International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.3203

(08/2011)

SERIES Q: SWITCHING AND SIGNALLING

Signalling requirements and protocols for the NGN – Signalling and control requirements and protocols to support attachment in NGN environments

Signalling requirements and architecture of network attachment control functions to support IP mobility

Recommendation ITU-T Q.3203

ITU-T Q-SERIES RECOMMENDATIONS

SWITCHING AND SIGNALLING

SIGNALLING IN THE INTERNATIONAL MANUAL SERVICE	Q.1–Q.3
INTERNATIONAL AUTOMATIC AND SEMI-AUTOMATIC WORKING	Q.4–Q.59
FUNCTIONS AND INFORMATION FLOWS FOR SERVICES IN THE ISDN	Q.60–Q.99
CLAUSES APPLICABLE TO ITU-T STANDARD SYSTEMS	Q.100–Q.119
SPECIFICATIONS OF SIGNALLING SYSTEMS No. 4, 5, 6, R1 AND R2	Q.120–Q.499
DIGITAL EXCHANGES	Q.500–Q.599
INTERWORKING OF SIGNALLING SYSTEMS	Q.600–Q.699
SPECIFICATIONS OF SIGNALLING SYSTEM No. 7	Q.700–Q.799
Q3 INTERFACE	Q.800–Q.849
DIGITAL SUBSCRIBER SIGNALLING SYSTEM No. 1	Q.850–Q.999
PUBLIC LAND MOBILE NETWORK	Q.1000–Q.1099
INTERWORKING WITH SATELLITE MOBILE SYSTEMS	Q.1100–Q.1199
INTELLIGENT NETWORK	Q.1200–Q.1699
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR IMT-2000	Q.1700–Q.1799
SPECIFICATIONS OF SIGNALLING RELATED TO BEARER INDEPENDENT CALL CONTROL (BICC)	Q.1900–Q.1999
BROADBAND ISDN	Q.2000–Q.2999
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR THE NGN	Q.3000–Q.3999
General	Q.3000–Q.3029
Network signalling and control functional architecture	Q.3030–Q.3099
Network data organization within the NGN	Q.3100–Q.3129
Bearer control signalling	Q.3130–Q.3179
Signalling and control requirements and protocols to support attachment in NGN environments	**Q.3200–Q.3249**
Resource control protocols	Q.3300–Q.3369
Service and session control protocols	Q.3400–Q.3499
Service and session control protocols – supplementary services	Q.3600–Q.3649
NGN applications	Q.3700–Q.3849
Testing for NGN networks	Q.3900–Q.3999

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

Recommendation ITU-T Q.3203

Signalling requirements and architecture of network attachment control functions to support IP mobility

Summary

The addition of IP mobility in access networks impacts the functionality of network attachment control functions (NACF), and raises additional signalling requirements of NACF with respect to the mechanism of IP address management and the signalling flows for mobility interface. Recommendation ITU-T Q.3203 proposes the generic signalling requirements and architecture for NACF functionality defined in Recommendation ITU-T Y.2014, with considerations of interfacing the mobility management functions described in Recommendation ITU-T Y.2018.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T Q.3203	2011-08-06	11

Keywords

IP mobility, NACF, NGN, signalling.

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 Q.3203

Signalling requirements and architecture of network attachment control functions to support IP mobility

1 Scope

This Recommendation describes signalling architecture and relevant interfaces of network attachment control functions (NACF) to support IP mobility in access networks, considering interaction with signalling and functionality of mobility management and control functions (MMCF) defined in [ITU-T Y.2018]. Additional signalling requirements of NACF are identified to support IP mobility in next generation access (NGA) networks, with respect to the mechanism of IP address management and the signalling flows for mobility interface. This Recommendation addresses the signalling requirements and architecture of NACF for mobility service based on [ITU-T Y.2014]. Mobility signalling of other functions (such as MMCF and resource and admission control functions (RACF)) is out of the scope of this Recommendation.

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 Q.1706] Recommendation ITU-T Q.1706/Y.2801 (2006), *Mobility management requirements for NGN*.

[ITU-T Q.1707] Recommendation ITU-T Q.1707/Y.2804 (2008), *Generic framework of mobility management for next generation networks.*

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

[ITU-T Y.2018] Recommendation ITU-T Y.2018 (2009), *Mobility management and control framework and architecture within the NGN transport stratum*.

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

[IETF RFC 4862] IETF RFC 4862 (2007), *IPv6 Stateless Address Autoconfiguration.*

3 Definition

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 handover: [ITU-T Q.1706].

3.1.2 host-based mobility: [ITU-T Y.2018].

3.1.3 network-based mobility: [ITU-T Y.2018].

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 mobility signalling: Signalling flows for delivering information related to location registration and handover management to support the mobility service.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AAA	Authentication, Authorization and Accounting
AM-FE	Access Management Functional Entity
AR-FE	Access Relay Functional Entity
CoA	Care of Address
CPE	Customer Premises Equipment
DHCP	Dynamic Host Configuration Protocol
EUI	Extended Unique Identifier
HA	Home Agent
HCF	Handover Control Function
HDC-FE	Handover Decision and Control Functional Entity
HDF	Handover Decision Function
HoA	Home Address
IP	Internet Protocol
LMA	Local Mobility Anchor
MAG	Mobile Access Gateway
MIPv4	Mobile IP for IPv4
MIPv6	Mobile IP for IPv6
MLM-FE	Mobile Location Management Functional Entity
MLM-FE(C)	An instance of the MLM-FE performing the central mobile location management role
MLM-FE(P)	An Instance of the MLM-FE performing the proxy mobile location management role
MMCF	Mobility Management and Control Function
MN	Mobile Node
NACF	Network Attachment Control Functions
NAC-FE	Network Access Configuration Functional Entity
NGN	Next Generation Network
NID-FE	Network Information Distribution Functional Entity
PIA	Persistent IP Address
PMIP	Proxy Mobile IP
PMIPv6	Proxy MIPv6

RA	Router Advertisement
RACF	Resource and Admission Control Functions
TAA-FE	Transport Authentication and Authorization Functional Entity
TIA	Temporary IP Address
TLM-FE	Transport Location Management Functional Entity
TUP-FE	Transport User Profile Functional Entity
UE	User Equipment

5 Conventions

This Recommendation does not use specific conventions.

6 Overview of protocol supporting IP mobility on the NGN access network

This Recommendation describes the signalling requirements and architecture of the network attachment control function (NACF) for both host- and network-based mobility management that rely on the signalling and functionality of the mobility management and control function (MMCF) added to support mobility management in the next generation network (NGN) transport stratum. NACF gives information about mobility management to MMCF, which is responsible for mobile location management and handover control.

In the IETF-based network architecture, two entities are generally considered to support IP mobility: a home agent (HA) and an access gateway. The home agent manages IP addresses in addition to mobile-user profiles, and it delivers packets to mobile nodes (MN). In the case of network-based mobility management, the access gateway detects a user's movement to a new network and registers the user's care of address (CoA) with the HA. This approach does not require any additional protocol for the MN to support IP mobility. However, in the case of host-based mobility management, users have to configure their new CoA. Whenever a user moves to a new network, the user configures its CoA and then registers it with the home agent. Appendix I describes the network architecture based on IETF mobile protocols.

The NGN mobility architecture, including components of NACF and MMCF, possibly applies to the general mobility architecture. In the NGN architecture model, NACF is responsible for allocating the IP address and performing authentication. NACF allocates two kinds of IP addresses: a persistent IP address (PIA) and a temporary IP address (TIA), and updates the UE's temporary IP address with the MMCF for mobility service. The NACF can optionally perform an authentication process when the UE changes network.

6.1 Network architecture

The MMCF defined in [ITU-T Y.2018] is required for mobility service in the NGN transport stratum [ITU-T Q.1707]. Also, mobility-specific transport functions are needed in the forwarding plane of the transport stratum, as shown in Figure 6.1. In the control plane, NACF has interaction with MMCF to transfer mobility service parameters.

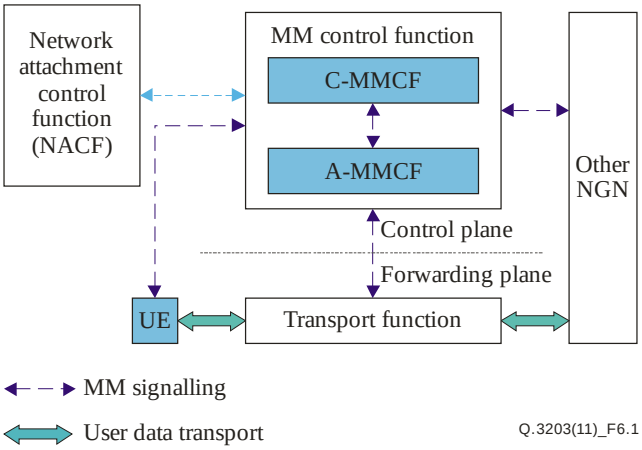

Figure 6.1 – Relationship between NACF and MMCF for IP mobility (see [ITU-T Q.1707] and [ITU-T Y.2014])

6.2 Host configuration

The UE initially sets its persistent IP address (PIA) with either a stateless or a stateful configuration. When using a stateless configuration, known as autoconfiguration based on [IETF RFC 4862], the UE builds an EUI-64-formatted IPv6 address using a network prefix contained in router advertisements (RAs) from transport function. In a stateful configuration, the IP address for PIA is obtained from a DHCP server. When an attachment between NACF and the mobile UE initially occurs, its PIA configuration is executed. Once a mobile UE has configured its IP address, it maintains its IP address within a home-agent domain. In the case of host-based mobility, the mobile node has to configure its temporary IP address (TIA) in addition to its PIA, while in the case of network-based mobility, the mobile node has its PIA maintained as user profile information. Whenever the mobile node is attached to a different access network, the mobile UE configures its TIA in a stateful or stateless manner (see clause 7.3.1).

During the attachment process, mobility authentication is also performed between the mobile UE and the NACF. Either the pre-authentication or the re-authentication method may be used to reduce authentication latency. In a host-based mobility case, the information derived from the UE authentication process is transferred from NACF to MMCF. Otherwise, NACF indicates the network-based mobility service to MMCF.

6.3 Handover management

The MMCF has handover control functions (HCFs) which provide session continuity for the mobile UE's sessions. The HCF concentrates on minimizing data loss and handover latency during the UE's movement. Also, the forwarding plane of the transport stratum performs the handover execution function to support IP mobility.

7 Mobility signalling requirements of NACF

7.1 Data structure

The mobility service parameters required to extend NACF for IP mobility are defined in [ITU-T Y.2014]; mobility service parameters consist of MLM-FEs' addresses, keying material, mobility protocol type (e.g., host-based or network-based mobility), an optional anchor point address, and an optional tunnel end point address.

In the access authentication procedure, shown in Figure 7, AM-FE obtains an identifier from a UE and requests a mobile UE's authentication to TAA-FE. TAA-FE receives the mobile UE's policy profile from TUP-FE through Nb reference point. A user profile may be downloaded from

the TAA-FE server in the home NGN network to the TAA-FE proxy in the visited NGN network. The TAA-FE responds to the AM-FE with the mobile node's policy profile. User data related to network location information in the policy profile may be transferred between TAA-FE and TLM-FE via the Nc reference point.

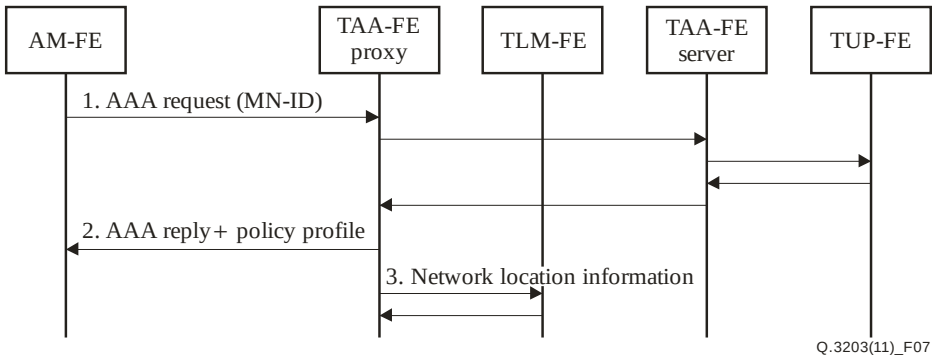

Figure 7 – NACF information flow for access authentication

7.2 Movement detection

Handover decision can be made by either the mobile node or the handover decision and control functional entity (HDC-FE) in MMCF. After the network attachment point is determined, the mobile node performs authentication for the target access network. When a user attaches to the target network, AM-FE forwards the user's authentication request to TAA-FE.

NACF may provide pre-authentication and re-authentication to reduce the handover latency. The user transport profile and mobility service parameters are sent from the TAA-FE in the home network to the TAA-FE in the target network. The mobility service parameters include the UE's PIA and the address of the MLM-FE (C). TAA-FE delivers mobility service parameters, including the keying material used between the mobile user and the MLM-FE (P), to TLM-FE.

7.3 Location registration

7.3.1 IP address allocation

During the authentication procedure, TAA-FE may request an IP address allocation to NAC-FE or use the IP address of user profile information in TUP-FE. After authentication, the user profile, including mobility service parameters, is delivered to TLM-FE. In the case of network-based mobility, only an IP address maintained in TUP-FE is used for IP configuration, and in the case of host-based mobility, NAC-FE delivers the allocated IP address to TLM-FE.

To communicate between the user and MLM-FE (P) in the target network, TLM-FE provides the address of the MLM-FE (P) as well as the user's IP address and keying material for the security associations between the user and MLM-FE (P), as well as HDC-FE and NID-FE. The TLM-FE stores the association between the allocated IP address and related network location information, including the mobility service parameters. TLM-FE also delivers mobility service parameters to NAC-FE after notification of binding information to MLM-FE.

7.3.2 Notification of binding information

In the host-based mobility service, a mobile node directly updates location information to MLM-FE (P). NAC-FE may bind the information between the mobility service subscriber ID and the persistent/temporary IP addresses. TLM-FE then sends the binding information to the MLM-FE (P): the user identity, the type of mobility service, and keying materials. However, TLM-FE delivers the indication of network-based mobility without keying material to MLM-FE (P). In the case of network-based mobility, the user has only the persistent address and no security association with MLM-FE (P).

8 NACF signalling architecture and interfaces for IP mobility

This clause describes the details of the NACF signalling architecture for IP mobility, including the functional entities and interfaces.

Figure 8.1 shows reference points between NACF and MMCF as defined in [ITU-T Y.2018].

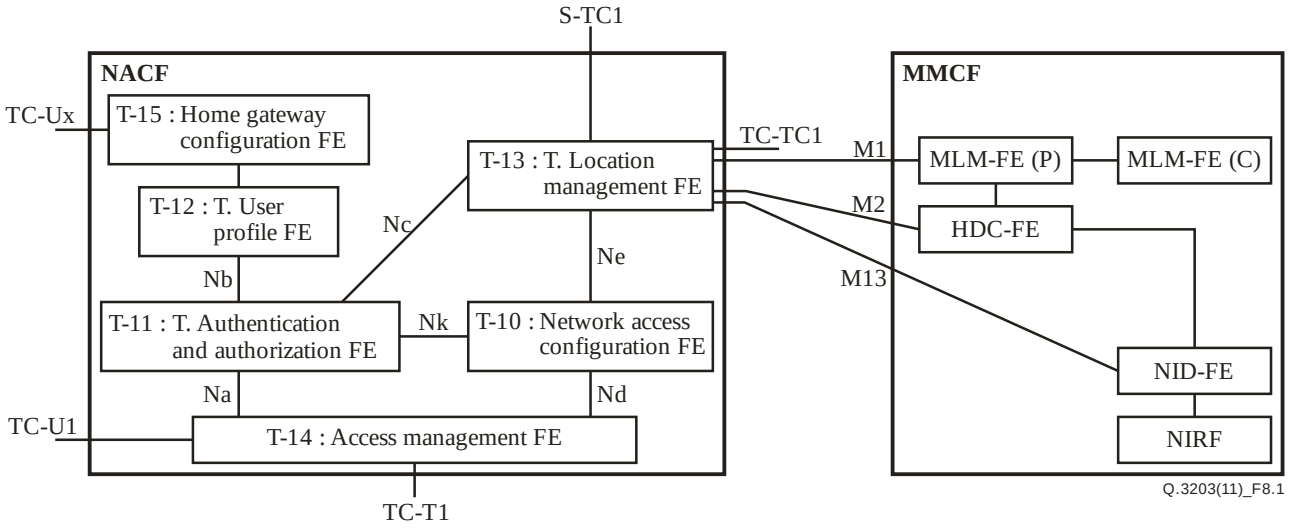

Figure 8.1 – Functional entities and reference points of NACF

8.1 Functional entities of NACF

The following FEs of NACF are involved in the mobility service:

- T-10 Network access configuration functional entity (NAC-FE)
- T-11 Transport authentication and authorization functional entity (TAA-FE)
- T-13 Transport location management functional entity (TLM-FE)

In order to support mobility defined in [ITU-T Y.2014], NAC-FE allocates two kinds of IP addresses to UE: persistent IP address (PIA) and temporary IP address (TIA). NAC-FE allocates IP addresses in association with TAA-FE, when the address allocation is needed during the UE's movement, in order to provide authentication.

TAA-FE may request NAC-FE to allocate an IP address in the case of host-based mobility, and it may use an IP address or IP prefix as user-profile information maintained in TUP-FE in both host-based and network-based mobility cases (see clause 7.2.4 of [ITU-T Y.2014]).

TLM-FE identifies the current network location of UE and keeps track of it. When the point of attachment is changed in the network, the TLM-FE updates the association between the IP address allocated to the UE and related network location information (see clause 7.2.3 of [ITU-T Y.2014]).

8.2 Relevant reference points

The following external reference points between NACF and MMCF are defined for the mobility service:

- M1 (TLM-FE, MLM-FE)
- M2 (TLM-FE, HDC-FE)
- M13 (TLM-FE, NID-FE)

The following internal reference points of NACF are extensively defined for mobility service:

- Nc (TAA-FE, TLM-FE)
- Ne (NAC-FE, TLM-FE)

8.3 Interface description

This clause provides the description of the relevant reference points and interfaces listed in clause 8.2.

8.3.1 M1

This reference point is for the distribution of information from TLM-FE to MLM-FE (P). The information is prepared through the internal procedures of NACF, as follows:

1) TLM-FE obtains persistent/temporary address from NAC-FE.
2) TAA-FE delivers the profile information, including mobility-service parameters as well as the address of MLM-FE (P), to the TLM-FE.
3) In the case of host-based mobility, TLM-FE obtains keying material from TAA-FE for the security associations between UE and MLM-FE (P).
4) In the case of network-based mobility, TLM-FE obtains the address of MLM-FE(C) and the address of tunnel end-point from TAA-FE.

TLM-FE informs MLM-FE (P) of mobile-user ID, persistent-IP address, and anchor-point address (the tunnel-end-point address) in addition to the information listed from 1 to 4. Optionally, binding information between the mobility-service-user ID and persistent-IP address, as well as the type of mobility protocol (e.g., host-based or network-based mobility service) can be included in the information.

8.3.2 M2

This reference point is for providing information from TLM-FE to HDC-FE, to support the security association required between the handover decision function (HDF) and the UE. The TLM-FE sends information including mobility-service-user ID and keying material to the HDC-FE.

The M2 interface is used for information flow providing the keying material derived from the UE authentication procedure.

8.3.3 M13

This reference point is for providing information from TLM-FE to the network information distribution functional entity (NID-FE) to support the security association. The TLM-FE sends information to the NID-FE, including-mobility-service-user ID and keying material.

M13 interface is used for the information flow providing the keying material derived from the UE authentication procedure.

8.3.4 Nc

The Nc reference point, between TAA-FE and TLM-FE, is extended for the mobility service according to [ITU-T Y.2014] to support TLM-FE for the location registration to MMCF. The procedures described in clause 8.3.1 show the information required for the provisioning of the TLM-FE, such as the address of MLM-FE, mobility protocol type, anchor point address, and the security association between UE and MMCF. This interface is extended in the format of transport resource information indication and transport resource information response information flows, from TAA-FE to TLM-FE.

8.3.5 Ne

The Ne reference point is extended for the mobility service according to [ITU-T Y.2014] to deliver mobility-service parameters between NAC-FE and TLM-FE. NAC-FE registers TLM-FE with the binding information between the mobility-service subscriber ID and persistent/temporary IP addresses. The TLM-FE informs the NAC-FE of the UE's PIA, mobility-protocol type, the address of MLM-FE(P), and keying material for the security associations between the UE and the MMCF. This interface is extended in the format of the mobility-service parameters indication information flow, from TLM-FE to NAC-FE.

9 Security considerations

Security requirements within the functional requirements and architecture of NACF are addressed by the security requirements for NGN [ITU-T Y.2701]. Interfaces of NACF related to the mobility service shall follow the security requirements of NACF.

Appendix I

Mapping to IETF mobility architecture

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

IETF has worked on IP mobility protocols, such as MIPv4 ([b-IETF RFC 3344]), MIPv6 ([b-IETF RFC 3775]), and proxy mobile IP (PMIP) ([b-IETF RFC 5213]). Generally, mobility architecture includes two physical entities in IP networks: a home agent and an access gateway (Figure I.1). The home agent is linked to all access gateways and manages user location information and profiles. The home agent can also be located in some access gateways. In this case, the function of the home agent is distributed to access gateways; access gateways have the function of the home agent in addition to their own function. The access gateway detects user movement to a new IP network. In the network-based mobility case, an IP address of the access gateway is used as a mobile node's CoA, so that packets destined to the mobile node are delivered to the access gateway on behalf of the mobile node. Then, the access gateway directly transfers them to the mobile node that just has an IPv6 specification. Within a domain, one home agent exists and more than one home agent will be considered in the future. However, in the case of host-based mobility, a mobile node has its own HoA and CoA and receives packets directly from the home agent or a sender.

NACF is responsible for IP address management and authentication to support IP mobility as some parts of access gateway functionality. MMCF can perform control parts of functions in both the home agent and access gateways, as it manages mobile node binding information.

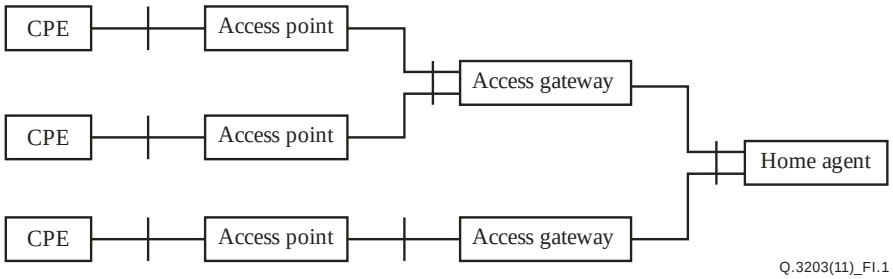

Figure I.1 – Network architecture for IP mobility

Appendix II

Mapping to PMIP domain

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

A mobile node in a proxy mobile IP (PMIP) domain is generally identified by an identifier (MN-Identifier) that has an associated policy profile. This information is typically configured in an AAA server. When a user accesses the network, the network needs to authenticate the user. NGN functions related to the access authentication in PMIP are shown in Figure II.1.

Figure II.1 – Functional architecture for access authentication

The data related to access authentication includes the subscriber identity, supported authentication methods, and authentication keys. Additionally, user data defined in the policy profile are needed in order to support PMIP [b-IETF RFC 5213]. The network entities in the PMIP domain have access to the mobile node's policy profile that contains the operational parameters required by the network entities for managing the mobile node's mobility service. Network entities, such as the mobile access gateway (MAG) and the local mobility anchor (LMA), can query this information using RADIUS [b-IETF RFC 2865] or DIAMETER [b-IETF RFC 3588] protocols.

The policy profile has two mandatory fields and other optional fields, as shown in Table II.1. TUP-FE stores this information for policy profile in PMIP and may permanently store two of their mandatory parameters. Additional user data for the policy profile can be added to the transport-user profile described in [b-ITU-T Q-Sup. 58]. The network entities in a PMIP domain can identify a mobile using its MN-Identifier obtained as part of the access authentication. The MN-Identifier may be the same as the user identifier (Subscriber ID), unless it is used from more than one mobile node operating in the same PMIP domain.

Table II.1 – Mobile node's policy profile

Field	Attribute	TUP-FE
The mobile node's identifier (MN-Identifier)	Mandatory	Permanent
The IPv6 address of the local mobility anchor (LMAA)	Mandatory	Permanent
The mobile node's IP home network prefix(es)	Optional	
The mobile node's IP home network prefix lifetime	Optional	
Permitted address configuration mode (stateful, stateless, or both)	Optional	

Appendix III

Mapping IPv6 user configuration for the mobility service

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

III.1 Initial allocation of IP address

A mobile CPE in the access network domain can configure one or more IP addresses on its interface using IPv6 stateless or stateful address autoconfiguration procedures. When stateless address autoconfiguration is supported on the link, the mobile node can generate one or more IPv6 addresses by combining the network prefix advertised on the access link with an interface identifier. When stateful address autoconfiguration is supported on the link, the mobile node obtains the address configuration from the DHCPv6 server using DHCPv6 client protocol.

III.2 Interaction with DHCP relay agent

If stateful address configuration using DHCP is supported on the link on which the mobile node is attached, the DHCP relay agent needs to be configured on the access router (e.g., AM-FE function in NACF). When the mobile node sends a DHCPv6 Request message, the relay agent function on the AM-FE must set the link-address field in the DHCPv6 message to the mobile node's local home network prefix, so as to provide a prefix hint to the DHCP server. Since the access link is a point-to-point link with the configured mobile node's prefix as the on-link prefix, the normal DHCP relay agent configuration on the AM-FE will ensure that the prefix hint is set to the mobile node's home network prefix.

If the mobile node is IPv4 enabled, the mobile CPE after the access authentication will be able to obtain the IPv4 address configuration for the connected interface by using DHCPv4.

III.3 IPv6 address autoconfiguration

Functions related to the IP address allocation are shown in Figure III.1. CPE communicates with NACF via the AR-FE in the transport functions. T-U1 and TC-T1 reference points are related to the IP address allocation. The T-U1 reference point enables the CPE to initiate requests for IP address allocation and other network configuration parameters. These requests are received by the AR-FE and are relayed to the AM-FE in NACF via the TC-T1 reference point. These reference points also provide transport IP address and network configuration information to the CPE for connecting to the network. Either DHCP or PPP is used as a method for IP address allocation and network configuration.

Figure III.1 – Functional architecture for IP address allocation

However, IPv6 defines both stateful address configuration and stateless address autoconfiguration, which requires no manual configuration of hosts. The stateless mechanism allows a host to generate its own addresses using a combination of locally available information and information advertised by routers. Both stateless address autoconfiguration and dynamic host configuration protocol for IPv6 (DHCPv6) [b-IETF RFC 3315] may be used simultaneously.

In the case of IPv6 stateless address allocation, a CPE does not use DHCP for manual configuration. Instead, CPE generates its own address using subnet prefixes advertised by routers. As NACF is not involved in the IPv6 stateless address configuration, the NAC-FE cannot maintain a mapping between the CPE and the assigned IP address and cannot forward this information to the TLM-FE, causing the TLM-FE not to respond to location queries from service control functions. In the case of autoconfiguration, an additional information flow is needed in order to register a CPE's IPv6 address to NACF via T-U1 and TC-T1 reference points. When a CPE connects to the network, it can use DHCPv6 [b-IETF RFC 3315] for IPv6 address allocation via T-U1 and TC-T1 reference points, or can configure its own address using IPv6 stateless address autoconfiguration. After an autoconfiguration process, the CPE registers its IPv6 address information to NACF.

IPv6 stateless address autoconfiguration mechanism [IETF RFC 4862] defines two functions mapped to the NGN functional architecture:

- The Host is a function of the CPE that autoconfigures its IPv6 address.
- The Router is a function of transport functions in charge of advertising network information.

As shown in Figure III.2, router solicitation (RS) and router advertisement (RA) are transmitted between the Host and the Router.

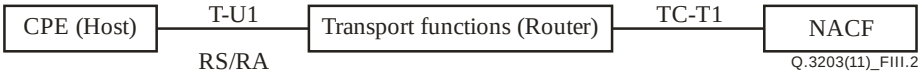

Figure III.2 – IPv6 autoconfiguration functional entities

Registration of the binding information between a configured IPv6 address and a CPE is needed via T-U1 and TC-T1 reference points. Table III.1 describes the elements contained in the registration information flow.

Table III.1 – Registration (CPE → NACF)

Information element	Description
Globally unique IP address information	A set of IP address information used for locating the access network to which the CPE is attached.
– Unique IP address	The IP address configured to the attached CPE.
– Address realm	The addressing domain in which the IP address is significant.
Physical connection identifier (optional)	A local identifier for physical connection of the access transport network to which the CPE is attached.
Logical connection identifier	A local identifier for logical connection of the access transport network to which the CPE is connected.
CPE type (optional)	The type of CPE.

The IPv6 stateful address allocation process can be completed by using DHCP messages. In DHCP mode, the transport functions include an AR-FE acting as a DHCP relay between the DHCP clients in the CPE and the DHCP server in NACF (see Figure III.3). To newly support IPv6 stateless address autoconfiguration, an additional registration flow is needed between a CPE and NACF. The CPE registers address information to the NAC-FE, after the CPE configures its own IPv6 address. This information is received by AR-FE and then relayed to the AM-FE via T-U1 and TC-T1 reference points.

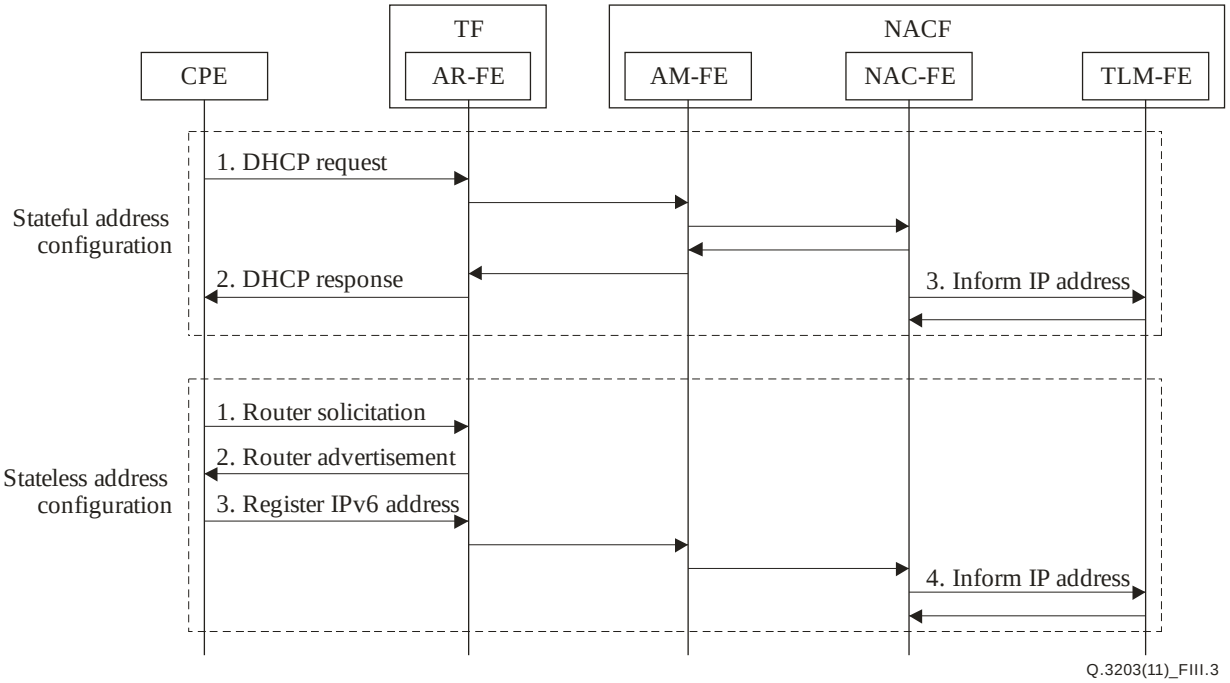

Figure III.3 – IPv6 address allocation flows

Bibliography

[b-ITU-T Q.1708] Recommendation ITU-T Q.1708/Y.2805 (2008), *Framework of location management for NGN*.

[b-ITU-T Q-Sup. 58] ITU-T Q-series Recommendations – Supplement 58 (2008), *Organization of NGN transport user data*.

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

[b-IETF RFC 2865] IETF RFC 2865 (2000), *Remote Authentication Dial In User Service (RADIUS)*.

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

[b-IETF RFC 3344] IETF RFC 3344 (2002), *IP Mobility Support for IPv4*.

[b-IETF RFC 3588] IETF RFC 3588 (2003), *Diameter Base Protocol*.

[b-IETF RFC 3775] IETF RFC 3775 (2004), *Mobility Support in IPv6*.

[b-IETF RFC 5213] IETF RFC 5213 (2008), *Proxy Mobile IPv6*.

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