International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2055

(03/2011)

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

Next Generation Networks – Frameworks and functional architecture models

Framework of object mapping using IPv6 in next generation networks

Recommendation ITU-T Y.2055

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.2055

Framework of object mapping using IPv6 in next generation networks

Summary

Recommendation ITU-T Y.2055 specifies the basic concept and requirements of object mapping using IPv6 in next generation networks (NGN) in order to provide networking capabilities to objects. This Recommendation also describes the mapping architecture, the relationship between identifiers and the relevant mechanisms for object mapping.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T Y.2055	2011-03-16	13

Keywords

IPv6, mapping, NGN, object.

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.2055

Framework of object mapping using IPv6 in next generation networks

1 Scope

This Recommendation describes the requirements and the mechanisms for object mapping using IPv6 in next generation networks (NGNs). This Recommendation covers the following:

- Basic concept and requirements of object mapping using IPv6;
- Mapping architecture and relationships between identifiers;
- Mechanisms for object mapping using IPv6.

This Recommendation does not intend to develop any specific protocols for object mapping.

As many new types of devices (i.e., objects) are connected to networks, this Recommendation assumes that IPv6 plays a key role in object-to-object communications. The objective of this Recommendation is to provide guidelines for mapping of information on objects for providing end-to-end connectivity 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, the 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 regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T G.805] Recommendation ITU-T G.805 (2000), *Generic functional architecture of transport networks.*

[ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications.*

[ITU-T X.811] Recommendation ITU-T X.811 (1995) | ISO/IEC 10181-2:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework.*

[ITU-T Y.1540] Recommendation ITU-T Y.1540 (2011), *Internet protocol data communication service – IP packet transfer and availability performance parameters.*

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

[ITU-T Y.2002] Recommendation ITU-T Y.2002 (2009), *Overview of ubiquitous networking and of its support in NGN.*

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

[ITU-T Y.2012] Recommendation ITU-T Y.2012 (2010), *Functional requirements and architecture of next generation networks.*

[ITU-T Y.2014] Recommendation ITU-T Y.2014 (2010), *Network attachment control functions in next generation networks.*

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

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

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

[ITU-T Y.2701] Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1.*

[ITU-T Y.2702] Recommendation ITU-T Y.2702 (2008), *Authentication and authorization requirements for NGN release 1.*

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

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 address [ITU-T Y.2091]: An address is the identifier for a specific termination point and is used for routing to this termination point.

3.1.2 authentication [ITU-T X.811]: Authentication provides assurance of the claimed identity of an entity.

3.1.3 authorization [ITU-T X.800]: The granting of rights, which includes the granting of access based on access rights.

3.1.4 binding [ITU-T G.805]: A direct relationship between a "transport processing function" or "transport entity" and another "transport processing function" or "transport entity" which represents the static connectivity that cannot be directly modified by management action.

3.1.5 context [ITU-T Y.2002]: The information that can be used to characterize the environment of a user.

NOTE – Context information may include where the user is, what resources (devices, access points, noise level, bandwidth, etc.) are near the user, at what time the user is moving, interaction history between person and objects, etc. According to specific applications, context information can be updated.

3.1.6 host [ITU-T Y.1540]: A computer that communicates using the Internet protocols. A host implements routing functions (i.e., it operates at the IP layer) and may implement additional functions including higher layer protocols (e.g., TCP in a source or destination host) and lower layer protocols (e.g., ATM).

3.1.7 identifier [ITU-T Y.2091]: An identifier is a series of digits, characters and symbols or any other form of data used to identify subscriber(s), user(s), network element(s), function(s), network entity(ies) providing services/applications, or other entities (e.g., physical or logical objects). Identifiers can be used for registration or authorization. They can be either public to all networks, shared between a limited number of networks or private to a specific network (private IDs are normally not disclosed to third parties).

3.1.8 identity [ITU-T Y.2720]: Information about an entity that is sufficient to identify that entity in a particular context.

3.1.9 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 multi-homing.

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 multi-homing implications.

3.1.10 object [ITU-T Y.2002]: An intrinsic representation of an entity that is described at an appropriate level of abstraction in terms of its attributes and functions.

NOTE 1 – An object is characterized by its behaviour. An object is distinct from any other object. An object interacts with its environment including other objects at its interaction points. An object is informally said to perform functions and offer services (an object which makes a function available is said to offer a service). For modelling purposes, these functions and services are specified in terms of the behaviour of the object and of its interfaces. An object can perform more than one function. A function can be performed by the cooperation of several objects.

NOTE 2 – Objects include terminal devices (e.g., used by a person to access the network such as mobile phones, Personal computers, etc.), remote monitoring devices (e.g., cameras, sensors, etc.), information devices (e.g., content delivery server), products, contents, and resources.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 mapping: A technique for forming associations between logical and physical interfaces.

3.2.2 object mapping: The process which an object identifier (object ID) is associated with an identifier (e.g., IPv6 address).

3.2.3 object ID: The identifier which identifies an object.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AM-FE	Access Management Functional Entity
AR-FE	Access Relay Functional Entity
ATM	Asynchronous Transfer Mode
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EPC	Electronic Product Code
EUI	Extended Unique Identifier
GW	Gateway
ID	Identifier
IdM	Identity Management
IP	Internet Protocol
IT	Information Technology
LOC	Locator
MAC	Medium Access Control
NACF	Network Attachment Control Function
NAC-FE	Network Access Configuration Functional Entity
NGN	Next Generation Network
PoA	Point of Attachment
RA	Router Advertisement
RACF	Resource Admission Control Function

RS	Router Solicitation
SCF	Service Control function
SCM	Supply Chain Management
TCP	Transmission Control Protocol
TLM-FE	Transport Location Management Functional Entity
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

5 Conventions

In this Recommendation, the keyword "NGN" indicates "IPv6-based NGN" as per [ITU-T Y.2051].

In clause 6.3:

The keywords "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

The keywords "is prohibited from" indicate a requirement which must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

The keywords "is not recommended" indicate a requirement which is not recommended but which is not specifically prohibited. Thus, conformance with this Recommendation can still be claimed even if this requirement is present.

The keywords "can optionally" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option, and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with this Recommendation.

6 Overview of object mapping using IPv6 in NGN

6.1 Classification of identifiers for object identification and mapping

Identifiers are used to facilitate reaching or using applications or services. There are many kinds of identifiers (IDs) such as ITU-T E.164 number code, EUI-64, MAC address or URI/URL. By using these identifiers, devices can be reachable to the other users and/or devices.

Identifiers have two functions. One is to identify an object in the real world. The other is to be used as an address or number to uniquely identify the location of an entity on the network. Two or more entities on the network can communicate with each other using identifiers or addresses.

An "Object ID" generally takes the form of an application-specific integer or pointer that uniquely identifies an object. This Recommendation considers an object as an end point of communication which is connected to the network excluding conventional terminal devices (e.g., used by a person to access devices such as mobile phones or personal computers). These objects include remote monitoring devices (e.g., cameras or sensors), information devices (e.g., content delivery server), products or contents.

Appendix I provides examples of mapping relationships between host and object(s). In the examples shown in Appendix I, conventional terminal devices have a one-to-one mapping where a host is equal to an object. On the other hand, most of the other objects have a one-to-many mapping where a host is not equal to an object.

This Recommendation mainly focuses on objects that have a one-to-many mapping relationship.

Figure 6-1 represents the relationship between object and network attachment in IPv6-based NGN. In this figure, the point of attachment (PoA) represents a physical end point of network and a termination point of connection with IPv6 address. There are fixed or mobile objects to be attached to the IPv6-based NGN. In the context of mobility of persons and objects, there is not necessarily any permanent relationship between the identity of an object to be involved in a telecommunication activity and its location (i.e., the place where it can be found) [ITU-T Y.2011]. The location of a given telecommunication object can be represented by the physical PoA, where the said object may be reached or found. At the border between the object and PoA in the network, the relevant mapping or binding should be done using the related ID information for connecting to objects irrespective of location change in the fixed and mobile environment.

The scope of this Recommendation is to consider the relationship with IPv6 address for association between the PoA and object(s) in IPv6-based NGN (see dotted box in Figure 6-1).

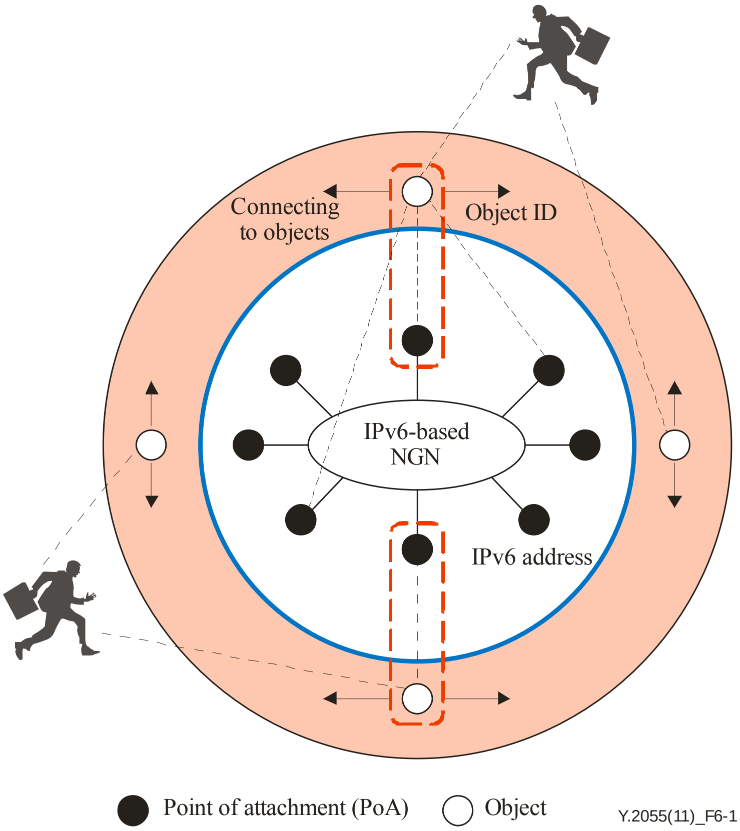


Figure 6-1 – Relationship between object and network attachment in IPv6-based NGN

6.2 Basic concept of object mapping

The identification and mapping of all objects for providing end-to-end connectivity is crucial. Identifiers are capable of identifying all relevant objects and facilitating object-to-object communication. In particular, globally unique identifiers enable a great many applications, including tracking, access control, and the protection of objects.

As shown in Figure 6-2, the layered architecture of NGN requires specific processing capabilities at each layer. Each user or object in applications is identified by an identity such as a name with a set of attributes of an entity. An attribute can be thought of as metadata that belongs to a specific entity in a specific context, some of which could be highly private or sensitive. The identity should be associated with object IDs through identification and authorization for identity management. Each object ID also should be associated with an IPv6 address through mapping (binding) for object mapping.

An ID resolution server such as domain name system (DNS) can provide a function to translate the identifier of an object into the IPv6 address to access ubiquitous networking services provided by database or application servers. From the IPv6-based NGN perspective, how to map (bind) the IPv6 address with other identifiers for providing end-to-end IP connectivity is critical.

Identity processing is comprised of identity management, object mapping, and ID/LOC separation. This Recommendation focuses on object mapping using IPv6.

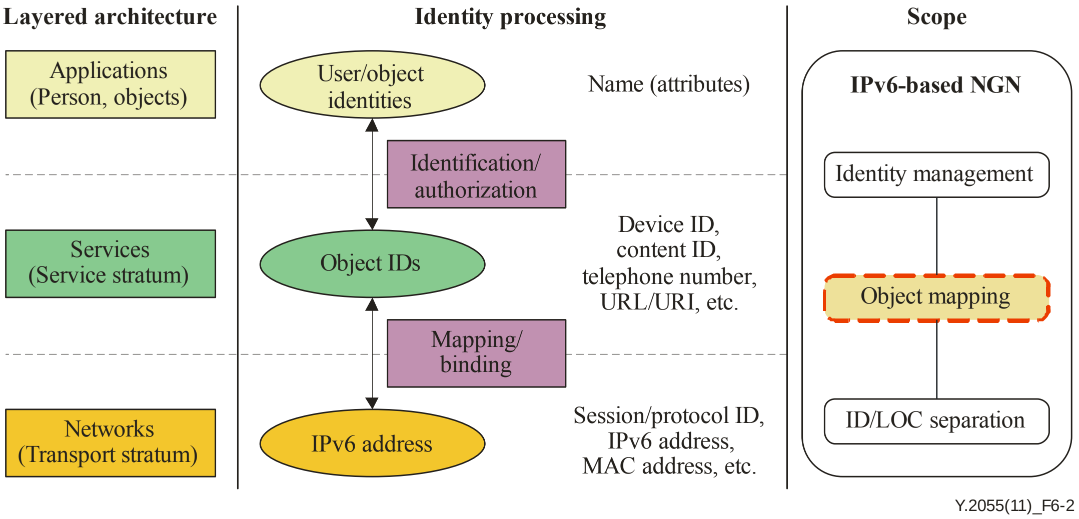

Layered architecture
Identity processing
Scope
Applications (Person, objects)
User/object identities
Name (attributes)
IPv6-based NGN
Identification/ authorization
Identity management
Services (Service stratum)
Object IDs
Device ID, content ID, telephone number, URL/URI, etc.
Object mapping
Mapping/ binding
Networks (Transport stratum)
IPv6 address
Session/protocol ID, IPv6 address, MAC address, etc.
ID/LOC separation
Y.2055(11)_F6-2

Figure 6-2 – Object identification through identity processing in IPv6-based NGN

6.3 Requirements for object mapping using IPv6

As described in clause 6.1, there are many kinds of identifiers. Using these identifiers, devices are recommended to be reachable to the other users or devices. For managing a large number of different identifiers to use IPv6 network infrastructure, it is recommended to use both the location information of the IPv6 address and the unique information of identifiers.

Accordingly, it is recommended to combine the IPv6 address with identifiers for end-to-end connectivity. Based on the identifier, the current IPv6 address structure would be changed to include the information of identifiers. Thus, the efficient combining method between the IPv6 address and the object ID is required as an example of address mapping.

Figure 6-3 shows address mapping (binding) with the IPv6 address for IPv6-based networking. The mechanism which maps/binds the IPv6 address and several identifiers can provide reachability to enable ubiquitous access to objects. Each identifier can be addressable in the IPv6-based NGN. The reachable scope can be defined by the IPv6 prefix used. Location computation software could directly communicate with devices from anywhere within the IPv6-based NGN.

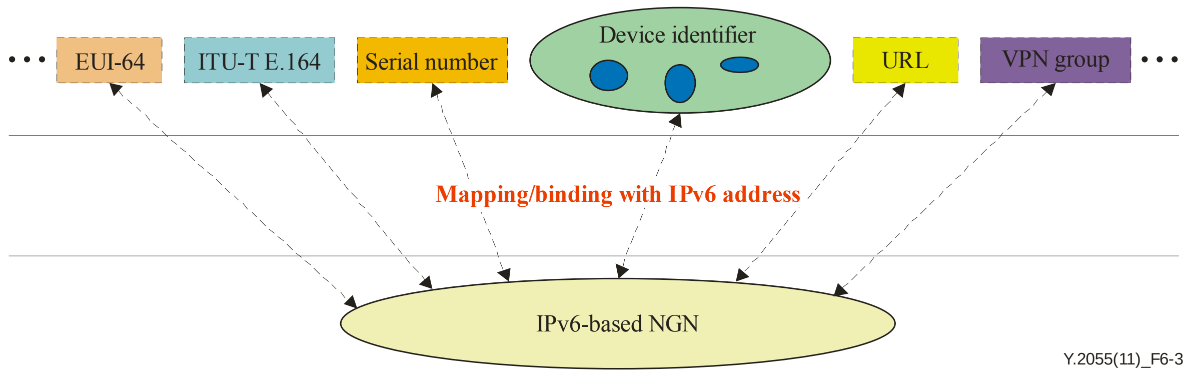


Figure 6-3 – Mapping or binding between IPv6 address and object IDs in IPv6-based NGN

7 Mapping architecture and relationship between identities

7.1 Mapping architecture between identifiers

7.1.1 Classification of network entities to be identified

Networks are comprised of entities and these network entities have a layered architecture which is used for naming, addressing and routing as shown in Figure 7-1.

- Services (i.e., information related to applications/services such as object ID)
- End points (i.e., IP termination points with globally unique identifier)
- Location (i.e., IPv6 address)
- Path (i.e., routing between network attachments).

In particular, for object-to-object communications, information for several kinds of object on top of end points should be identified in the network.

7.1.2 Layered mapping architecture between identifiers

The architecture in Figure 7-1 has the following relationship at each layer.

A service is an entity that is either an instance of a specific application service or a specific data object. The identity of the object persists over time and is not tied to the end system hosting the service or data. An application layer has a capability for object mapping.

A Location is identified with some sort of network address or locator. These locators often depend on the network topology and technology used. The network layer includes the locator information of the host which resides in a node in a network. ID/LOC separation can be performed in this layer.

A Path represents a physical route between physical devices for connectivity (e.g., PoA).

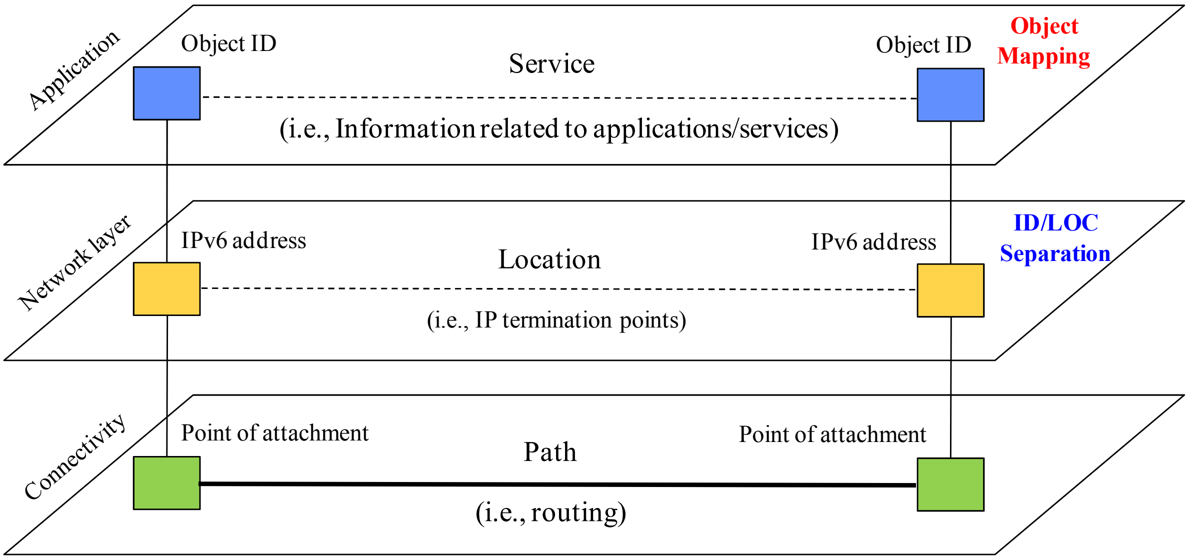


Figure 7-1 – Layered mapping architecture between identifiers

One purpose of defining a layered architecture is to provide mappings (bindings) between entities at different levels. With mappings (bindings), identities of entities become location independent. Furthermore, different types of mobility, such as for nodes and services, become possible without resorting to add-on mechanisms.

7.2 Mapping relationships between identifiers

For object mapping, two mapping relationship could be considered as follows (see Figure 7-2):

– Direct mapping

An object at the application layer is directly reachable to the host entity at the PoA to which the IP is terminated. This object is located on top of the TCP/IP protocol stack (e.g., objects inside a server).

– Indirect mapping

An object at the application layer is remotely reachable through the non-IP interface to the host entity at the PoA to which IP is terminated. This object is located outside the physical network attachment to which IP is terminated.

Indirect mapping can additionally support advanced mobility schemes, such as moving objects, and explicitly control middle boxes. Indirect means that the name of an entity does not bind "down" within the same node, but sideways to another location where an intermediary takes care of forwarding the communication to the entity's actual location. A simple application of this mechanism enables servers to operate behind a gateway without explicit configuration.

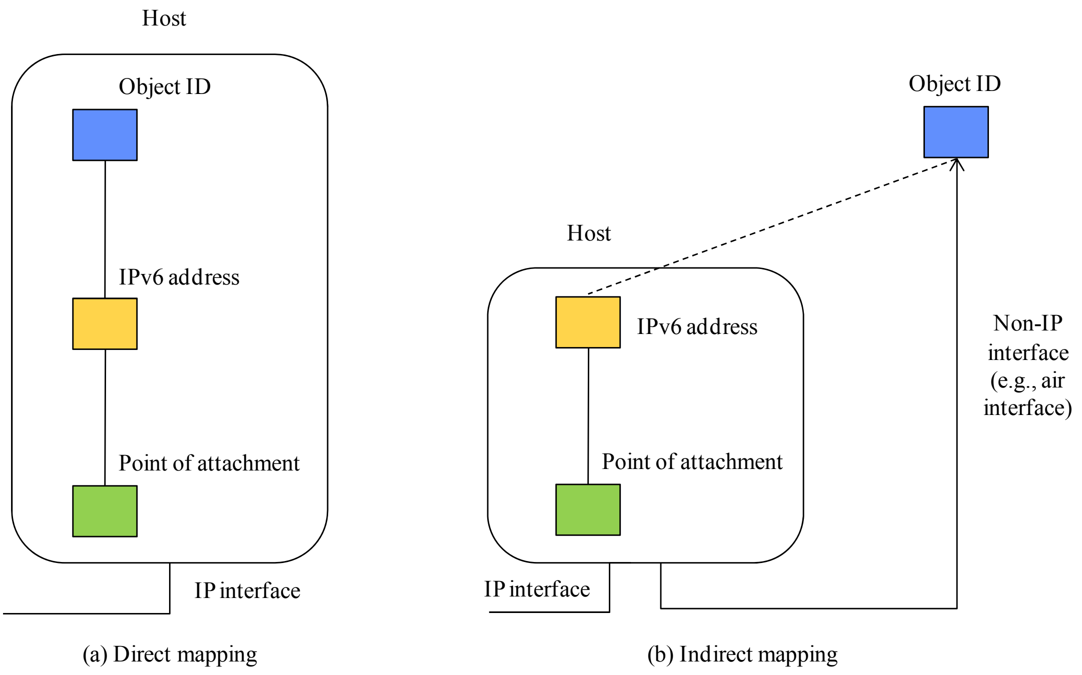


Figure 7-2 – Mapping relationship between identifiers

7.2.1 ID bindings under direct mapping

The IPv6 address is a typical example of identifiers which are used for data transportation in IPv6-based NGN. Binding between the object ID and the IPv6 address is done in two ways, namely explicit binding and implicit binding.

Explicit binding is a one-to-one association between the IPv6 address and the object ID. In most cases, it would be a mapping-table based mechanism. With each IPv6 address, the related object ID could be retrieved by checking against the mapping table. Explicit binding can also be used in the case of single IPv6 address mapping to multiple object IDs. In this case, the host is using the same IPv6 address to serve more than one service. The host sends the router solicitation (for stateless address configuration) or the DHCP request (for stateful address configuration) to request subnet prefix or IPv6 address. Next, the network attachment control function (NACF) [ITU-T Y.2014] allocates the subnet prefix or address; the service control functions may register the binding on the object ID and the IPv6 address. With this approach, the binding of object ID and IPv6 address is achieved at both the service stratum and transport stratum.

Implicit binding is to implicitly embed the related object ID into the IPv6 address. Such information may be included in the subnet ID field of the IPv6 address. In the IPv6 network, every single device may have an address due to the huge addressing space. Some of these addresses may only be used for single services such as a remote monitoring device. In this case, the host sends router solicitation (for stateless address configuration) or DHCP request (for stateful address configuration) with service type information. According to some mapping relationship between the service type or ID and subnet prefix, router responses with router advertisement (for stateless address configuration) or DHCP response (for stateful address configuration) containing the subnet prefix of the corresponding service type/ID. For stateful address configuration, the host directly receives the IPv6 address with the embedded object ID information. For stateless address configuration, the host uses the received subnet prefix to generate an IPv6 address. With this approach, binding of object ID and IPv6 address is achieved implicitly.

NOTE – ID binding under indirect mapping is out of scope in the Recommendation.

8 Mechanisms for object mapping

8.1 ID bindings in NGN architecture

NGN architecture [ITU-T Y.2012] is basically composed of the service stratum and transport stratum. Service stratum has service control functions and the application/service support functions. Transport stratum further comprises transport functions and transport control functions. There are two major functions, NACF and resource admission control function (RACF) [b-ITU-T Y.2111], in transport control functions. Appendix II presents NACF functional architecture for NGN.

The ID bindings involve the interaction between the service stratum and transport stratum， especially the service control functions and network access control functions.

Explicit binding may happen after the network access. It is loosely coupled to the IPv6 address provisioning procedures. Implicit binding most likely happens at the time of IPv6 address allocation. As IPv6 supports DHCP-based stateful address allocation and RS or RA-based stateless address allocation, both cases need to be taken care of.

Appendix III provides information flows of explicit binding and implicit binding.

8.2 Object mapping mechanism

Figure 8-1 shows the basic mechanism of sending a data packet to an object and mappings (bindings). The relevant procedures include:

– Find a node on which the required object resides. This requires finding the object and end point through object ID registration. Name resolution using domain name system (DNS) is optionally required.

– Find a network attachment point to which the node is connected. This requires finding a location. For this, a client obtains a binding information object ID and an IPv6 address.

– Find a path from the client to object(s). The client can directly connect to object(s) using routing.

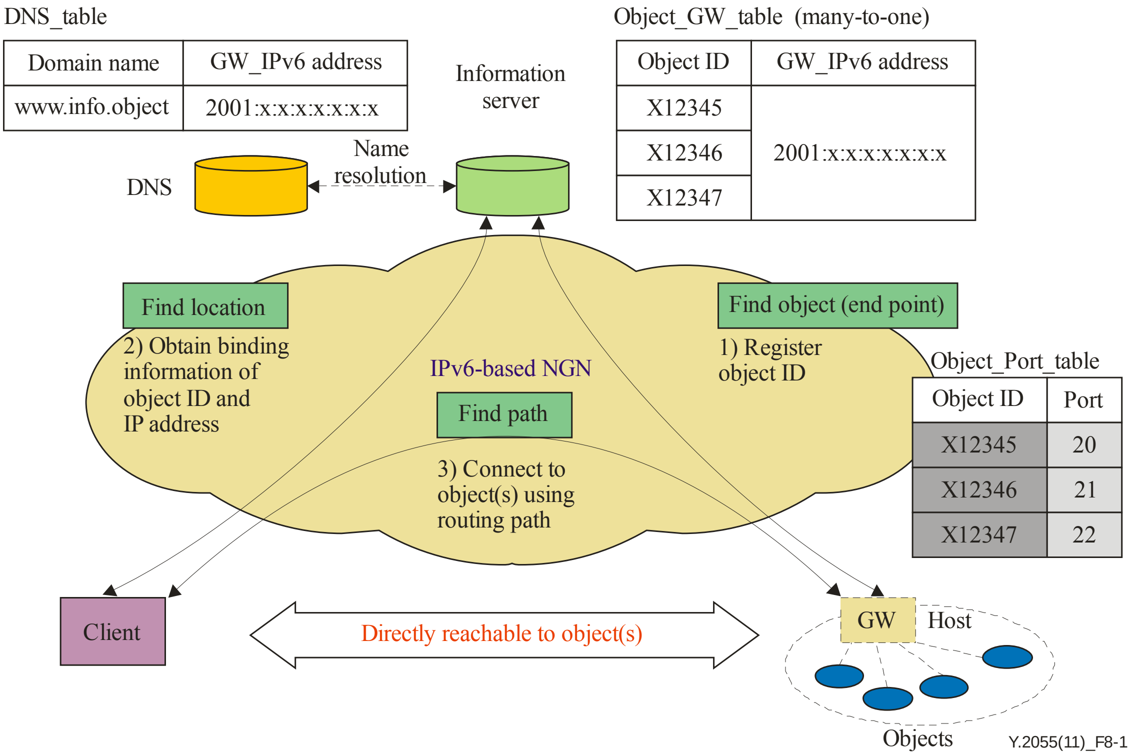
For object mapping, the following mapping tables are required:

– DNS_table: includes mapping information between the domain name and the IPv6 address of gateway (GW).

– Object_GW_table: includes mapping information between object IDs and the IPv6 address of GW.

– Object_Port_table: includes mapping information between object IDs and port numbers.

The detailed protocols for object mapping mechanism are out of scope in this Recommendation.



DNS_table

Domain name	GW_IPv6 address
www.info.object	2001:x:x:x:x:x:x:x

Object_GW_table (many-to-one)

Object ID	GW_IPv6 address
X12345	2001:x:x:x:x:x:x:x
X12346	
X12347	

Object_Port_table

Object ID	Port
X12345	20
X12346	21
X12347	22

Figure 8-1 – Object mapping mechanism

9 Security considerations

Basic considerations on security architecture for NGN are addressed in [ITU-T Y.2001] while security requirements of the NGN are described in [ITU-T Y.2701]. Concerning the specifics of ubiquitous networking, the various kinds of terminals, devices and contents that can be involved will have to conform to the security requirements of the network they are willing to attach. When attaching to the NGN, the corresponding authentication and authorization requirements, as described in [ITU-T Y.2702], are applicable. These requirements can be applied to IPv6-based NGN.

In this Recommendation, objects involved in the IPv6-based NGN have their own identities and are interconnected involving more interactions throughout a dynamic and heterogeneous environment. Accordingly, security, including the design of the security architecture for a secure information discovery and delivery to users including persons and objects, is very crucial.

Appendix I

Examples of mapping between host and object(s)

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

This appendix introduces an example of mapping relationships between the host and object(s).

1 Host = Object (one-to-one mapping)

When a host is equal to an object, there is a one-to-one mapping relationship between the host and the object. Most of the information technology (IT) devices such as personal computer (PC) are included in this case.

For example, if one uses a telephone device, the device as host can be allocated a telephone number as an ID for the service and be treated the same as an object.

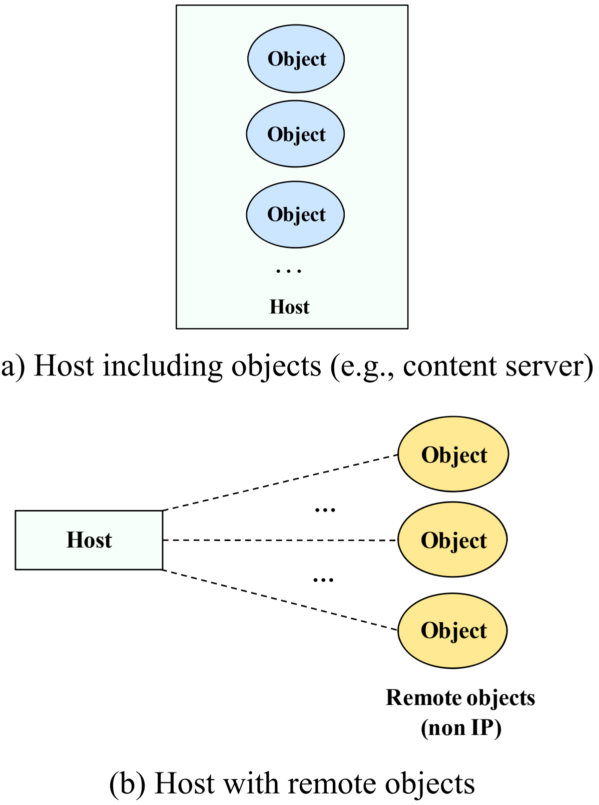
2 Host ≠ Object (one-to-many mapping)

When a host is not equal to an object, there is a one-to-many mapping relationship between the host and object(s).

There are two kinds of one-to-many mapping as follows:

As shown in Figure I.1-a, Host including objects such as content servers: a host includes many objects and these objects should be identified using content ID, etc.

As shown in Figure I.1-b, Host with remote objects: a host has many remote objects and these objects should be identified using identifiers. In this case, each object might be a non-IP.



(a) Host including objects (e.g., content server)

(b) Host with remote objects

Figure I.1 – Mapping between host and objects (one-to-many mapping)

Appendix II

Network attachment control faction (NACF) functional architecture

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

Figure II.1 describes the NACF functional architecture with the functional entities and the relevant reference points. The details for NACF are specified in [ITU-T Y.2014].

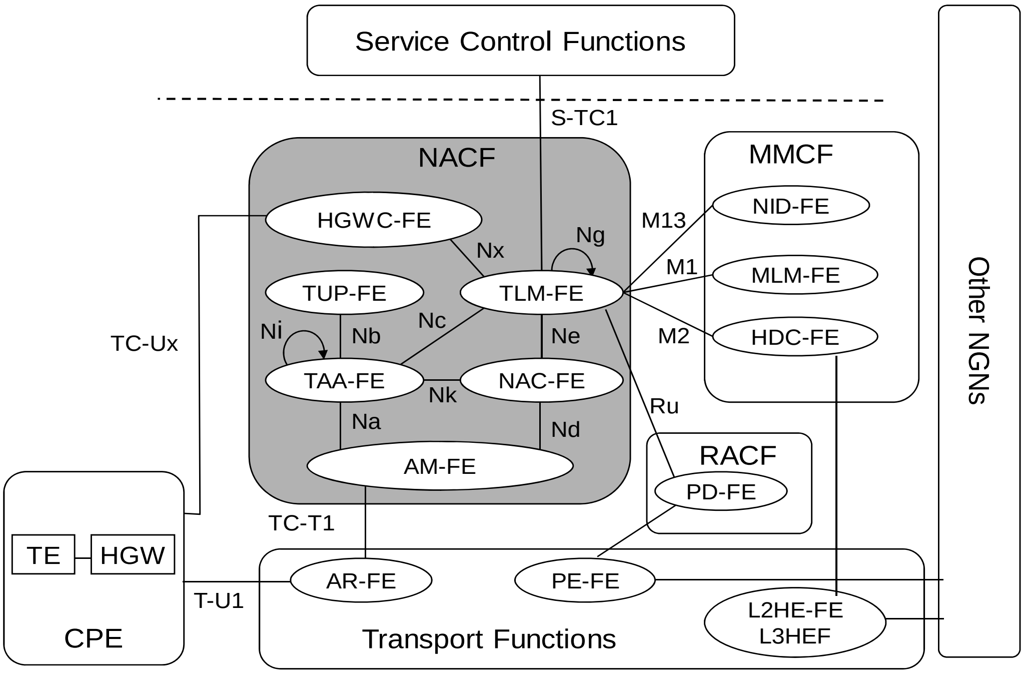


Figure II.1 – NACF functional architecture

The NACF comprises the following functional entities:

- Network access control functional entity (NAC-FE)
- Access management functional entity (AM-FE)
- Transport location management functional entity (TLM-FE)
- Transport authentication and authorization functional entity (TAA-FE)
- Transport user profile functional entity (TUP-FE)
- Home gateway configuration functional entity (HGWC-FE)

NOTE – Meaning of other terms used in Figure II.1: terminal equipment (TE), home gateway (HGW), access relay functional entity (AR-FE), policy enforcement functional entities (PE-FE), policy decision functional entity (PD-FE), network information distribution functional entity (NID-FE), mobile location management functional entity (MLM-FE), handover decision and control functional entity (HDC-FE).

Appendix III

Information flows of explicit binding and implicit binding

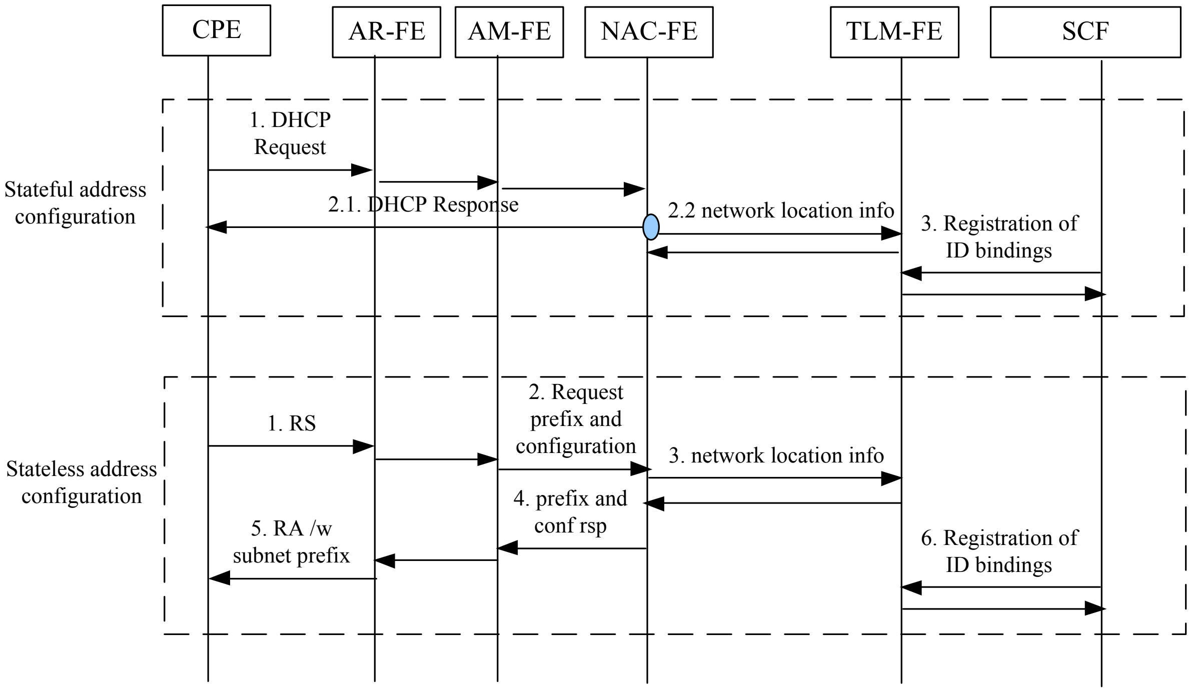
(This appendix does not form an integral part of this Recommendation.)

Figure III.1 shows the information flow of explicit binding and Figure III.2 shows the information flow of implicit binding.

In the explicit binding case, the host obtains the IPv6 address or subnet prefix as usual. Service control functions must be able to do the event registration of ID bindings when a user logs on to the service. Object ID is part of the information in this event registration request from SCF to TLM-FE via reference point S-TC1.

In the implicit binding case, the host gives the implicit indication of the service type it would like to access at the time of sending the address allocation request. The subnet ID of the prefix is allocated to the host, based on the service type information. TLM-FE can notify the SCF via reference point S-TC1 about the binding of the address and object ID without waiting for the user to log on to the service.

NOTE – S-TC1 indicates the relationship between service stratum functional entity and transport control functional entity in [ITU-T Y.2012].



CPE
AR-FE
AM-FE
NAC-FE
TLM-FE
SCF
Stateful address configuration
1. DHCP Request
2.1. DHCP Response
2.2 network location info
3. Registration of ID bindings
Stateless address configuration
1. RS
2. Request prefix and configuration
3. network location info
4. prefix and conf rsp
5. RA /w subnet prefix
6. Registration of ID bindings

Figure III.1 – Information flow of explicit binding

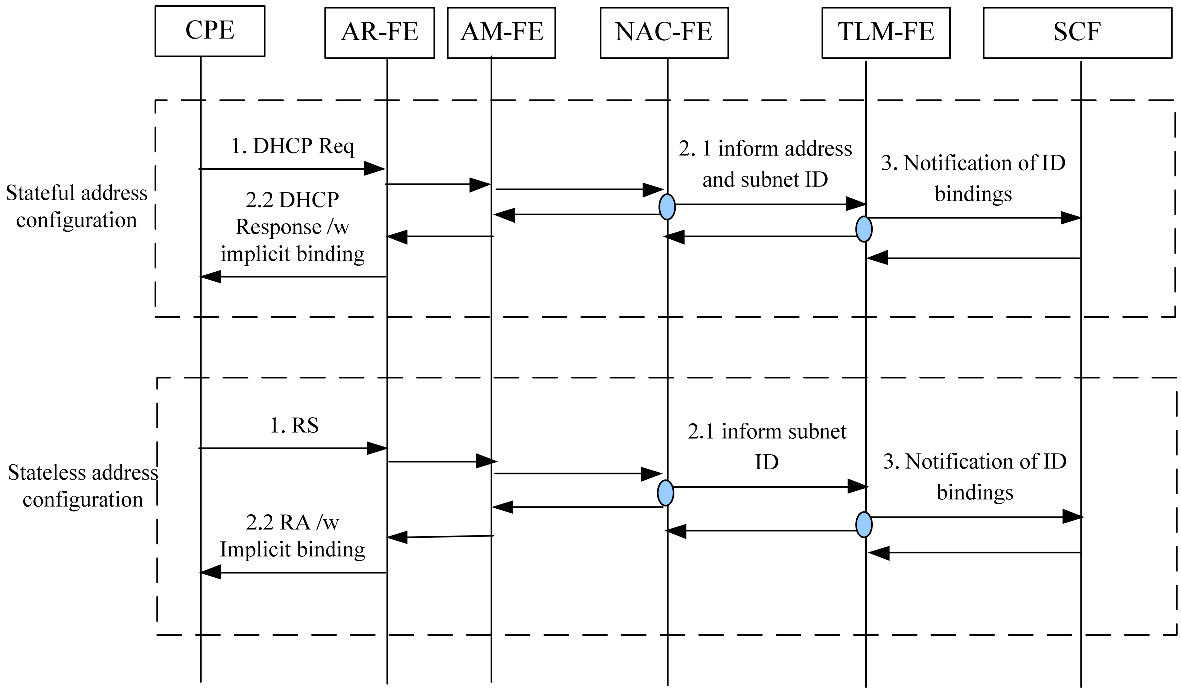

CPE
AR-FE
AM-FE
NAC-FE
TLM-FE
SCF
Stateful address configuration
1. DHCP Req
2.2 DHCP Response /w implicit binding
2. 1 inform address and subnet ID
3. Notification of ID bindings
Stateless address configuration
1. RS
2.2 RA /w Implicit binding
2.1 inform subnet ID
3. Notification of ID bindings

Figure III.2 – Information flow of implicit binding

It is noted that for stateless address configuration, only the subnet prefix is sent via the router advertisement but not the whole address. In this case, the subnet prefix could be used as an ID for transport to be bound with an object ID. If there is a requirement on finer granularity of binding, it is possible to do the binding on the address and object ID. The host generates the address based on the received subnet prefix. Then it should inform the TLM-FE about that IPv6 address it generated. Following that, TLM-FE will notify the service control function with the enhanced or detailed binding information.

Appendix IV

Examples for services using object mapping

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

Using the object processing including identification and mapping, IPv6-based NGN can provide an integrated solution for personal location and management through identification/naming/ addressing including ID registration, location tracking, dynamic mobility control, and security using the following ubiquitous networking services:

– IdM services for the management of the identity life cycle of objects including managing unique IDs, attributes, credentials, entitlements to consistently enforce business and security policies.

– Context-aware services for improving the usability and providing personalized services based on context recognition through adapting the service to the context.

– Location management services for real-time location tracking, monitoring, and information processing of moving objects similar to the supply chain management (SCM).

– Directory services for searching and retrieving information from a catalogue of well-defined objects, and domain name services for translating human-readable names into the IPv6 addresses that the network equipment needs to deliver information.

Bibliography

[b-ITU-T Y.2111] Recommendation ITU-T Y.2111 (2008), *Resource and admission control functions in next generation networks*.

[b-ITU-T Y.2201] Recommendation ITU-T Y.2201 (2009), *Requirements and capabilities for ITU-T NGN*.

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