In this Recommendation, there are two types of locator: local-scoped locator and global-scoped locator. Generally, a locator means the global IPv6 address.

3.1.6 multihoming [b-ITU-T G.8081]: Multiple links between an end-point and one or more transport networks. Multihoming may be used, for example, for load balancing or protection via diverse routes.

3.1.7 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.

3.1.8 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.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 ID/locator mapping record: An ID/locator mapping record contains the relationship between a node IDv6 and a locator. An ID/locator mapping record pertaining to an end-user function contains the node IDv6 and locator that the end-user function possesses.

NOTE – The end-user function should possess at least one node IDv6 and one locator at any time. When the end-user function possesses many locators (e.g., when it is multihomed), its node IDv6 may relate to many locators at the same time.

3.2.2 IPv6 address separation: IPv6 address separation is the approach of using the IPv6 address space for deriving both node IDs and locators to be used in the NGNv6.

NOTE – The node ID and locator namespaces may overlap or be isolated. If the node ID and locator namespaces are overlapped, an IPv6 address derived from the overlapped space can be a node ID, a locator, or both, depending on approaches of implementing ID/locator separation.

3.2.3 namespace: A collection of IPv6 addresses from which the node IDs and locators can be derived in the IPv6-based NGN.

3.2.4 node IDv4: A node ID used in the ID/LOC separation architecture of IPv4-based NGNs.

NOTE – Similar to an IPv4 address, the node IDv4 is allowed to have a hierarchical representation consisting of prefix, scope, version and other fields.

3.2.5 node IDv6: A node ID used in the ID/LOC separation architecture of IPv6-based NGN.

NOTE – Similar to an IPv6 address, the node IDv6 is recommended 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
DNS	Domain Name System
EUF	End-User Function
FE	Functional Entity
ILCF	ID/LOC mapping Control Functions
ILM-FE	ID/Locator Mapping – Functional Entity
ILMF	ID/LOC Mapping Functions
ILMS-FE	ID/Locator Mapping Storage – Functional Entity
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
NACF	Network Attachment Control Functions
NGN	Next Generation Network
NGNv4	IPv4-based NGN
NGNv6	IPv6-based NGN
ORCHID	Overlay Routable Cryptographic Hash Identifiers
SCF	Service Control Functions
SUP-FE	Service User Profile Functional Entity
TCF	Transport Control Function
TLM-FE	Transport Location Management Functional Entity
TUP-FE	Transport User Profile Functional Entity

5 Conventions

None.

6 IPv6 addressing schemes for ID/LOC separation in NGNv6

In the conventional Internet protocol (IP)-based network, an Internet protocol version six (IPv6) address assigned to an end node has two meanings, node ID and locator, as shown in Figure 1. The node ID uniquely identifies the end node while the locator uniquely indicates the position of the end node in the network topology. The locator also provides information to the routing system for determining a path to reach the end node. Thus, the separation of IPv6 address space is required in order to apply the ID/LOC separation in NGNv6.

ID/LOC separation is a mechanism that decouples the transport layer from the network layer so that an end-to-end communication session is not bound to IPv6 addresses that are used in the IP layer for forwarding packets by the routing system. As shown in Figure 1, the transport and upper layer protocols use node IDs to identify the communication endpoints while the network layer uses locators to locate the endpoints and forward packets towards them. To apply ID/locator separation to the IPv6-based NGN, the IPv6 address space is separated into node ID and locator namespaces. The ID/locator mapping storage functions store and provide the node ID to locator mappings.

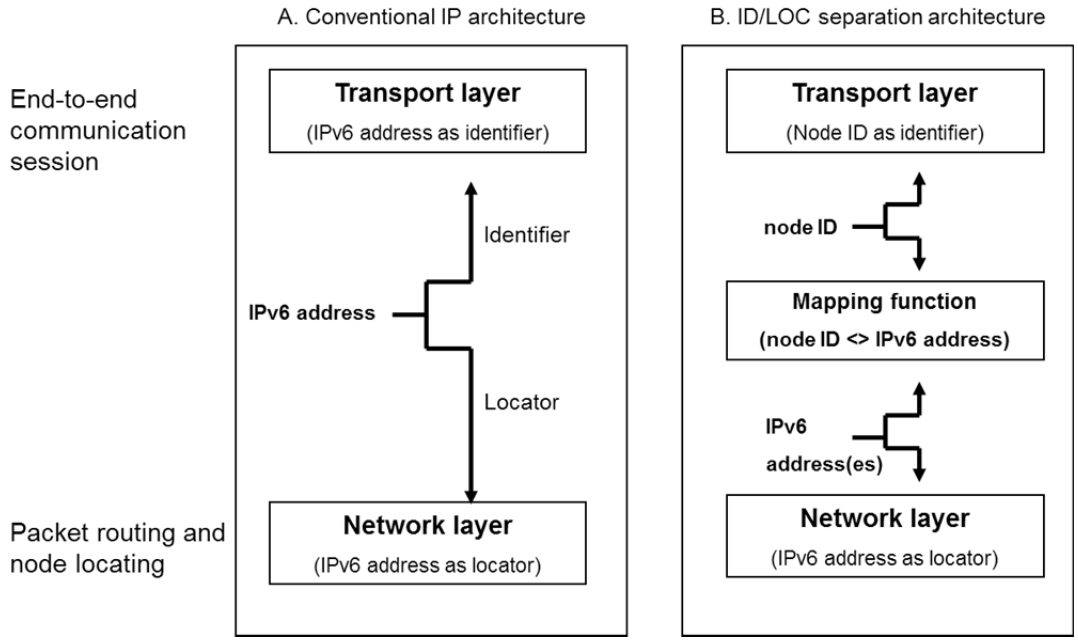

Figure 1 – Comparison between conventional IPv6 architecture and ID/LOC separation IPv6 architecture

6.1 IPv6 address space separation

Figure 2 shows the node ID and locator namespaces in the IPv6 address space. The figure shows that node ID and locator namespaces may be overlapped, or be isolated.

From the overlapped namespace, an IPv6 address is allowed to be used as a node ID or as a locator, depending on the approaches of ID/locator separation implemented in the NGNv6.

From the isolated namespace, an IP address is allowed to be used as either a node ID or a locator, but not both. The end hosts or network service nodes that implement ID/locator separation in the NGNv6 derive their node IDs and locators from these distinct namespaces. Some parts of the IPv6 address would distinguish if the given IPv6 address is a node ID or a locator.

In both the overlapped and isolated namespaces, the ID/locator mapping storage functions can help hosts or network nodes to determine if the given IPv6 address is a node ID or a locator.

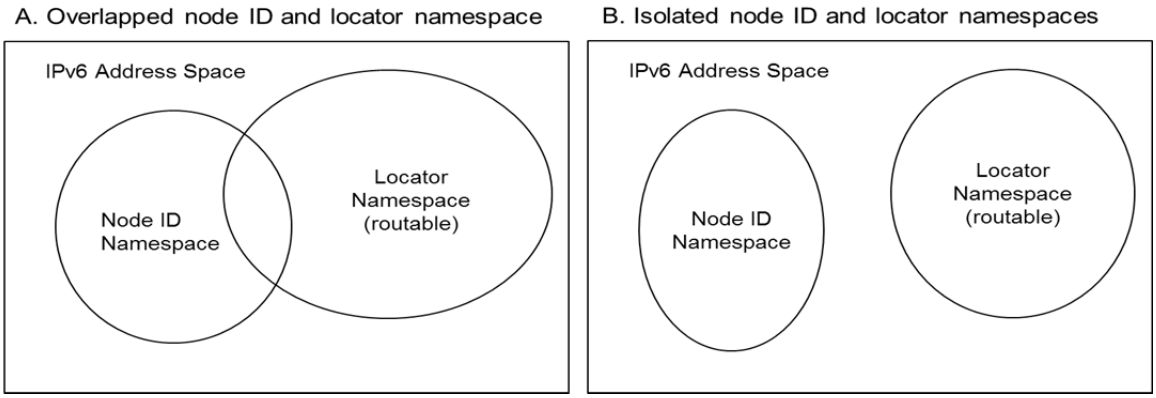

Figure 2 – Node ID and locator namespaces in IPv6 address space

6.1.1 Host-based IPv6 address separation

In host-based ID/locator separation, an end user function (EUF) possesses the ID/locator mapping functional entity (ILM-FE) that makes the EUF capable of distinguishing if an IPv6 address is a node ID or a locator. As shown in Figure 3, the EUF obtains its node ID from a portion of an IPv6 address space maintained by the service user profile functional entity (SUP-FE) and its locator from the other portion maintained in the transport user profile functional entity (TUP-FE). The EUF may obtain its peer or correspondent EUF's node ID and locator from the ID/locator mapping storage functional entity (ILMS-FE). The EUF's ILM-FE performs the node ID to locator mapping and uses only locators in the IP header of packets. The locators are used by the transport stratum to forward data from the source host to the destination host.

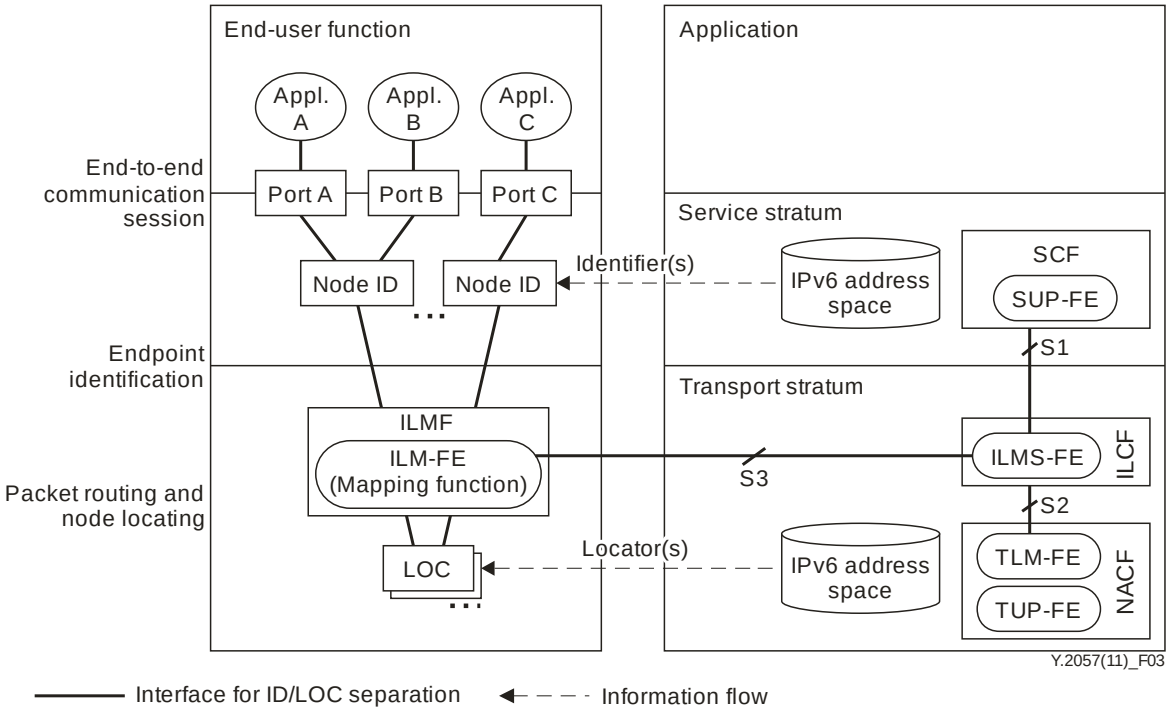

Figure 3 – Host-based IPv6 address separation

6.1.2 Network-based IPv6 address separation

In network-based ID/locator separation, an EUF may not possess the ILM-FE and thus may not be capable of distinguishing if an IPv6 address is a node ID or a locator. Instead, the ILM-FE is located in the network nodes as shown in Figure 4. In this case, the EUF may use the same routable IPv6 address as the node ID and local-scoped locator. When the packet from the EUF reaches the ILM-FE located in the network by using source node ID, the ILM-FE searches the corresponding global-scoped locator from the ILMS-FE using the corresponding node ID. Then, the ILM-FE forwards the packet in the transport stratum using the corresponding locator. The corresponding locator is used by the transport stratum to forward data from the source network to the destination network.

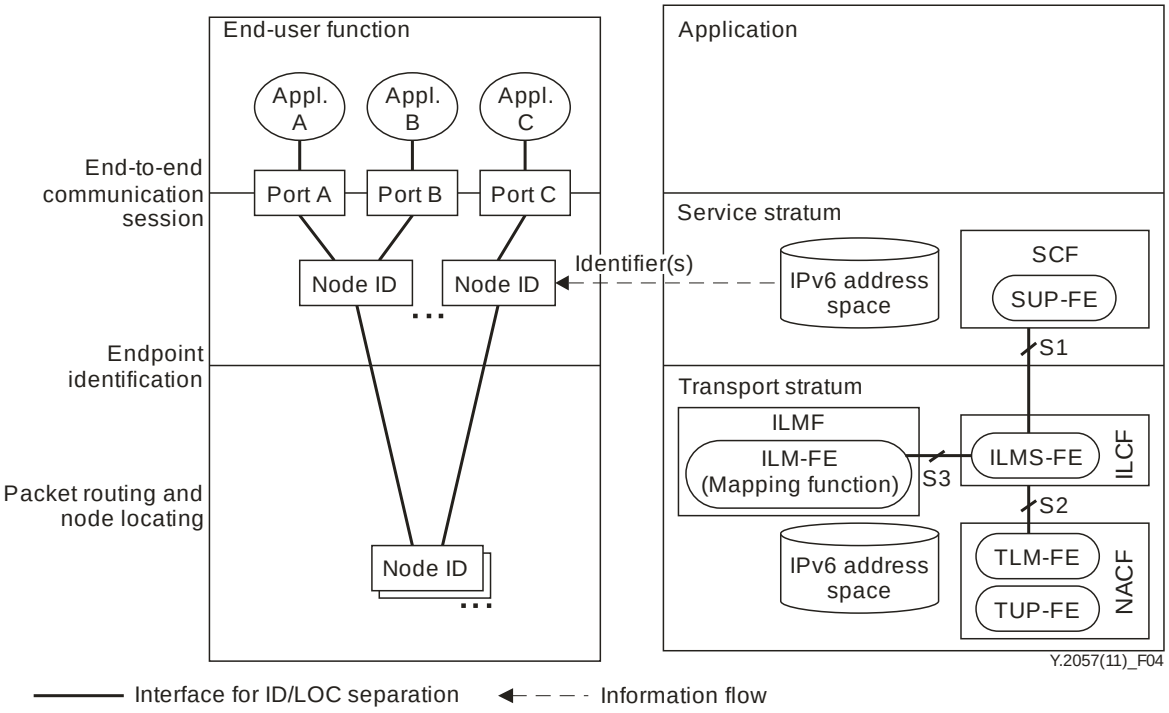

Figure 4 – Network-based IPv6 address separation

6.2 Node ID and locator configuration

6.2.1 Host-based configuration

In this configuration, the host is primarily responsible for configuring its own node ID by using a hint manually provided by the administrator or automatically assigned by the network through a negotiation process. The host may configure one or more of its IDs and may activate or deprecate them. Following the host configuration, the network maintains the node ID at the service user profile. Basically a node ID can be configured in the same way as in normal IPv6 address configuration using a hint (or prefix) from the uniquely defined node ID namespace or the overlapped node ID and locator namespace.

As mentioned earlier, the host can configure a node ID that can be exclusively used as a node ID (i.e., only in the transport and upper layer protocols) or also as a locator (i.e., when the host is not supporting ID/locator separation). Below are some possible IPv6 address configuration methods a host may use to configure a node ID.

– Routable IPv6 address as node ID: dynamic host configuration protocol for IPv6 (DHCPv6) [b-IETF RFC 3315] [b-IETF RFC 3646] [b-IETF RFC 3736], auto configuration [b-IETF RFC 2462], and any other methods specific to NGN may be used to configure a node ID.

– Uniquely defined IPv6 address as node ID: Node IDs can be configured from the IPv6 address space by using one of the following methods.

  i) Persistent IPv6 address as node ID: A persistent IPv6 address, derived from an IPv6 address space, can be used as a node ID. That is, there can be the reserved blocks of global IPv6 address space for node IDs. This is the role of authority of IPv6 address allocation. The persistent IP address can continuously be used by the protocols of the transport and higher layers 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 may also be routable as long as the node remains in the home network. Thus a 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.

  ii) IPv6 address with specific prefix as node ID: To distinctly separate node ID and locator namespaces from each other, specific prefixes may be used for configuring node IDs. Examples of such prefixes are overlay routable cryptographic hash identifiers (ORCHID) [b-IETF RFC 4843] and unique local IPv6 unicast addresses [b-IETF RFC 4193]. Such node IDs are not routable in the IPv6 routing space.

  iii) IPv6 address with specific values in type and scope fields as node ID: Similar to the node ID, the host can configure its one or more locators from the IPv6 address space allocated for the locator space. The value of a locator depends on the current location of the host in the network topology. The locator may be routable in a local scope or in the global scope of the network. Any IPv6 address configuration methods available in the access network can be used for this purpose. It can be a stateful address configuration based upon DHCPv6 as described in [b-IETF RFC 3315], [b-IETF RFC 3646] and [b-IETF RFC 3736] or, alternatively, an auto-address configuration specified in [b-IETF RFC 2462], or any other methods specific to the IPv6-based NGN.

6.2.2 Network-based configuration

In this configuration, the network is responsible for carrying out the ID/locator mapping function such as ILM-FE and ILMS-FE. The EUF may not possess the ID/locator functions and it may use the routable IPv6 addresses as the node ID and local-scoped locator. The EUF may use one or more of the methods explained in the previous subsection to configure its node ID. The node ID is recommended to use the unique local IPv6 addresses [b-IETF RFC 4193].

The network may also allocate one or more additional locators for the EUF. However, information about this allocation may not be given to the EUF. These global-scoped locators can identify the egress interfaces of the edge routers or border gateways located between the access and the core networks. These global-scoped locators can be configured using one of the methods specified in the previous subsection. The network stores the EUF's node ID to locator mapping in the ILMS-FE.

When another EUF located in another access network wants to communicate with the EUF, the former first obtains the latter's node ID to locator mapping from the ILMS-FE. The EUF then uses the peer EUF's node ID and locator in the data packet header and dispatches the packet. The packet reaches the edge router, which possesses the ILM-FE. It replaces the destination locator by the local locator (which is also the node ID) of the EUF and forwards the packet towards the EUF. For the packets dispatched from the EUF, ILM-FE replaces the EUF's local locator by the global locator of the edge router in the source locator field.

7 Functions and procedures for ID/LOC separation in NGNv6

According to [ITU-T Y.2015], there exist three relationships between NGN identifier, node ID, and LOC for implementing ID/LOC separation functions. Figure 5 depicts these relationships to adopt the ID/LOC separation rules to NGNv6 [ITU-T Y.2051]. An NGN identifier is translated into a node ID or a LOC when starting an application service. The node ID is then used as an identifier in the service and transport strata to identify the endpoint of the communication session. The LOC is used in transport stratum to locate the endpoint and forward packets over the routing infrastructure. However, it is not necessary that there exists a permanent relationship between the NGN identifier, node IDs and LOCs.

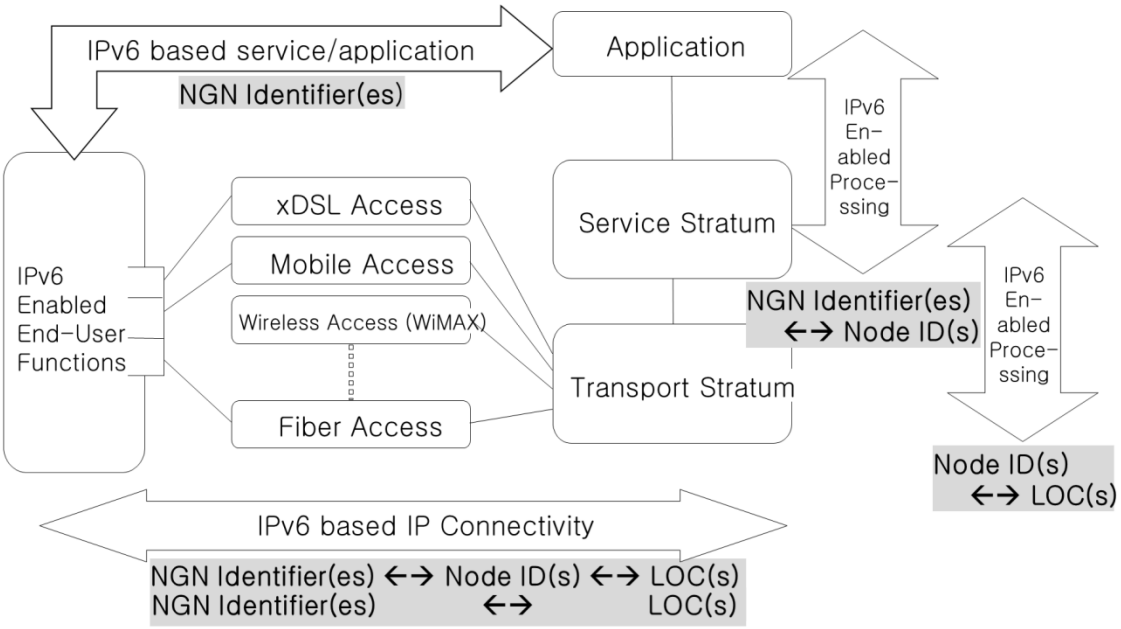

Figure 5 – Extension of IPv6-based NGN to support ID/LOC separation

NOTE 1 – From the vertical point of view, mapping between the NGN identifier and node ID is performed between the application and service stratum, and mapping between the node ID and LOC is performed between the service stratum and transport stratum.

NOTE 2 – From the horizontal point of view, mapping between the NGN identifier and node ID is performed between the EUF and access network, and mapping between the node ID and LOC is performed between the access network and core network.

7.1 Functions for ID/LOC separation in NGNv6

The mapping function for ID/LOC separation involves two major components: ID/LOC mapping functional entity (ILM-FE) and ID/LOC mapping storage functional entity (ILMS-FE) specified in [ITU-T Y.2015] and [ITU-T Y.2022]. Figure 6 shows the relationship between these FEs. Note that although the ILMS-FE and ILM-FE are shown separately in Figure 6, they can be physically collocated in an EUF or a transport control function (TCF).

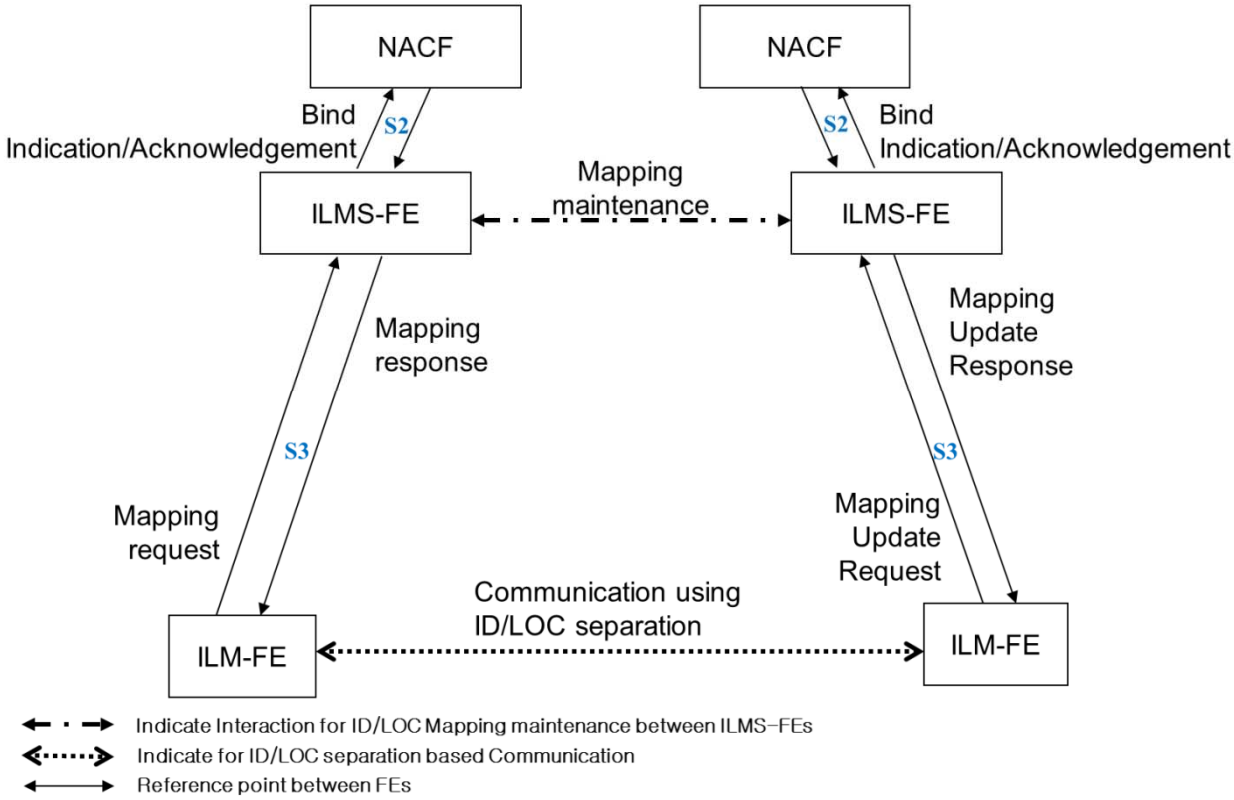

Figure 6 – ID/LOC separation architectural components in NGN

There are two reference points to define relations with functional entities (FEs) referred by [ITU-T Y.2022]: the S2 reference point defines relations between network attachment control function (NACF) and ILMS-FE to maintain and authorize ID/LOC mapping information, and the S3 reference point defines relations between ILM-FE and ILMS-FE to use ID/LOC mapping information.

An ILM-FE is the major component of the ID/locator separation architecture to perform ID/LOC mapping function in NGNv6. It obtains an ID/locator mapping record from ILMS-FE through the S3 interface. The ILM-FE uses node IDv6 in the transport and upper layer protocols and locators in the network layer protocol and a packet header. Using the node IDv6 as a reference value, the ILM-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 ILM-FE thus hides the effect of locator changes from the transport and upper layer services.

ILMS-FE stores and updates ID/locator mapping records. It accepts an ID/locator mapping record lookup request and mapping record update request from the ILM-FE through the S3 interface. It also binds the ID/locator mapping records to NACF's records and carries them out from NACF through S2.

7.2 Procedures for ID/LOC separation in NGNv6

7.2.1 Mapping record maintenance in ILMS-FE

ILMS-FE is responsible for maintaining ID/LOC mapping records. That is, the ILMS-FE collects ID/LOC mapping records either from relevant ILMS-FEs or ILM-FEs in EUFs or TCFs, distributes the mapping records among relevant ILMS-FEs, and provides the mapping records to ILM-FE when requested. The ILMS-FEs can be connected to each other in different structures or compositions so that they can efficiently collect, store and distribute up-to-date ID/LOC mapping

records. 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 domain name server (DNS) [b-IETF RFC 1035] may work well for the ILMS-FE in the case where the node IDv6 has hierarchical representation as domain names [b-IETF RFC 1034]. That is, the hierarchical ILMS-FE system is scalable for faster lookup of ID/LOC mapping records by end nodes because multiple cached copies of the mapping records are found in different locations of the system. However, such a system may be suitable only for maintaining static mapping records (e.g., that do not change frequently) because the existence of multiple cached copies makes it difficult to globally update dynamic mapping records in a short time.
– A flat structure of ILMS-FEs can be suitable for dynamic mapping records that require frequent updating. In a mobile environment where the access network topology changes frequently and thus the EUF locators change frequently, the flat structure of the ILMS-FEs may be a better design choice
– 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 would have additional flat structure. The hierarchical structure will be used for finding ID/LOC mapping records by utilizing the hierarchical notation of node IDv6, whereas the flat structure of authoritative storages are recommended to be used for faster updating of ID/LOC mapping records.

The ILMS-FE gets the ID/locator mapping record of EUFs from the NACF when the EUF is attached to the network. That is, when the NACF accepts a connection request from the EUF, it assigns an IPv6 address as the locator to the EUF. NACF then informs the ILMS-FE about the ID/locator mapping record of the EUFs.

7.2.2 Mapping record exchange between ILM-FE and ILMS-FE

The ILMF-FE can get the mapping records of an attached EUF from either the NACF or ILMS-FE. When the EUF gets its new locator (either by configuring the locator by itself using the advertised network parameters or by obtaining the locator by some other means like DHCP), it may send information about its ID/LOC mapping to the ILMS-FE through the ILM-FE. Or, in case the NACF assigns a new locator to the EUFs or detects the locator change by some other means (e.g., intercepting DHCP signal), it may send information about the ID/LOC mapping to the ILMS-FE. In this way, the ILM-FE can register and update the ID/locator mapping record of an EUF in the ILMS-FE.

7.2.3 Mapping record change detection and failure recovery

Since a node IDv6 persists for a long time, the ID/LOC mapping record changes only when the EUF changes its locator. The EUF changes its locator when it physically moves from one network to another or simply activates a new interface. When a mobile EUF changes its locator while having communication sessions with a peer EUF, the peer EUF should be able to detect the locator change of the mobile EUF in a short time. For this purpose, the peer EUF may use one of several approaches. It may get a mapping record change notification either from the mobile EUF or from the TCFs located closer to the mobile EUFs. The ILMS-FE can also push the mapping record change notification to the peer EUF.

The EUFs or TCFs can recover from the failure caused by the mapping changes, i.e., due to mobility. As soon as a mapping change is detected, the ILMF-FE of the EUFs or TCFs 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.

7.2.4 Data communication using ID/LOC separation

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

The ILM-FE residing in the EUF can perform host-based mobility and multihoming management. The ILMS-FE residing in the TCF can provide network-based mobility and multihoming management.

In addition to supporting mobility, multihoming and traffic engineering, the ILMS-FE should be able to change locators in the TCF 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 locators in the network layer header of packets, the TCF may employ one of the following mechanisms: translation and tunnelling. In the case of translation, the TCF 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 tunnelling, the TCF 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 TCF located in the access network of the peer EUF, the translation and tunnelling processes are reversed. That is, in the case of translation, the TCFs replace the locators used in the core network with the locators of the access networks, and, in the case of tunnelling, the outer network layer header is simply removed from the packets.

8 Considerations for deployment of ID/LOC separation in NGNv6

This clause specifies some technical considerations for deployment of ID/LOC separation in NGNv6 depending on the situation of IPv6 namespace. As the node IDs and LOCs are derived only from IPv6 address space, to deploy the ID/LOC separation, consideration should be given to whether the node ID namespace is overlapped with the locator name space or not. The clause is based on the assumption that most of the access networks and the core network would have IPv6 capability.

8.1 Node ID namespace is not overlapped with locator namespace

Node ID namespace is defined in IPv6 address space as shown in Figure 1. This clause describes technical issues to deploy the ID/LOC separation in Figure 1, whereby the omission of the common part of the namespace is to be considered. In the namespace, mapping function is recommended to reside in the EUF, because a node ID, which is a non-routable IPv6 address, is required to be mapped to a routable IPv6 address as the locator before the EUF dispatches packets into the network.

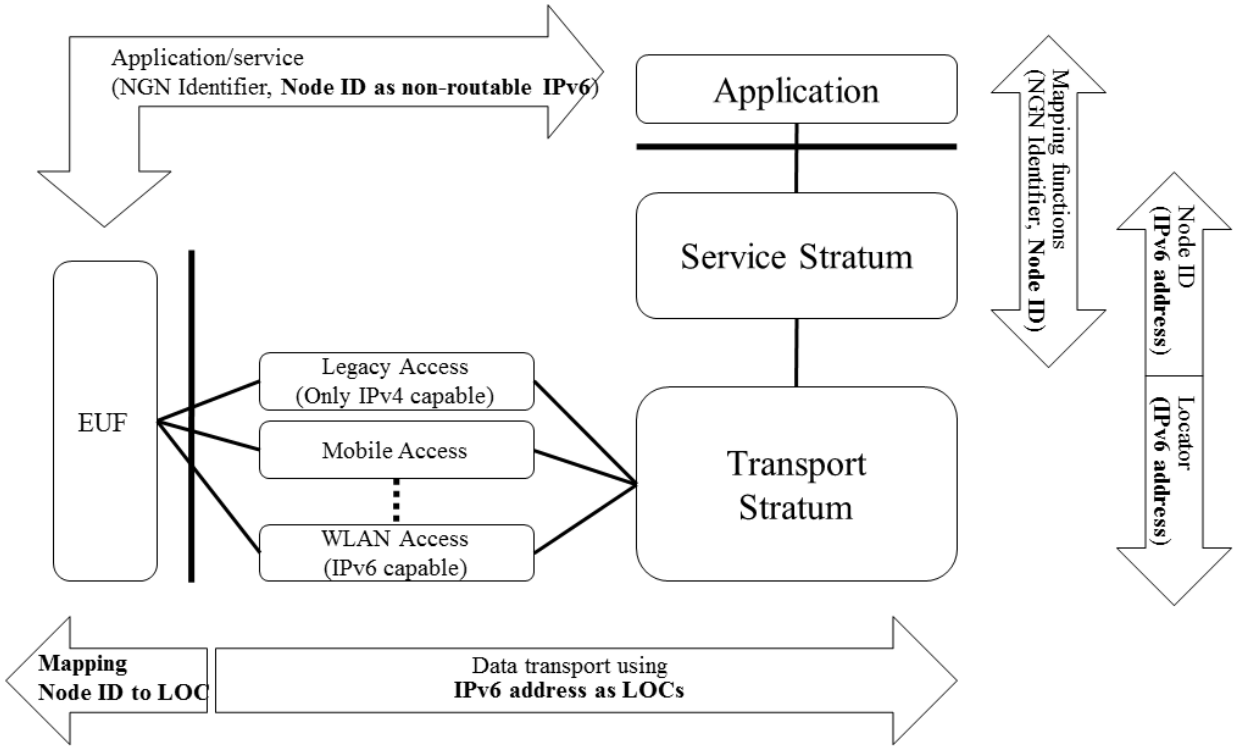

Figure 7 – General ID/LOC separation architecture – Node ID as a non-routable IPv6 address and LOC as an IPv6 address

The ID/LOC mapping function will cover between the EUF and access network to bind node IDs to LOCs as shown in Figure 7.

The node ID is derived from a non-routable IPv6 address, so that the node ID is recommended to be represented by authority organization or domain provider. Later, new node IDs can be extended as contents, public key, or virtual ID.

The ID/LOC separation is recommended to be deployed by the host-based approach, which means that the ILM-FE resides in the EUF. So the ILM-FE can perform host-based mobility and multihoming management by using ID/LOC mapping information obtained from the ILMS-FE. For mobility management, the ILM-FE is required to obtain a new locator whenever the end user moves to a different network. The ILM-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 that use the node ID. Similarly, to support multihoming, the ILM-FE switches locators in the network layer protocols based on the dynamically changing characteristics of the available networks.

Regarding the ID/LOC mapping function, all node IDs are required to be mapped to locators and the mapping function is recommended to support dynamic updates of the relationship between node IDs and LOCs at EUF. This requirement of dynamically updating ID/locator mappings may entail other issues, such as security, privacy, and manageability. These are not within the scope of this Recommendation.

8.2 Node ID namespace is overlapped with locator namespace

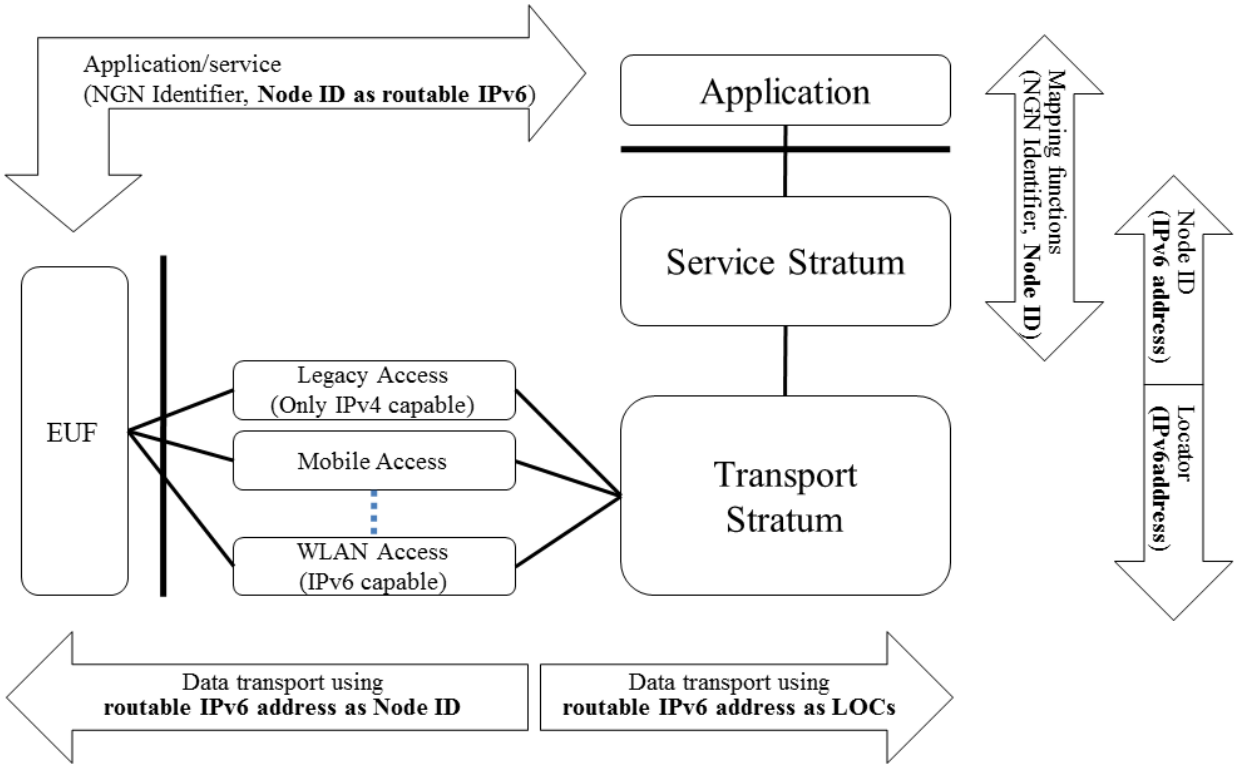

Figure 8 – General ID/LOC separation architecture – Node ID as an IPv6 address and LOC as an IPv6 address

This clause describes technical issues when deploying the ID/LOC separation of Figure 1, whereby the common part of the namespace is considered. So, for a routable IPv6 address, a specifically overlapped namespace is recommended to be allocated to the EUF as the node ID. The ID/LOC mapping function will be covered between the access network and the core network as shown in Figure 8.

This scenario would be helpful for the incremental deployment of the ID/LOC separation architecture as it does not demand that ID/locator mapping functions be implemented in the EUF. Therefore, a conventional EUF, which does not understand node ID, can be assisted by the ID/locator mapping function in the network.

The ID/LOC separation is recommended to be deployed by the network-based approach, which means that ILM-FE resides in the transport location management functional entity (TLM-FE) of TCFs. So the ILM-FE can provide network-based mobility and multihoming management. For the network-based mobility support, after establishing application setup, the ILM-FE in the TCF traces the moving EUF and manages its mobility information by changing locators in the outgoing and incoming data packets. Similarly, to support multihoming, the ILM-FE 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.

Regarding the ID/LOC mapping function, the routable node IDs are recommended to be mapped to a locator on the network, such as TCF.

9 Security considerations

This Recommendation has some security considerations similar to those pertinent to IPv6 addresses and aligns with the security requirements specified in [ITU-T Y.2701]. Specifically, the following are required:

– Node ID assignment: the newly defined node ID space is required to be secured and also have good privacy protection.

– ID/LOC mapping function: network entities should possess the ID/locator mapping functions to change locators based on the current ID/locator mapping information obtained from the trusted ILMS-FE.

– ID/LOC mapping storage function: The ID/LOC mapping database is required to be retrieved and updated by only authenticated end users or network entities.

Appendix I

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 IPv4-based NGN (NGNv4). In these scenarios, node IDs and LOCs are an IPv6 and/or an IPv4 address. Figure I.1 shows just one case.

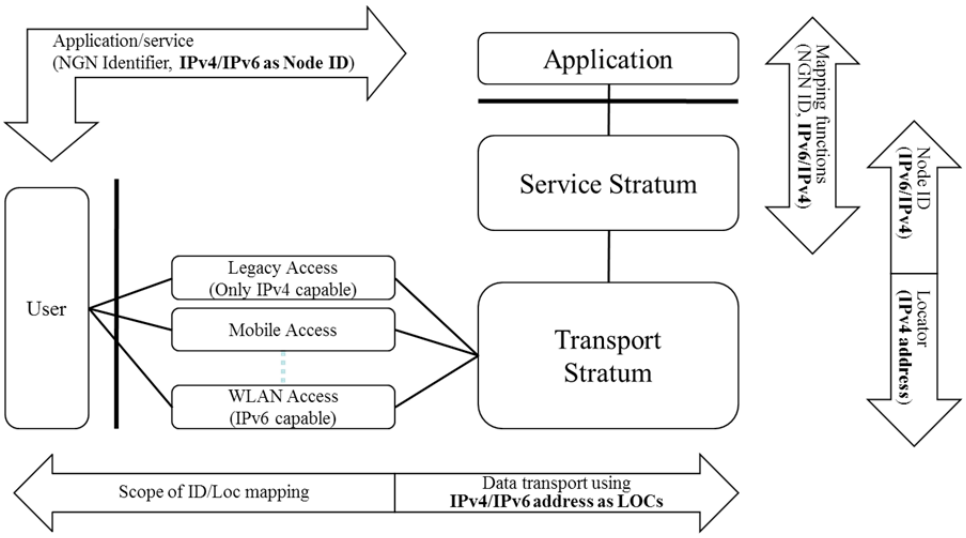

Figure I.1 – General ID/LOC separation architecture – IPv6 node ID and IPv4 LOC

I.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 the current IP network conditions where most access networks are only IPv4 capable networks and the core network can transport IPv4 data only. Therefore the node ID is an IPv6 address, and the locator is an IPv4 address.

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

If a node ID can be used in IPv6 address, all user equipment would have the ability to start a service and application using an IPv6 address as the node ID. For instance, current applications and services established communication sessions by using 32 bit IPv4 addresses, but on the other hand, most applications and services will be able to be established 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 an IPv4 network, a transition mechanism should be needed; but the ID/LOC separation can be translated from an IPv6 address as the node ID to an IPv4 address, which can be used as the real locator using the ID/LOC mapping function without considering transition mechanisms. Therefore the transition from IPv6 to IPv4 will be achieved naturally, so that data packets should be transported to a core network using an IPv4 address.

Regarding the IPv6 capable access network's interoperability, the ID/LOC mapping function can be located and activated between the access network and core network, so that the translation from an IPv6 address to an 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 has already been achieved up to a certain point, where the core network is an IPv6 capable network. Therefore, we should only consider a legacy IPv4 access network to support connectivity to an IPv6 core network.

Regarding interoperability with an IPv4 legacy access network and an IPv6 core network, the ID/LOC mapping function can be performed twice; once for the translation from an IPv6 address as node ID to an IPv4 address as the locator within a legacy access network; then for the translation from the IPv4 address to the IPv6 address as locator in the core network. For instance, in the mapping between user equipment and the access network, binding from an IPv6 address as node ID to an IPv4 address as locator can be accomplished first. Then also the transition from an IPv4 address to an IPv6 address should be achieved to transport data packets.

I.2 Interworking scenarios between hosts in different node ID namespaces

According to [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 identifiers and LOCs. So, we can think that an IPv4 address could be used as the node ID. The scenario in which an IPv4 address could be a node ID comes under the adoption of ID/Loc separation in NGNv4. To encourage IPv6 deployment, this Recommendation requires the use of the IPv6 address as the node ID, so that we are not concerned with the node IDv4. However there are some capabilities of coexisting node IDv4 and node IDv6; an interworking scenario shall be considered for interoperability between end nodes.

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

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

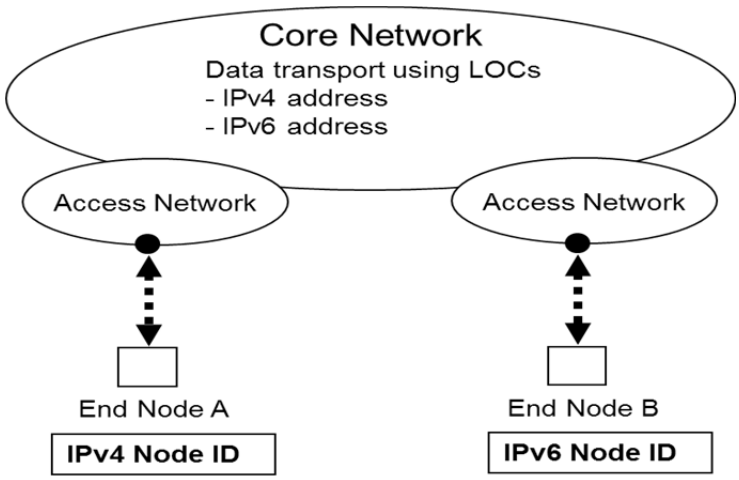

Figure I.2 – IPv4 node ID and IPv6 node ID

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

If a node ID can be used in an IPv6 address, all user equipment would be able to start a service and an application using an IPv6 address by 128 bits form. So application developers shall choose IPv6 capable APIs to make IPv6-based services or applications. But a correspondent end host B uses node IDv6, so that the ID/LOC mapping architecture takes account of mapping IPv4 node ID to the locator as well as mapping node IDv6 to the 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. The address translator from IPv6 to IPv4 and vice versa could be adopted in the architecture between the end node and access network, especially.

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

Case 1: node ID namespace exists in IPv4/IPv6 address space and locator namespace exists in IPv4 address space.

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

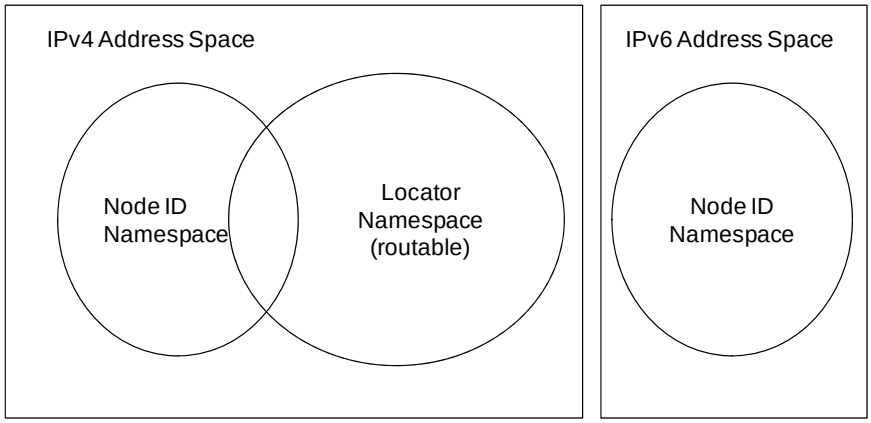

Figure I.3 – Node ID namespaces in an IPv6/IPv4 address space and locator namespace in an IPv4 address space

Case 2: node ID namespace exists in IPv4/IPv6 address space and a locator namespace exists in IPv6 address space.

This scenario assumes the future IP network conditions, where the majority of access networks are only IPv6 capable networks and the core network can transport IPv6 data only. The majority of node IDs use an IPv6 address, but an IPv4 address is still used as the node ID. In such cases, the locator is an IPv6 address. In this case, interworking schemes using different node IDs should be considered.

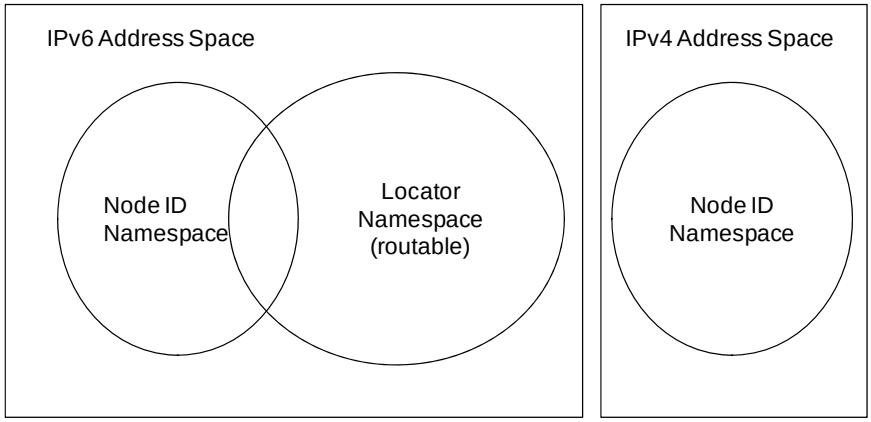

Figure I.4 – Node ID namespaces in IPv6/IPv4 address space and locator namespace in IPv6 address space

Bibliography

[b-ITU-T G.8081] Recommendation ITU-T G.8081/Y.1353 (2004), *Terms and definitions for Automatically Switched Optical Networks (ASON).*

[b-ITU-T Y.2012] Recommendation ITU-T Y.2012 (2006), *Functional requirements and architecture of the NGN release 1*.

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

[b-ITU-T Y.2091] Recommendation ITU-T Y.2091 (2011), *Terms and definitions for next generation networks.*

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

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

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

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

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects and next-generation networks**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2012