ACKNOWLEDGEMENT

By utilizing this website and/or documentation, I hereby acknowledge as follows:

Effective October 1, 2012, QUALCOMM Incorporated completed a corporate reorganization in which the assets of certain of its businesses and groups, as well as the stock of certain of its direct and indirect subsidiaries, were contributed to Qualcomm Technologies, Inc. (QTI), a wholly-owned subsidiary of QUALCOMM Incorporated that was created for purposes of the reorganization.

Qualcomm Technology Licensing (QTL), the Company's patent licensing business, continues to be operated by QUALCOMM Incorporated, which continues to own the vast majority of the Company's patent portfolio. Substantially all of the Company's products and services businesses, including QCT, as well as substantially all of the Company's engineering, research and development functions, are now operated by QTI and its direct and indirect subsidiaries[1]. Neither QTI nor any of its subsidiaries has any right, power or authority to grant any licenses or other rights under or to any patents owned by QUALCOMM Incorporated.

No use of this website and/or documentation, including but not limited to the downloading of any software, programs, manuals or other materials of any kind or nature whatsoever, and no purchase or use of any products or services, grants any licenses or other rights, of any kind or nature whatsoever, under or to any patents owned by QUALCOMM Incorporated or any of its subsidiaries. A separate patent license or other similar patent-related agreement from QUALCOMM Incorporated is needed to make, have made, use, sell, import and dispose of any products or services that would infringe any patent owned by QUALCOMM Incorporated in the absence of the grant by QUALCOMM Incorporated of a patent license or other applicable rights under such patent.

Any copyright notice referencing QUALCOMM Incorporated, Qualcomm Incorporated, QUALCOMM Inc., Qualcomm Inc., Qualcomm or similar designation, and which is associated with any of the products or services businesses or the engineering, research or development groups which are now operated by QTI and its direct and indirect subsidiaries, should properly reference, and shall be read to reference, QTI.

[1] The products and services businesses, and the engineering, research and development groups, which are now operated by QTI and its subsidiaries include, but are not limited to, QCT, Qualcomm Mobile & Computing (QMC), Qualcomm Atheros (QCA), Qualcomm Internet Services (QIS), Qualcomm Government Technologies (QGOV), Corporate Research & Development, Qualcomm Corporate Engineering Services (QCES), Office of the Chief Technology Officer (OCTO), Office of the Chief Scientist (OCS), Corporate Technical Advisory Group, Global Market Development (GMD), Global Business Operations (GBO), Qualcomm Ventures, Qualcomm Life (QLife), Quest, Qualcomm Labs (QLabs), Snaptracs/QCS, Firethorn, Qualcomm MEMS Technologies (QMT), Pixtronix, Qualcomm Innovation Center (QuIC), Qualcomm iSkoot, Qualcomm Poole and Xiam.

Data Services Aspects for E-UTRA/eHRPD/1xRTT Mobility

Feature Definition Document

80-VR258-1 B

July 25, 2012

Submit technical questions at:
https://support.cdmatech.com/

Qualcomm Confidential and Proprietary

QUALCOMM Incorporated
5775 Morehouse Drive
San Diego, CA 92121-1714
U.S.A.

Contents

Figures

Tables

Revision history

Revision	Date	Description
A	Nov 2010	Initial release
B	Jul 2012	Updated Table 1-1, Chapter 2, Chapter 5, Chapter 6, Chapter 8, Chapter 9, and Chapter 11; added Chapter 13, Chapter 14, and Chapter 15

1 Introduction

1.1 Purpose

This document describes the data services aspects for Evolved UMTS Terrestrial Radio Access (E-UTRA) and evolved High-Rate Packet Data (eHRPD) mobility.

1.2 Scope

This document is intended for operators, infrastructure vendors, test equipment vendors, and other partners who are interested in the Qualcomm LTE/eHRPD/1xRTT Packet Data Mobility solution. Mappings between the LTE/eHRPD/1xRTT Packet Data Mobility features and AMSS software releases are not covered in this document.

Table 1-1 shows the Multimode Packet Data feature breakdown.

NOTE: The following table has been updated.

Table 1-1 Multimode Packet Data feature breakdown

Feature number	Feature	Subfeature number	Subfeature
1	Authentication	A	EAP-AKA-based authentication for eHRPD
		B	Legacy CHAP-based authentication for 1xRTT and HRPD
		C	EPS-AKA-based service authentication for LTE
2	IP address allocation	A	PDN connection establishment procedures
		B	One or more IPv4/IPv6 address allocations through one or more VSNCP procedures
		C	RS and RA support
		D	IPv4/IPv6 traffic support
		E	Simple IP support over eHRPD personality and client MIP support over non-eHRPD personality based on client capability at the UE
		F	Deferred IP address assignment through Dynamic Host Configuration Protocol (DHCP)

Feature number	Feature	Subfeature number	Subfeature
		G	PCO in VSNCP ▪ DNS address ▪ P-CSCF address request
		H	Multiple PDN support, VSNP support for PDN multiplexing on 9xFF flow data path
3	QoS support	A	UE-initiated QoS configuration
		B	Network-initiated QoS configuration
		C	QoS support over IPv4/IPv6
		D	Coexistence of UE-initiated and network-initiated QoS flows
		E	QoS API and interactions with applications
		F	QoS maintenance during UE IRAT transitions
4	UE-based PDN inactivity triggered PDN disconnect		
5	Data call throttling and blocking functions	A	IPv4 address request throttling
		B	IPv5 address request throttling
		C	IPv4+IPv5 address request throttling
6	APN enable/disable functions		
7	Dual-IP bearer support		
8	eHRPD to E-UTRA transitions with packet session continuity		
9	E-UTRA to eHRPD transitions with packet session continuity		
10	1xRTT/HRPD to E-UTRA transitions with packet session continuity		
11	E-UTRA to 1xRTT/HRPD transitions with packet session continuity		
12	Tethered mode operation	A	DUN
		B	Qualcomm Modem Interface (QMI)
13	eHRPD preregistration on LTE		

1.3 Conventions

Function declarations, function names, type declarations, and code samples appear in a different font, e.g., `#include`.

Code variables appear in angle brackets, e.g., `<number>`.

Commands to be entered appear in a different font, e.g., **`copy a:*.* b:`**.

Button and key names appear in bold font, e.g., click **Save** or press **Enter**.

Keys that are pressed in combination are indicated with a plus sign, e.g., press **Ctrl+C**.

Shading indicates content that has been added or changed in this revision of the document.

1.4 References

Reference documents, which may include Qualcomm, standards, and resource documents, are listed in Table 1-2. Reference documents that are no longer applicable are deleted from this table; therefore, reference numbers may not be sequential.

Table 1-2 Reference documents and standards

Ref.	Document	
Qualcomm		
Q1	*Application Note: Software Glossary for Customers*	CL93-V3077-1
Q2	*eHRPD Feature Definition Document*	80-VM260-2
Q3	*Long Term Evolution (LTE/FDD) Fundamentals*	80-W1738-1
Q4	*Out of Service (OoS) Based Inter-RAT Mobility Feature Definition Document*	80-VR257-1
Q5	*Qualcomm MSM™ Interface (QMI) Architecture*	80-VB816-1
Q6	*RM Network (RmNet) Feature Description Document*	80-VT270-1
Q7	*Packet Data Origination Throttling*	80-V0934-1
Q8	*Quality of Service (QoS) Feature for 1xEV-DO Revision A*	80-VB296-1
Q9	*Long Term Evolution (LTE) Protocols (Release 2.0) Feature Definition Document*	80-VR580-1
Standards		
S1	*3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) Enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) Access (Release 8)*	3GPP TS 23.401 V8.1.0 (2008-03)
S2	*3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Mobile Radio Interface Layer 3 Specification; Core Network Protocols; Stage 3 (Release 8)*	3GPP TS 24.008 V8.5.0 (2009-03)
S3	*3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Non-Access-Stratum (NAS) Protocol for Evolved Packet System (EPS); Stage 3 (Release 8)*	3GPP TS 24.301 V8.1.0 (2009-03)
S4	*3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE): Security Architecture; (Release 8)*	3GPP TS 33.401 V8.3.1 (2009-03)
S5	*E-UTRAN – eHRPD Connectivity and Interworking: Core Network Aspects*	3GPP2 X.S0057-0 (2009-04)
S6	*3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Architecture Enhancements for non-3GPP Accesses*	3GPP TS 23.402
S7	*Point-to-Point Protocol (PPP) Vendor Protocol*	IETF RFC 3772
S8	*PPP Authentication Protocols*	RFC1334
S9	*PPP Challenge Handshake Authentication Protocol (CHAP)*	RFC1994
S10	*Mobile Radio Interface Layer 3 Specification; Core Network Protocols; Stage 3*	

1.5 Technical assistance

For assistance or clarification on information in this guide, submit a case to Qualcomm CDMA Technologies at https://support.cdmatech.com/.

If you do not have access to the CDMATech Support Service website, register for access or send email to support.cdmatech@qualcomm.com.

1.6 Definitions and acronyms

For definitions of terms and abbreviations, see [Q1]. The following terms are specific to this document:

- EPS bearer – Uniquely identifies an SDF aggregate between a UE and a PDN gateway (GTP S5/S8) or between a UE and the SGW (PMIP S5/S8)
- Flow profile ID –Scalar value that represents the QoS characteristics of an IP flow in a 3GPP2 access system
- Mixed mode – EPC-capable access system supporting both UE-initiated and network-initiated QoS
- PDN context – Association between a UE represented by one IPv4 address and/or one IPv6 prefix/address, and a PDN represented by an APN
- QoS context – QoS flow represents an IP flow characterized by an IP filter, TFT, associated with a specific set of QoS parameters
- SDF – In E-UTRA, SDF represents an IP flow characterized by an IP filter, TFT, associated with a specific set of QoS parameters
- Packet filter – Set of rules to separate specific packets in a data stream; e.g., specific fields in the packet header must match specific values or value ranges
- TFT – Traffic Flow Template
- Radio bearer – Bearers established over the radio link to carry signaling and data packets between the device and the RAN
- IP bearer – Bearers established between the device and the gateway, e.g., PDSN and PDN-GW, that connects the cellular network to the IP core network and the carrier user plane data; IP bearer is the EPS bearer for LTE
- Bearer – Consists of radio and IP bearers together and is applicable only in Connected mode
- Single Address Default Bearer (SADB) – Up to a maximum of two bearers established between the device and gateway associated with a given APN covering the radio and IP bearers and allowing for support of IPv4 and IPv6 traffic, each over an independent bearer
  - Option 1: SADB – One bearer is possible, SADB-1B; the UE is allowed only one IPv4 or IPv6 assignment for that APN; only one SADB can be supported for the given APN
  - Option 2: SADB – Two bearers are possible, SADB-2B; independent PDN connectivity procedures need to run for IPv4 and IPv6; IPv4 and IPv6 bearers can each be established independently; up to two SADB can be supported for the given APN; releasing the IPv4 bearer releases the IPv4 context and does not impact the IPv6 context

- Dual Address Default Bearer (DADB) – Bearer established between the device and gateway associated with a given APN covering the radio bearer and an IP bearer and allowing support of both IPv4 and IPv6 traffic; a single PDN connectivity procedure is used for both IPv4 and IPv6

NOTE: Both IPv4 and IPv6 addresses are supported on this bearer and the IPv4 address can be deferred. When this bearer is released, both IPv4 and IPv6 contexts are released. IPv6 deferred assignment is not supported, per [S6].

This concept can be extended to eHRPD in reference to the IP bearer alone, as a single 0xFF reservation is used to carry all BE traffic at the radio level and applies when both IPv4 and IPv6 are established with a single VSNCP connection.

- Dual-IP stack – Support of both IPv4 and IPv6 IP addresses simultaneously; does not imply support of IPv4 and IPv6 address association with a single APN, just the capability to support both IPV4 and IPv6 address assignments
- Default APN – When the device does not specify the APN as part of PDN connection procedures, the APN selected by the network is referred to as the default APN; device may also explicitly specify the default APN in PDN connect procedures
- Default PDN-GW – PDN-GW associated with the default APN
- Application profile – Profiles stored in the AMSS that provide the required parameters for the application to associate with the network, e.g., stores the APN, IPv4, and/or IPv6 association requirement, PCO parameters, etc.; each application profile is identified through an application profile identifier used by the application to indicate the desired application profile required by the application

  One or more apps can request association with the network based on a given application profile. When an application profile is not specified by the application, the default application profile is used by the AMSS to associate the application with the network.
- Default application profile – Single application profile defined in the AMSS that is used by the AMSS to associate as part of the initial attach procedures for LTE and for associating with the network when the application initiates an IP connection without providing a specific application profile
- Default bearer – Radio and IP bearer created with each PDN connection; the default bearer is deleted only when the PDN connection is disconnected; there is a one-to-one mapping between the radio and the IP bearer for LTE; for eHRPD, a single radio flow is associated with the 0xFF reservation that carried the default bearer traffic for all IP flows
- Default QoS – QoS provided over the default bearer; although the default bearer is typically carried as BE traffic, it may also be associated with grades of QoS, e.g., based on subscriptions such as gold, silver, and bronze classifications
- Dedicated bearer – QoS flow explicitly created with an independent radio bearer that meets required QoS metrics, along with the associated IP level filters that define IP packets that must be filtered in this QoS flow; for LTE, there is a one-to-one mapping between the IP/QoS flows and the radio bearer; also typically true for eHRPD, although multiple QoS IP filters could be mapped to a single radio bearer (QoS reservation label); QoS flows creation can be triggered either from the UE or by the network

1.6.1 Keyword conventions

The key words must, must not, required, shall, shall not, should, should not, recommended, may, and optional in this specification are to be interpreted as follows:

- Must, required, or shall – These words mean that the definition is an absolute requirement of the specification.
- Must not – This phrase, or the phrase shall not, means that the definition is an absolute prohibition of the specification.
- Should or recommended – These words mean that there may exist valid reasons under certain circumstances to ignore a particular item, but the full implication must be understood and carefully weighed before choosing a different course.
- Should not or not recommended – These phrases mean that there may exist valid reasons under certain circumstances when the particular behavior is acceptable or even useful, but the full implication should be understood and the case carefully weighed before implementing any behavior described with this label.
- May or optional – These words mean that an item is truly optional. In one instance, the item may be included because a particular marketplace requires it or because a customer feels that it enhances the product, while another customer may omit the same item. An implementation that does not include a particular option must be prepared to interoperate with another implementation that does include the option, though perhaps with reduced functionality. In the same vein, an implementation that does include a particular option must be prepared to interoperate with another implementation that does not include the option, except for the feature the option provides.

2 Requirements

NOTE: Numerous changes were made in this chapter.

This chapter provides the high-level requirements for the data services protocol layer to support inter-RAT mobility between E-UTRA and eHRPD/1X. This includes IP address establishment and maintenance, QoS, dual-IP support, etc. Additional behavioral requirements are defined in the call flows in Chapter 3.

2.1 Assumptions

The network allows the UE to generate multiple IIDs for an IPv6 prefix assignment.

It is expected that the applications required to establish UE-initiated QoS flows will provide explicit QoS metrics for each technology.

2.2 Requirements

2.2.1 Authentication

The authentication requirements are:

- The UE operating in E-UTRA mode shall execute an EPS-AKA authentication procedure to associate itself with the EPC network, as per [S4].
- The UE operating in eHRPD mode shall execute an EAP-AKA authentication procedure to associate itself with the HSGW; see [Q2].
- The UE operating in HRPD/1X mode shall execute a CHAP/PAP authentication procedure to associate itself with the 1X network.

2.2.2 PDN connectivity

When moving across E-UTRA and eHRPD RATs, the UE shall maintain PDN connectivity for all PDN connections that existed prior to the inter-RAT transition, with the exception of those PDN connections that are closed by the applications.

Both E-UTRA and eHRPD standards support only UE-initiated PDN connectivity establishment. As clarification, the trigger to do this always comes from the UE. Applications must request PDN connectivity over eHRPD and LTE. One exception over LTE is that the default PDN connection is provided during the attach procedure, even when the application using this PDN is not active.

2.2.3 IP address allocation

The IP address allocation requirements are:

- The UE shall support IPv4 and IPv6 APN/PDN associations. For each APN/PDN association, the UE indicates support for both IPv4 and IPv6. The network determines whether to grant either an IPv4, IPv6, or IPv4v6 address for each APN/PDN association.
- The UE shall allow packet data handoff across client-MIP, proxy-MIP, and simple-IP regions for both IPv6 and IPv4.
- The UE shall allow packet routing across multiple available interfaces across different RATs.
- The UE shall allow packet routing across multiple QoS flows per interface.
- The UE shall allow simultaneous association and operation with multiple PDN connections. The UE shall allow simultaneous association of up to four PDN connections.
- The UE shall allow packet calls to be supported over all supported technologies.
- The UE shall request the DNS address and the P-CSCF address via PCO in the PDN connection procedure, when needed.

2.2.4 IP address mobility aspects

2.2.4.1 IP connectivity moving within EPC-capable networks

The UE shall retain the IP context when moving across LTE and eHRPD networks. The UE shall perform a handoff attach over the target domain for PDN contexts that are not already created and contexts that were associated with the source domain and that are still in use.

2.2.4.2 IP connectivity moving between EPC-capable and noncapable networks

When switching between a system that is EPC-capable and EPC noncapable, the IP context over the source and the target domains cannot be reused. Hence, the UE shall abandon the source IP context and reestablish IP contexts over the target domain, based on the application request.

- The device does not abandon the source IP context until the device is associated with the target system. When the target system is acquired, a technology change notification is provided to the application.
- The interfaces created over the source domain are brought down and the applications are notified.
- Upon subsequent activation from the application layer, the AMSS establishes the packet session with the newly associated network.

2.2.5 QoS

When QoS is declared, applications shall be notified and packet sessions shall be in the Dormant state, with the application flow controlled. However, in 1xRTT+HRPD Hybrid mode operation, when the device is in eHRPD personality and the UE declares QoS on eHRPD, the packet session context over EPC shall be aborted immediately and subsequent packet calls shall be supported over 1xRTT.

2.2.6 QoS support

The QoS support requirements are:

- The UE shall support UE-initiated QoS procedures.
- The UE shall support network-initiated QoS procedures.
- After mobility transition and if the target network supports UE-initiated QoS, the AMSS shall initiate QoS establishment, without the intervention of applications, for QoS flow if the application has the handle to this QoS flow.

2.3 Packet data capability for LTE and eHRPD

Table 2-1 shows the packet data capability for LTE and eHRPD.

Table 2-1 Packet data capability for LTE and eHRPD

Feature	LTE	eHRPD
Dual-IP Stack	Applicable	Applicable
Dual Address Default Bearer	Applicable	Applicable
Single Address Default Bearer – Option 1 (SADB-1B)	Applicable	Applicable
Single Address Default Bearer – Option 2 (SADB-2B)	Applicable	Not applicable
UE-Initiated Dedicated Bearer	Applicable	Applicable
Network-Initiated Dedicated Bearer	Applicable	Not applicable
Tethered Mode Support	Applicable	Applicable
Maximum Simultaneous Number of APNs	▪ Five ▪ Embedded mode operation – Up to five PDN connections; up to five different APNs in the case of Dual Bearer ▪ Tethered mode operation – Up to two PDN connections, one each for IPv4 and IPv6; up to two different APNs, one APN if dual bearer[1] ▪ Combined Embedded and Tethered mode operation – Up to five total PDN connections, with the restriction on Tethered mode of up to two PDN connections, one each for IPv4 and IPv6	▪ Five ▪ Embedded mode operation – Up to five PDN connections; up to five different APNs in the case of dual bearer ▪ Tethered mode operation – Up to two PDN connections, one each for IPv4 and IPv6l; up to two different APNs, one APN if dual bearer ▪ Combined Embedded and Tethered mode operation – Up to five total PDN connections, with the restriction on Tethered mode of up to two PDN connections, one each for IPv4 and IPv6

[1]Tethered mode is supported via the Qualcomm MSM interface, see [Q5].

Feature	LTE	eHRPD
Maximum Number of Default Bearers, including tethered and embedded connections	Up to eight default bearers, if no restriction on maximum simultaneous number of APNs	Up to five default bearers; VSNCP PDN connections
Maximum Number of Dedicated Bearers, including tethered and embedded connections	Up to seven dedicated bearers	▪ Up to six RLPs ▪ Up to 15 Reservation labels
Maximum Number of Bearers, including default and dedicated, supported	Up to eight bearers; default and dedicated bearers combined	▪ Up to seven RLPs ▪ Up to 16 Reservation labels
Dual Address Default Bearer Mobility Across LTE and eHRPD	Applicable	
UE-initiated dedicated bearer mobility across LTE and eHRPD	Applicable	
Network-initiated dedicated bearer mobility across LTE and eHRPD	Not applicable	

3 Use Cases

This chapter describes the use cases for mobile packet data behavior as it moves between packet domains that can and cannot associate with the 3GPP Enhanced Packet Core (EPC). The organization of the use cases is shown in Figure 3-1.

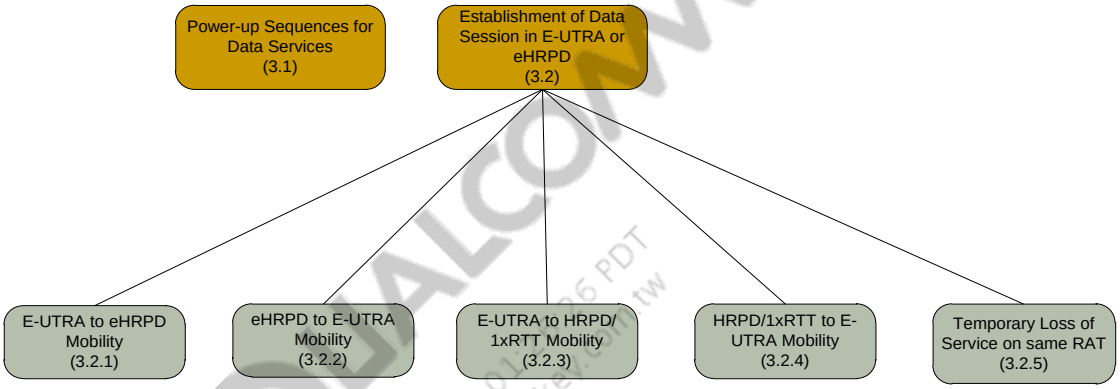

Figure 3-1 Organization of use cases

3.1 Power-up sequences for data services

The following sequence of steps is executed in the UE from the time the UE is powered up to when the UE achieves connectivity to the first PDN over E-UTRA:

1. The UE maintains the following data structures:
   a. Attach Profile, containing parameters required for connecting to a specific PDN at EUTRA Attach; profile contains the APN name and other desired protocol configuration information for this PDN
   b. List of profiles for different PDNs, each containing the APN name and desired PCO for respective PDNs
   c. Default Profile ID, which points to one of the profiles in the previous list of profiles
2. Upon powerup, the previous data structures are read from the UE NV memory and are ready for use as soon as the UE camps on a RAT.
3. If the UE camps on E-UTRA, the UE NAS layer consults the DS layer for information pertaining to the PDN that the UE must connect to at Attach.
4. If the Attach Profile exists, the DS layer presents the NAS with information from that profile. If the Attach Profile does not exist, the DS layer presents the NAS with information from the profile pointed to by the Default Profile ID. If the Default Profile ID is not present, the first profile from the list of configured profiles is presented to the NAS.

5. The UE NAS layer packages information received from the DS layer into the NAS messages and proceeds to perform the E-UTRA Attach procedure.

NOTE: This behavior is specific to the E-UTRA and results from its always-on nature. The UE does not connect to a PDN on power-up if it is camped on any other RAT, including eHRPD.

3.2 Establishment of data session in E-UTRA or eHRPD

This scenario describes successful establishment of a data session in E-UTRA or eHRPD.

Preconditions

- The UE is powered off.
- The UE is within the eHRPD or E-UTRA coverage area.

Triggers

- For eHRPD, at least one application requested data services.
- For LTE, the UE is powered up.

Description

Figure 3-2 shows the application start. Figure 3-3 shows the call flow for the application start.

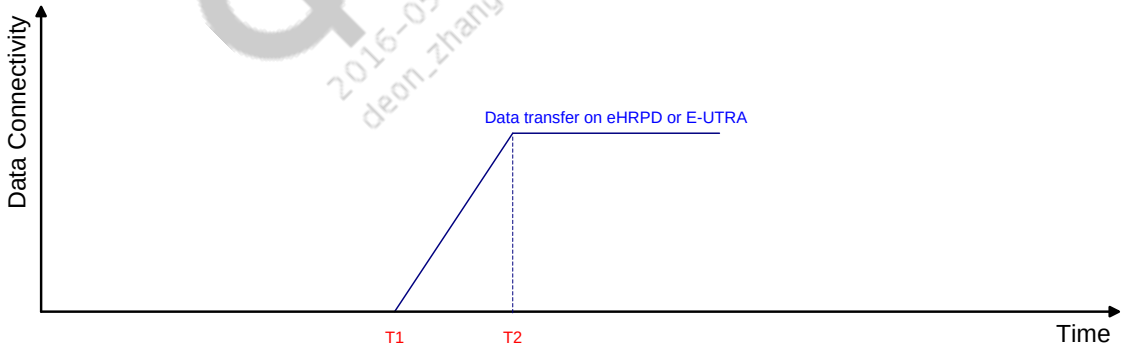

Figure 3-2 Application start

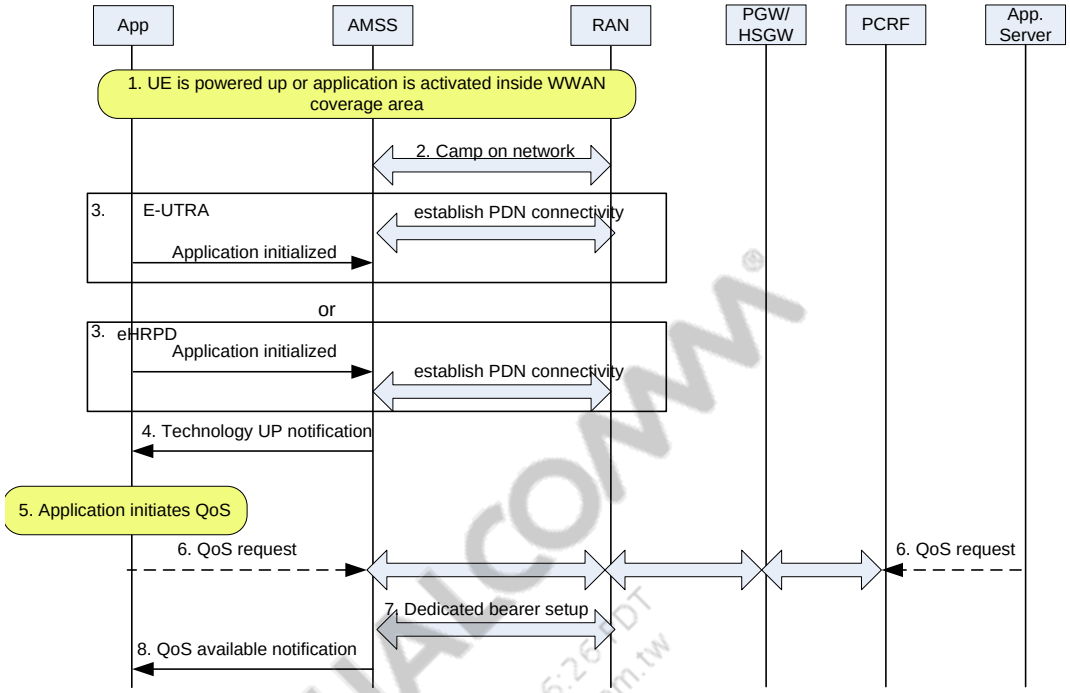

Figure 3-3 Call flow for application start

The following numbered paragraphs correspond to Figure 3-3:

1. The UE is powered up or the application is activated by the user inside the E-UTRA or eHRPD coverage area. This is Event T1 in Figure 3-2.
2. The UE camps on the network.
3. In the case of E-UTRA, the UE establishes PDN connectivity to the network. After that, the application may request a data session via the sockets interface. In the case of eHRPD, the application initializes a data session via the sockets interface, which triggers the UE establishing PDN connectivity to the network.
4. The AMSS notifies the application that the interface is UP (IFACE_UP). At this point, the socket becomes readable/writable and the application can send and receive data on a best-effort flow. This is Event T2 in Figure 3-2.
5. Later, the application may initiate a QoS flow.
6. The QoS request may be initiated by the application. The application may indicate acceptable QoS for one or more RANs, e.g., E-UTRA and eHRPD. The QoS request may also be initiated by the application server.
7. The DS layer sets up dedicated bearers for the QoS flow.
8. If the application has made the request, the AMSS notifies the application that QoS is now available. The application can now push data onto the QoS flow.

Postcondition

The UE established a data session and may be either in Idle or Connected mode. Connected mode in LTE corresponds to Active mode in eHRPD.

3.2.1 E-UTRA-to-eHRPD mobility

This scenario describes successful mobility from E-UTRA to eHRPD.

Preconditions

- The UE is on E-UTRA, either in Idle or Connected mode.
- eHRPD radio session context may be available, based on the UE having previously visited the eHRPD network.

Triggers

E-UTRA → eHRPD mobility is triggered via one of the following:

- BSR – Idle mode better system reselection, if eHRPD is more preferred than serving the E-UTRA system
- OoS in E-UTRA, followed by MMSS
- Redirection
- Cell reselection

Description

Figure 3-4 shows the successful packet context transfer from E-UTRA to eHRPD. Figure 3-5 shows the call flow for a successful packet context transfer from E-UTRA to eHRPD.

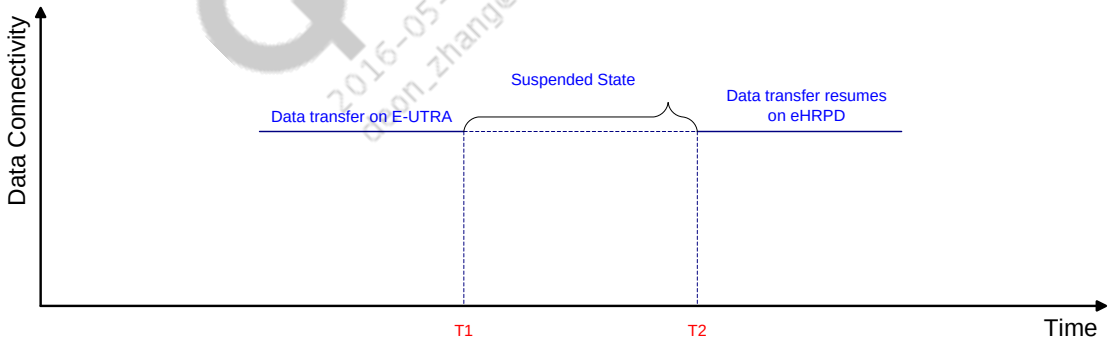

Figure 3-4 Successful packet context transfer from E-UTRA to eHRPD

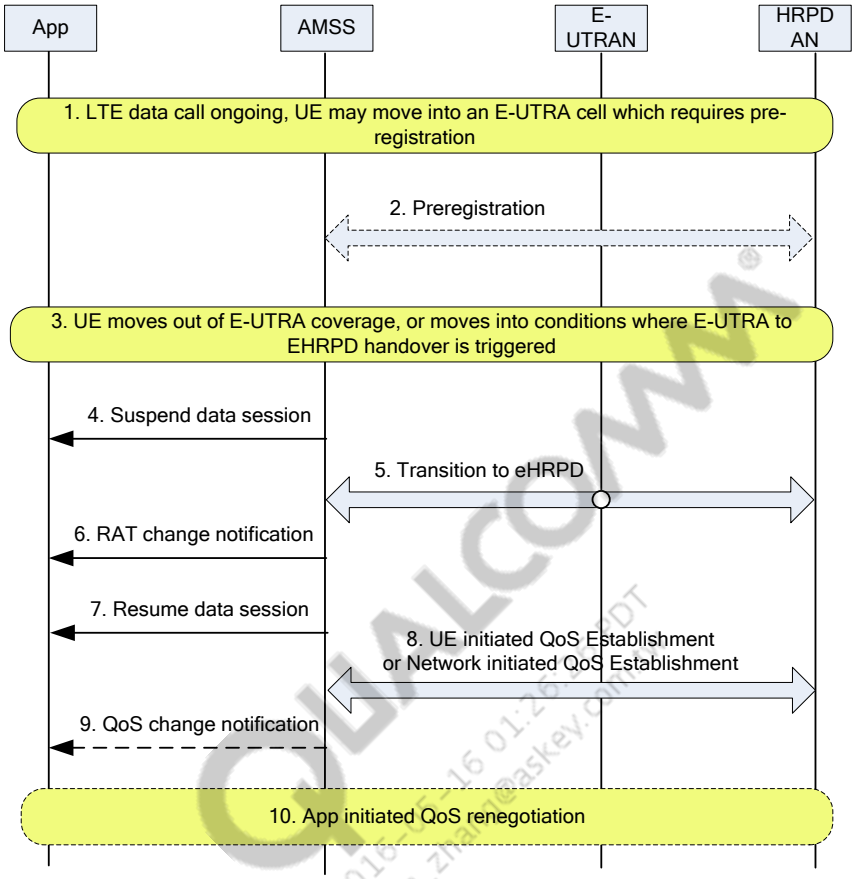

Figure 3-5 Call flow for successful packet context transfer from E-UTRA→eHRPD

The following numbered paragraphs correspond to Figure 3-5:

1. A data call is in progress on E-UTRA. Optionally, the UE may move into an E-UTRA cell in which preregistration is required.
2. If preregistration is triggered in step 1, the UE performs the preregistration procedure with the HRPD AN via the tunnel.
3. Later, the UE moves into an area where E-UTRA coverage is lost, or E-UTRA to eHRPD mobility is triggered.
4. The AMSS indicates to the application to suspend data services, (stop data flow to the socket and do not allow bringing up new QoS flows). If mobility is triggered by cell reselection, step 4 actually occurs after step 5, because the CM is not aware of inter-RAT mobility – T1.
5. The UE performs the mobility procedure with the E-UTRAN and HRPD AN. At this point, QoS flows are merely turned on, since QoS flows were already created in the eHRPD AN in step 2 (preregistration). If preregistration was not performed in step 2, the registration procedure, including establishment of all QoS flows, must be performed from scratch. The PPP context established over the E-UTRA tunnel, or established directly over eHRPD, is used to reactivate the packet session over eHRPD. It is up to the network to run PPP resync if the PPP context between the UE and the HSGW is out of sync.

6. If step 5 is successful, the AMSS notifies the application about the RAT change (eHRPD acquired).
7. The AMSS indicates to the application to resume data services (enable data flow and allow bringing up new QoS flows again) – T2.
8. The QoS request provided by the application can be for multiple technologies, LTE and eHRPD. When the UE transitions to eHRPD, it autonomously requests the UE-initiated QoS flows over eHRPD when only UE-initiated QoS is supported over that domain.

   If network-initiated QoS is also supported over eHRPD, the UE waits for the network to push the QoS. After a time period of not receiving the QoS flow from the network, the UE places the request with the network. All network-initiated QoS flows must only be pushed by the network. QoS flows are suspended with the application until QoS flows are established over eHRPD. The applications are notified of the granted profileId when the QoS flow is configured. While the QoS flow is suspended, the application is free to transmit data over the best-effort default flow.
9. If one or more UE-initiated QoS flows could not be established, the AMSS notifies the corresponding applications.
10. When the application is notified that QoS was changed or unavailable, the application may attempt to reinitiate QoS or it may decide to release the data session.

Postcondition

The UE continues the data session on eHRPD and is in either Dormant or Active mode.

3.2.1.1 PDN connectivity or QoS change during mobility procedure

This scenario describes the behavior when the UE is in the process of performing a mobility procedure and creation/modification/release of PDN connectivity and/or QoS flows are triggered.

Description

If at any point during the mobility procedure a PDN connectivity or QoS flows are created, modified, or deleted, the AMSS indicates failure to the applications and does not take action. Considering different triggers of the mobility procedures, in the case of handoff, the UE should not allow QoS changes or PDN connectivity changes from the time handover from the E-UTRA request message is issued until the eHRPD system is acquired over the traffic channel. In the case of redirection, the UE should not allow QoSs changes or PDN connectivity changes from the time mobility from the E-UTRA request message is issued until the UE is idle camping over eHRPD, having acquired the overhead information. In BSR, the UE should not allow QoS changes or PDN connectivity changes from the moment when the decision to transition out of LTE is made until the UE is idle camping over eHRPD, having acquired the overhead information.

3.2.1.2 Mobility procedure during PDN connectivity or QoS change

This scenario describes the behavior when the UE is in the process of creating/modifying/ releasing PDN connectivity and/or QoS flows and a mobility procedure is triggered.

Description

If a mobility procedure is triggered at any point during a procedure by which PDN connectivity or QoS flows are created, modified, or deleted, the UE should:

- Abort the ongoing PDN connectivity or QoS procedure
- Complete the mobility procedure

Applications are notified that the ongoing PDN connectivity or QoS procedure is aborted.

3.2.1.3 Mobility procedure – IP address mismatch

This scenario describes the behavior when the IP address does not match after a mobility between eHRPD and E-UTRA, due to the network not deploying the same LMA for eHRPD and E-UTRA.

Description

The scenario is similar to the regular mobility scenario, except that the application must reestablish the IP session. This is triggered by sending a IP Address Change notification with the new IP address to the application, which, in turn, may bring up the IP session again.

3.2.1.4 Mobility from E-UTRA – No IP address is assigned

This scenario describes when the UE is attached on E-UTRA, but no IP address was assigned at the time of handover or reselection.

Description

In this case, E-UTRA to eHRPD mobility is completed without the IP address being assigned. Depending on preconditions and whether the application registered with the DS API, different actions are taken after the transition, as shown in Table 3-1. See Chapter 12 for UE handling of cases when the eHRPD network does not support SADB-2B.

Table 3-1 Mobility from E-UTRA with no IP address in various scenarios

Precondition – One IP address is assigned in the DADB or SADB-2B case	App registered with DS API (app attached)	Actions after mobility, e-UTRA to eHRPD, completes
DHCP IPv4 address not assigned	App not attached	Wait for app to trigger DHCP request
DHCP IPv4 lease expired	App not attached	Wait for app to trigger DHCP request
	App attached	Renew lease
IPv6 RS/RA failed and IPv6 throttling timer expires	App not attached	Wait for app to request RS
	App attached	Start RS
RA lifetime expired	App not attached	Wait for app to request RS

Precondition – One IP address is assigned in the DADB or SADB-2B case	App registered with DS API (app attached)	Actions after mobility, e-UTRA to eHRPD, completes
	App attached	Start RS

3.2.1.5 Mobility – QoS mismatch between source/target

This scenario describes UE behavior if the QoS parameters after inter-RAT mobility are reduced below what is acceptable for the application.

Description

When the UE is not receiving the QoS grant from the network within a predefined period of time during inter-RAT mobility for QoS flows with an explicit application request, the UE starts the UE-initiated QoS procedure. Subsequently, for those application-specified TFTs for which QoS changed, the AMSS notifies the application about the granted QoS. When the granted QoS does not match the QoS requested by the application for the associated technology, the application must act appropriately.

3.2.1.6 Mobility – Not all QoS flows could be reestablished

This scenario describes the case when not all QoS flows were reestablished during the E-UTRA/eHRPD mobility scenario.

Description

When the UE does not receive the QoS grant from the network within a predefined period of time during inter-RAT mobility for QoS flows with an explicit application request, the UE starts the UE-initiated QoS procedure. Subsequently, for those application-specified TFTs for which QoS cannot be reestablished, the AMSS notifies the applications for those QoSs that were released.

3.2.1.7 E-UTRA→eHRPD mobility – Failure with fallback

This scenario describes when mobility to the eHRPD fails and the UE comes back to E-UTRA to continue.

Description

Figure 3-6 shows the call flow for E-UTRA-to-eHRPD mobility with a fallback to E-UTRA.

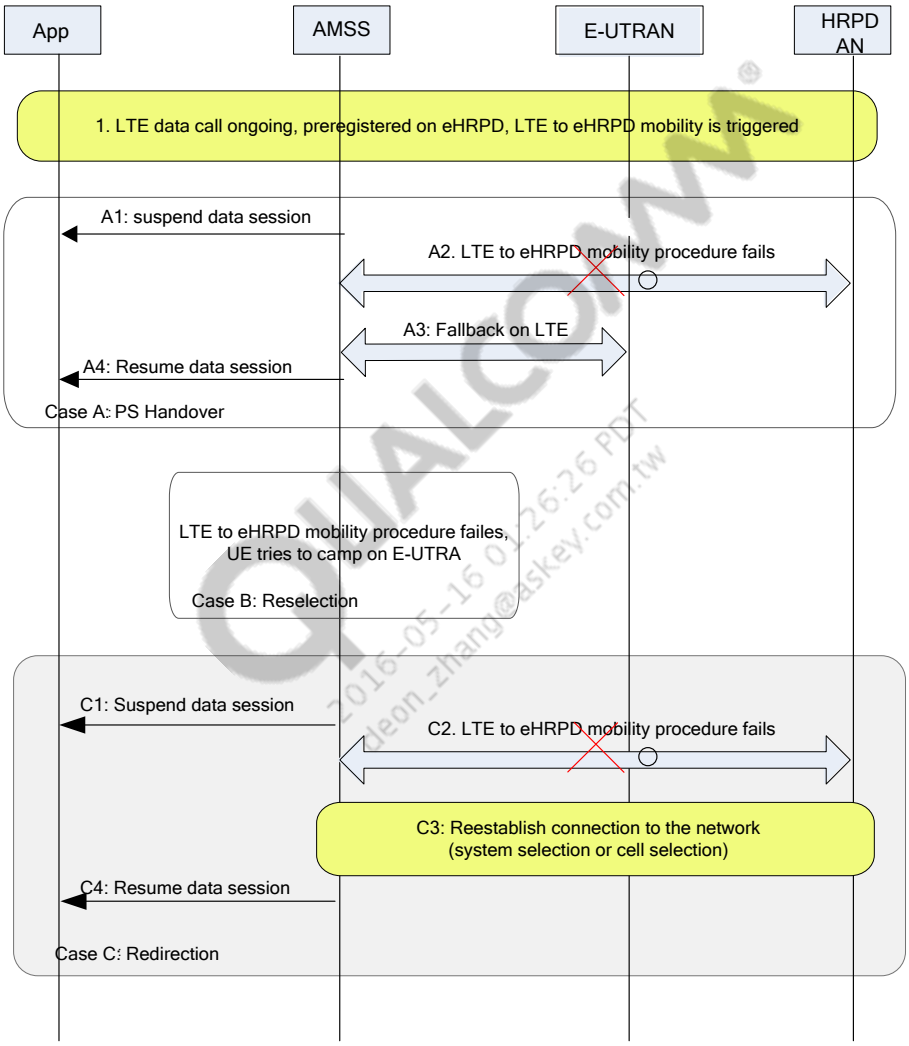

Figure 3-6 Call flow for E-UTRA-to-eHRPD mobility with fallback to E-UTRA

The following numbered paragraphs correspond to Figure 3-6:

1. The E-UTRA data call is ongoing (Idle or Connected mode). The UE may optionally have preregistered on eHRPD. At this point, E-UTRA-to-eHRPD mobility is triggered.
2. The mobility procedure is carried out, but fails at some point. A fallback is only applicable if mobility fails due to radio or RAN-related problems. It is not considered a mobility failure if PDN connectivity or QoS is not granted on the new network.

Case A – PS Handover

A1. – In the case of PS Handover, the application is notified to suspend the data session.

A2. – The mobility procedure is carried out, but fails at some point. A fallback is only applicable if mobility fails due to radio or RAN-related problems. It is not considered a mobility failure if PDN connectivity or QoS is not granted on the new network.

A3. – UE performs the connection reestablishment procedure to E-UTRA.

A4. – If successful, the application is notified that the data session can be resumed.

Case B – Reselection

The LTE→eHRPD mobility procedure fails. The UE tries to camp on the E-UTRA network. If it is successful, no further action is necessary, assuming that the UE can find a cell in the same LTE tracking area.

Case C – Redirection

C1. – In the case of redirection, the application is notified to suspend the data session.

C2. – The mobility procedure is carried out, but fails at some point. A fallback is only applicable if mobility fails due to radio or RAN-related problems. It is not considered a mobility failure if PDN connectivity or QoS is not granted on the new network.

C3. – The UE attempts to find service on any RAT. The UE may simply try the last good cell or may perform system selection.

C4. – If successful, the application is notified that the data session can be resumed.

NOTE: If the IP context is reestablished during these procedures, the application is notified with an IP Address Change notification. This triggers the application to reestablish the IP session.

3.2.2 eHRPD-to-E-UTRA mobility – Success

This scenario describes successful mobility from eHRPD to E-UTRA.

Assumptions

- The UE moves out of HRPD coverage and into E-UTRA coverage.
- In this case, the system change is expected to occur via OoS/system selection/cell reselection.

Preconditions

- The UE is on eHRPD, has a PPP context established, and may be in Dormant mode.
- If it is in eHRPD Dormant mode for the case of cell reselection, the UE read the eHRPD system information containing E-UTRA neighbor cell information.
- If it is in eHRPD Dormant mode for the case of system reselection, the operator provisioned system priority information, i.e., E-UTRA is higher priority than eHRPD, in the MMSS table.

Triggers

eHRPD → E-UTRA mobility is triggered via one of the following:

- BSR – Idle/Dormant mode better system reselection
- Cell reselection

Description

Figure 3-7 shows a successful packet context transfer from eHRPD to E-UTRA. Figure 3-8 shows the call flow for a successful packet transfer from eHRPD to E-UTRA.

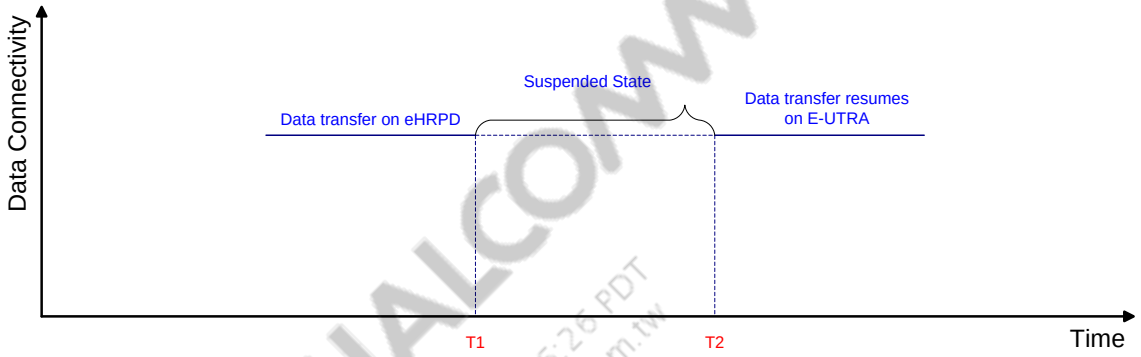

Figure 3-7 Successful packet context transfer from eHRPD→E-UTRA

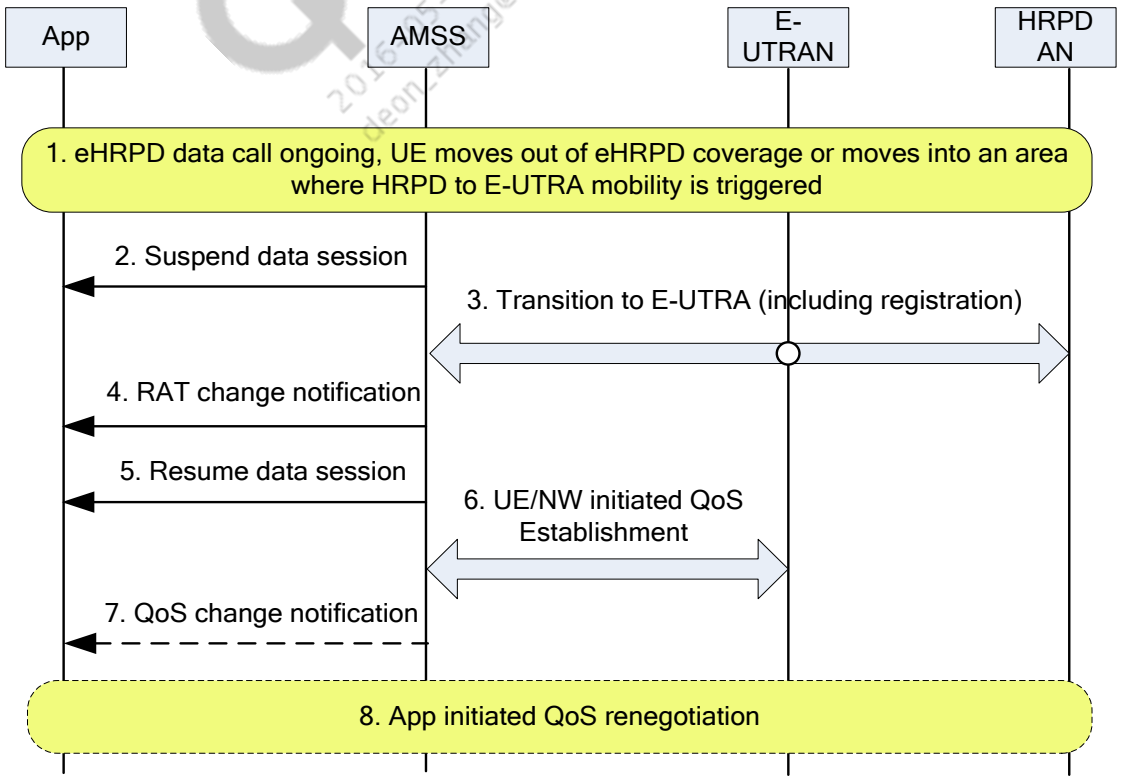

Figure 3-8 Call flow for successful packet transfer from eHRPD to E-UTRA

The following numbered paragraphs correspond to Figure 3-8:

1. The eHRPD data call is ongoing; meanwhile, the UE moves out of eHRPD coverage or moves into an area with better E-UTRA coverage, triggering mobility.
2. The AMSS indicates to the application to suspend the data services (stop data flow to the socket, and do not allow bringing up new QoS flows) – T1.
3. The transition to E-UTRA is via system selection, cell reselection, or OoS.
4. If successful, the RAT change notification E-UTRA acquired is signaled to the application.
5. The AMSS indicates to the application to resume data services (enable data flow and allow bringing up new QoS flows again) – T2.
6. The network may attempt to establish QoS flows that existed on eHRPD. The UE performs filter matching to determine which flows were assigned adequate QoS. Subsequently, the UE tries to initiate QoS for flows[2] for which the network did not establish QoS.
7. If some QoS flows could not be established, corresponding applications are notified.
8. The applications may reinitiate UE-initiated QoS for flows that did not get QoS.

Postcondition

- For a UE on E-UTRA, active data transfer may continue.
- The UE maintains the PPP context with eHRPD systems to enable Tunnel mode operation and/or for quick activation when reentering eHPRD.

3.2.2.1 eHRPD-to-E-UTRA mobility – Failure with fallback

This scenario describes when mobility to E-UTRA fails and the UE returns to eHRPD to continue.

Assumptions

See Section 3.2.2.

Preconditions

See Section 3.2.2.

Triggers

See Section 3.2.2.

[2]Only for UE-initiated flows for which applications provided E-UTRA-specific QoS parameters

Description

Figure 3-9 shows call flow for eHRPD →E-UTRA mobility with fallback to eHRPD.

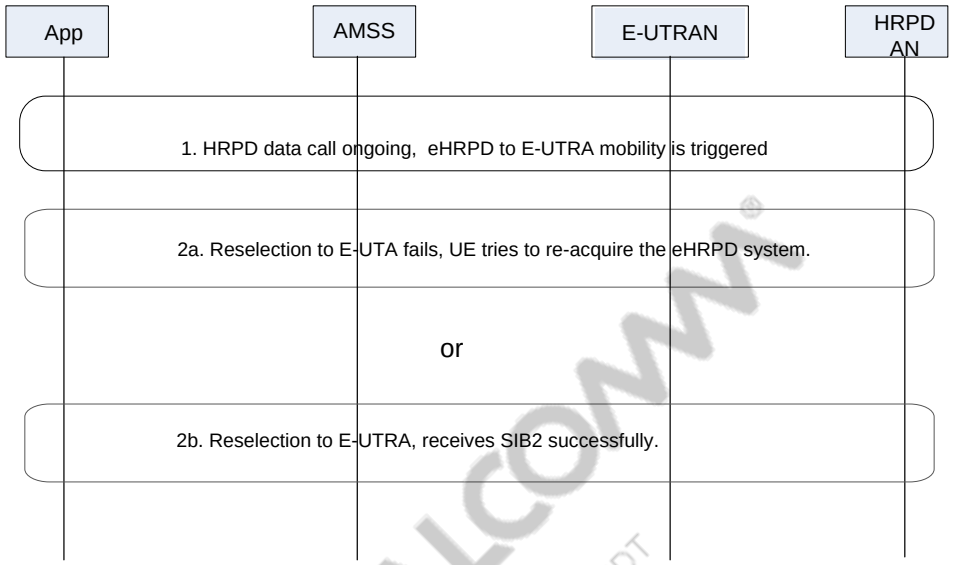

Figure 3-9 Call flow for eHRPD→E-UTRA mobility with fallback to eHRPD

The following numbered paragraphs correspond to Figure 3-9:

1. The eHRPD data call is ongoing, in Dormant or Active mode. At this point, eHRPD→E-UTRA mobility is triggered.
2. The mobility procedure occurs as follows:
   a. If the UE fails to acquire the E-UTRA system, it tries to reacquire the eHRPD system.
   b. If the UE is able to acquire the E-UTRA system and receives SIB2 successfully, it tries to establish connection to the E-UTRA network. If connection establishment fails, the UE starts the MMSS procedure.

NOTE: If the IP context is reestablished during these procedures, the application is notified with an IP Address Change notification. This triggers the application to reestablish the IP session.

3.2.3 E-UTRA→HRPD/1xRTT mobility – Success

This scenario describes successful mobility from E-UTRA→HRPD/1xRTT.

Assumptions

The UE moves from an area with E-UTRA coverage to an area with HRPD or 1xRTT coverage.

Precondition

- The UE is on E-UTRA, either in Idle or Connected mode.
- If it is in E-UTRA Connected mode, the UE was configured by the E-UTRAN to send HRPD/1xRTT measurement reports.

- If it is in E-UTRA Idle mode, the UE read the E-UTRA system information containing HRPD/1xRTT neighbor cell information.
- If it is in E-UTRA Idle mode for the case of system reselection, the operator provisioned system priority information, i.e., eHRPD is higher priority than E-UTRA, in the MMSS table.

Triggers

E-UTRA→HRPD/1xRTT mobility is triggered via one of the following:

- BSR – Idle mode with PRL-assisted measurements
- RLF in E-UTRA Connected/OoS in E-UTRA Idle – Multimode system selection Redirection – No resources on the new cell, i.e., blind or with measurement gaps, via Idle
- Cell reselection – Idle mode with SIB-assisted measurements

Description

Figure 3-10 shows a successful E-UTRA→HRPD/1xRTT packet context transfer. Figure 3-11 shows the call flow for a successful packet context transfer from E-UTRA→HRPD/1xRTT.

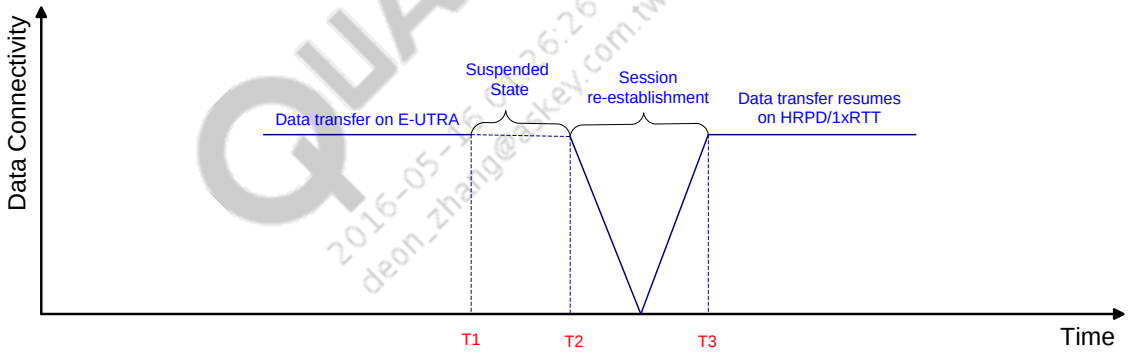

Figure 3-10 Successful packet context transfer from E-UTRA→HRPD/1xRTT

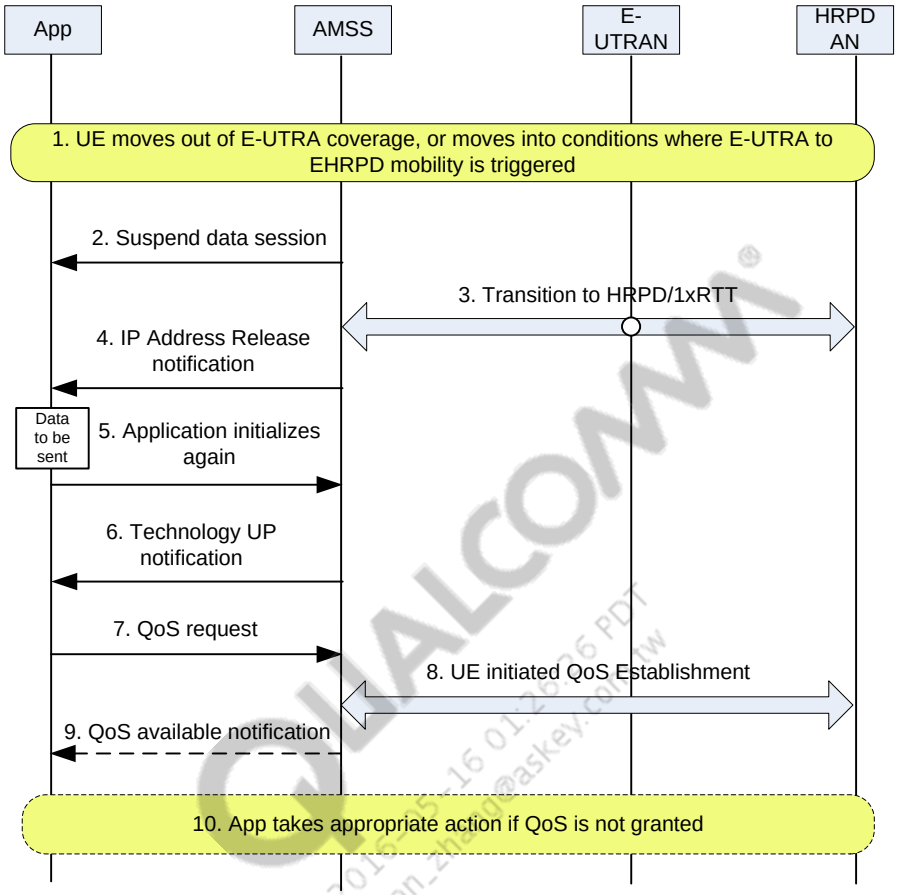

Figure 3-11 Call flow for successful packet context transfer from E-UTRA to HRPD/1xRTT

The following numbered paragraphs correspond to Figure 4-10:

1. The UE moves into an area where E-UTRA coverage is lost or E-UTRA→HRPD/1xRTT mobility is triggered.
2. The DS layer indicates to the application to suspend data services, i.e., stop data flow to the socket and do not allow bringing up new QoS flows) – T1.
3. The UE performs the mobility procedure with the E-UTRAN and HRPD/1xRTT AN.
4. The application is notified that the IP address was released – T2.
5. When data starts, the application reinitializes the IP session with the AMSS. At this point, the AMSS initiates PPP and IPCP.
6. The AMSS indicates to the application that the technology is UP and that data can be written to the socket – T3.
7. The application may request QoS.
8. If the application requests QoS, the UE-initiated QoS flows are established with HRPD AN.

9. For UE-initiated QoS flows, the AMSS notifies the corresponding applications of whether QoS is available.
10. When QoS is not available, the application takes appropriate actions, such as releasing the data session.

Postcondition

The UE establishes the data session on HRPD/1xRTT.

3.2.3.1 E-UTRA→HRPD/1xRTT mobility – Failure with fallback

This scenario describes the behavior when the mobility to HRPD/1xRTT fails and the UE returns to the legacy E-UTRA cell.

Assumptions

See Section 3.2.3.

Preconditions

See Section 3.2.3.

Triggers

See Section 3.2.3.

Description

The same behavior applies as for a E-UTRA→eHRPD mobility failure with fallback. See Section 3.2.1.7.

3.2.4 HRPD/1xRTT→E-UTRA mobility – Success

This scenario describes successful mobility from HRPD/1xRTT to E-UTRA.

Description

This scenario is conceptually very similar to the E-UTRA→HRPD/1xRTT case. In this case, the IP session is moved from a non-EPC-based core network to an EPC-based core network. The same mechanisms are used to reestablish the IP session with the application. UE-initiated QoS may be established by the application after the technology-up notification.

3.2.4.1 HRPD/1xRTT→E-UTRA mobility – Failure with fallback

This scenario describes the behavior when mobility to E-UTRA fails and the UE returns to the legacy HRPD/1xRTT cell.

Description

See Section 3.2.2.1. If failure occurs after the Attach procedure is completed in E-UTRA, the IP session must be reestablished because the IP session was torn down by the UE when it attached to E-UTRA; otherwise, the IP session can be retained.

3.2.5 Temporary loss of service on same RAT

This scenario describes how the UE goes to OoS and then returns on the same RAT.

Assumptions

None

Preconditions

- The UE is Idle/Connected mode on a particular RAT, either E-UTRAN, eHRPD, or 1xRTT.
- The IP context and QoS are established.

Triggers

The UE in Idle or Connected mode temporarily moves out of coverage long enough to declare OoS and then moves back into coverage and reestablishes radio connection on the same RAT.

Description

Figure 3-12 shows the call flow for temporary loss of service on the same RAT.

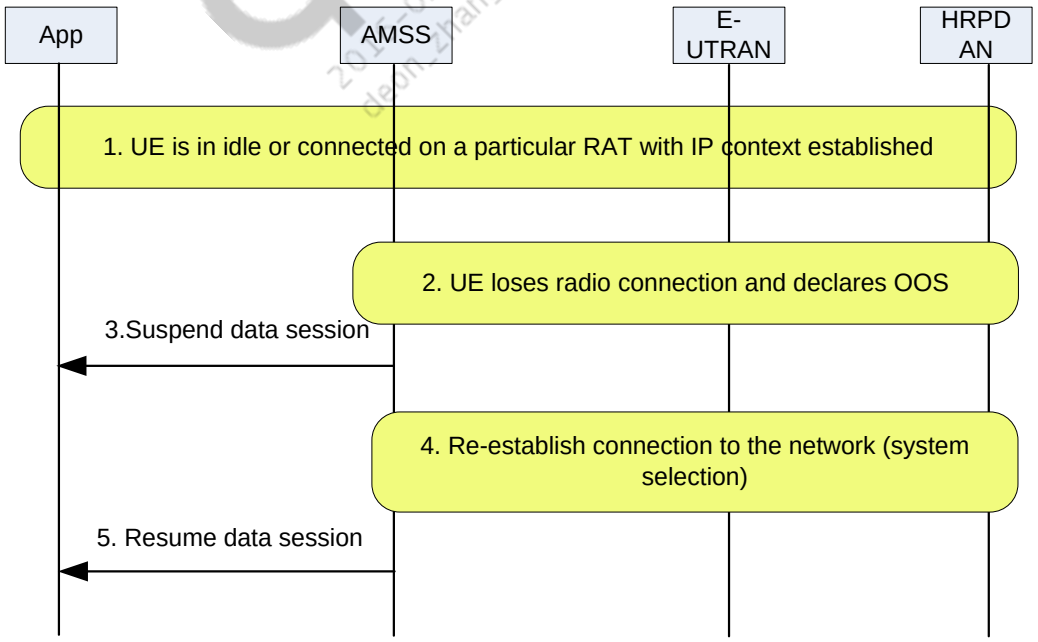

Figure 3-12 Temporary loss of service on the same RAT

The following numbered paragraphs correspond to Figure 3-12:

1. The UE is in Idle or Connected mode on a particular RAT with IP context established.
2. The UE loses radio connection and declares OoS.
3. The application is notified that the data session is suspended.
4. The UE performs a system selection and is able to camp on the same network, entering either the Idle or Connected state.
5. The application is notified that the data session is resumed.

4 Mobile Packet Data Behavior When Moving Across Packet Domains

This chapter describes the mobile packet data behavior as it moves between packet domains that are associated with the 3GPP2 packet core and packet domains that are associated with the EPC, 3GPP Enhanced Packet Core.

4.1 State machine

Figure 4-1 shows the logical representation of the state machine and state transitions as the mobile moves between 1xRTT/HRPD, the 3GPP2 packet core, and eHRPD/E-UTRA (EPC) systems.

NOTE: This state machine is a conceptual representation. It is not the actual UE implementation.

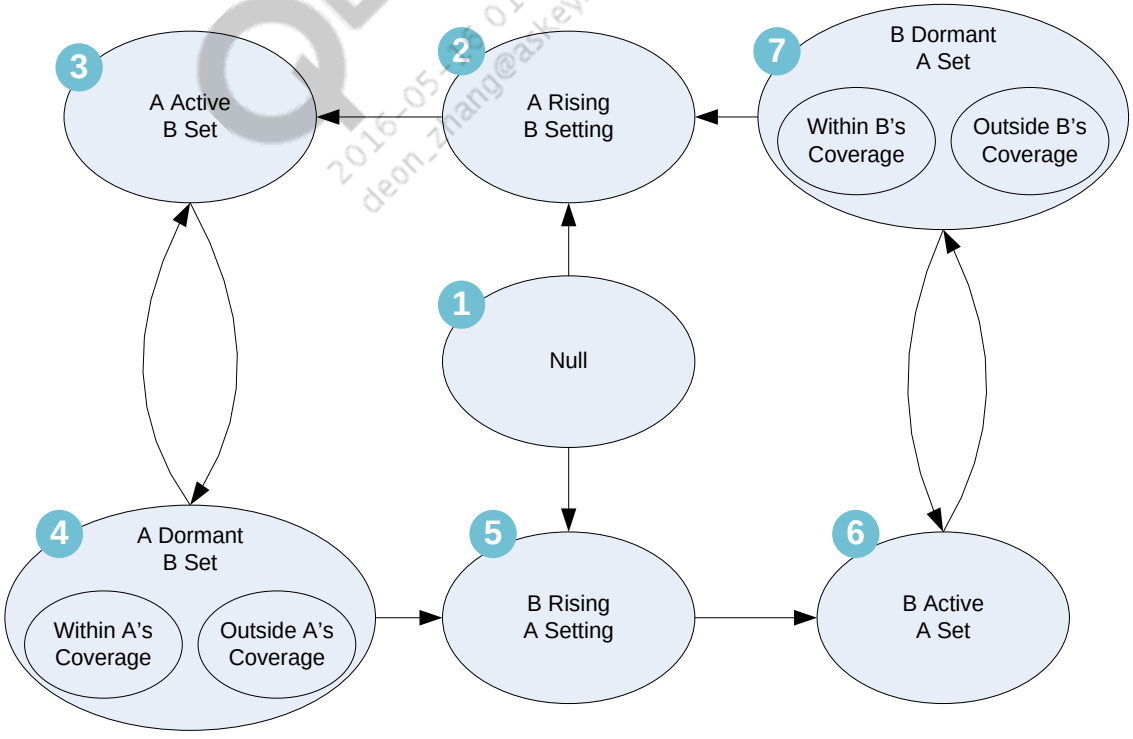

Figure 4-1 3GPP2↔3GPP packet data roaming state machine

A, B ∈ {1xRTT/HRPD with no EPC association, eHRPD/E-UTRA with EPC association}; where A ≠ B

4.1.1 States description

- (1) Null – The mobile enters this state as soon as the mobile powers up. In this state, the mobile has not found a valid system with which to associate itself. The mobile, when it acquires either A or B, will subsequently not reenter this state until it undergoes another power cycle.

NOTE: The mobile deletes an established packet data context only after it acquires a system, potentially a different system that requires the context to be reestablished.

- (2) A Rising B Setting – The mobile enters this state when it has acquired A. In this state, if the mobile was active over B earlier, it releases the packet data context information associated with B. The applications are provided with a system change notification and the interfaces associated with B are torn down. When there is no prior packet data context, the application is provided with a system acquired notification. At this point, it is left up to the application to reactivate the packet data context before it can support packet data services over A.
- (3) A Active B Set – The mobile enters this state when at least one application activated and established packet data context over A. At this point, all packet data context of B is deleted. The mobile transitions between this state and the A Dormant B Set state, depending on when the mobile is actively exchanging packet data versus being idle.
- (4) A Dormant B Set – The mobile has packet data context established with A. The mobile enters this state when there is no packet data activity. The mobile transitions between this state and the A Active B Set state, depending on when the mobile is actively exchanging packet data versus being idle.

NOTE: The mobile may or may not be within coverage of A while it is in this state. The packet data context may be retained based on the lifetime of the context maintained between the mobile and the network.

- (5) B Rising A Setting – The mobile enters this state when it has acquired B. In this state, if the mobile was active over A earlier, it releases all packet data context information associated with A. The applications are provided with a system change notification and the interfaces associated with A are torn down. When there is no prior packet data context, the application is provided with a system acquired notification. At this point, it is left up to the application to reactivate the packet data context before it can support packet data services over B.
- (6) B Active A Set – The mobile enters this state when at least one application has activated and has established packet data context over B. At this point, all packet data context of A is deleted. The mobile transitions between this state and the B Dormant A Set state, depending on when the mobile is actively exchanging packet data versus being idle.
- (7) B Dormant A Set – The mobile has packet data context established with B. The mobile enters this state when there is no packet data activity. The mobile transitions between this state and the B Active A Set state, depending on when the mobile is actively exchanging packet data versus being idle. The packet data context may be retained based on the lifetime of the context maintained between the mobile and the network.

4.1.2 State transitions

- (1)→(2) – The mobile makes this transition when, after power up, the mobile acquires A as the first system.
- (1)→(5) – The mobile makes this transition when, after power up, the mobile acquires B as the first system.
- (2)→(3) – After acquiring A, the application activates the packet data context over A.
- (3)→(4) – The packet data session transitions from active to idle. The mobile may or may not go out of A coverage.
- (2)→(3) – The packet data session transitions from being idle to active.
- (4)→(5) – The mobile acquired B. This can happen when the mobile is still within A coverage and B is a more preferred system in that region, or when the mobile is no longer in A coverage.
- (5)→(6) – After acquiring B, the application activates the packet data context over B.
- (6)→(7) – The packet data session transitions from active to idle. The mobile may or may not go out of B coverage.
- (5)→(6) – The packet data session transitions from idle to active.
- (7)→(2) – The mobile acquired A. This can happen when the mobile is still within B coverage and A is a more preferred system in that region, or when the mobile is no longer in B coverage.

4.2 LTE packet state machines

4.2.1 State machine 2 – LTE state machine

Figure 4-2 shows the LTE protocol state machine. Salient aspects of this implementation are:

- The UE LTE context is deleted when the UE camps on a 3GPP2 RAT. Essentially, the UE performs the same actions as powering down while on LTE.
- When it moves from eHRPD→LTE, the UE LTE protocol stack attempts to restore QoS flows that might have been set up on eHRPD. This involves accepting network-initiated QoS flow setup and executing UE-initiated QoS flow setup procedures for UE-initiated flows that were not set up by the network. The applications do not see a QoS break, provided the network sets up the necessary QoS flows or grants QoS when the UE executes UE-initiated QoS setup procedures.
- S101 tunneling is supported. However, eHRPD QoS over S101 tunneling is not supported.

Figure 4-2 shows LTE packet data FSM.

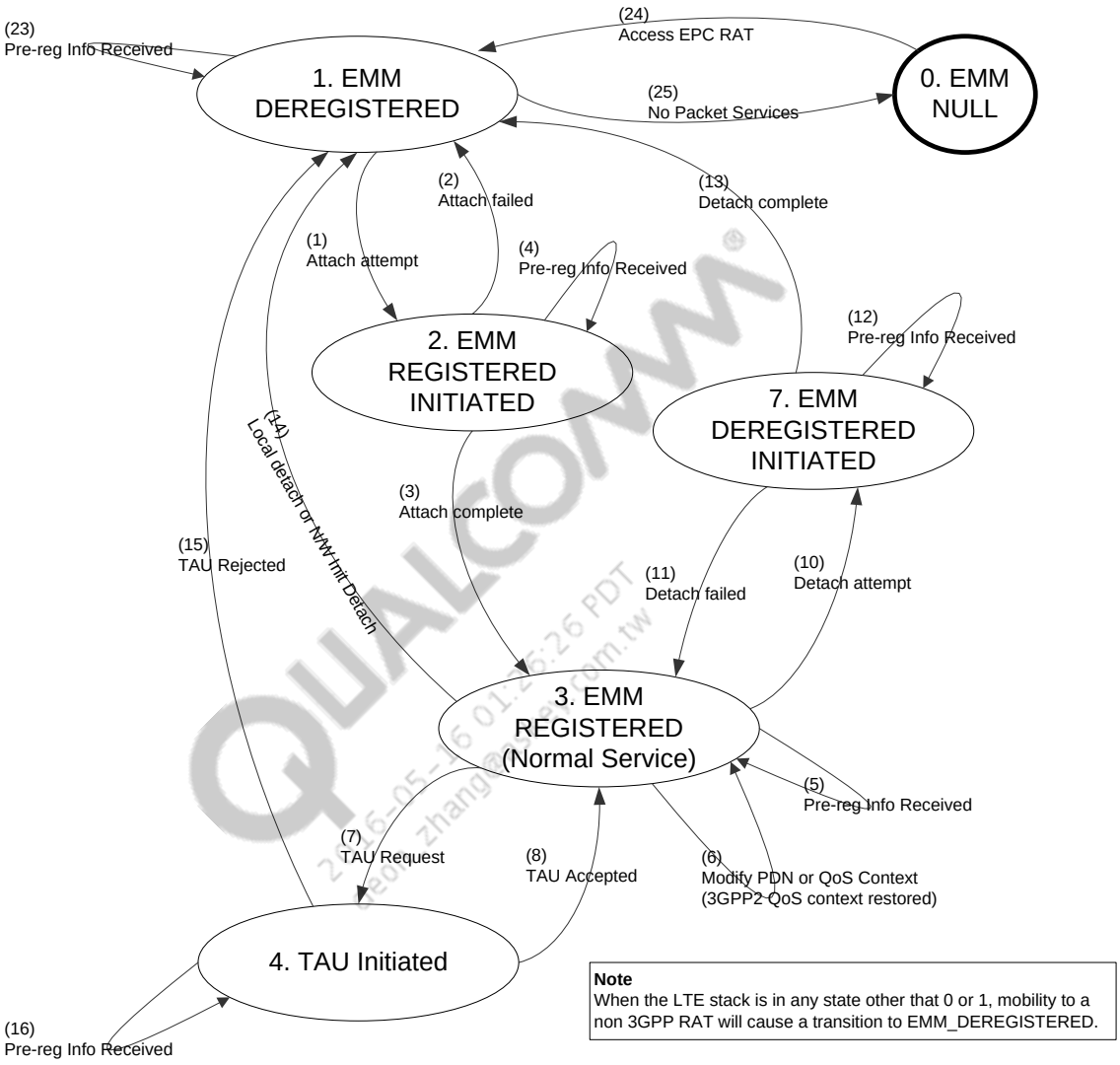

Figure 4-2 LTE packet data FSM

Table 4-1 shows the states of the LTE packet data FSM.

Table 4-1 States of the LTE packet data FSM

State name	Description
LTE_STATE_0	EMM Null – The UE has no EPS capability in this state.
LTEs_STATE_1	EMM Deregistered – The UE has no EMM context established in the network. The UE may still be connected to the EPC through another EPC-capable RAT. The UE is not reachable over the LTE air interface.
LTE_STATE_2	EMM Registered Initiated – The UE initiated the Attach procedure and is waiting for a response from the network.
LTE_STATE_3	EMM Registered (Normal Service) – The UE is attached to the EPC via LTE. The UE may be in Idle or Connected mode. The UE may be preregistered over the eHRPD network, but is reachable only over the LTE air interface.
LTE_STATE_4	TAU Initiated – The UE initiated the TAU procedure and is waiting for the network's response.
LTE_STATE_7	EMM Deregistered Initiated – The UE initiated the Detach procedure and is waiting for a response from the network.

Table 4-2 shows state transitions of the LTE packet data FSM.

Table 4-2 State transitions of the LTE packet data FSM

Transition	Trigger	Condition	Action	Event
LTE_TRANSITION_1	▪ Service found on LTE ▪ Mobility to LTE from nonEPC RAT	None	Send Attach Request; use existing context, if available	LTE_ATTACH_INIT
LTE_TRANSITION_2	▪ Attach rejected ▪ Lower layer failures ▪ T3410 timeout	None	Local Maintenance per 24.301, Section 5.5.1.2 [S3]	
LTE_TRANSITION_3	Attach Accept received and default bearer created successfully	None	Attach Complete sent	LTE_ATACH_ COMPLETE
LTE_TRANSITION_4	SIB8 received	None	Convey prereg information to C2K upper layers	LTE_PREREG_ RECEIVED
LTE_TRANSITION_5	SIB8 received	None	Convey prereg information to C2K upper layers	LTE_PREREG_ RECEIVED

Transition	Trigger	Condition	Action	Event
LTE_TRANSITION_6	▪ Triggers to modify PDN or QoS Context ▪ LTE protocol stack connects to each PDN UE was connected to on eHRPD ▪ LTE protocol stack attempts to restore QoS context set up on eHRPD ▪ Applications do not experience a QoS break	None	NAS protocol actions to modify PDN or QoS context	LTE_CONTEXT_ CHANGE
LTE_TRANSITION_7	TAU triggers	None	TAU Request sent	
LTE_TRANSITION_8	TAU Accepted/ TAU Rejected (#13, #15, #25)/T3430 Timeout	None	Local Maintenance per 24.301, Section 5.5.3 [S3]	
LTE_TRANSITION_10	Detach triggers	None	Send Detach request	
LTE_TRANSITION_11	Detach Failure triggers	None	Local maintenance per 24.301, Section 5.5.2 [S3]	
LTE_TRANSITION_12	SIB8 received	None	Convey prereg information to C2K upper layers	LTE_PREREG_ RECEIVED
LTE_TRANSITION_13	Detach Accept received	None	PDN and QoS context cleared; other local maintenance per 24.301, Section 5.5.2 [S3]	LTE_DETACHED
LTE_TRANSITION_14	Local Detach or Network-Initiated Detach or Mobility to nonEPC RAT	None	PDN and QoS context cleared; other local maintenance per 24.301, Section 5.5.2 [S3]	LTE_DETACHED
LTE_TRANSITION_15	TAU rejected, except #13, #15, #25, or mobility to nonEPC RAT	None	PDN and QoS context cleared; other local maintenance per 24.301, Section 5.5.3 [S3]	LTE_DETACHED

Transition	Trigger	Condition	Action	Event
LTE_TRANSITION_16	SIB8 received	None	Convey prereg information to C2K upper layers	LTE_PREREG_ RECEIVED
LTE_TRANSITION_23	SIB8 received	None	Convey prereg information to C2K upper layers	LTE_PREREG_ RECEIVED

4.2.2 State machine 3.1 – LTE PDN state machine

Figure 4-3 shows the IP connectivity state machine, LTE.

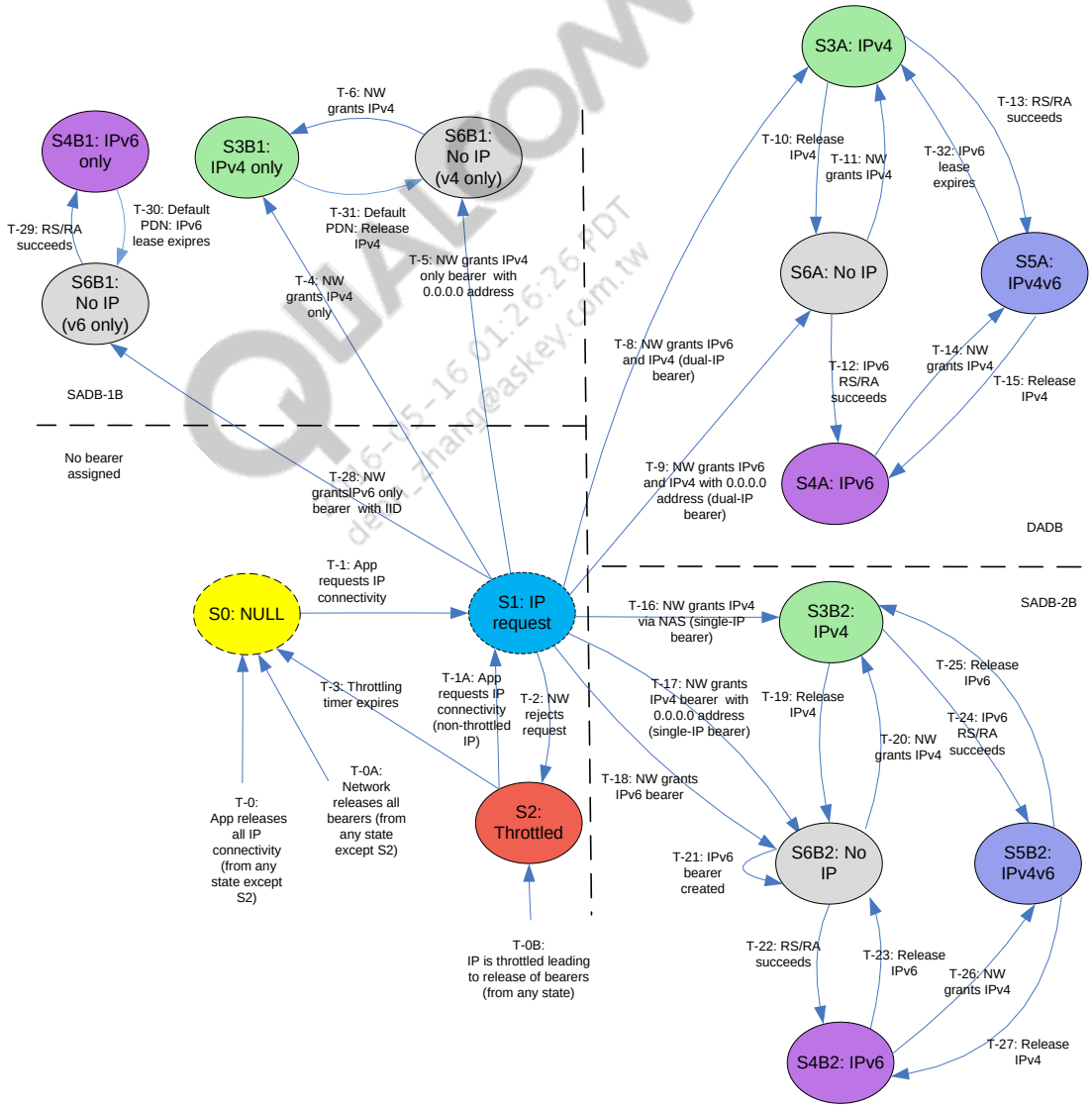

Figure 4-3 IP connectivity state machine, LTE

Table 4-3 shows details about the LTE IP connectivity state machine, states.

Table 4-3 Details about LTE IP connectivity state machine, states

#	State name	Description
S0	NULL	No IP connectivity
S1	IP request	IP connectivity requested, waiting for network response
S2	Throttled	Network rejected connectivity to this PDN, further requests are blocked until timer expires
S3A	IPv4 (DADB)	Dual address bearer is set up by network and IPv4 address is assigned via NAS or DHCP
S3B1	IPv4 (SADB-1)	▪ Single address bearer is set up for IPv4 and IPv4 address is assigned via NAS or DHCP ▪ No separate bearer for IPv6 is allowed
S3B2	IPv4 (SADB-2)	▪ Single address bearer is set up for IPv4 and IPv4 address is assigned via NAS or DHCP ▪ Separate IPv6 bearer is allowed by the network
S4A	IPv6 (DADB)	Dual address bearer is set up by the network and IPv6 address, IID+prefix, is assigned
S4B1	IPv6 (SADB-1)	▪ Single address bearer is set up for IPv4 and IPv6 address, IID+prefix, is assigned ▪ No separate bearer for IPv4 is allowed
S4B2	IPv6 (SADB-2)	▪ Single address bearer is set up for IPv4 and IPv6 address, IID+prefix, is assigned ▪ Separate IPv4 bearer is allowed by the network
S5A	IPv4v6 (DADB)	Dual address bearer is set up by the network and IPv4 and IPv6 addresses are assigned
S5B2	IPv4v6 (SADB-2)	Two single address bearers are set up separately for IPv4 and IPv6 and IPv4 and IPv6 addresses are assigned
S6A	No IP (DADB)	Dual address bearer is set up by the network, but neither IPv4 nor IPv6 address is assigned
S6B1	No IP (SADB-1)	▪ Single address bearer is set up, but neither IPv4 nor IPv6 address is assigned ▪ No second bearer is allowed
S6B2	No IP (SADB-2)	Two separate single address bearers are set up, but neither IPv4 nor IPv6 address is assigned

Table 4-4 shows details about LTE IP Connectivity state machine transitions.

Table 4-4 Details about LTE IP Connectivity state machine transitions

Transition	Trigger	Condition	Action
T-0	No application requires this PDN connection any more, neither IPv4 nor IPv6		
T-0A	Network releases all connections to this PDN		Apps are notified that IPv4/IPv6 connectivity is lost
T-0B	PDN connection is released while throttling is in effect		If they are active, throttling timers are kept running
T-1	Application requests IP connectivity		IP PDN connectivity request is triggered
T-1A	Application requests IP connectivity for nonthrottled IP address)		IP PDN connectivity request is triggered; clear throttling timer
T-2	Network rejects IP connectivity request for IPv4 and IPv6		Consider this PDN as throttled for both IPv4 and IPv6; notify application and start throttling timer
T-3	Throttling timer expires		
T-4	Network grants SADB with IPv4 address (NAS) only, IPv6 not allowed		Provide IPv4 address to apps
T-5	Network grants SADB with deferred IPv4 address (DHCP) only, IPv6 not allowed		Initiate DHCP procedures to obtain IPv4 address
T-6	Network grants IPv4 address via DHCP, IPv6 not allowed		Provide IPv4 address to apps
T-8	Network grants DADB with IPv4 address (NAS) and IPv6 IID		Provide IPv4 address to apps; initiate RS/RA if IPv6 address is needed
T-9	Network grants DADB with deferred IPv4 address (DHCP) and IPv6 IID		Initiate DHCP procedures if IPv4 address is needed; initiate RS/RA if IPv6 address is needed
T-10	IPv4 address obtained via DHCP is released, release not renewed or revoked by network		Apps are notified that IPv4 connectivity is unavailable
T-11	Network grants IPv4 address via DHCP		Provide IPv4 address to apps
T-12	IPv6 prefix assigned via RS/RA		Provide IPv6 address to apps
T-13	IPv6 prefix assigned via RS/RA		Provide IPv6 address to apps
T-14	Network grants IPv4 address via DHCP		Provide IPv4 address to apps
T-15	IPv4 address obtained via DHCP is released, release not renewed or revoked by network		Apps are notified that IPv4 connectivity is unavailable
T-16	Network grants SADB with IPv4 address (NAS), allows separate IPv6 bearer request		Provide IPv4 address to apps; initiate IPv6 bearer request procedures if IPv6 address is needed

Transition	Trigger	Condition	Action
T-17	Network grants SADB with deferred IPv4 address (DHCP), allows separate IPv6 bearer request		Initiate IPv6 bearer request procedures if IPv6 address is needed
T-18	Network grants SADB with IPv6 IID, allows separate IPv4 bearer request		Initiate RS/RA procedure to obtain IPv6 prefix; initiate IPv4 bearer request procedures if IPv4 address is needed
T-19	IPv4 address obtained via DHCP is released (release not renewed or revoked by network) <OR> IPv4 bearer is released		Apps are notified that IPv4 connectivity is unavailable
T-20	Network grants IPv4 address via DHCP on an existing bearer, or grants a bearer with IPv4 (NAS)		Provide IPv4 address to apps
T-21	Network grants SADB with IPv6 IID, in addition to existing IPv4 bearer		Initiate RS/RA procedure to obtain IPv6 prefix
T-22	Network grants IPv6 prefix		Provide IPv6 address to apps
T-23	Network releases IPv6 bearer		Apps are notified that IPv6 connectivity is unavailable
T-24	IPv6 prefix assigned via RS/RA		Provide IPv6 address to apps
T-25	Network releases IPv6 bearer		Apps are notified that IPv6 connectivity is unavailable
T-26	Network grants IPv4 address via DHCP on existing bearer, or grants bearer with IPv4 (NAS)		Provide IPv4 address to apps
T-27	IPv4 address obtained via DHCP is released (release not renewed or revoked by network) <OR> IPv4 bearer is released		Apps are notified that IPv4 connectivity is unavailable
T-28	Network grants SADB with IPv6 IID only, IPv4 not allowed		Initiate RS/RA if IPv6 address is needed
T-29	IPv6 prefix assigned via RS/RA, IPv4 not allowed		Provide IPv6 address to apps
T-30	IPv6 lease expires		Apps are notified that IPv6 connectivity is unavailable
T-31	IPv4 lease expires		Apps are notified that IPv4 connectivity is unavailable
T-32	IPv6 lease expires		Apps are notified that IPv6 connectivity is unavailable

1

4.2.2.1 PDN connectivity FSM, LTE substates

Figure 4-4 shows the substates in S3A: DADB with IPv4.

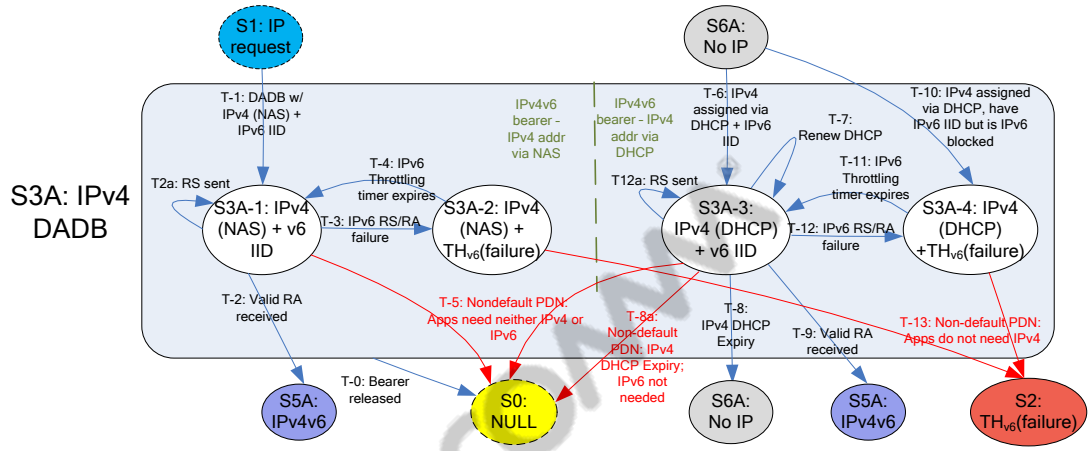

Figure 4-4 Substates in S3A: DADB with IPv4

Table 4-5 shows the substates in S3A: DADB with IPv4.

Table 4-5 Substates in S3A: DADB with IPv4

#	State name	Description
S3A-1	IPv4 (NAS) + IPv6 IID	Dual address bearer established; IPv4 address assigned via NAS, IPv6 IID assigned but no prefix yet
S3A-1	IPv4 (NAS) + IPv6 throttled	Dual address bearer established; IPv4 address assigned via NAS, IPv6 address requests are throttled due to RS/RA failure
S3A-2	IPv4 (DHCP) + IPv6 IID	Dual address bearer established; IPv4 address assigned via DHCP, IPv6 IID assigned but no prefix yet
S3A-3	IPv4 (DHCP) + IPv6 throttled	Dual address bearer established; IPv4 address assigned via DHCP, IPv6 address requests are throttled due to RS/RA failure

Table 4-6 shows the transitions in S3A: DADB with IPv4.

Table 4-6 Transitions in S3A: DADB with IPv4

Transition	Trigger	Condition	Action
T-0	Network releases dual-address bearer		Apps are notified that IPv4 connectivity is unavailable
T-1	Network assigns dual-address bearer with IPv4 address (NAS) and IPv6 IID		Provide IPv4 address to apps
T-2	Valid RA with IPv6 prefix is received		Provide IPv6 address to apps
T-2a	Timeout waiting for RA		Send RS to obtain IPv6 prefix
T-3	RS/RA procedure failure		Consider PDN to be throttled for IPv6; start IPv6 throttling timer
T-4	IPv6 throttling timer expires		No action, apps are no longer throttled to request IPv6
T-5	Apps no longer need IPv4 or IPv6	Nondefault PDN	Release dual address bearer
T-6	IPv4 address assigned via DHCP to existing dual address bearer with IPv6 IID		Provide IPv4 address to apps
T-7	DHCP IPv4 lease is renewed successfully		
T-8	DHCP IPv4 lease expires or is revoked		Apps are notified that IPv4 connectivity is unavailable
T-8a	DHCP IPv4 lease expires or is revoked; IPv6 is not needed	Nondefault PDN	Apps are notified that IPv4 connectivity is unavailable, release bearer
T-9	Valid RA with IPv6 prefix is received		Provide IPv6 address to apps
T-10	IPv4 is assigned via DHCP to existing dual address bearer with IPv6 throttled		Provide IPv4 address to Apps
T-11	IPv6 throttling timer expires		No action. apps are no longer throttled to request IPv6
T-12	RS/RA procedure failure		Consider PDN to be throttled for IPv6; start IPv6 throttling timer
T-12a	Timeout waiting for RA		Send RS to obtain IPv6 prefix
T-13	Apps no longer need IPv4	Nondefault PDN	Release dual address bearer; continue to throttle IPv6 requests

Figure 4-5 shows the substates in S4A: DADB with IPv6.

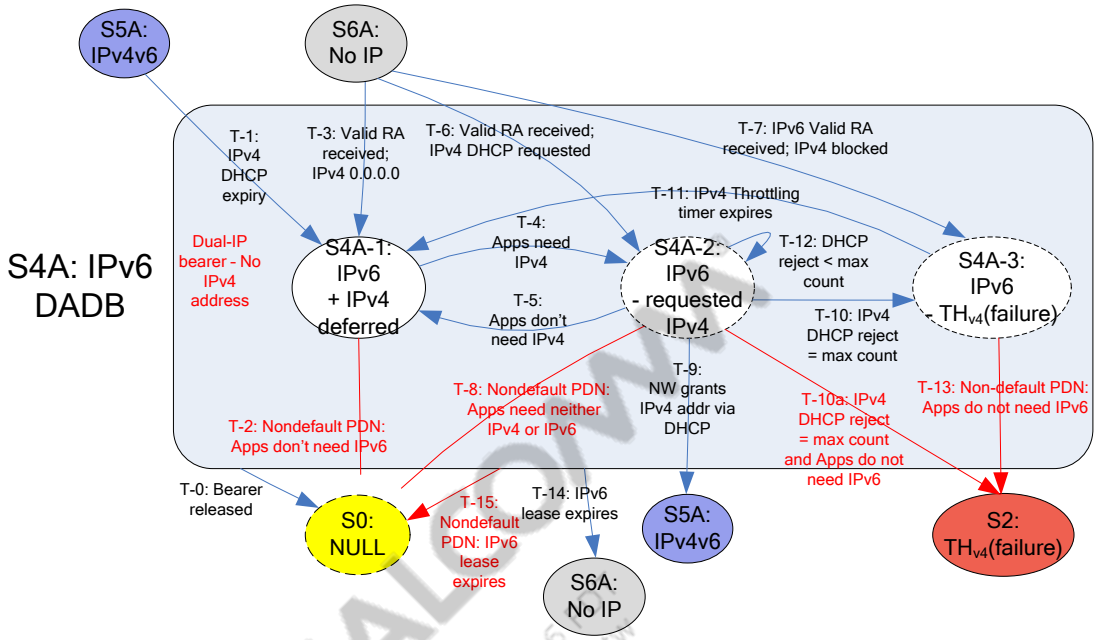

Figure 4-5 Substates in S4A: DADB with IPv6

Table 4-7 shows the substates in S4A: DADB with IPv6.

Table 4-7 Substates in S4A: DADB with IPv6

#	State name	Description
S4A-1	IPv6+IPv4 deferred	Dual address bearer established; IPv6 address assigned, IID + prefix; IPv4 address deferred
S4A-2	IPv6+requested IPv4	Dual address bearer established; IPv6 address assigned, IID + prefix; IPv4 address requested
S3A-3	IPv6+IPv4 throttled	Dual address bearer established; IPv6 address assigned, IID + prefix; IPv4 address throttled

Table 4-8 shows the transitions in S4A: DADB with IPv6.

Table 4-8 Transitions in S4A: DADB with IPv6

Transition	Trigger	Condition	Action
T-0	Network releases dual address bearer		Apps are notified that IPv6 connectivity is unavailable
T-1	IPv4 DHCP lease expires or is revoked		Apps are notified that IPv4 connectivity is unavailable
T-2	Apps no longer need IPv4 or IPv6	Nondefault PDN	Release dual address bearer
T-3	Valid RA with IPv6 prefix is received while IPv4 is deferred		Provide IPv6 address to apps
T-4	Apps need IPv4 address		Send DHCP request for IPv4 address
T-5	Apps do not need IPv4 address		
T-6	Valid RA with IPv6 prefix is received while request for IPv4 is pending		Provide IPv6 address to apps
T-7	Valid RA with IPv6 prefix is received while IPv4 is throttled		Provide IPv6 address to apps
T-8	Apps no longer need IPv4 or IPv6	Nondefault PDN	Release dual address bearer
T-9	IPv4 is assigned via DHCP, to existing dual address bearer with IPv6 address		Provide IPv4 address to apps
T-10	DHCP request for IPv4 address unsuccessful after reaching maximum attempts		Consider IPv4 to be throttled, start IPv4 throttling timer
T-10a	DHCP request for IPv4 address unsuccessful after reaching maximum attempts; IPv6 no longer needed	Nondefault PDN	Consider IPv4 to be throttled; start IPv4 throttling timer, release dual address bearer
T-11	IPv4 throttling timer expires		No action, apps are no longer throttled to request IPv4
T-12	DHCP request for IPv4 address unsuccessful before reaching maximum attempts		Increment counter, retry DHCP request
T-13	Apps no longer need IPv6	Nondefault PDN	Release dual address bearer, continue to throttle IPv4 requests
T-14	IPv6 lease expires		Apps are notified that IPv6 connectivity is unavailable
T-15	IPv6 lease expires	Nondefault PDN	Apps are notified that IPv6 connectivity is unavailable; dual address bearer is released

Figure 4-6 shows the substates in S5A: DADB with IPv4v6.

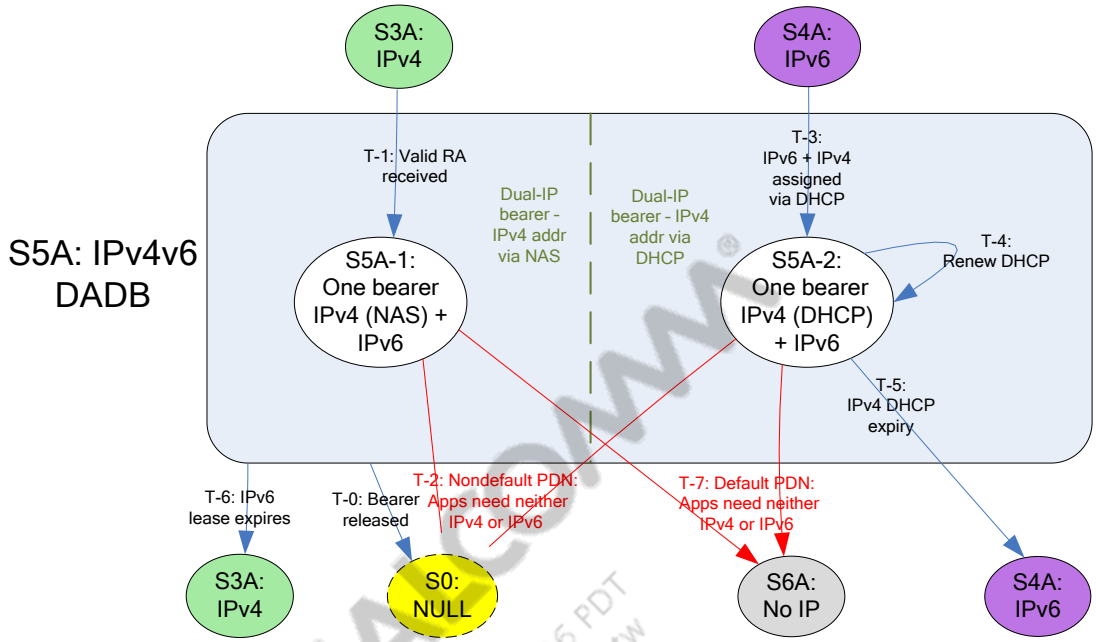

Figure 4-6 Substates in S5A: DADB with IPv4v6

Table 4-9 shows the substates in S5A: DADB with IPv4v6.

Table 4-9 Substates in S5A: DADB with IPv4v6

#	State name	Description
S5A-1	IPv6+IPv4 via NAS	Dual address bearer established; IPv6 address assigned, IID + prefix; IPv4 address assigned via NAS
S5A-2	IPv6+IPv4 via DHCP	Dual address bearer established; IPv6 address assigned, IID + prefix; IPv4 address assigned via DHCP

Table 4-10 shows the transitions in S5A: DADB with IPv4v6.

Table 4-10 Transitions in S5A: DADB with IPv4v6

Transition	Trigger	Condition	Action
T-0	Network releases dual address bearer		Apps are notified that IPv4 and IPv6 connectivity is unavailable
T-1	Valid RA with IPv6 prefix is received while IPv4 is assigned via NAS		Provide IPv6 address to apps
T-2	Apps need neither IPv4 nor IPv6	Nondefault PDN	Release dual address bearer
T-3	IPv4 is assigned via DHCP to existing dual address bearer with IPv6 address		Provide IPv4 address to apps
T-4	DHCP IPv4 lease is renewed successfully		
T-5	IPv4 DHCP lease expires or is revoked		Apps are notified that IPv4 connectivity is unavailable
T-6	IPv6 lease expires		Apps are notified that IPv6 connectivity is unavailable
T-7	Apps need neither IPv4 nor IPv6		

Figure 4-7 shows the substates in S6A: DADB with no IP.

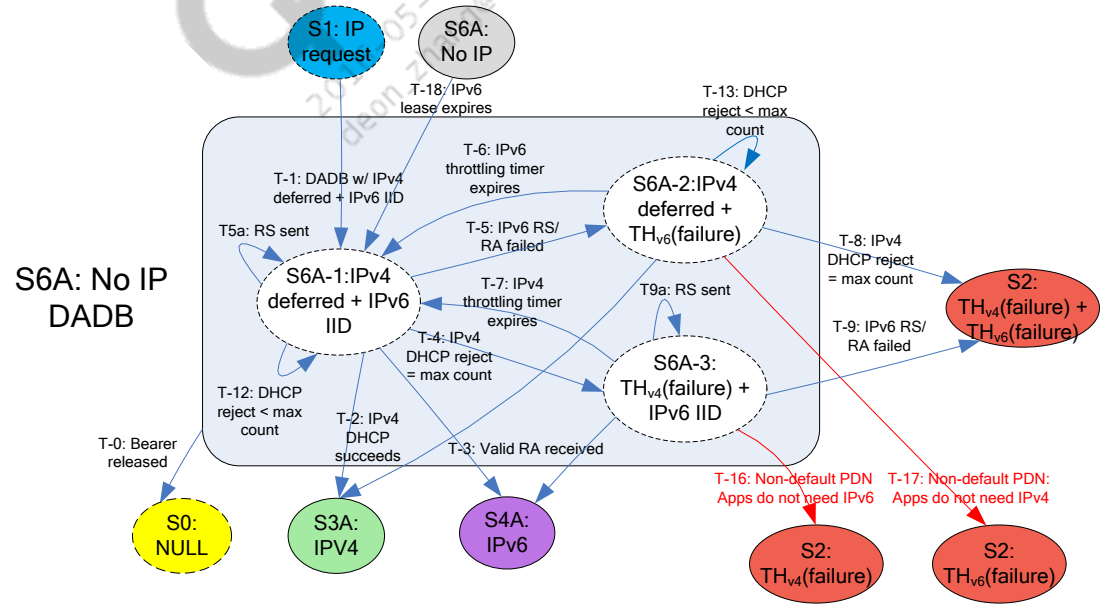

Figure 4-7 Substates in S6A: DADB with no IP

Table 4-11 shows the substates in S6A: DADB with no IP.

Table 4-11 Substates in S6A: DADB with no IP

#	State Name	Description
S6A-1	IPv4 deferred + IPv6 IID	Dual address bearer established; IPv4 address deferred; IPv6 prefix requested
S6A-2	IPv4 deferred + IPv6 throttled	Dual address bearer established; IPv4 address deferred; IPv6 address requests throttled
S6A-3	IPv4 throttled + IPv6 IID	Dual address bearer established; IPv4 address requests throttled; IPv6 prefix requested

Table 4-12 shows transitions in S6A: DADB with no IP.

Table 4-12 Transitions in S6A: DADB with no IP

Transition	Trigger	Condition	Action
T-0	Network releases dual address bearer		Apps are notified that IPv4 and IPv6 connectivity is unavailable
T-1	Network establishes dual address bearer with deferred IPv4 and IPv6 IID		IPv6 prefix is requested via RS/RA procedure
T-2	IPv4 is assigned via DHCP to existing dual address bearer		Provide IPv4 address to apps
T-3	Valid RA with IPv6 prefix is received		Provide IPv6 address to apps
T-4	DHCP request for IPv4 address unsuccessful after reaching maximum attempts		Consider IPv4 to be throttled, start IPv4 throttling timer
T-5	RS/RA procedure failure		Consider PDN to be throttled for IPv6; start IPv6 throttling timer
T-5a	Timeout waiting for RA		Send RS to obtain IPv6 prefix
T-6	IPv6 throttling timer expires		No action, apps are no longer throttled to request IPv6
T-7	IPv4 throttling timer expires		No action, apps are no longer throttled to request IPv4
T-8	DHCP request for IPv4 address unsuccessful after reaching maximum attempts while IPv6 is throttled		Consider IPv4 to be throttled, start IPv4 throttling timer; release bearer (nondefault PDN) or detach (default PDN)
T-9	RS/RA procedure failure while IPv4 is throttled)		Consider PDN to be throttled for IPv6, start IPv6 throttling timer; release bearer (nondefault PDN) or detach (default PDN)
T-9a	Timeout waiting for RA		Send RS to obtain IPv6 prefix
T-12	DHCP request for IPv4 address unsuccessful before reaching maximum attempts		Increment counter, retry DHCP request
T-13	DHCP request for IPv4 address unsuccessful before reaching maximum attempts		Increment counter, retry DHCP request

Transition	Trigger	Condition	Action
T-16	Apps do not need IPv6	Nondefault PDN	Release dual address bearer
T-17	Apps do not need IPv4	Nondefault PDN	Release dual address bearer

Figure 4-8 shows the substates in S3B1: SADB-1B with IPv4.

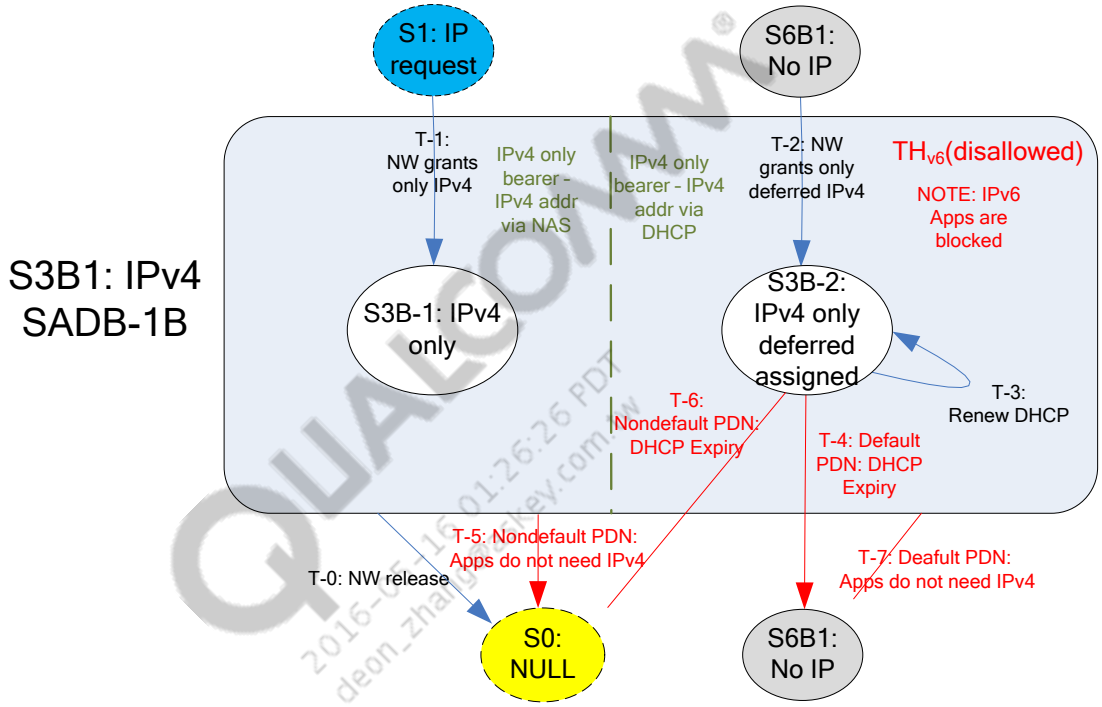

Figure 4-8 Substates in S3B1: SADB-1B with IPv4

Table 4-13 shows substates in S3B1: SADB-1 with IPv4.

Table 4-13 Substates in S3B1: SADB-1 with IPv4

#	State Name	Description
S3B-1	IPv4 only via NAS	Single address bearer for IPv4 established; IPv4 address assigned (NAS); Separate bearer for IPv6 is not allowed.
S3B-2	IPv4 only via NAS	Single address bearer for IPv4 established; IPv4 address assigned (DHCP); Separate bearer for IPv6 is not allowed.

Table 4-14 shows transitions in S3B1: SADB-1 with IPv4.

Table 4-14 Transitions in S3B1: SADB-1 with IPv4

Transition	Trigger	Condition	Action
T-0	Network releases single address bearer		Apps are notified that IPv4 and IPv6 connectivity is unavailable
T-1	Network establishes single address bearer with IPv4 address (NAS); IPv6 address is not allowed		Provide IPv4 address to apps
T-2	IPv4 address assigned via DHCP to existing single address bearer		Provide IPv4 address to apps
T-3	IPv4 DHCP lease is renewed successfully		
T-4	IPv4 DHCP lease expires or is revoked		Apps are notified that IPv4 connectivity is unavailable
T-5	Apps no longer need IPv4	Nondefault PDN	Release single address bearer
T-6	IPv4 DHCP lease expires or is revoked	Nondefault PDN	Release single address bearer
T-7	Apps no longer need IPv4		

Figure 4-9 shows substates in S4B1: SADB-1B with IPv6.

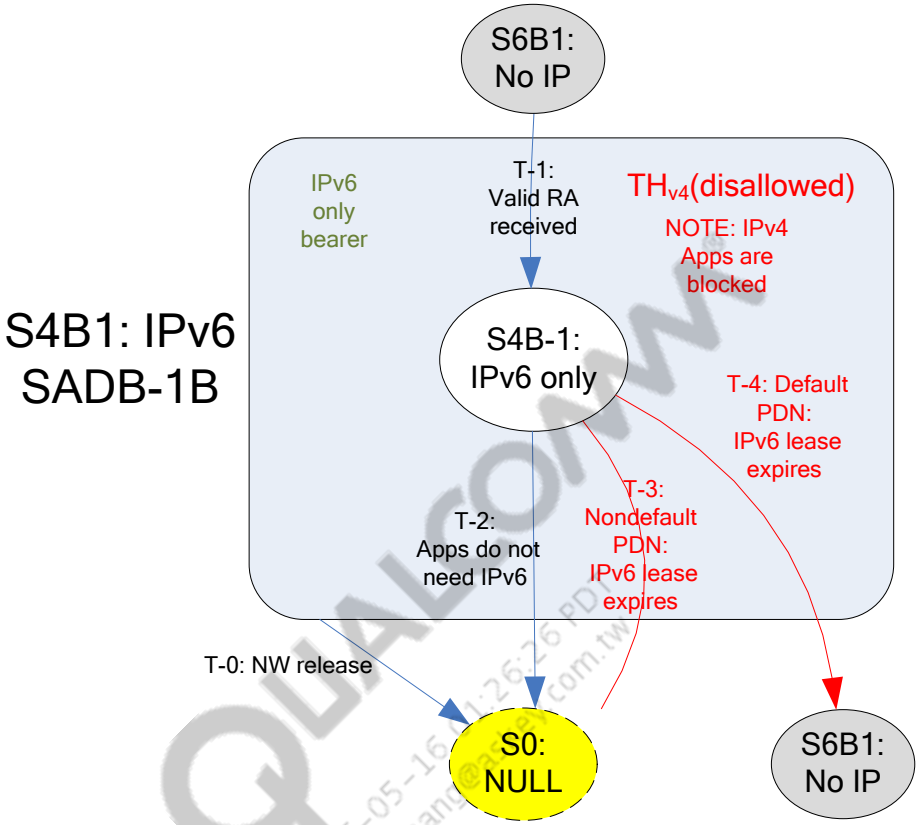

Figure 4-9 Substates in S4B1: SADB-1B with IPv6

Table 4-15 shows substates in S4B1: SADB-1 with IPv6.

Table 4-15 Substates in S4B1: SADB-1 with IPv6

#	State name	Description
S4B-1	IPv6 only	Single address bearer for IPv6 established; IPv6 address assigned (IID + prefix); separate bearer for IPv4 is not allowed

Table 4-16 shows transitions in S4B1: SADB-1 with IPv6.

Table 4-16 Transitions in S4B1: SADB-1 with IPv6

Transition	Trigger	Condition	Action
T-0	Network releases single address bearer		Apps are notified that IPv6 connectivity is unavailable
T-1	Valid RA with IPv6 prefix is received		Provide IPv6 address to apps
T-2	Apps no longer need IPv6		Release single address bearer
T-3	IPv6 lease expires	Nondefault PDN	Apps are notified that IPv6 connectivity is unavailable; release single address bearer
T-4	IPv6 lease expires	Nondefault PDN	Apps are notified that IPv6 connectivity is unavailable

Figure 4-10 shows substates in S6B1: SADB-1B with no IP.

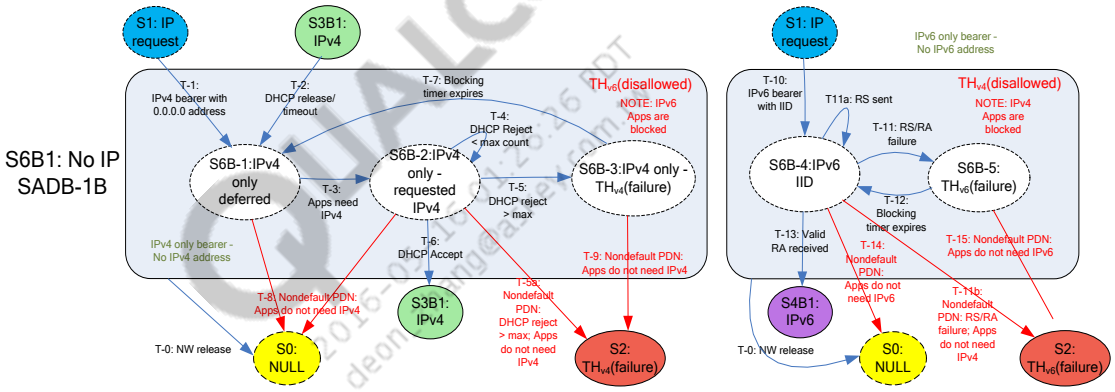

Figure 4-10 Substates in S6B1: SADB-1B with no IP

Table 4-17 shows substates in S6B1: SADB-1 with no IP.

Table 4-17 Substates in S6B1: SADB-1 with no IP

#	State name	Description
S6B-1	IPv4 only deferred	Single address bearer for IPv4 established; IPv4 address is deferred; separate bearer for IPv6 is not allowed
S6B-2	IPv4 only requested IPv4	Single address bearer for IPv4 established; request for IPv4 address is pending; separate bearer for IPv6 is not allowed
S6B-3	IPv4 only IPv4 throttled	Single address bearer for IPv4 established; IPv4 address is throttled; separate bearer for IPv6 is not allowed
S6B-4	IPv6 only IID	Single address bearer for IPv6 established; IPv6 IID received, but prefix request is pending; separate bearer for IPv4 is not allowed
S6B-5	IPv6 only throttled	Single address bearer for IPv6 established; IPv6 address is throttled due to unsuccessful RS/RA procedure; separate bearer for IPv4 is not allowed

Table 4-18 shows transitions in S6B1: SADB-1 with no IP.

Table 4-18 Transitions in S6B1: SADB-1 with no IP

Transition	Trigger	Condition	Action
T-0	Network releases single address bearer		Apps are notified that IPv4 and IPv6 connectivity is unavailable
T-1	Network establishes single address bearer with IPv4 address deferred; IPv6 address is not allowed		
T-2	IPv4 DHCP lease expires or is revoked		Apps are notified that IPv4 connectivity is unavailable
T-3	Apps need IPv4 address		Send DHCP request for IPv4 address
T-4	DHCP request for IPv4 address unsuccessful, less than maximum number of times		Reattempt DHCP procedure
T-5	DHCP request for IPv4 address unsuccessful, equal to maximum number of times		Consider PDN to be throttled for IPv4, start IPv4 throttling timer
T-5a	DHCP request for IPv4 address unsuccessful, equal to maximum number of times; apps no longer need IPv4	Nondefault PDN	Consider PDN to be throttled for IPv4, start IPv4 throttling timer; release single address bearer
T-6	IPv4 address assigned via DHCP to existing single address bearer		Provide IPv4 address to apps
T-7	IPv4 throttling timer expires		No Action, apps are no longer throttled to request IPv4
T-8	Apps no longer need IPv4	Nondefault PDN	Release single address bearer
T-9	Apps no longer need IPv4	Nondefault PDN	Release single address bearer; start IPv4 throttling timer
T-10	Network establishes a single address bearer with IPv6 IID.		IPv6 prefix is requested via RS/RA procedure
T-11	RS/RA procedure failure		Consider PDN to be throttled for IPv6; start IPv6 throttling timer
T-11a	Timeout waiting for RA		Send RS to obtain IPv6 prefix
T-11b	RS/RA procedure failure; apps no longer need IPv4	Nondefault PDN	Consider PDN to be throttled for IPv6; start IPv6 throttling timer; release single address bearer
T-12	IPv6 throttling timer expires		No action, apps are no longer throttled to request IPv6
T-13	Valid RA with IPv6 prefix is received		Provide IPv6 address to apps
T-14	Apps no longer need IPv6	Nondefault PDN	Release single address bearer
T-15	Apps no longer need IPv6	Nondefault PDN	Release single address bearer; start IPv6 throttling timer

Figure 4-11 shows the substates for SADB-2B: Independent state machines maintained for IPv4 (top) and IPv6 bearers (bottom).

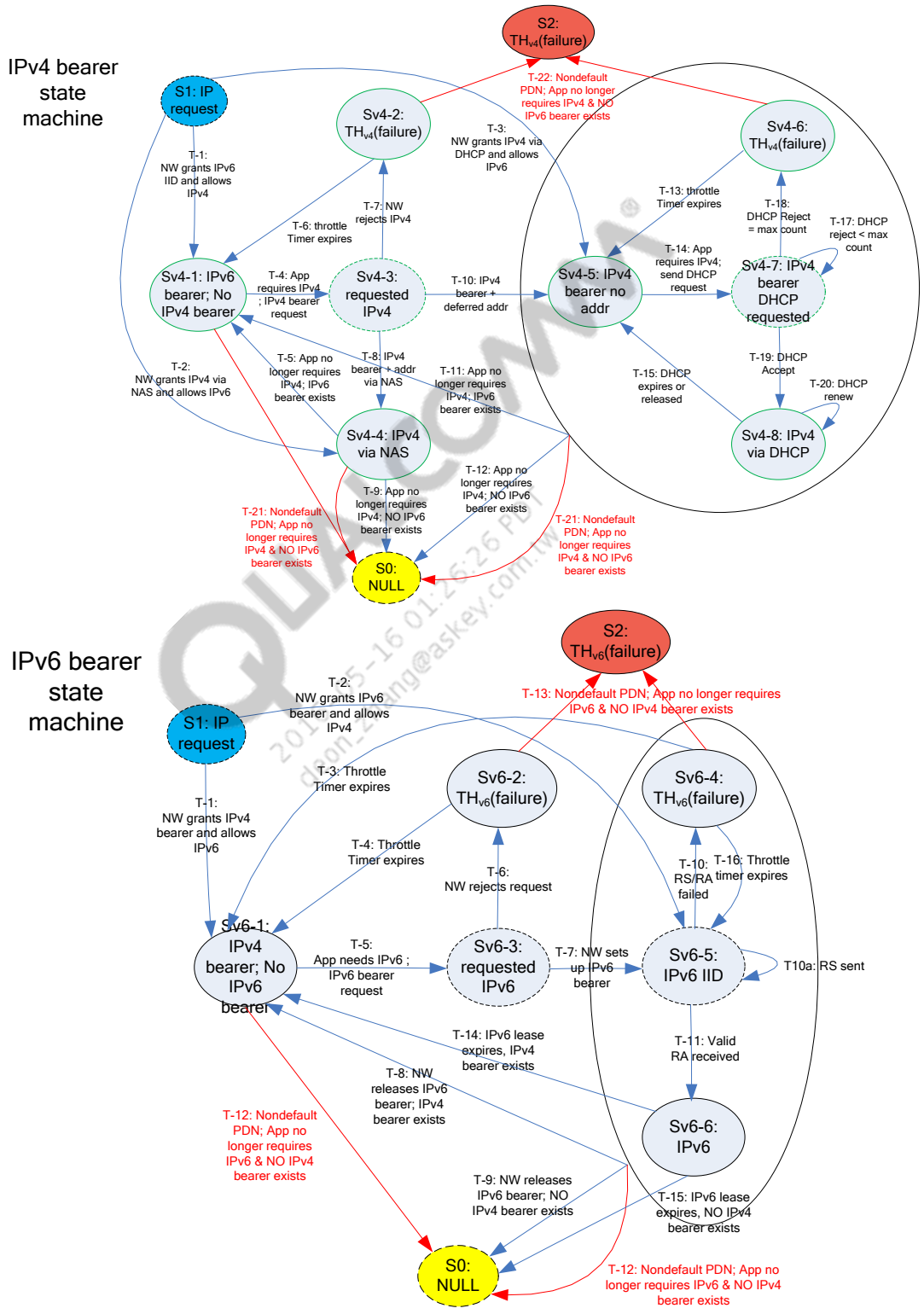

Figure 4-11 Substates for SADB-2B: Independent state machines maintained for IPv4 (top) and IPv6 bearers (bottom)

Table 4-19 shows the substates for the IPv4 bearer state machine.

Table 4-19 Substates for IPv4 bearer state machine

#	State name	Description
Sv4-1	No IPv4 bearer	No IPv4 bearer established, IPv6 bearer exists
Sv4-2	IPv4 bearer throttled	IPv4 bearer is throttle
Sv4-3	Requested IPv4	IPv4 bearer requested
Sv4-4	IPv4 bearer; IPv4 via NAS	IPv4 bearer established; IPv4 address assigned (NAS)
Sv4-5	IPv4 bearer; no IPv4 address	IPv4 bearer established; IPv4 address deferred (DHCP)
Sv4-6	IPv4 bearer; IPv4 DHCP throttled	IPv4 bearer established; IPv4 address throttled (DHCP unsuccessful)
Sv4-7	IPv4 bearer; IPv4 DHCP requested	IPv4 bearer established; IPv4 address requested via DHCP
Sv4-8	IPv4 bearer; IPv4 via DHCP	IPv4 bearer established; IPv4 address assigned (DHCP)

Table 4-20 shows transitions in the IPv4 bearer state machine.

Table 4-20 Transitions in IPv4 bearer state machine

Transition	Trigger	Condition	Action
T-1	Network establishes single address bearer with IPv6 IID; request for IPv4 address is allowed		IPv6 prefix is requested via RS/RA procedure
T-2	Network establishes single address bearer with IPv4 address (NAS); request for IPv6 address is allowed		Provide IPv4 address to apps
T-3	Network establishes single address bearer with deferred IPv4 address (DHCP); request for IPv6 address is allowed		
T-4	Apps trigger request for IPv4 address		PDN connectivity request for IPv4 bearer is sent
T-5	Network releases IPv4 bearer, IPv6 bearer still exists		Apps are notified that IPv4 connectivity is unavailable
T-6	IPv4 throttling timer expires		No action, apps are no longer throttled to request IPv4
T-7	Network rejects IPv4 bearer request		Consider IPv4 to be throttled; start IPv4 throttling timer
T-8	Network establishes single address bearer with IPv4 address (NAS)		Provide IPv4 address to apps
T-9	Network releases IPv4 bearer, no IPv6 bearer exists		Apps are notified that IPv4 connectivity is unavailable

Transition	Trigger	Condition	Action
T-10	Network establishes single address bearer with deferred IPv4 address (DHCP)		
T-11	Network releases IPv4 bearer, IPv6 bearer still exists		Apps are notified that IPv4 connectivity is unavailable
T-12	Network releases IPv4 bearer, No IPv6 bearer exists		Apps are notified that IPv4 connectivity is unavailable
T-13	IPv4 throttling timer expires		No action, apps are no longer throttled to request IPv4
T-14	Apps trigger a request for IPv4 address		DHCP request for IPv4 address is sent
T-15	IPv4 DHCP lease expires or is revoked		Apps are notified that IPv4 connectivity is unavailable
T-17	DHCP request for IPv4 address unsuccessful, less than maximum number of times		Reattempt DHCP procedure
T-18	DHCP request for IPv4 address unsuccessful, equal to maximum number of times		Consider PDN to be throttled for IPv4; start IPv4 throttling timer
T-19	Network grants IPv4 address via DHCP		Provide IPv4 address to apps
T-20	DHCP IPv4 lease is renewed successfully		
T-21	Apps do not need IPv4 and no IPv6 bearer exists while throttling timer is running	Non-default PDN	Release single address bearer
T-22	Apps do not need IPv4 and no IPv6 bearer exists	Non-default PDN	Release single address bearer; start IPv6 throttling timer

Table 4-21 shows substates for the IPv6 bearer state machine.

Table 4-21 Substates for IPv6 bearer state machine

#	State name	Description
Sv6-1	No IPv4 bearer	No IPv6 bearer established, IPv4 bearer exists
Sv6-2	IPv6 bearer throttled	IPv6 bearer is throttled
Sv6-3	Requested IPv6	IPv6 bearer requested
Sv6-4	IPv6 prefix throttled	IPv6 bearer established; IPv6 prefix allocation is throttled
Sv6-5	IPv6 IID	IPv6 bearer established; IPv6 IID assigned, prefix requested
Sv6-6	IPv6	IPv6 bearer established; IPv6 address assigned, IID+prefix

Table 4-22 shows transitions in the IPv6 bearer state machine.

Table 4-22 Transitions in IPv6 bearer state machine

Transition	Trigger	Condition	Action
T-1	Network establishes single address bearer for IPv4; request for IPv6 address is allowed		No action
T-2	Network establishes single address bearer with IPv6 address; request for IPv4 address is allowed		IPv6 prefix is requested via RS/RA procedure
T-3	IPv6 throttling timer expires		No action, apps are no longer throttled to request IPv6
T-4	IPv6 throttling timer expires		No action, apps are no longer throttled to request IPv6
T-5	Apps trigger a request for IPv6 address		PDN connectivity request for IPv6 bearer is sent
T-6	Network rejects IPv6 bearer request		Consider IPv6 to be throttled; start IPv6 throttling timer
T-7	Network establishes single address bearer with IPv6 IID		IPv6 prefix is requested via RS/RA procedure
T-8	Network releases IPv6 bearer, IPv4 bearer still exists		Apps are notified that IPv6 connectivity is unavailable
T-9	Network releases IPv6 bearer, no IPv6 bearer exists		Apps are notified that IPv6 connectivity is unavailable
T-10	RS/RA procedure failure		Consider PDN to be throttled for IPv6; start IPv6 throttling timer
T-10a	Timeout waiting for RA		Send RS to obtain IPv6 prefix
T-11	Valid RA with IPv6 prefix is received		Provide IPv6 address to apps
T-12	Apps do not need IPv6 and no IPv4 bearer exists	Nondefault PDN	Release single address bearer
T-13	Apps do not need IPv6 and no IPv4 bearer exists	Nondefault PDN	Release single-address bearer
T-14	IPv6 address lease expires, IPv4 bearer still exists		Apps are notified that IPv6 connectivity is unavailable
T-15	IPv6 address lease expires, no IPv4 bearer exists		Apps are notified that IPv6 connectivity is unavailable; release single address bearer
T-16	IPv6 throttling timer expires		IPv6 prefix is requested via RS/RA procedure

4.2.3 State machine 3.2 – LTE QoS state machine

The assumption is that there can be two different ways QoS is established per application. The way QoS is established depends on how the application is configured in the application profile.

- UE-initiated QoS – In this case, all QoS is established and released by the application. The application must provide the required QoS for all supported RATs.
- Network-initiated QoS – The application is unaware of QoS. In this case, QoS is controlled by the network and the application is not aware of whether QoS is available.
- Network-initated QoS – The application is aware of QoS. In this case, the application registers for a notification when a certain QoS level is established for a certain packet filter. When a dedicated bearer that meets the QoS for the packet filter is set up, the application is notified and may take further action.

4.2.3.1 Requirements and assumptions

When checking for QoS, the DS layer only performs exact filter matching to determine if a bearer has been set up for a QoS filter defined by an application.

When a bearer has been created by the network and the filter matches the one specified by an application, then the corresponding QoS is notified to the application. The application decides if the QoS is acceptable.

4.2.3.2 UE-initiated QoS

For UE-initiated QoS, the required QoS is specified for each supported RAT in the application profile. This means:

- For LTE, the QCI, GBR, and MBR are specified.
- For UTRAN/GERAN, the GPRS QoS parameters are specified.
- For eHRPD, the flow profile ID is specified.

Figure 4-12 shows QoS FSM and LTE, or UE-initiated QoS.

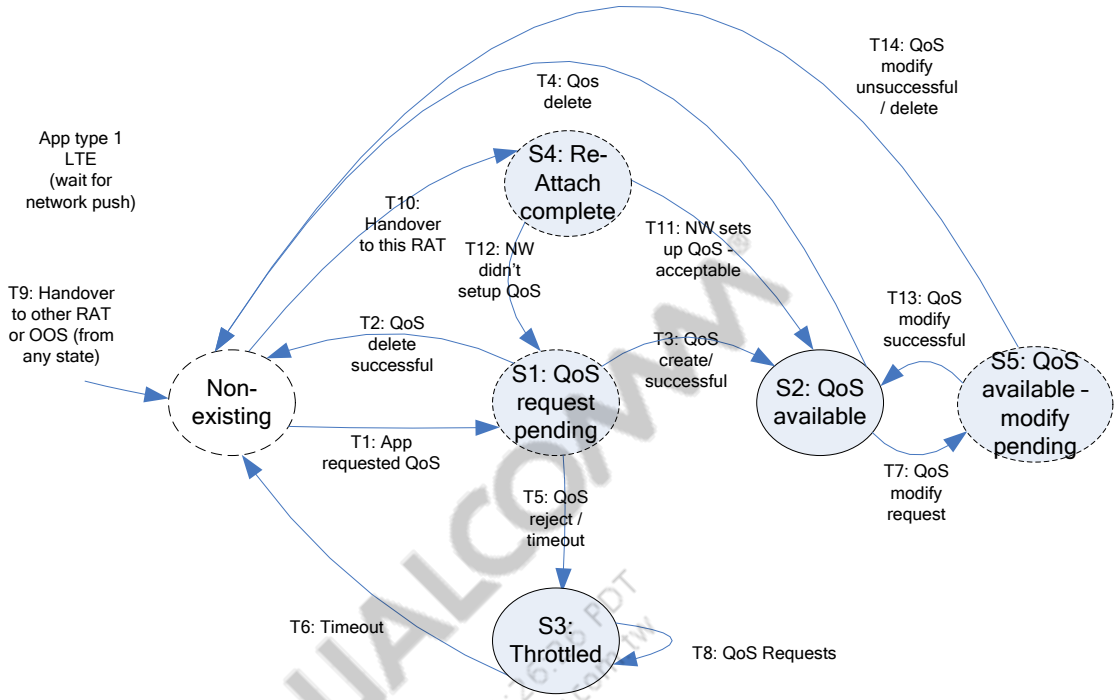

Figure 4-12 QoS FSM and LTE, UE-initiated QoS

Table 4-23 shows details about the LTE QoS FSM states.

Table 4-23 Details about LTE QoS FSM states

#	State name	Description
S1	QoS request pending	UE sent a QoS request to the network waiting for a response; QoS request timer is running
S2	QoS available	Network granted QoS
S3	Throttled	QoS requests from the application are throttled, i.e., ignored; throttling timer is running
S4	Reattach complete	UE has just successfully handed over to E-UTRAN from another RAT; QoS not yet established on this RAT; UE is waiting for an indication whether QoS is UE or network-initiated, indicated as part of the attach/dedicated bearer setup procedure
S5	QoS available – Modify pending	Application requested to modify the QoS, upon which a QoS modify request was sent to the network; QoS modify timer is running

Table 4-24 shows the details of LTE QoS FSM state transitions.

Table 4-24 Details of LTE QoS FSM state transitions

Transition	Trigger	Condition	Action
T1	App requested QoS		Send QoS request to the network; start QoS timer
T2	App deleted QoS before network granted it		Send QoS delete to the network; delete QoS context locally
T3	QoS create successful		Response received by the network that the QoS bearer was successfully created; app is notified that QoS is available
T4	QoS delete		App or network deleted the QoS bearer; if deleted by the network, the app is notified; QoS context is deleted
T5	QoS reject		Network rejected the QoS request; throttling timer is started and further app requests for this specific TFT/filter are rejected until the timer expires
T6	QoS timer expires		Further app requests for QoS for this TFT/filter are no longer rejected
T7	QoS modify request		App requests modification of the QoS; request is sent to the network
T8	QoS requests		In the Throttled state, further QoS requests from the app are rejected
T9	Handover to another RAT from any state		Handover to another RAT is triggered; QoS context may or may not be transferred to the new RAT, however, in the context of E-UTRAN, the QoS context is deleted
T10	Handover to E-UTRAN from another RAT		Handover to E-UTRAN from another RAT is triggered; acceptable QoS will be determined; QoS handover timer is started, waiting for network-initiated QoS to be set up on E-UTRAN
T11	Network sets up QoS – Acceptable		Network sets up QoS and QoS is deemed acceptable; QoS available notification is sent to the app
T12	Network did not set up QoS		Network sets up QoS, but QoS is deemed unacceptable or the QoS handover timer expires; in this case, a QoS request is sent to the network and the QoS timer is started
T13	QoS modify request successful		Network granted the QoS modify request; app is notified that new QoS is available
T14	QoS modify request unsuccessful		Network did not grant the QoS modify request or deleted the QoS bearer; app is notified that the QoS is unavailable

4.2.3.3 Network-initiated QoS handling, app is aware of QoS case

This section describes how network-initiated QoS could be handled in case UE-initiated QoS is not supported in the network.

The application is set up with a profile similar to a UE-initiated application. One of the application parameters will be a network-initiated QoS flag, indicating if the application is configured for network-initiated QoS. If this is the case, the DS behaves in a certain way, in particular during HO. One example application could be the IMS stack, which will only perform certain actions, i.e., registration, when it knows that QoS is available.

A special API should allow the application to register for a notification from the DS when the network sets up a QoS bearer with certain characteristics that are specified by a given TFT and a minimum QoS. This notification is sent to the application when a matching bearer that satisfied the minimum QoS level specified by the application is established. Similarly, another notification is sent by the DS to the application when the QoS bearer is removed or modified so that the QoS is no longer satisfactory.

NOTE: This entire behavior is only applicable for the initial QoS request. For QoS mobility between radio technologies, the behavior is dictated by the RAT.

For eHRPD, the Bearer Control Mode (BCM) flag indicates whether the UE or the network moves over the QoS.

For LTE, the expectation is that the network always moves over the QoS.

4.2.3.3.1 State machine for network-initiated QoS, application is aware of QoS

Figure 4-13 shows the QoS FSM and LTE network-initiated QoS when the application is aware of QoS.

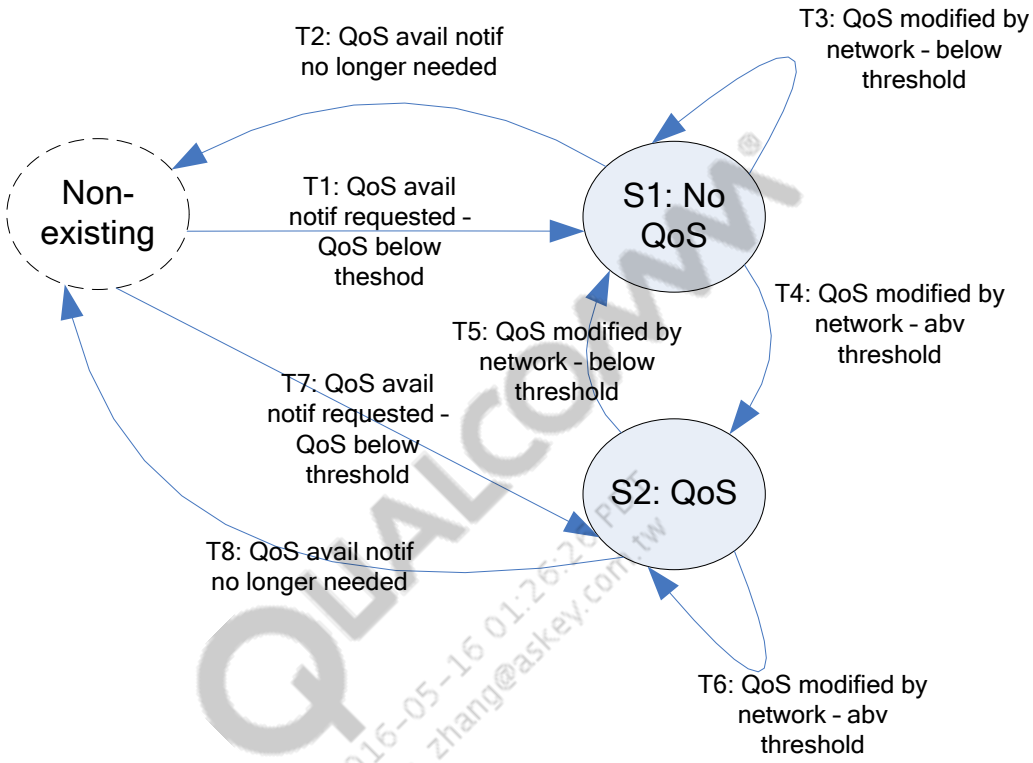

Figure 4-13 QoS FSM and LTE, network-initiated QoS – app aware

Table 4-25 shows details of the LTE QoS FSM state transitions.

Table 4-25 Details of LTE QoS FSM state transitions

#	State name	Description
S1	No QoS	QoS is unavailable or below the threshold required
S2	QoS	QoS is available

Table 4-26 shows details of the LTE QoS FSM state transitions.

Table 4-26 Details of LTE QoS FSM state transitions

Transition	Trigger	Condition	Action
T1	QoS availability notification requested – Below threshold		▪ App requests QoS available notifications, but no QoS bearer is deemed acceptable according to the specified QoS and TFT/filter combination already exists ▪ App is notified that QoS is unavailable ▪ Context is created for this app, setting up notifications to be sent to the app when the QoS for a specified TFT/filter crosses a given acceptable threshold
T2	QoS availability notification no longer needed		QoS availability notification is no longer needed by the app; QoS aware context for this app is deleted
T3	QoS modified by network – Below threshold		QoS bearer was modified by the network, but remains below the acceptable threshold
T4	QoS modified by network – Above threshold		QoS bearer was modified by the network and is above the acceptable threshold; app is notified that QoS is available
T5	QoS modified by network – Below threshold		QoS bearer was modified by the network and is below the acceptable threshold; app is notified that QoS is unavailable
T6	QoS modified by network – Above threshold		QoS bearer was modified by the network, but remains above the acceptable threshold
T7	QoS availability notification requested – Above threshold		▪ App requests QoS available notifications and a QoS bearer that is deemed acceptable according to the specified QoS and TFT/filter combination already exists ▪ App is notified that QoS is available ▪ Context is created for this app, setting up notifications to be sent to the app when the QoS for a specified TFT/filter crosses a given acceptable threshold
T8	QoS availability notification no longer needed		QoS availability notification is no longer needed by the app; QoS aware context for this app is deleted

4.3 eHRPD packet state machines

4.3.1 State machine 3 – eHRPD state machine

The state machine depicting the behavior of the eHRPD stack in the first commercial release timeframe is shown in Figure 4-14.

Table 4-27 displays state machine 3 – eHRPD state machine.

Table 4-27 State machine 3 – eHRPD state machine

State name	Description
eDO_STATE_1	The UE does not have an eHRPD personality in this state.
eDO_STATE_2	The UE acquired a DO system and is performing session negotiation.
eDO_STATE_3	The UE successfully completed session negotiation and the Inuse personality is the eHRPD personality.
eDO_STATE_4	The UE starts the PPP setup procedures when the first application comes up. It transitions to state 4 after the LCP and Auth procedures succeed.
eDO_STATE_5	The UE successfully attached to the PDN and set up the required QoS flows. The UE enters this state with the first PDN connection and remains in this state providing at least one app exists. The subsequent starting of new apps or exiting of existing apps lead to self-transitions within this state.
eDO_STATE_8	The UE is attached to the LTE network. It has a DO session state with an eHRPD personality. In Figure 4-14, the state was created directly over the eHRPD air-interface.
eDO_STATE_9	The UE is attached to the LTE network. It has a DO session state with an eHRPD personality. It also has partial PPP (LCP+Auth) context that it retained after moving from eHRPD to LTE. In this case, both states were created directly over the eHRPD air interface.
eDO_STATE_12	The eDO Session is deleted due to one of the triggers, but partial PPP context exists. The UE is attempting DO session negotiation.
eDO_STATE_13	The eDO Session is deleted due to one of the triggers, but full PPP context exists. The UE is attempting DO session negotiation.

Figure 4-14 shows the state machine representing the eHRPD stack.

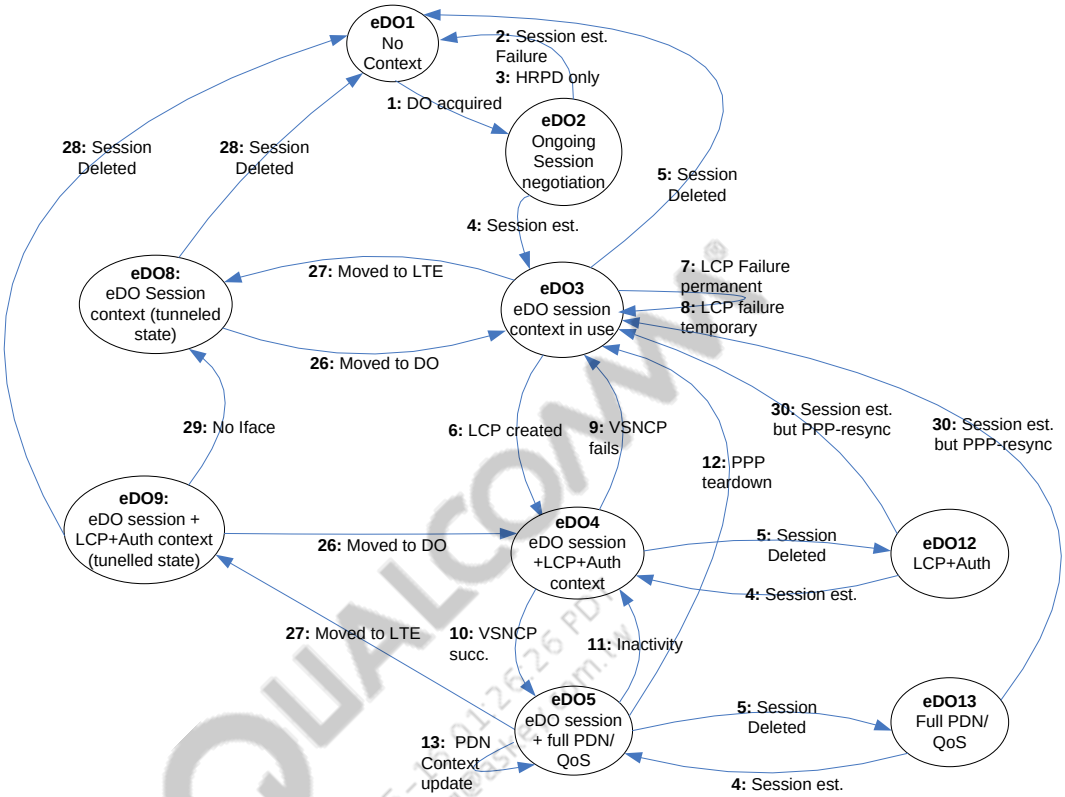

Figure 4-14 State machine representing the eHRPD stack

Table 4-28 lists the eHRPD Packet State machine triggers and transitions.

Table 4-28 eHRPD Packet State machine triggers and transitions

Transition	Trigger	Condition	Action	Event
eDO_Transition_1	DO system acquired	None	Start Session Negotiation	None
eDO_Transition_2	Session negotiation failure	None	Add channels to avoidance list based on failure reason	None
eDO_Transition_3	eDO personality not assigned	None	Inform CM/SD that UE is camped on DO	
eDO_Transition_4	eDO personality assigned	None	Inform CM/SD that UE is camped on eDO	None
eDO_Transition_5	Session loss triggers ▪ Session-Close received ▪ Session-Timer expires	None	Delete Session	None

Transition	Trigger	Condition	Action	Event
eDO_Transition_6	At least one interface exists and LCP succeeds	None	If (max PPP inactivity supported && UE received max PPP inactivity timer), UE sets PPP inactivity = max PPP inactivity timer and maxPPP_inactivity_ rcvd = TRUE Else, PPP inactivity = default inactivity timer in NV and maxPPP_ inactivity_rcvd = FALSE	None
eDO_Transition_7	At least one iface exists and LCP fails due to permanent failure	None	Avoid DO system/channel for eDCTMtimer (hard failure)	None
eDO_Transition_8	At least one Iface exists and LCP fails due to temporary failure	None	Avoid DO system/ channel for eDCTMtimer (soft failure)	None
eDO_Transition_9	VSNCP procedure fails	None	Tear down LCP	VSNCP_ FAILS
eDO_Transition_10	VSNCP procedure succeeds	App exists	Inform app interface is up	VSNCP_ SUCCESS
eDO_Transition_11	PPP inactivity timer expires	maxPPP_inac tivity_rcvd FLAG = TRUE	Tear down all PDN context but retain LCP+Auth context	None
eDO_Transition_12	PPP teardown triggers ▪ Last Iface is torn down ▪ PPP-resync received ▪ max_PPP_ inactivity_rcvd flag = FALSE AND PPP inactivity timer expires Transitioned to HRPD-only network	None	Tear down PPP	None
eDO_Transition_13	Iface requesting new APN OR Last interface connected to APN exits	None	VSNCP procedure to connect to/disconnect from PDN	None
eDO_Transition_26	DO acquired	Connection-Request/IRMI succeeds	None	VSNCP_ SUCCESS
eDO_Transition_27	LTE_ATTACH_INIT	None	Delete PDN context	None

Transition	Trigger	Condition	Action	Event
eDO_Transition_28	Session Loss Triggers OR DO acquired and Connection-Request/IRMI fails		Delete Session context	
eDO_Transition_29	Last iface is brought down		Tear down PPP	
eDO_Transition_30	eDO session established and LCP Configure request received		Reestablish PPP	

4.3.2 State machine 3.1 – eHRPD PDN state machine

This section describes the PDN state machine for eHRPD. The PDN state machine illustrates the states in terms of IP address assignment for a PDN connection.

4.3.2.1 PDN state machine

Deferred IPv4 address assignment is not supported.

4.3.2.1.1 Top-level PDN state machine

The top-level PDN state machine is shown in Figure 4-15.

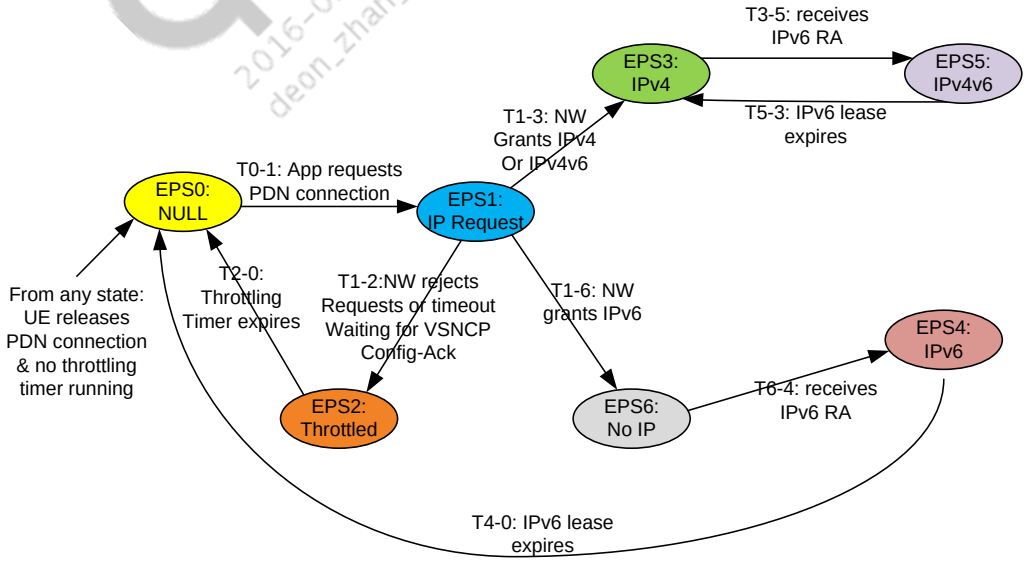

Figure 4-15 Top-level PDN state machine for eHRPD (no support of deferred IPv4 assignment)

The states are described in Table 4-29. The state transitions are listed in Table 4-30.

Table 4-29 shows the top-level PDN states.

Table 4-29 Top-level PDN states

State name	Description
S0: NULL	The PDN connection does not exist in this state. This is the initial state.
S1: IP request	The UE requests to establish the PDN connection. The UE indicates IPv4v6 capability in the VSNCP Config-Req message.
S2: Throttled	Throttling is performed to avoid repeated requests and is applied to PDN connection and/or RA procedures when a failure is encountered.
S3: IPv4	The UE has an IPv4 address only for the PDN connection.
S4: IPv6	The UE has an IPv6 address only for the PDN connection.
S5: IPv4v6	The UE has both IPv4 and IPv6 addresses for the PDN connection.
S6: No IP	The UE has no IP address assigned for the PDN connection.

Table 4-30 shows the top-level PDN state transitions.

Table 4-30 Top level PDN state transitions

Transition	Trigger	Condition	Action	Event
T0-1	An application is activated and requests the PDN connection. The UE sends VSNCP Config-Req.	▪ The UE is in eHRPD personality. ▪ LCP and authentication phases of PPP are complete. ▪ The UE indicates IPv4v6 capabilities.	The UE sends VSNCP Config-Req.	
T1-2	The network rejects the request or the UE times out waiting for VSNCP Config-Ack.	The UE receives rejection from the network or times out waiting for VSNCP Config-Ack.		
T1-3	The network grants IPv4 or IPv4v6.	One of the following two cases: ▪ VSNCP Config-Ack contains an IPv4 address assigned to the UE. ▪ VSNCP Config-Ack contains an IPv4 address and an IPv6 IID.		
T1-6	The network grants IPv6.	The VSNCP Config-Ack contains an IPv6 IID.		
T3-5	The UE receives an RA message.		The UE generates an IPv6 address.	
T6-4	The UE receives an RA message.		The UE generates an IPv6 address.	
T2-0	The throttling timer expires.			
T5-3	The IPv6 lease expires.		An IPv6 address is released.	

Transition	Trigger	Condition	Action	Event
T4-0	IPv6 lease expires.		An IPv6 address is released. A PDN connection is released.	
From any state to NULL state	The UE releases the PDN connection and no throttling timer is running.			

4.3.2.1.2 Substates in IPv4 state (S3)

Figure 4-16 shows the substates in the IPv4 state, i.e., state S3.

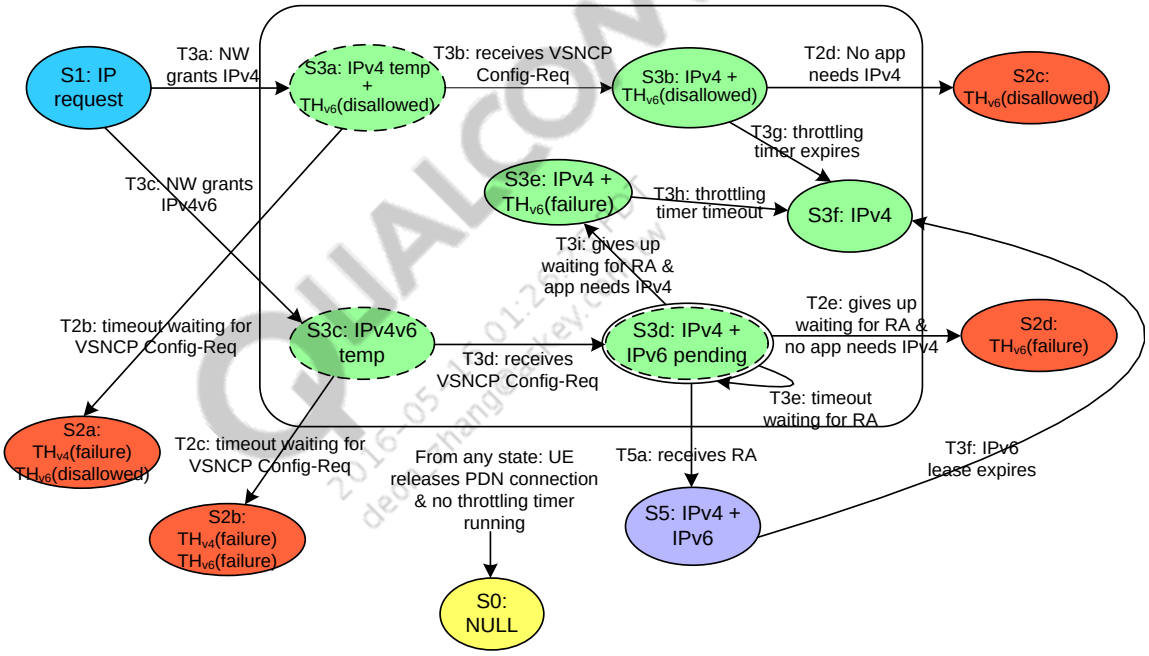

Figure 4-16 Substates in S3, no support of deferred IPv4 assignment

The substates are explained in detail in Table 4-31. The state transitions are listed in Table 4-32.

Table 4-31 Substates in S3

Substate name	Description
S3a	The UE enters this substate upon receiving the VSNCP Config-Ack message containing an IPv4 address.
S3b	The UE enters this substate upon receiving the VSNCP Config-Req message from the network to complete the protocol. The UE has an IPv4 address available.
S3c	The UE enters this substate upon receiving the VSNCP Config-Ack message containing an IPv4 address and an IPv6 IID.
S3d	The UE enters this substate upon receiving the VSNCP Config-Req message from the network to complete the protocol. The UE has an IPv4 address available. The UE is expecting an RA message from the network to generate the IPv6 address.
S3e	The UE enters this substate when it ceases to wait for an RA and the application needs the IPv4 address. The UE has an IPv4 address available. The UE is throttling an RS request.
S3f	The UE has only an IPv4 address available.
S2a	Throttle IPv4 and IPv6 requests. The throttling timer is defined in Table 12-2.
S2b	These are throttle IPv4 and IPv6 requests.
S2c	These are throttle IPv6 requests.
S2d	These are throttle IPv6 requests.

Table 4-32 State transitions to and from S2 substates

Transition	Trigger	Condition	Action	Event
T3a	The UE receives VSNCP Config-Ack and the network grants an IPv4 address.	The VSNCP Config-Ack contains an IPv4 address assigned to the UE.		
T3b	The UE receives VSNCP Config-Req from the HSGW.		The UE notifies the application with the IPv4 address if the application requests an IPv4 address.	
T3c	The UE receives VSNCP Config-Ack and the network grants an IPv4 address.	The VSNCP Config-Ack contains an IPv4 address and an IPv6 IID.		
T3d	The UE receives VSNCP Config-Req from the HSGW.		The UE notifies the application with the IPv4 address if the application requests an IPv4 address.	
T3e	The UE times out waiting for an RA.		The UE sends an RS message.	
T3f	The IPv6 lease expired.		IPv6 address is released.	

Transition	Trigger	Condition	Action	Event
T3g	The IPv6 throttling timer expired.			
T3h	The IPv6 throttling timer expired.			
T3i	The UE gives up waiting for an RA and the application needs an IPv4 address.	The application needs the IPv4 address.	The UE shall throttle the RS request.	
T5a	The UE receives the RA message.		The UE generates an IPv6 global unicast address via IPv6 SLAAC or IPv6 Privacy Extensions. The UE notifies the application if the application requests an IPv6 address.	
T2b	The UE times out waiting for the VSNCP Config-Req.		There is a throttle IPv4 due to a failure. There is a throttle IPv6 because the network does not grant an IPv6 address. The AMSS declares a failure and notifies the application.	
T2c	The UE times out waiting for the VSNCP Config-Req.		There is a throttle IPv4 due to a failure. There is a throttle IPv6 due to a failure. The AMSS declares a failure and notifies the application.	
T2d	No application needs an IPv4 address.		The PDN connection is closed. There is a throttle IPv6 because the network does not grant an IPv6 address.	
T2e	The UE gives up waiting for an RA.	No application needs the IPv4 address.	The PDN connection is closed. There is a throttle IPv6 due to a failure.	

1

4.3.2.1.3 Substates in the IPv6 state, S4

Figure 4-17 shows the substates in the IPv6 state, i.e., state S4.

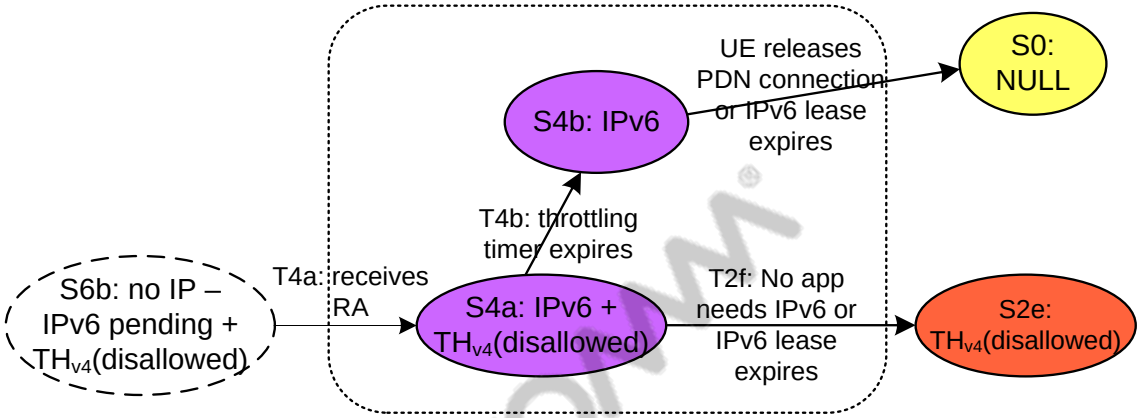

Figure 4-17 Substates in S4, no support of deferred IPv4 assignment

The substates are explained in detail in Table 4-33. The state transitions are listed in Table 4-34.

Table 4-33 Substates in S4

Substate name	Description
S4a	The UE has an IPv6 address for the PDN connection. The IPv4 request is throttled.
S4b	The UE has an IPv6 address for the PDN connection. An IPv4 throttling timer has expired.
S2e	There are throttle IPv4 requests.

Table 4-34 State transitions to and from S4 substates

Transition	Trigger	Condition	Action	Event
T4a	The UE receives the RA message.	The UE has no IP address for the PDN connection. The UE is expecting the RA message from the network.	The UE generates an IPv6 global unicast address via IPv6 SLAAC or IPv6 Privacy Extensions. The UE notifies the application if the application requests for IPv6 address.	
T4b	The IPv4 throttling timer expires.			
T2f	No application needs an IPv6 address or the IPv6 lease expires.		The UE closes the PDN connection. Throttle IPv4 application's request if IPv4 throttling timer has not expired.	

4.3.2.1.4 Substates of IPv4v6 state (S5)

Figure 4-18 shows the substates in the IPv4v6 state, i.e., state S5.

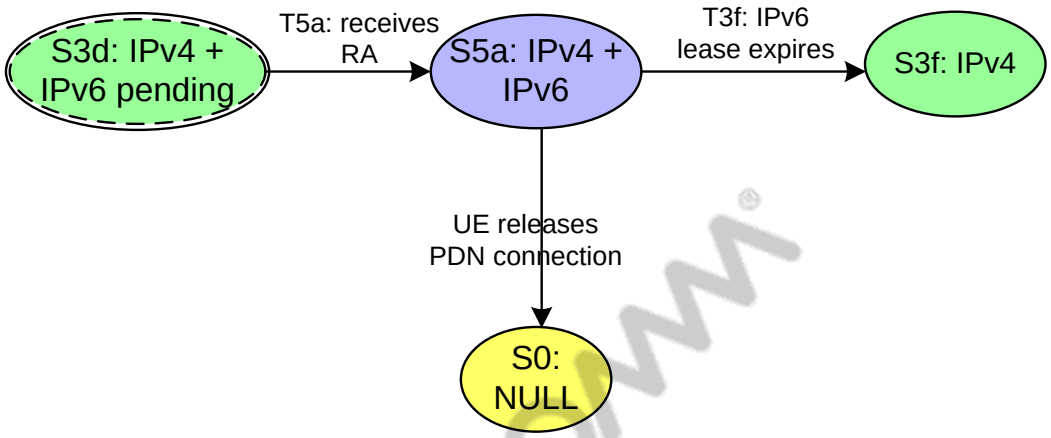

Figure 4-18 Substates in S5, no support of deferred IPv4 assignment

The substates are explained in detail in Table 4-35. The state transitions are listed in Table 4-36.

Table 4-35 Substates in S5

State name	Description
S5a	The UE has both an IPv4 address and an IPv6 address for the PDN connection.

Table 4-36 State transitions to and from S5 substates

Transition	Trigger	Condition	Action	Event
T5a	The UE receives the RA message.	The UE already has an IPv4 address for the PDN connection. The UE is waiting for the RA message.	The UE generates an IPv6 global unicast address via IPv6 SLAAC or IPv6 privacy extensions. The UE notifies the application if the application requests an IPv6 address.	

4.3.2.1.5 Substates of No IP state, S6

Figure 4-19 shows the substates in the No IP state, i.e., state S6.

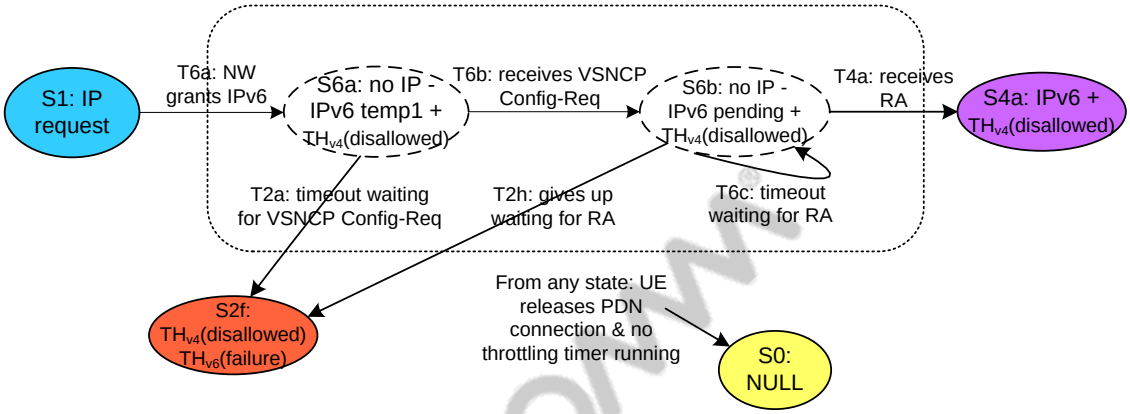

Figure 4-19 Substates in S6, no support of deferred IPv4 assignment

The substates are explained in detail in Table 4-37. The state transitions are listed in Table 4-38.

Table 4-37 Substates in S6

State name	Description
S6a	The UE does not have an IP address for the PDN connection. The UE is waiting for the VSNCP Config-Req from the network to complete the protocol. The network grants IPv6 IID.
S6b	The UE does not have an IP address for the PDN connection. The UE is waiting for the RA message from the network for IPv6 address generation.
S2f	There are throttle IPv4 and IPv6 requests.

Table 4-38 State transitions to and from S6 substates

Transition	Trigger	Condition	Action	Event
T6a	The UE receives a VSNCP Config-Ack and the network grants an IPv6 address.	The VSNCP Config-Ack contains an IPv6 IID.		
T6b	The UE receives VSNCP Config-Req from the HSGW.			
T6c	The UE times out waiting for RA.		The UE sends out the RS.	

Transition	Trigger	Condition	Action	Event
T4a	The UE receives an RA.		The UE generates an IPv6 global unicast address via IPv6 SLAAC or IPv6 privacy extensions. The AMSS notifies the application if the application requests an IPv6 address.	
T2a	The UE times out waiting for the VSNCP Config-Req.		There is a throttle IPv4 because the network does not grant an IPv4 address. There is a throttle IPv6 due to a failure. The AMSS declares a failure and notifies the application.	
T2h	The UE gives up waiting for an RA.		The UE closes the PDN connection. There is a throttle IPv4 because the network does not grant an IPv4 address. There is a throttle IPv6 due to a failure.	

4.3.3 State machine 3.2 – eHRPD QoS state machine without network-initiated QoS

When an application requiring QoS is activated, a series of steps must be performed before the RAN and the network are configured to provide the requested QoS. This section provides details about a state machine, shown in Figure 4-20, that outlines the series of steps that must be performed when the UE only supports UE-initiated QoS on eHRPD. States of the state machine are described in Table 4-39; state transitions are described in Table 4-40.

Table 4-39 eHRPD QoS states

State name	Description
eDO_STATE_1	The AMSS does not have an eHRPD network-level QoS state related to the application.
eDO_STATE_2	The AMSS initiated the QoS check procedure with a set of flowProfileIDs. The set of flowprofileIDs is received from the application.
eDO_STATE_3	The AMSS received a QoS Check Conf from the HSGW. This contains a list of Authorized flowprofileIDs that the app can use.
eDO_STATE_4	The AMSS initiated AuR procedures to set up QoS at the eAN. This contains the list of authorized flowprofileIDs and reservation labels. It also initiates the RSVP procedures in parallel, to set up the TFT at HSGW.
eDO_STATE_5	The UE received a Resv Conf message from the HSGW, but only received an Attribute Accept message from the eAN. Consequently, the AuR from the eAN that is needed to configure the RAN flows is still needed.

State name	Description
eDO_STATE_6	In this state, the QoS context was set up at the network and the RAN level. However, the RAN level QoS flows have not been turned ON.
eDO_STATE_7	In this state, the QoS flows have been turned ON.

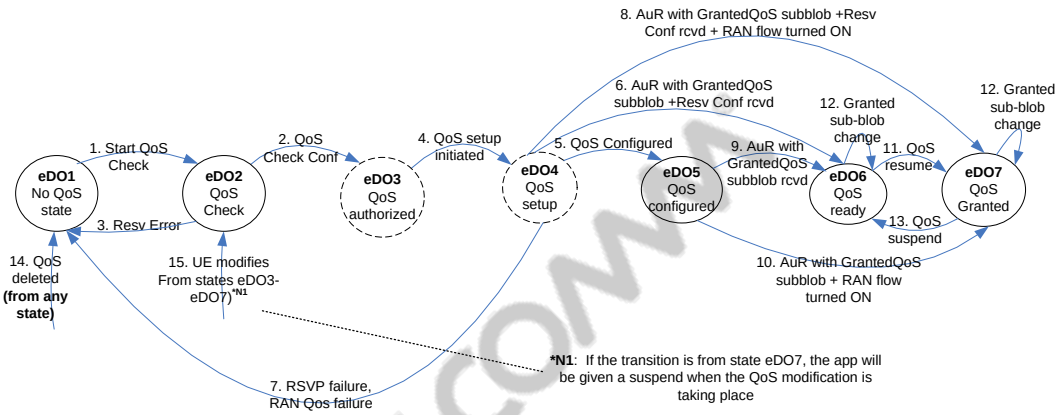

Figure 4-20 State machine representing QoS context for a UE-initiated app in eHRPD

Table 4-40 shows the eHRPD QoS state transitions.

Table 4-40 eHRPD QoS state transitions

Transition	Trigger	Condition	Action	Event
eDO_Transition_1	QoS configure/QoS request from app or Transition from LTE to eHRPD and Selected BCM = MS only	None or App gave parameters for LTE and eHRPD and PDN attach succeeded	Send Resv with QoS check and flowprofileID list	None
eDO_Transition_2	Resv Conf received	None	Store list of authorized flowprofileIDs	None
eDO_Transition_3	RSVP timeout or RSVP error received	None	Inform app of QoS failure	None
eDO_Transition_4	▪ RSVP procedures are initiated if needed, see condition ▪ RAN QoS setup procedures are initiated if needed, see condition	▪ RSVP procedures are avoided if the app modified the flow profile ID and not the TFT ▪ RAN QoS setup procedures may be eliminated if a prior DO session exists in the eAN	None	None

Transition	Trigger	Condition	Action	Event
eDO_Transition_5	Resv Conf received and AuAccept received	AuR with a granted QoS subblob was not received.	None	None
eDO_Transition_6	AuR with granted QoS subblob + Resv Conf received	None	Inform app that QoS is ready and specify granted QoS	None
eDO_Transition_7	Resv Error OR Attribute Update reject OR Timeout	None	Inform app of no QoS	None
eDO_Transition_8	AuR with Granted QoS subblob + Resv Conf received; flow is also turned by default, because of the ReservationKK IdleState setting	None	Inform app that QoS is ready and specify granted QoS	None
eDO_Transition_9	Autonomous AuR with granted subblob from eAN OR triggered by app calling QoS resume	None	Inform app that QoS is ready and specify granted QoS	None
eDO_Transition_10	Autonomous AuR with granted subblob from eAN OR triggered by app calling QoS resume; flow is also turned by default, because of the ReservationKK IdleState setting	None	Inform app that QoS is ready and specify granted QoS	None
eDO_Transition_11	App calls QoS resume	None	None	None
eDO_Transition_12	RAN sends AuR with a new granted QoS subblob	None	Inform app that QoS is modified	None
eDO_Transition_13	App calls QoS suspend	None	None	None
eDO_Transition_14	App deletes QoS OR app exits OR UE attaches to LTE	None	Delete network-level QoS context at UE	None
eDO_Transition_15	App calls QoS modify with nonauthorized flowprofileID	None	Trigger QoS Check procedure	None
eDO_Transition_16	App calls QoS modify with authorized flowprofileID	None	Trigger RAN and HSGW-level QoS setup procedures	None

5 APN Enable/Disable

NOTE: Numerous changes were made in this chapter.

This chapter describes the UE's behavior for supporting APN enable/disable.

5.1 Assumptions

- The design for eHRPD is consistent with LTE.
- The APNs in the MinAPNList1 and MinAPNList2 should be provisioned by the operator. If the operator does not provision the APN names, the UE shall treat the list as empty.

5.2 Requirements

- Definition of Enabled APN – The APN for which the PDN connection is allowed to be established is called the Enabled APN.
  - The UE shall request a PDN connection only if the associated APN is enabled.
- An APN is an enabled APN if:
  - The application profile check succeeds, i.e., the APN shall be listed and enabled in the application profile.
  - The UICC APN check succeeds, i.e., if the EF_{ACL} file exists in the UICC, the APN shall be listed in the EF_{ACL} under USIM. If the EF file does not exist, it implies that the UICC APN check succeeds.
- Definition of MinAPNList1 – All APNs in MinAPNList1 shall be enabled for the UE to access the operator's network. If any APN in the MinAPNList1 is not enabled, the UE shall not attempt to attach to any APN for some configurable period of time, e.g., an infinite time period means until the UICC is removed and replaced.
- Definition of MinAPNList2 – If the UE is already attached to the operator's network and it needs to connect to an APN listed in the MinAPNList2 but this APN is not enabled, the UE shall detach from the network and shall not reattempt to attach to any APN for some configurable period of time, e.g., an infinite time period means until the UICC is removed and replaced.
- In the design, if the APN check for MinAPNList1 fails, the UE shall not advertise eHRPD capability during DO session negotiation for eHRPD. If the current DO session is eHRPD, the UE shall close the current session and shall not propose eHRPD capability when opening a new session. See [Q2] for details. For LTE, the UE shall detach from LTE. MinAPNList2 is treated the same as MinAPNList1.

5.3 APN check procedure for APNs listed in MinAPNList1 after powerup

The UE shall perform the APN check procedure for all APNs listed in the MinAPNList1 after power-up, software reset, or an application profile update. The UE shall set the AllowToAttach flag accordingly during this procedure: if the APN check for MinAPNList1 succeeds, the UE sets AllowToAttach to True; otherwise, the UE sets AllowToAttach to False, as shown in Table 5-1.

Table 5-1 AllowToAttach variable

Name	Unit	Default	Description
AllowToAttach	Boolean	TRUE	Identifies whether the UE is allowed to access the operator's network. The UE shall perform an APN check for the APNs listed in MinAPNList1 after powerup, soft reset, or an application profile update. If an APN in MinAPNList1 is not enabled, AllowToAttach shall be set to FALSE.

This scenario describes how the UE performs an APN check for the APNs listed in MinAPNList1 after a powerup or software reset.

Preconditions

None

Assumptions

None

Triggers

The UE powers up or the software is reset or is notified of an application profile update.

Description

Figure 5-1 shows the APN check for the MinAPNList1 flow chart.

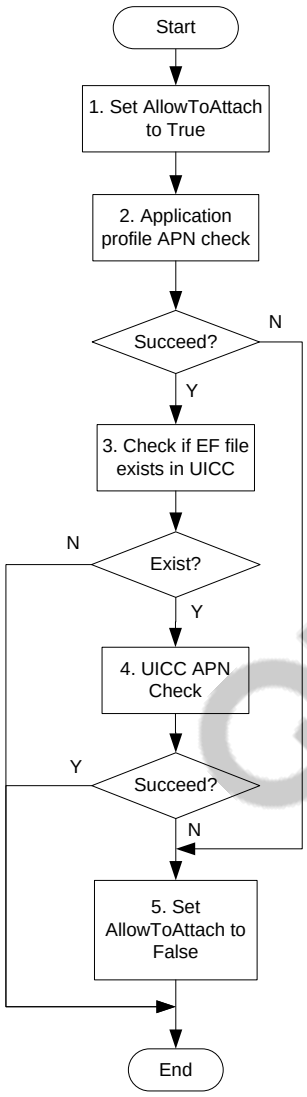

Figure 5-1 APN check for MinAPNList1

The following numbered paragraphs correspond to Figure 5-1:

1. The UE initially sets AllowToAttach to TRUE.
2. The UE performs an application profile APN check for all APNs listed in MinAPNList1. If all APNs are enabled in the application profile, go to the next step. Otherwise, if any one APN is disabled in the application profile, go to step 5.
3. The UE checks if service no. 35 of the USIM is available (the EF_{ACL} file exists) in the UICC. If yes, go to the next setup. Otherwise, stop.
4. The UE checks if all APNs in MinAPNList1 are listed in EF_{ACL}. If all APNs are present in EF_{ACL}, stop. Otherwise, if any one APN is not present, go to the next step.
5. The UE sets AllowToAttach to FALSE. Stop.

Postcondition

The postcondition can be one of the following:

- If AllowToAttach = TRUE, the UE is allowed to access the operator's network.
- If AllowToAttach = FALSE, the UE shall not advertise eHRPD capability during DO session negotiation for eHRPD. If the current DO session is eHRPD, the UE shall close the current session and shall not propose eHRPD capability when opening a new session. For LTE, the UE shall detach from LTE.

5.4 APN check procedure for APNs not listed in MinAPNList1

This scenario describes how the UE performs an APN check before it requests a PDN connection to an APN that is not listed in MinAPNList1.

Preconditions

The preconditions can be one of the following:

- The UE is in eHRPD personality and has a valid eHRPD session established.
- The UE is attached to LTE.

Assumptions

None

Triggers

An application is activated and requests a PDN connection establishment.

Description

Figure 5-2 shows the APN check flowchart.

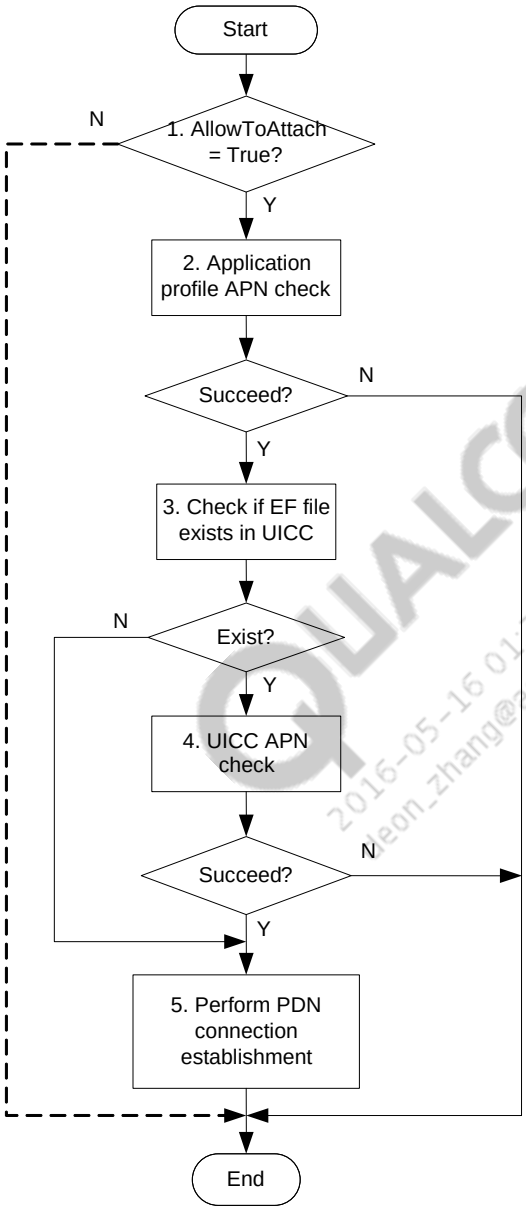

Figure 5-2 APN check flowchart

The following numbered paragraphs correspond to Figure 5-2:

1. Upon receiving the PDN connection request from the application, the UE checks the AllowToAttach flag. If AllowToAttach = TRUE, go to the next step. Otherwise, stop. In this use case, AllowToAttach is always TRUE.
2. The UE checks the application profile. If the APN is set to enabled in the application profile, go to the next step. Otherwise, stop.
3. The UE checks if service no. 35 of the USIM is available (the EF_{ACL} file exists) in the UICC. If yes, go to the next setup. Otherwise, go to step 5.
4. The UE checks if the APN of the requested PDN connection is listed in EF_{ACL}. If yes, go to the next step. Otherwise, stop.
5. The UE proceeds with PDN connection establishment with the APN. Stop.

Postcondition

The postcondition can be one of the following:

- If the APN check succeeds and the PDN connection is successfully established, the UE and the network have the PDN context setup.
- If the APN check fails, the UE ceases PDN connection establishment.

6 PDN Inactivity

NOTE: Numerous changes were made in this chapter.

This chapter describes the UE's behavior for supporting a PDN inactivity timer.

6.1 Assumptions

The design for eHRPD is consistent with LTE.

6.2 Requirements

- The UE shall maintain an individual inactivity timer, PDNInactivityTimer, for each PDN to which the UE is connected.
- The UE shall support a feature over eHRPD. When this feature is turned on, the UE shall ignore the inactivity timer expiration if this is the last PDN connection. The NV item for this feature is defined in Table 6-1.
- Upon expiration of the associated PDNInactivityTimer, the UE on eHRPD shall release the PDN connection, unless this is the last PDN connection and IgnoreLastPDNIATimer is set to True.
- Upon expiration of the associated PDNInactivityTimer, the UE on LTE shall release the PDN connection, unless this is the last PDN connection.

Table 6-1 NV item for ignoring the last PDN inactivity timer

Name	Unit	Default	Description
IgnoreLastPDNIATimer	Boolean	FALSE	Specifies whether the UE shall ignore inactivity timer expiration if this is the last PDN connection

- If the UE attempts to release one PDN connection but receives a reject from the network with the error code last PDN disconnection not allowed, the UE shall detach and reattach to the network.

6.3 Recommendations

- The value for the IMS PDNInactivityTimer on the UE shall be greater than the IMS reregistration timer and not greater than the IMS PDNInactivityTimer on the network.
- If the IMS PDNInactivityTimer expires, the UE shall release the IMS PDN connection and notify the application. The IMS application is free to immediately request a PDN connection to the IMS APN.

6.4 PDN inactivity timer

The PDNInactivityTimer is maintained for each PDN connection. The inactivity timer value for each PDN connection is set in the application profile, as shown in Table 6-1.

Table 6-2 PDNInactivityTimer variable

Name	Unit	Default	Description
PDNInactivityTimer	Minute	0	▪ Identifies the period of time during which the connection to the PDN goes to idle, i.e., the UE considers the PDN connection inactive. The UE shall release the PDN connection when this period of time has elapsed. ▪ The default setting of zero is treated as an infinite value, which means that the inactivity timer never expires. It is recommended that the operator should provision a finite value for each PDNInactivityTimer.

The UE shall start this timer when the connection to a PDN becomes idle, i.e., the UE is not sending or receiving data on any bearer associated with the PDN connection. The UE shall reset this timer when:

- The UE successfully attached to a PDN following a PDN connection request from the device.
- The UE starts sending data on a bearer associated with the PDN connection.
- The UE starts receiving data on a bearer associated with the PDN connection.

6.5 Use case 1 – UE-initiated PDN release due to PDN inactivity timer expiration

This scenario describes the use case when the UE initiates a PDN context release due to PDN inactivity timer expiration. This is an example use case of eHRPD. If this is the last PDN connection, this use case applies only if IgnoreLastPDNIATimer is set to False.

Preconditions

- The UE is in eHRPD personality and has a valid eHRPD session established.
- The UE established the PDN context.

Assumptions

None

Triggers

The associated PDN inactivity timer expires.

Description

Figure 6-1 shows the call flow.

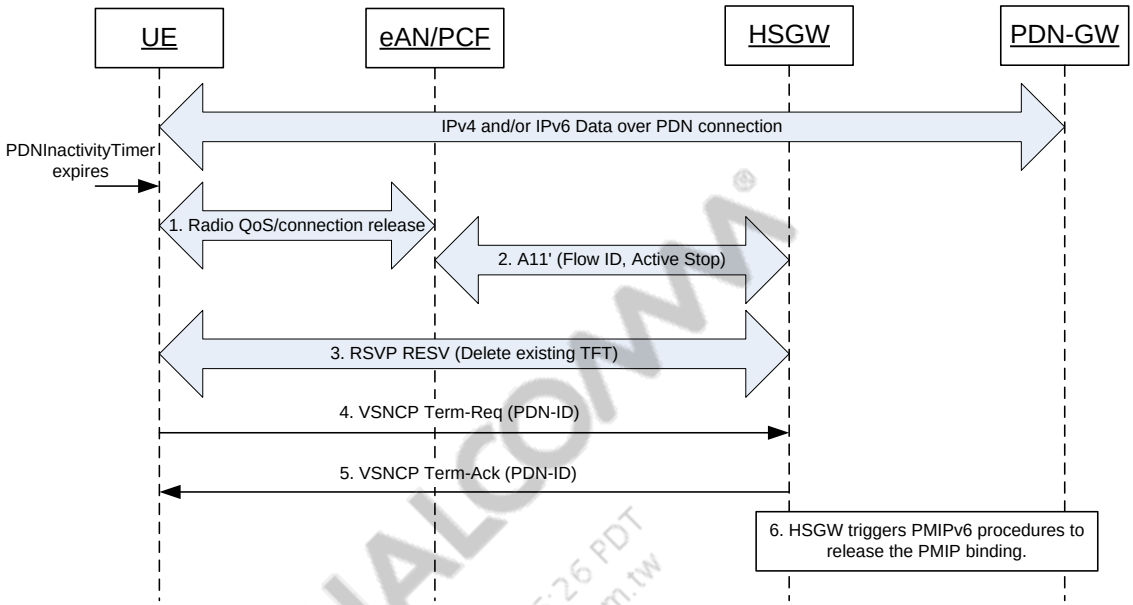

Figure 6-1 UC 1 – UE-initiated PDN release

The following numbered paragraphs correspond to Figure 6-1:

1. When the PDNInactivityTimer expires, the UE shall initiate the PDN release. The UE initiates radio QoS/connection release for the connections associated with the APN.
2. The eAN sends an A11 Registration Request message to the HSGW, indicating the removed Flow ID. If the last Flow ID associated with the auxiliary A10 is removed, the auxiliary A10 will also be removed.
3. Steps 3 through 5 occur in parallel with steps 1 through 2. The UE sends an RSVP RESV message to the HSGW to indicate the removed flows. The HSGW clears the TFTs associated with the PDN and responds with a RESVConf message.
4. The UE sends a VSNCP Terminate-Request message to the HSGW. The message contains the PDN-ID of the PDN with which the UE is closing the connection.
5. The HSGW sends a VSNCP Terminate-Ack to the UE to indicate that it received the request to terminate a connection to a PDN.
6. The HSGW triggers the PMIPv6 procedures to release the PMIP bindings.

Postcondition

- The PDN context associated with the APN is released at both the UE and HSGW.
- The assigned IP addresses are released.

7 Single and Dual-IP Bearer Transition

This chapter describes the UE's behavior for supporting single and dual-IP bearer transitioning across eHRPD and LTE.

7.1 Requirements

- The UE shall specify IPv4v6 capable if the UE is dual-IP stack capable.
- During an initial attach to one APN, if the UE specifies IPv4v6 capable and the network assigns two addresses, the UE shall retain both addresses even if only one address is needed by the application, provided the UE is capable of handling two IP addresses for one APN.

  If the UE is not capable of handling two IP addresses for one APN, the UE shall ignore the address that is not needed by the application.
- If the UE transitions from one network that supports SADB-2B to another network that only supports SADB-1B and DADB, the UE shall include both assigned IP addresses when it performs a handover attach for the APN. This is described in Use Case 1. In this case, the network should not reject and release the PDN connection due to the inclusion of two IP addresses being. The network should grant one or two IP addresses.
- In this case, the UE requests a PDN connection and encounters a certain error with one address type, which causes throttling for that IP address and APN. The other IP address assignment for the APN succeeded. During transitioning to a different technology, the UE performs a handover attach to the APN to which the UE connected. If the network grants both IP addresses, the UE shall reset the throttling timer if it is still running. The previously throttled IP address is available to the application the next time the application requests it. If the network does not grant the IP address type that has been throttling, the throttling timer shall continue to run.

7.2 Use case 1 – Transitioning from SADB-2B to eHRPD

This scenario describes when the UE transitions from a source network that supports SADB-2B to eHRPD that supports only DADB and SADB-1B.

Preconditions

- The UE is in eHRPD personality and has a valid eHRPD session established.
- The LCP and authentication phases of PPP are complete.
- The UE has an SADB-2B bearer established in the source network.

Assumptions

No deferred IPv4 assignment is supported.

Triggers

The UE transitions to eHRPD and the LCP and PPS authentication phases are complete. The UE attempts to establish the PDN connection to which it had attachments within the source network.

Description

Figure 7-1 shows the call flow.

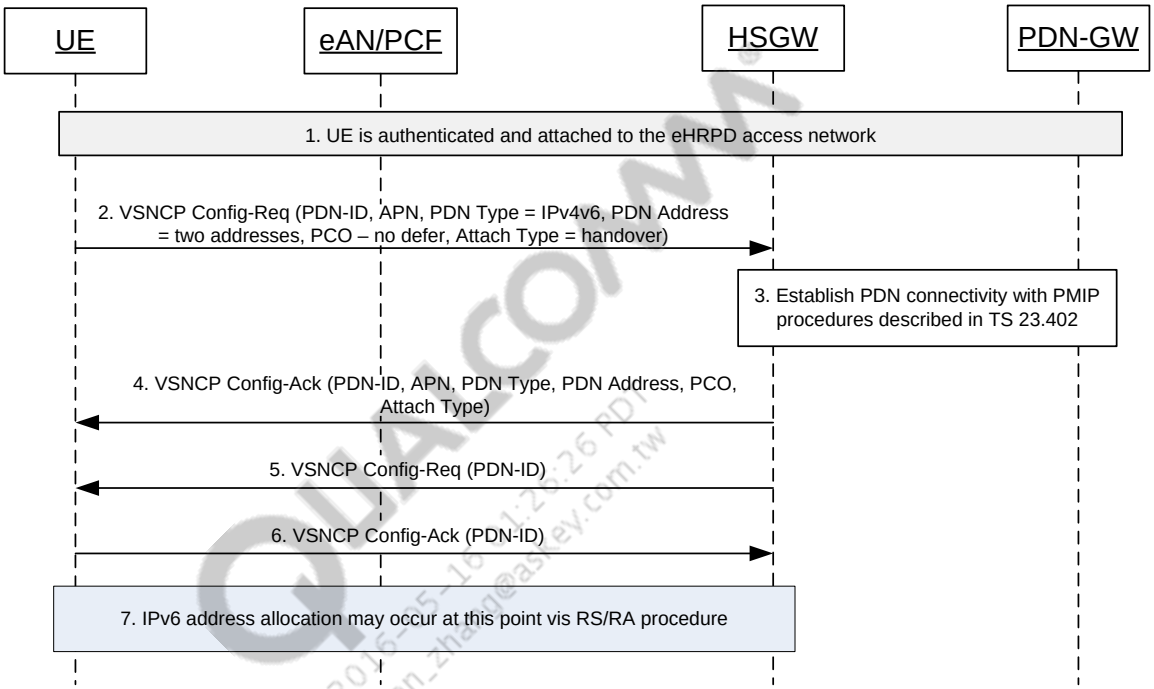

Figure 7-1 PDN connection establishment when transitioning to eHRPD

The following numbered paragraphs correspond to Figure 7-1:

1. The UE performed successful authentication and is attached to the eHRPD access network.
2. The UE sends a VSNCP Configure-Request message over the main service connection. The information in the message includes:
   - PDN-ID
   - APN
   - PDN Type = IPv4v6
   - PDN Address that contains both IPv4 and IPv6 addresses assigned to the UE for the same APN in the source network
   - Protocol Configuration Options (PCO)
   - Attach Type = Handover attach
   - Address Allocation Cause = 0

3. The UE shall also set the IPv4 Default Router Address to the currently assigned IPv4 default router address. Using the Address Allocation Preference contained in the PCO, the UE indicates that it wants to perform IPv4 address allocation during the PDN connection establishment procedure.
4. The HSGW triggers the PMIP procedures described in [S6].
5. After the HSGW receives the indication of completion of the PMIP procedures, it sends the VSNCP Configuration-Ack (PDN-ID, APN, PDN Type, PDN Address, PCO, and Attach Type) message to the UE over the main service connection.
6. The HSGW sends a VSNCP Configure-Request message to complete the protocol specified in [S7].
7. The UE responds with a VSNCP Configure-Ack message (PDN-ID).
8. If an IPv6 address allocation is applied, the UE and the HSGW perform RS/RA procedures.

Postcondition

There are two possible postconditions:

- The network grants two IP addresses.
- The network grants only one IP address. The UE reports the failure to the application that requests the IP address that is not granted. The IP address on that PDN connection is throttled.

Failure scenario

If the network rejects the request and releases the PDN connection, the UE shall report the failure to the applications that request this PDN connection. The PDN connection is throttled. The application is free to retry after the throttling timer expires.

8 QoS and Interactions with Applications

NOTE: Numerous changes were made in this chapter.

This chapter describes the UE's behavior for supporting QoS for a multimode system, including a QoS API and interactions with the application.

8.1 Definitions

The network-initiated and UE-initiated QoS flows are defined as:

- The QoS flow is considered to be a UE-init QoS flow if it is initially established based on the UE request. The UE-initiated QoS flow remains a UE-init QoS flow until it is released, even if the network modifies the associated QoS flow metrics, i.e., FlowProfileID and/or packet filter (5-tuple or less) and/or precedence for UE-init QoS flows on eHRPD and QCI and/or packet filters (5-tuple or less) for UE-init QoS flows on E-UTRA)[3].
- The QoS flow is considered to be a network-initiated QoS flow if is initially pushed by the network. The network-initiated QoS flow remains a network-initiated QoS flow until it is released, even if the application invokes the Request QoS API to get the handle to the QoS flow or the application requests a modification to the associated QoS flow metrics, i.e., FlowProfileID for network-initiated QoS flows on eHRPD and QCI for network-initiated QoS flows on E-UTRA)[4]. The packet filter (5-tuple or less) and precedence shall not be modified by the UE for a network-initiated QoS flow. The network-initiated QoS flow shall not be released by the UE.

8.2 Network-initiated QoS

8.2.1 Requirements

The following operations shall be supported in the UE:

- The design for eHRPD shall be consistent with LTE.
- The UE shall be able to attach to a network that supports network-initiated QoS.
- The UE shall be able to attach to a network that does not support network-initiated QoS.
- Each IPv4 and IPv6 address assigned to a specific PDN connection shall have an independent TFT container.

[3]Modification of UE-init QoS flow metrics by the network are allowed only if coexistence of UE and network-initiated QoS is supported.
[4]Modification of network-init QoS flow metrics by the UE are allowed only if coexistence of UE and network-initiated QoS is supported.

- The UE shall support network-initiated QoS flow establishment.
- The UE shall support network-initiated QoS flow deletion initiated by the network.
- The UE shall support modification of QoS parameters, i.e., packet filters/FlowProfileIDs/ precedences for eHRPD, and packet filters/QCIs for E-UTRA, initiated by the network for the configured network-initiated QoS flows.
- If the UE receives a network-initiated QoS establishment request from the network, the UE shall perform packet-filter matching with the existing QoS flows[5]. If the requested network-initiated QoS bit-wise matches both the packet filter and the precedence of any existing QoS flow, the UE shall reject the request.
- After the application registers a notification callback with requested packet filters with the AMSS, the AMSS shall invoke this callback to notify the application of the event about network-initiated QoS states. The AMSS shall maintain the registered callback until the notification is revoked.
- The AMSS shall perform packet-filter matching when it receives IP packets from the application. If a given packet matches more than one of the packet filters, the filter of the highest precedence shall be chosen.
- On eHRPD, the RL reservation is turned on and off by the AMSS for network-initiated QoS flows. The RL reservation can also be turned on and off by the network for network-initiated QoS flows. See [Q2] for details.

8.2.2 Assumptions

- Upon receiving the VSNCP Config-Req message containing the BCM, the HSGW returns the selected BCM in the VSNCP Config-Ack to the UE. The selected BCM shall be set to MS/network-initiated if the network supports network-initiated QoS.
- If the network pushes a QoS flow but the associated packet filter(s) are already set up at the UE, the network should clear the associated resource before pushing the QoS.
- On eHRPD, the FL reservation is turned on and off by the network for network-initiated QoS flows. Sending data over the FL on the QoS flow implicitly turns on the FL reservation.
- During eHRPD PPP resync, the QoS context is released locally in the UE. After a successful PPP resync, if the selected BCM is MS/NW-initiated, the HSGW shall perform the network-initiated QoS setup procedures to set up the QoS flows for all established flows based on the QoS policy received from the PCRF.

8.2.3 Packet-filter matching

A packet filter consists of an evaluation precedence and a list of packet filter contents. The 5-tuple packet filter content consists of:

- Source IP address
- Source port number
- Destination IP address

[5]Filter matching is applied to both UE-initiated and network-initiated QoS flows if coexistence of UE and network-initiated QoS is supported.

- Destination port number
- TOS/DSCP

8.2.3.1 Reverse-traffic processing

The AMSS shall perform packet-filter matching when it receives an IP packet from the application. The AMSS shall check the 5-tuple packet filter content against the IP packet received from the application.

If a packet filter match is found, the packet is sent to the link flow associated with the flow identifier corresponding to the matched packet filter.

If a given packet matches more than one of the packet filters, including a wildcard match, the one that has the highest precedence shall be selected.

If no packet-filter match is found, the packet is sent to the best-effort flow.

8.2.3.2 QoS request processing and duplicate flow detection

When the AMSS receives a QoS setup request from the network, the AMSS shall perform packet-filter matching. When receiving a network-initiated QoS setup request, the AMSS shall consider a duplicate flow as detected if the 5-tuple packet filter content, if it is present in the packet filter included in the QoS signaling, and the precedence are bitwise-matched to any existing QoS flow.

When the AMSS receives a QoS setup request from the application, the AMSS shall perform packet-filter matching. When receiving a UE-initiated QoS setup request, the AMSS shall consider a duplicate flow as detected if the 5-tuple packet filter content, if it is present in the packet filter included in the QoS request, is bitwise-matched to any existing QoS flow.

8.2.4 Notification of QoS states/events

Three high-level QoS states are defined for eHRPD:

- No QoS – There is no QoS context established.
- QoS Activated – QoS is considered activated if all of the following conditions are satisfied:
  - The radio QoS request is successfully accepted by eAN.
  - All RLP and RTCMAC bindings are complete. RLP and RTCMAC are active.
  - RSVP messaging is successful.
  - The RL reservation is turned on.
- QoS Configured – QoS is considered to be configured if the radio QoS request is successfully accepted by the eAN and RSVP messaging is successful. When QoS is in the Configured state, the RL reservation is in the Close state and RLP and RTCMAC binding and activation procedures may or may not be performed[6].

[6]This enables the Early Reservation On feature [Q5].

By successfully turning on the RL reservation and successfully completing the RLP and RTCMAC binding and activation procedures, which may be triggered by turning on the reservation if the Early Reservation On feature is used, the QoS state transitions from Configured to Activated.

Two high-level QoS states are defined for E-UTRA:

- No QoS – There is no QoS context established.
- QoS Activated – QoS is considered to be activated if the EPS bearer is activated successfully.

Based on the QoS states and QoS procedures performed, the AMSS can provide notification about QoS states/events to the application that has registered a notification callback. The network-initiated QoS notifications, which may be similar to those that are defined for UE-initiated QoS (see [Q8]), are listed as[7]:

- QoS Unavailable
- QoS Activate
- QoS Suspend
- QoS Failure
- QoS Modify Success/Fail
- QoS Release

As shown in Figure 8-1and Figure 8-2, in the xxx/yyy shown on the arrows of state transitions, xxx represents QoS procedures and yyy represents QoS notifications the AMSS sends to the application.

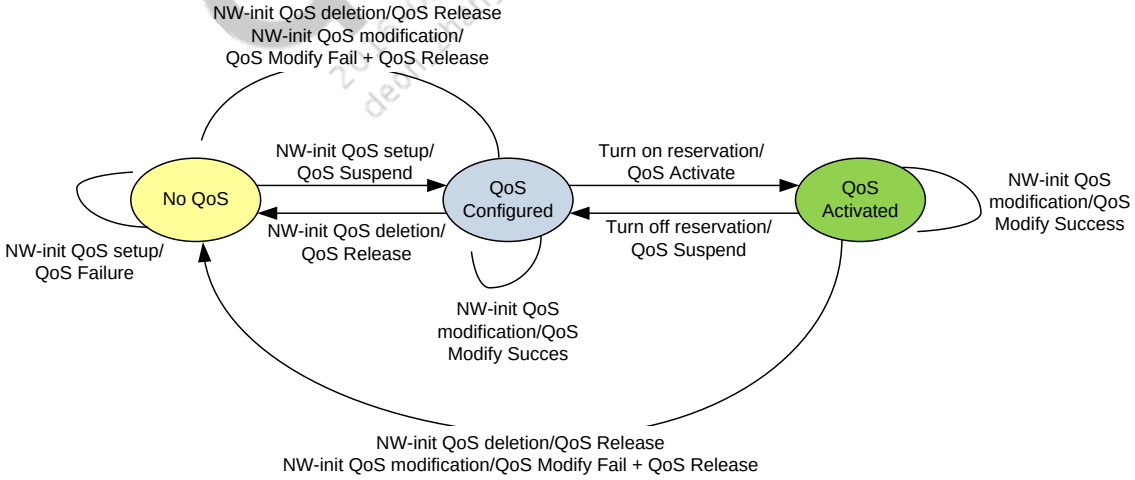

Figure 8-1 QoS states and QoS notifications, eHRPD

[7]The format of notifications is implementation-dependent.

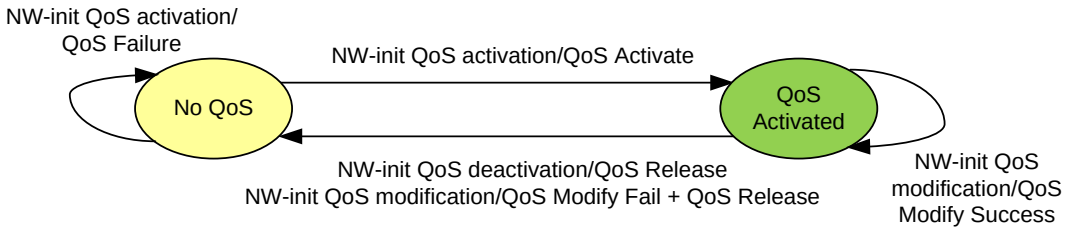

Figure 8-2 QoS states and QoS notifications, E-UTRA

NOTE: There are multiple notifications during the network-initiated QoS modification procedure. In the successful case, they are QoS Suspend, QoS Modify Success, and QoS Activate. In the failure case, they are QoS Suspend, QoS Modify Fail, and QoS Release. For details, see the network-initiated QoS modification use cases in [Q8].

8.2.5 Network-initiated QoS procedures

See [Q2] for eHRPD network-initiated QoS procedures.

See [Q9] for LTE network-initiated QoS procedures.

8.3 Network-initiated QoS interaction with QoS-unaware applications

Applications can be classified into QoS-aware and QoS-unaware. For QoS-unaware applications, only network-initiated QoS procedures apply. This is shown in Table 8-1.

Table 8-1 QoS-aware and QoS-unaware applications

	QoS-aware applications	QoS-unaware applications
Network-initiated QoS procedures	Applicable	Applicable
UE-initiated QoS procedures	Applicable	N/A

8.3.1 Use case 1 – QoS-unaware application sends data

The use case describes the scenario when the QoS-unaware application sends data before and after the QoS is initiated by the network.

Preconditions

- The UE is in eHRPD personality or the UE is attached to E-UTRA.
- The PPP session is established if on eHRPD.
- The UE established the PDN connection to the APN, for which the bearer/QoS will be established.

Assumptions

None

Trigger

The application is activated and starts sending data.

Description

The call flow is shown in Figure 8-3.

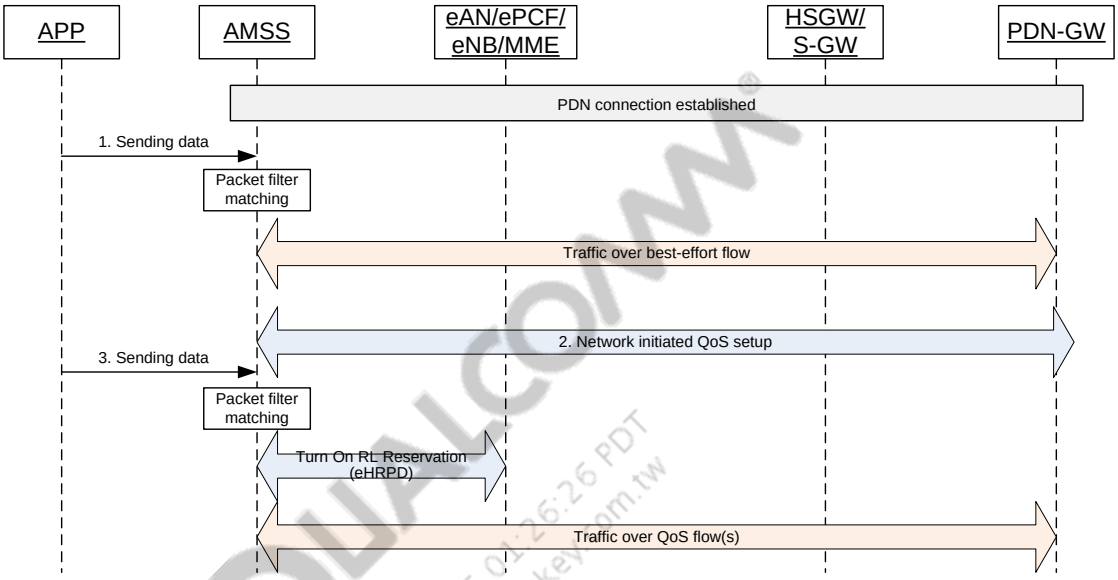

Figure 8-3 QoS-unaware application sends data before and after network pushes QoS

The following numbered paragraphs correspond to Figure 8-3:

1. The application is activated and starts sending data. The AMSS performs filter matching and the packet being transmitted does not match any packet filter. Therefore, the AMSS sends the data using best-effort flow. Note that the QoS-unaware application does not request QoS.
2. In this step, the network-initiated QoS setup procedures are performed. The packet filter(s) are set up in the AMSS. Note that the AMSS does not notify the QoS-unaware application after the packet filter(s) are set up.
3. This step only applies to eHRPD. The incoming data shall trigger the AMSS to turn on the RL reservation.
4. Since the QoS flow(s) are configured and the RL reservation is activated successfully, the AMSS filters the data and sends it using the QoS flow(s).

Postconditions

The QoS flow(s) are configured. The RL reservation is activated if on eHRPD.

8.4 Network-initiated QoS interactions with QoS-aware applications

The QoS-aware applications can be categorized into the following QoS configuration preferences:

- QoSRequired – QoS configuration and activation (reservation turn on) are required for the application. If QoS configuration or activation fails, the application shall block sending data.
- QoSPreferred – If QoS configuration or activation fails, the application may proceed with sending data using a best-effort flow.

The AMSS shall provide the following APIs to QoS-aware applications:

- The AMSS shall allow the application to register a notification callback with requested packet filters. The AMSS shall invoke this callback to notify the application of the event about network-initiated QoS states. The AMSS shall maintain the registered callback until the notification is revoked. The AMSS may return the QoS flow parameters, FlowProfileIDs for eHRPD or QCIs for E-UTRA, in the notification.
- The AMSS shall allow the application to query the QoS state and QoS parameters. Upon a query from the application, the AMSS shall report the QoS state and QoS parameters to the application.
- This only applies to eHRPD. The AMSS shall allow the application to indicate the Immediate-Reservation-On option when registering the notification callback. If the application indicates Immediate-Reservation-On, the AMSS shall immediately request to turn on the reservation after the network-initiated QoS setup is complete, without any trigger from, for example, the application.
- This only applies to eHRPD. The AMSS shall allow the application to invoke a Resume QoS API to turn on the reservation.

8.4.1 Use case 2 – QoS-aware application registers a notification callback

The use case describes the following scenarios:

- The QoS-aware application uses a new API to register a notification callback with the AMSS.
- The AMSS notifies the application when the QoS is pushed by the network.

Preconditions

- The UE is in eHRPD personality or the UE is attached to E-UTRA.
- The PPP session is established if in eHRPD.
- The application is activated. The UE established the PDN connection for the application to the APN, for which the bearer/QoS will be established.

Assumptions

None

Trigger

Based on the notification of PDN connectivity establishment and/or other application layer signaling, the application makes the decision of registering a QoS notification callback with the AMSS.

Description

The call flow is shown in Figure 8-4.

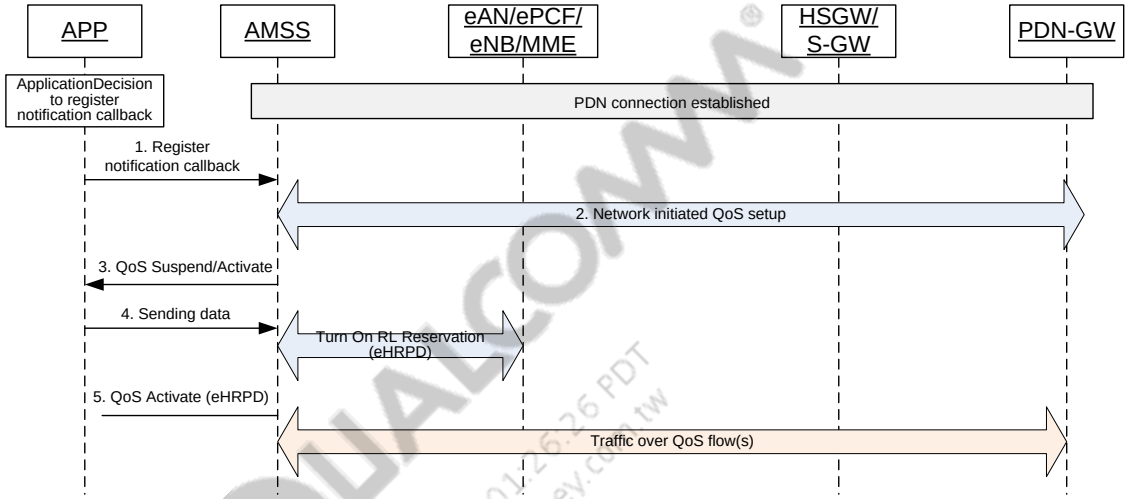

Figure 8-4 Application registers a notification callback with AMSS

The following numbered paragraphs correspond to Figure 8-4:

1. Based on the trigger, the application registers a notification callback with requested filters with the AMSS. Before the QoS is configured, and activated, if needed, the application may send the data using the best-effort flow if the application QoS configuration preference is QoSPreferred. If the application QoS configuration preference is QoSRequired, the application shall block sending data until the QoS flow is configured and successfully activated.
2. In this step, the network-initiated QoS procedures are performed. The packet filter(s) are set up in the AMSS.
3. The AMSS performs filter matching. If the filter matches the application-registered filters, the AMSS notifies the application of QoS Activate or QoS Suspend, if QoS activation is needed. The AMSS can also report the QoS flow parameter(s) to the application.
4. This step only applies to eHRPD. Upon receiving data from the application, the AMSS shall turn on the RL reservation.
5. This step only applies to eHRPD. The AMSS notifies the application of QoS Activate.

Postconditions

The QoS flow(s) are activated and are ready to transfer packets for the application.

Error scenario

In eHRPD, if the reservation is not turned on successfully, the AMSS shall attempt to activate the RL reservation next time when it receives data from the application until the RL reservation is activated successfully.

8.4.2 Alternative scenario of Use case 2 – QoS-aware application registers notification callback and indicates Immediate-Reservation-On

This alternative use case only applies to eHRPD. This use case describes the following scenario:

- The QoS-aware application uses a new API to register a notification callback with the AMSS and indicates Immediate-Reservation-On.
- The AMSS notifies the application when QoS is pushed by the network.

Preconditions

- The UE is in eHRPD personality.
- The PPP session is established.
- The application is activated. The UE established the PDN connection for the application to the APN, for which the bearer/QoS will be established. The UE shall include the BCM parameter in the PCO option when sending the VSNCP config-Req to the HSGW.

Assumptions

None

Trigger

Based on the notification of PDN connectivity establishment and/or other application layer signaling, the application makes a decision about registering a QoS notification callback with the AMSS.

Description

The call flow is shown in Figure 8-5.

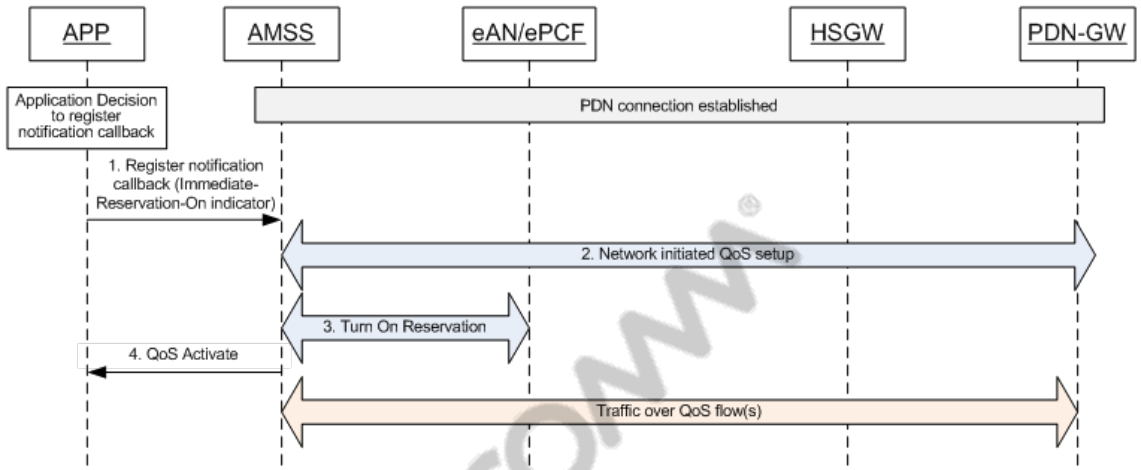

Figure 8-5 Application registers notification callback and indicates Immediate-Reservation-On

The following numbered paragraphs correspond to Figure 8-5:

1. Based on the trigger, the application registers a notification callback with requested filters with the AMSS and indicates Immediate-Reservation-On. Before the QoS is configured and activated, the application may send the data using the best-effort flow if the application QoS configuration preference is QoSPreferred. If the application QoS configuration preference is QoSRequired, the application shall block sending data until the QoS flow is configured and activated successfully.
2. In this step, network-initiated QoS procedures are performed and packet filter(s) are set up in the AMSS.
3. The AMSS performs filter matching. If the filter matches the application registered filters, the AMSS shall turn on the reservation for the QoS flow(s) that were just set up.
4. The AMSS notifies the application of QoS Activate. The AMSS may report to the application the ProfileID(s) specified in the network-initiated QoS. The QoS flow(s) are ready to send packets for the application.

Postconditions

The QoS flow(s) are configured and the reservation is activated.

Error scenario

If the reservation is not turned on successfully, the AMSS shall attempt to activate the reservation the next time when it receives data from the application or when the application requests to turn on reservation explicitly.

8.4.3 Use case 3 – QoS-aware application requests to turn on reservation

This use case only applies to eHRPD. This use case describes the scenario when the QoS-aware application requests to turn on the reservation after network-initiated QoS setup is complete.

Preconditions

- The UE is in eHRPD personality.
- The PPP session is established.
- The application is activated. The UE established the PDN connection for the application to the APN, for which the bearer/QoS will be established.
- The application registered a notification callback with the AMSS.

Assumptions

None

Trigger

QoS flow(s) are pushed by the network.

Description

The call flow is shown in Figure 8-6.

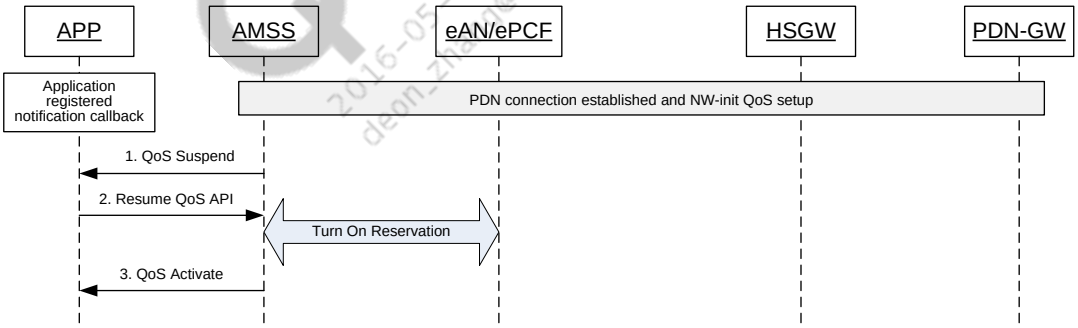

Figure 8-6 Application requests AMSS to turn on reservation

The following numbered paragraphs correspond to Figure 8-6:

1. After the network-initiated QoS setup procedures are complete, packet filter(s) are set up in the AMSS. The AMSS performs filter matching and the filter matches the application registered filters. The AMSS shall notify the application of QoS Suspend. The AMSS may report to the application the ProfileID(s) specified in the network-initiated QoS.
2. The application invokes the Resume QoS API to request the AMSS to turn on the reservation for the QoS flow(s) that were just set up.
3. The AMSS notifies the application of QoS Activate. The QoS flow(s) are ready to send packets for the application.

Postconditions

The QoS reservation is activated.

Error scenario

If the reservation is not turned on successfully, the AMSS shall attempt to activate the reservation the next time when it receives data from the application or when the application requests to turn on reservation explicitly.

8.4.4 Use case 4 – QoS-aware application queries QoS state and parameters

The use case describes the following scenarios:

- The QoS-aware application uses a new API to query QoS state and/or parameters with the AMSS.
- The AMSS notifies the application of QoS state and/or QoS parameters.

Preconditions

- The UE is in eHRPD personality or the UE is attached to E-UTRA.
- The PPP session is established if in eHRPD.
- The application is activated. The UE established the PDN connection for the application to the APN.

Assumptions

None

Trigger

The application sends the QoS query to the AMSS.

Description

The call flow is shown in Figure 8-7.

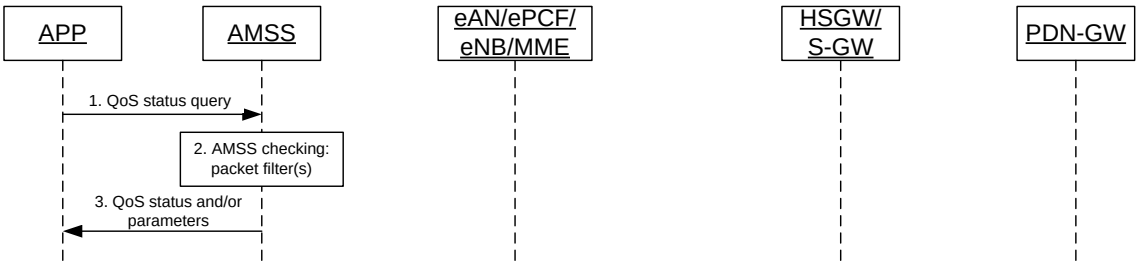

Figure 8-7 Application queries QoS state and/or parameters with AMSS

The following numbered paragraphs correspond to Figure 8-7:

1. The application queries the QoS state and/or parameters with requested filters with the AMSS.
2. The AMSS performs filter matching.
3. If the filter matches the application queried filter, the AMSS notifies the application of the QoS state and QoS parameters if they are available, e.g., FlowProfileIDs for eHRPD and QCIs/MBRs/GBRs for E-UTRA. Otherwise, if there is no packet filter that matches the application queried filter, the AMSS notifies the application of QoS Unavailable.

Postconditions

The application is aware of the QoS state and/or QoS parameters.

8.5 Coexistence of UE and network-initiated QoS

See [Q2] and [Q8] for eHRPD UE-initiated QoS procedures.

If both UE-initiated and network-initiated QoS flows are concurrently supported in a given network, the operations on network-initiated and UE-initiated QoS flows are summarized as shown in Table 8-2.

Table 8-2 Operations on network-initiated and UE-initiated QoS flows

Operator		Operations initiated by network			Operations initiated by UE		
Operation		Modify packet filter (5-tuples or less) and/or precedence	Modify FlowProfile ID/QCI	Delete QoS flow	Modify packet filter (5-tuples or less) and/or precedence	Modify FlowProfile ID/QCI	Delete QoS flow
QoS flow	Network-initiated QoS flow	Allowed	Allowed	Allowed	Not allowed	Allowed	Not allowed
	UE-initiated QoS flow	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed

8.5.1 Assumptions

During the Network-initiated QoS establishment procedure, the filter precedence field is present in the RSVP message sent by the network to the UE. This information field is used to prioritize packet filters between network-initiated and UE-initiated QoS flows. The network should set the UE-initiated and network-initiated QoS flow precedence values to avoid having the same precedence value for any two flows for the same UE IP address.

8.5.2 Requirements

- If the application calls the Request QoS API, the AMSS shall perform packet-filter matching with the existing network-initiated QoS flows. If it is present in the QoS, the 5-tuple packet filter bit-wise matches the packet filter of any existing network-initiated QoS flow and the AMSS shall link the existing filter to the application. Thus, the application obtains the handle to the network-initiated QoS flow and the handle is available until the QoS context is released. Meanwhile, the AMSS shall treat the QoS request as a modification of the existing network-initiated QoS flow[8]. eHRPD, i.e., Profile, as the QoS metric, is the example.

NOTE: The QoS Check step only applies to eHRPD.

  - If Condition 8.1 is satisfied, the AMSS shall notify the application of QoS Activate/Suspend, without proceeding with QoS modification[9].
  - If Condition 8.1 is not satisfied, the AMSS shall proceed with QoS modification of the existing network-initiated QoS flow. If ($\text{ProfileSet}_{\text{Requested}} \subseteq \text{ProfileSet}_{\text{Authorized}}$) holds (both sets are treated as unordered lists when checking this condition), the AMSS shall skip QoS Check and only modify radio QoS. Otherwise, if ($\text{ProfileSet}_{\text{Requested}} \subseteq \text{ProfileSet}_{\text{Authorized}}$) does not hold, the AMSS shall perform the Union operation of $\text{ProfileSet}_{\text{Requested}}$ and $\text{ProfileSet}_{\text{Authorized}}$ and shall then run Modify QoS with the resulted Profile set from QoS Check. When the UE sends the Profile set to the network in the QoS Check step and/or radio QoS configuration step, if applicable, the UE shall list the requested Profile set in a higher priority than the rest.

    The previous steps are summarized here:

    [Condition 8.1] The RAN-granted Profile of the existing NW-init QoS flow is the most preferred in the requested Profile set, and the requested Profile set is a subset of the HSGW-authorized Profile set of the existing NW-init QoS flow i.e. ($\text{ProfileSet}_{\text{Requested}} \subseteq \text{ProfileSet}_{\text{Authorized}}$).

    If Condition 8.1 is satisfied

    Then return QoS Activate/Suspend (no modification)

    Else (i.e., Condition 8.1 is not satisfied)

    If $\text{ProfileSet}_{\text{Requested}} \subseteq \text{ProfileSet}_{\text{Authorized}}$ (as unordered lists)

    Then skip QoS Check and only perform radio QoS modification (with the requested Profile set put in the higher priority than the rest)

    Else

    Perform $\text{ProfileSet}_{\text{Requested}} \cup \text{ProfileSet}_{\text{Authorized}}$ and

    Perform QoS modification with the resulted Profile set from QoS Check (with the requested Profile set put in a higher priority than the rest)

    End

[8]The authorized Profile set maintained in the AMSS shall be updated based on the authorized QoS List provided by the HSGW.

[9]The currently requested Profiles were previously authorized by the HSGW. The RAN is likely to grant the same Profile as the currently used one. Therefore, the AMSS does not proceed with QoS modification.

End

- On eHRPD, if the application requests to modify the QoS metrics and the QoS Check step fails, the AMSS shall retain the legacy QoS metrics and shall notify the application of QoS Suspend/Activate. If the TFT Setup or Radio QoS step fails, the AMSS shall abandon QoS and shall notify the application of QoS Release.
- On eHRPD, the AMSS shall allow the network to modify the precedence of a UE-init QoS flow during QoS setup procedures. If the network assigns a new precedence value in the ResvConf message with OpCode QoS Check Confirm, the UE shall set up the TFTs with the modified precedence.
- If the application has the handle to the network-initiated QoS flow, the AMSS shall allow the application to delete the handle but shall not allow deletion of the network-initiated QoS flow.
- The AMSS shall not allow the application to modify the packet filters associated with network-initiated QoS flow. The AMSS shall allow the application to modify the FlowProfileIDs or QCIs associated with network-initiated QoS flow.
- The AMSS shall allow the network to modify the packet filter and/or precedence and/or FlowProfileID associated with the UE-initiated QoS flow.

8.5.3 Use case 5 – QoS-aware application requests QoS when QoS was already configured by the network

The use case describes the scenario when the QoS-aware application requests QoS and QoS has already been configured by the network. In this use case, Condition 8.1, defined in Section 8.2.2, is satisfied.

Preconditions

- The UE is in eHRPD personality or the UE is attached to E-UTRA.
- The PPP session is established if in eHRPD.
- The UE established the PDN connection to the APN, for which the bearer/QoS will be established.
- QoS flow(s) are already configured by the network.

Assumptions

None

Trigger

The application calls the Request QoS API.

Description

The call flow is shown in Figure 8-8.

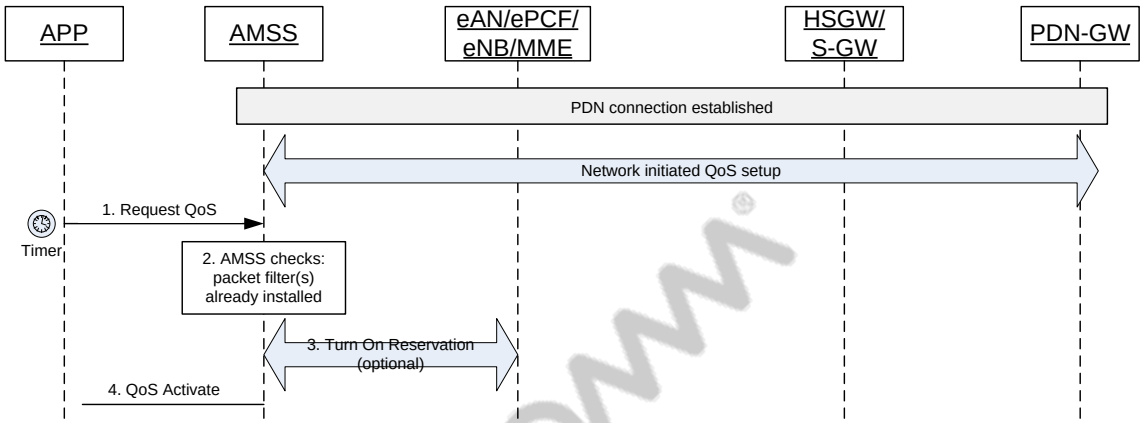

Figure 8-8 QoS-aware application requests QoS when QoS was already configured by the network

The following numbered paragraphs correspond to Figure 8-8:

1. The application calls the Request QoS API. The application may start a timer after it calls this API into the AMSS.
2. The AMSS checks if the requested packet filter(s) are already installed. By performing filter matching (see Section 8.4.2), if the installed packet filter(s) match the requested packet filter(s), the AMSS considers that the requested packet filter(s) are installed. In this use case, the requested packet filter(s) were already installed by the network-initiated QoS procedure. The AMSS shall also check if Condition 8.1 is satisfied. In this use case, Condition 8.1 is satisfied.
3. This step is optional and only applies to eHRPD. The AMSS shall turn on the reservation if it is not already activated.
4. The AMSS notifies the application by invoking the QoS Activate callback.

Postconditions

QoS flow(s) are configured and the reservation is activated.

8.5.4 Alternative scenario of use case 5

This is an alternative scenario of use case 3, in which the QoS-aware application requests QoS and the QoS was already configured by the network. In this use case, Condition 8.1 is not satisfied. The AMSS shall proceed with QoS metrics modification of the established network-initiated QoS flow.

Preconditions

- The UE is in eHRPD personality or the UE is attached to E-UTRA.
- The PPP session is established if in eHRPD.

- The UE established the PDN connection to the APN, for which the bearer/QoS will be established.
- QoS flow(s) are already configured by the network.

Assumptions

None

Trigger

The application calls the Request QoS API.

Description

The call flow is shown in Figure 8-9.

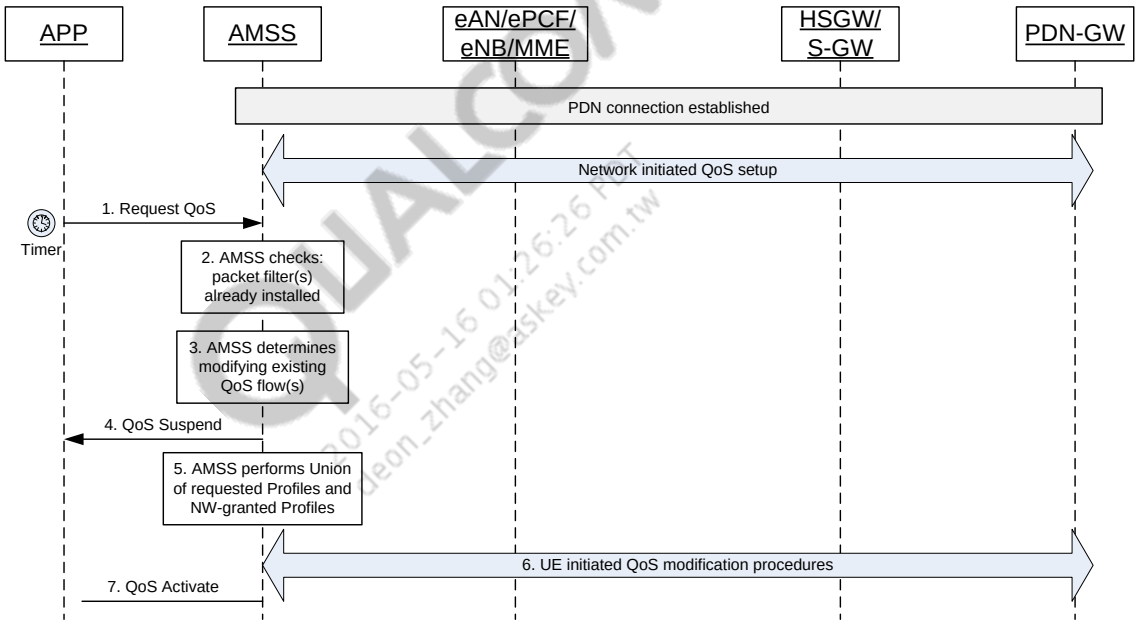

Figure 8-9 Alternative scenario of use case 5

The following numbered paragraphs correspond to Figure 8-9:

1. The application calls the Request QoS API. The application may start a timer after it calls this API into the AMSS.
2. The AMSS checks if the requested packet filter(s) are already installed. By performing filter matching (see Section 8.4.2), if the installed packet filter(s) match the requested packet filter(s), the AMSS considers the requested packet filter(s) to be installed. In this use case, the requested packet filter(s) are already installed by the network-initiated QoS procedure.
3. The AMSS shall check if Condition 8.1 is satisfied. In this use case, Condition 8.1 is not satisfied and the AMSS must perform UE-init QoS modification.
4. The AMSS gives a QoS Suspend notification to the application.
5. The AMSS performs a Union operation of the requested Profile/QCI set and the HSGW/S-GW-authorized Profile/QCI set of the existing QoS flow.

6. The AMSS performs the UE-init QoS modification procedure. The UE shall list the requested Profile/QCI set in the beginning of the Profile/QCI set sent to the network.
7. The AMSS notifies the application by invoking the QoS Activate callback.

Postconditions

The QoS flow(s) are modified.

8.5.5 Use case 6 – QoS-aware application requests QoS while QoS is not yet configured

The use case describes the scenario when the QoS-aware application requests QoS and QoS is not yet configured.

Preconditions

- The UE is in eHRPD personality or the UE is attached to E-UTRA
- The PPP session is established if in eHRPD.
- The UE established the PDN connection to the APN, for which the bearer/QoS will be established.

Assumptions

None

Trigger

The application calls the Request QoS API.

Description

The call flow is shown in Figure 8-10.

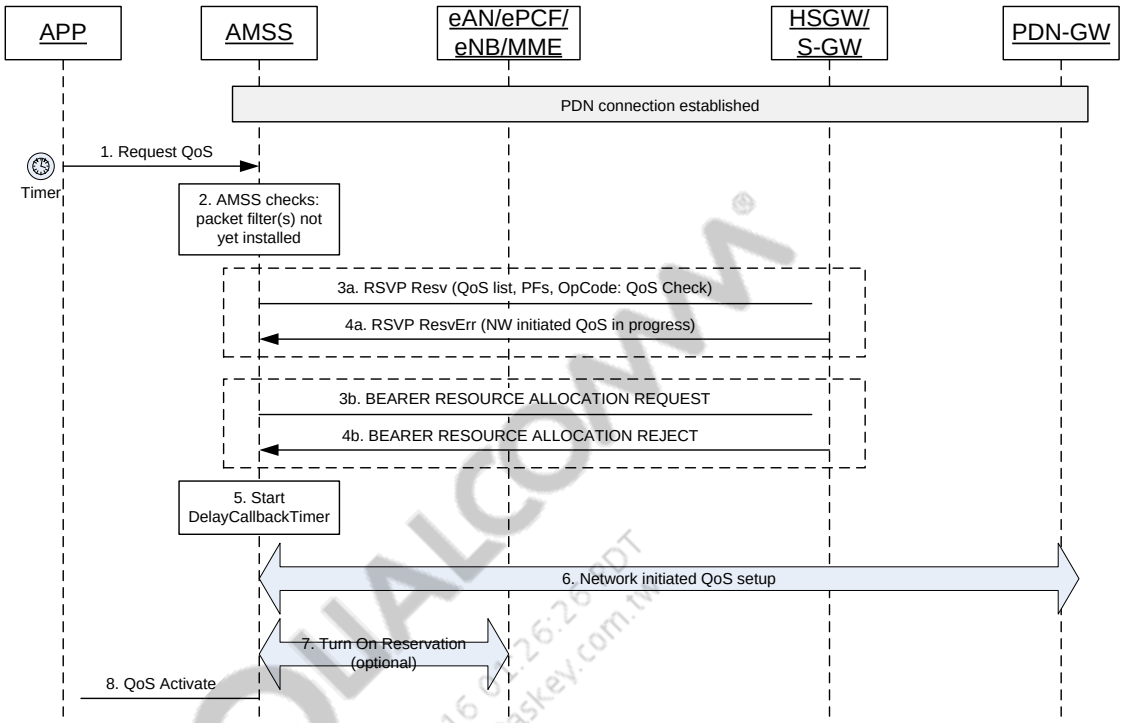

Figure 8-10 QoS-aware application requests QoS while QoS is not yet configured by the network

The following numbered paragraphs correspond to Figure 8-10:

1. The application calls the Request QoS API. The application may start a timer after it calls this API into the AMSS.
2. The AMSS checks if the requested packet filter(s) are already installed. By performing filter matching (see Section 8.4.2), if the installed packet filter(s) match the requested packet filter(s), the AMSS considers the requested packet filter(s) to be installed. In this use case, the requested QoS flow(s) are not yet installed.
   - If the UE is in eHRPD – The UE sends an RSVP Resv message to the HSGW.
   - If the UE is in LTE – The UE sends the NAS message Bearer Resource Allocation Request.
   - If the UE is in eHRPD – If the network is setting up QoS for the flows that the UE is trying to set up, the HSGW responds with an RSVP ResvErr message with the error code NW-initiated QoS in progress.
   - If the UE is in LTE – The network responds with the NAS message Bearer Resource Allocation Reject.

3. In eHRPD, upon receipt of the cause code NW-initiated QoS in progress, the AMSS shall start a configurable DelayCallbackTimer, as defined in Table 8-3. In LTE, since there is no NW-initiated QoS in progress cause code in LTE, the AMSS shall start the DelayCallbackTimer when any error from the network is received. The UE waits for the network to push QoS before notifying the application. The UE shall maintain the requested QoS context and links to the application until this timer expires. Before the QoS flow(s) are configured and activated, the application may send data using the best-effort flow if the application QoS configuration preference is QoSPreferred. If the application QoS configuration preference is QoSRequired, the application shall block sending data until QoS flow is successfully activated.

Table 8-3 Configurable DelayCallbackTimer variable

Name	Unit	Default	Description
DelayCallbackTimer	Second	30	The variable identifies the period of time, counted from the time when the UE receives any error from the network. The UE shall not report any error to the application before this timer expires.

4. In this step, network-initiated QoS procedures are performed. The packet filter(s) are set up in the AMSS.
5. This step is optional and only applies to eHRPD. The AMSS shall turn on the reservation for network-initiated QoS flows.
6. The AMSS notifies the application by invoking QoS Activate callback.

Postconditions

The QoS flow(s) are activated and are ready to exchange packets for the application.

8.5.6 Error scenario 1 of use case 6 – DelayCallbackTimer times out while waiting for network to push QoS

This use case describes the following scenario:

- The QoS-aware application requests QoS and the QoS is not yet configured.
- The DelayCallbackTimer times out while the UE waits for the network to push QoS.

Preconditions

- The UE is in eHRPD personality or the UE is attached to E-UTRA.
- The PPP session is established if in eHRPD.
- The UE established the PDN connection to the APN, for which the bearer/QoS will be established.

Assumptions

None

Trigger

The application calls the Request QoS API.

Description

The call flow is shown in Figure 8-11.

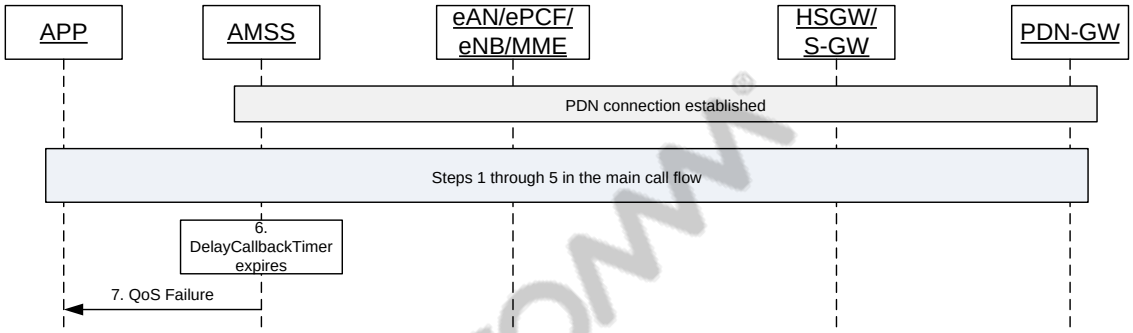

Figure 8-11 DelayCallbackTimer times out while waiting for network to push QoS

Steps 1 through 5 follow the same behavior shown in the main flow in Figure 8-11.

The following numbered paragraphs correspond to Figure 8-11:

1. The DelayCallbackTimer has expired.
2. The AMSS notifies the application of the failure.

Postconditions

- No QoS flow(s) are set up. The QoS context is released.
- If the application registered the notification callback with the AMSS, the application does receive QoS notification after the network pushes QoS. Otherwise, the application does not receive QoS notification after the network successfully pushes QoS. The application does still receive QoS treatment.

8.5.7 Error scenario 2 of use case 6 – Application times out waiting for QoS setup

The use case describes the following scenario:

- The QoS-aware application requests QoS and QoS is not yet configured.
- The application timer times out before it receives any QoS notification from the AMSS. The AMSS is notified of this timeout event.

Preconditions

- The UE is in eHRPD personality or the UE is attached to E-UTRA.
- The PPP session is established if in eHRPD.
- The UE established the PDN connection to the APN, for which the bearer/QoS will be established.

Assumptions

None

Trigger

The application calls the Request QoS API.

Description

The call flow is shown in Figure 8-12.

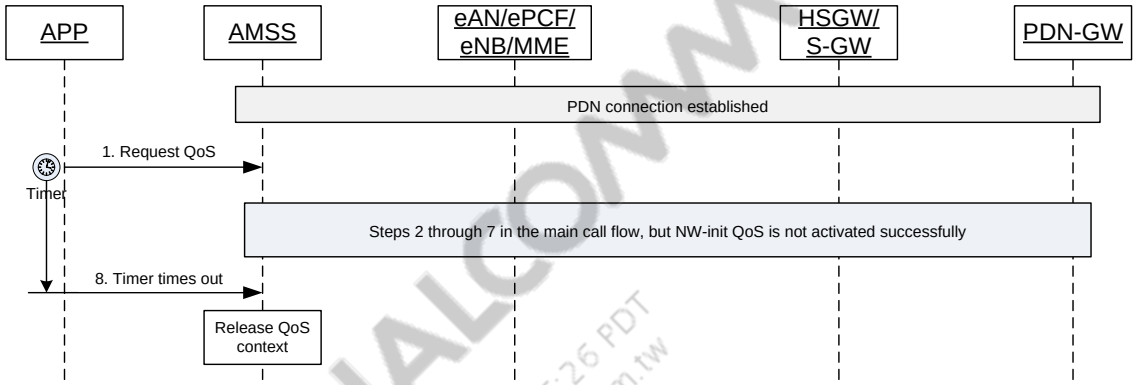

Figure 8-12 Application times out before QoS notification is received from the AMSS

Steps 1 through 7 of this scenario follow the same behavior shown in the call flow of Figure 8-12, except network-initiated is not activated successfully, i.e., some steps may not occur, before the event in step 8 occurs.

The following paragraph corresponds to Figure 8-12:

The application times out while waiting for the Network-initiated QoS is activated successfully. Upon getting the timeout notification from the application, the AMSS shall release the QoS context.

Postconditions

- No QoS flow(s) are set up. The QoS context is released at the AMSS.
- If the application registered the notification callback with the AMSS, the application receives QoS notification after the network pushes the QoS. Otherwise, the application does not receive QoS notification, though it still receives QoS treatment, after the network successfully pushes QoS.

8.5.8 Use case 7 – QoS-aware application requests QoS modification

The use case describes the scenario when the QoS-aware application requests modification of a configured QoS. The QoS flow to be modified may be UE-initiated or network-initiated. The AMSS shall not allow the application to request modification of the filter(s) of any configured network-initiated QoS flow.

Preconditions

- The UE is in eHRPD personality or the UE is attached to E-UTRA.
- The PPP session is established if in eHRPD.
- The UE established the PDN connection to the APN and the QoS flow is configured over the PDN connection to the APN.

Assumptions

None

Trigger

The application calls the Modify QoS API. If the QoS flow to be modified is network-initiated, the application does not request a modification of the associated filter(s).

Description

The call flow is shown in Figure 8-13.

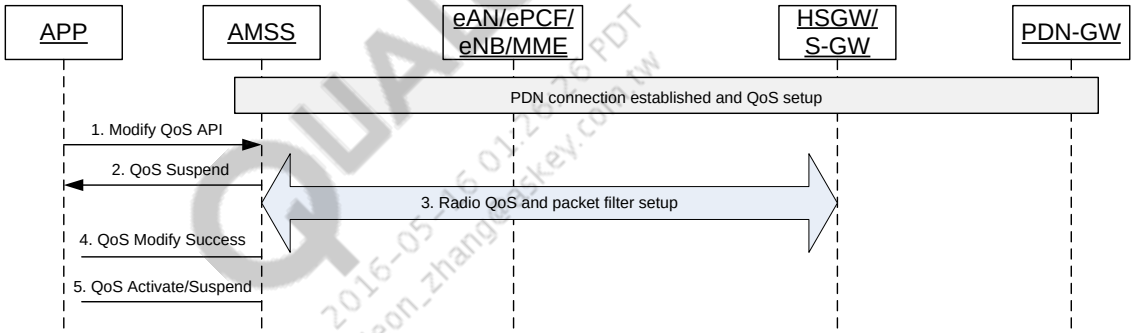

Figure 8-13 QoS-aware application requests QoS modification

The following numbered paragraphs correspond to Figure 8-13:

1. The application calls Modify QoS API into the AMSS.
2. The AMSS notifies the application of QoS Suspend.
3. The AMSS and the network exchange messages to set up radio QoS and packet filter(s).
4. The AMSS notifies the application of QoS Modify Success.
5. The AMSS notifies the application of QoS Suspend/Activate, depending on the QoS state before modification.

Postconditions

- The QoS is modified.
- The QoS state is not changed.

8.5.9 Error scenario 1 of use case 7 – Failure occurs but legacy QoS is retained

The use case describes the scenario when the QoS-aware application requests modification of a configured QoS and one of the following failures occurs:

- Any failure if the UE is in LTE mode
- A QoS Check failure if the UE is in eHRPD mode

Preconditions

- The UE is in eHRPD personality or the UE is attached to E-UTRA.
- The PPP session is established if in eHRPD.
- The UE established the PDN connection to the APN and the QoS flow is configured over the PDN connection to the APN.

Assumptions

None

Trigger

The application calls the Modify QoS API. If the QoS flow to be modified is network-initiated, the application does not request a modification of the associated filter(s).

Description

The call flow is shown in Figure 8-14.

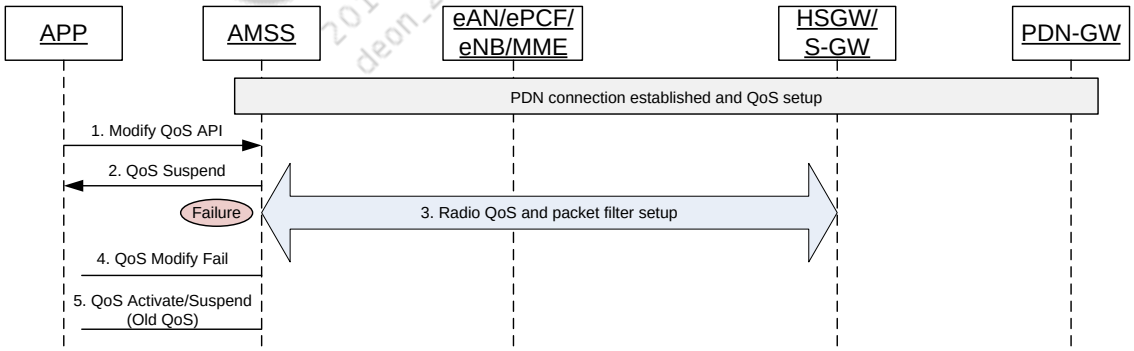

Figure 8-14 Error scenario 1 – QoS-aware application requests QoS modification

The following numbered paragraphs correspond to Figure 8-14:

1. The application calls Modify QoS API into the AMSS.
2. The AMSS notifies the application of QoS Suspend.
3. The AMSS and the network exchange messages to set up radio QoS and packet filter(s). One of the failures listed earlier for this use case occurs in this step.
4. The AMSS notifies the application of QoS Modify Fail.
5. The AMSS notifies the application of QoS Suspend/Activate, depending on the QoS state before modification.

Postconditions

- The legacy QoS is retained.
- The QoS state is not changed.

8.5.10 Error scenario 2 of use case 7 – Failure occurs and QoS is released

The use case describes the scenario when the QoS-aware application requests modification of a configured QoS and one of the following failures occurs:

- Radio QoS configuration failure if the UE is in eHRPD mode
- TFT setup failure if the UE is in eHRPD mode

Preconditions

- The UE is in eHRPD personality or the UE is attached to E-UTRA.
- The PPP session is established if in eHRPD.
- The UE established the PDN connection to the APN and the QoS flow is configured over the PDN connection to the APN.

Assumptions

None

Trigger

The application calls the Modify QoS API. If the QoS flow to be modified is network-initiated, the application does not request a modification of the associated filter(s).

Description

The call flow is shown in Figure 8-15.

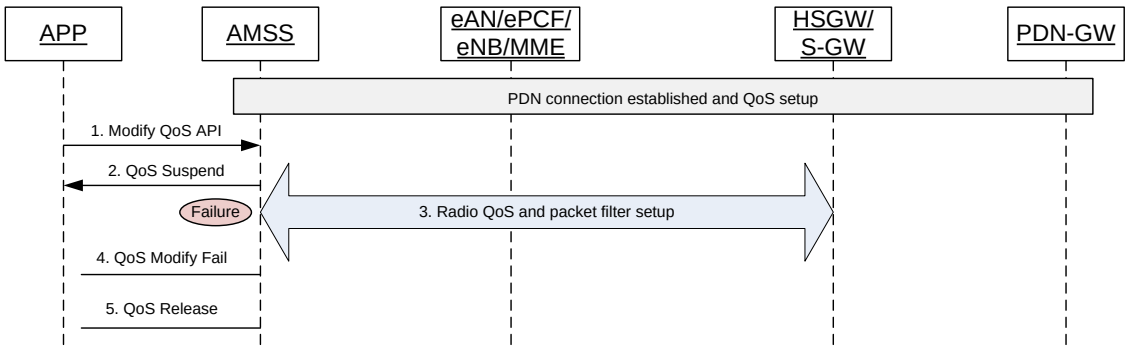

Figure 8-15 QoS-aware application requests QoS modification and radio QoS/TFT Setup fails

The following numbered paragraphs correspond to Figure 8-15:

1. The application calls the Modify QoS API into the AMSS.
2. The AMSS notifies the application of Suspend QoS.

3. The AMSS and the network exchange messages to set up radio QoS and packet filter(s). One of the failures listed earlier for this use case occurs in this step.
4. The AMSS notifies the application of QoS Modify Fail.
5. The AMSS notifies the application of QoS Release.

Postconditions

The QoS is released.

9 QoS Mobility Scenarios

NOTE: Numerous changes were made in this chapter.

This chapter describes UE behavior when the UE transitions between networks with different operator policies on the QoS initialization configuration, e.g., network-initiated, MS-initiated, or MS/network-initiated QoS.

9.1 Assumptions

- The design for eHRPD is consistent with LTE.
- In eHRPD, if an H1/H2 context transfer is supported, the full context in the source HSGW, including PPP, authentication, IP, QoS, lifetime, and related information, shall be transferred to the target HSGW.

9.2 QoS released or suspended during IRAT transition

There are two design options during UE transitions from one RAT to another RAT:

- QoS released during transition – The UE shall locally release the QoS context over the source domain when it leaves the source RAT and shall notify the application of QoS Release. It is up to the application to perform QoS failure handling. After transitioning to the target RAT, the UE considers the QoS context established over the target domain as new, i.e., there is no QoS mobility.
- QoS suspended during transition – The UE shall notify the application of a RAT change. After the UE transitions to the target RAT and the QoS context is established over the target domain, the UE shall replace with the new QoS context and notify the application of QoS Configure/Activate.

9.3 Only network-initiated QoS supported

9.3.1 QoS released during transition use case – Target network is network-initiated QoS-capable and network pushes QoS successfully

The use case describes the scenario when the UE moves to a network-initiated only or UE/network-initiated QoS-capable network and the target network successfully pushes the QoS over the target network. This use case does not support QoS mobility.

Preconditions

- The UE is in eHRPD personality or the UE is attached to E-UTRA.
- The PPP session is established if in eHRPD.

- The UE established the PDN connection to the APN via the Source RAN (S-RAN) and Source HSGW/S-GW (S-HSGW/S-SGW) and the QoS is set up for the bearer over the PDN connection with the APN.
- The target network is UE/network-initiated or network-initiated only capable.

Assumptions

None

Trigger

The UE transitions from S-RAN to T-RAN. The Target RAN (T-RAN) selects a Target HSGW/ T-SGW (T-HSGW/T-SGW).

Description

The scenario is shown in Figure 9-1.

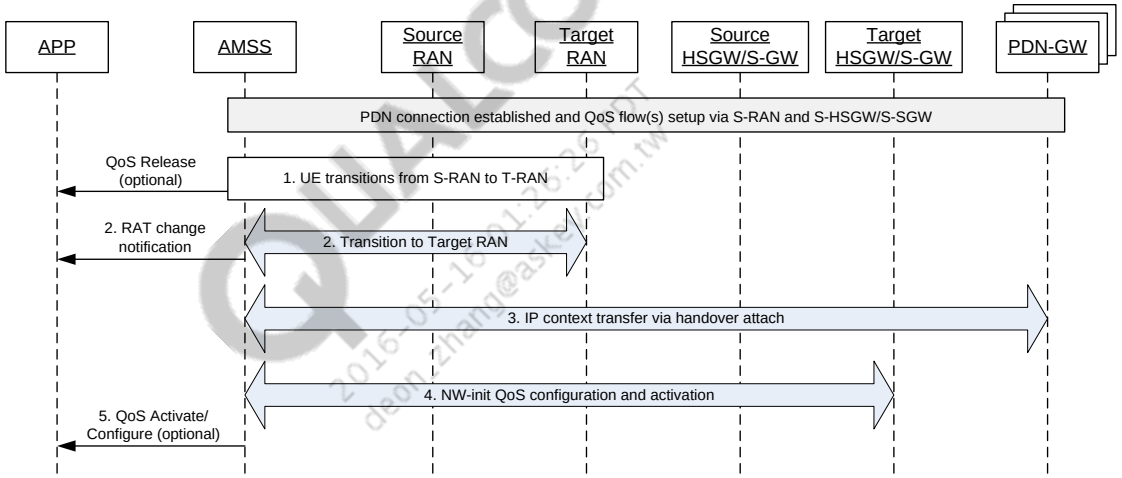

Figure 9-1 QoS released during transition use case

The following numbered paragraphs correspond to Figure 9-1:

1. The UE transitions from S-RAN to T-RAN. This could be an active handoff or a dormant handoff. The AMSS locally releases the QoS context established on the source network. The AMSS shall also notify the application of Release QoS if the API exists.
2. The UE transitions to T-RAN. The AMSS sends a RAT change notification to the application.
3. If the target network is eHRPD, the UE shall create the PPP session and perform EAP-AKA authentication. If the target network is E-UTRA, the UE shall perform the E-UTRA Attach procedure. The UE performs an IP context transfer via the handover attach procedure for each PDN connection to which it is attached within the source RAN.
4. The QoS is pushed by the network.
5. After the QoS flow(s) are activated/configured successfully, the AMSS notifies the application of QoS Activate/Suspend if the API exists.

Postconditions

The QoS flow(s) are configured over the target network.

9.3.2 QoS suspended during transition

9.3.2.1 QoS mobility use case 1 – Target network is network-initiated QoS-capable and network pushes QoS successfully

The use case describes the scenario when the UE moves to a network-initiated only or UE/network-initiated QoS-capable network and the target network successfully pushes the QoS within some configurable period of time.

Preconditions

- The UE is in eHRPD personality or the UE is attached to E-UTRA.
- The PPP session is established if in eHRPD.
- The UE established the PDN connection to the APN via the S-RAN and Source HSGW/S-GW, i.e., S-HSGW/S-SGW, and the QoS is set up for the bearer over the PDN connection with the APN.
- The target network is UE/network-initiated or network-initiated only-capable.

Assumptions

None

Trigger

The UE transitions from S-RAN→T-RAN. The T-RAN selects a T-HSGW/T-SGW.

Description

The scenario is shown in Figure 9-2.

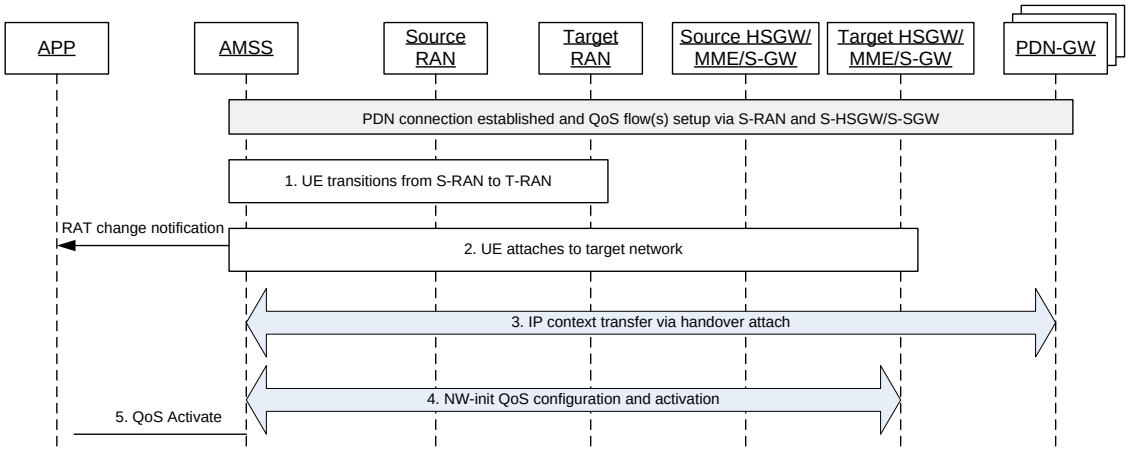

Figure 9-2 QoS mobility use case 1

The following numbered paragraphs correspond to Figure 9-2:

1. The UE transitions from S-RAN to T-RAN. This could be an active handoff or a dormant handoff.
2. The UE attaches to the target network and notifies applications of a radio technology change. If the target network is eHRPD, the UE shall create the PPP session and perform EAP-AKA authentication if no partial context is available at the UE before handoff. If the target network is E-UTRA, the UE shall perform the E-UTRA Attach procedure.
3. The UE performs an IP context transfer via the handover attach procedure for each PDN connection to which it has attachments within the source RAN.
4. The QoS flow is pushed by the network.
5. After the QoS flow(s) are activated successfully, the AMSS notifies the application of QoS Activate if the API exists.

Postconditions

The QoS flow(s) are activated in the target network.

9.4 Coexistence of network and UE-initiated QoS cases

This section is focused on maintaining QoS during transitions. Therefore, the option of QoS suspended during transition is only considered.

9.4.1 Requirements

- The UE shall have knowledge of the target network's QoS capable between network-initiated only and UE/network-initiated through network provisioning.
- After transition, if the target network supports UE-initiated QoS, the AMSS shall initiate QoS establishment, without the intervention of applications, for the QoS flow if this QoS flow satisfies both of the following two conditions:
  - The application has the handle to this QoS flow.
  - The AMSS has RAN-specific QoS parameters for this QoS flow.
- If QoS modification is initiated by either the UE or the network during handoffs, QoS modification is postponed until QoS mobility is complete.

9.4.2 Overview of QoS mobility scenarios

Define the original network as the first network where QoS flow(s) are established. When QoS flow(s) are configured in the original network, they can be UE-initiated or network-initiated. Later, the UE moves to a target network that is capable of being UE-initiated only, UE/network-initiated, or network-initiated only[10], depending on the Selected BCM set by the network, i.e., MS-only or MS/network.

[10]Network-initiated only is not an option specified by the standard [S5], but may be deployed by the operator.

QoS mobility use scenarios when the target network is network-initiated only QoS-capable are covered in Section 9.3.2. QoS mobility use scenarios when the target network is UE/network-initiated or UE-initiated-only QoS-capable are covered in this section. The possible scenarios are summarized in Table 9-1.

Table 9-1 QoS flow mobility use cases

		Target network capability of QoS initialization		
		Network only	**MS only**	**MS/network**
QoS initialization of QoS flow(s) in the original network	UE-initiated	QoS mobility use case 1	QoS mobility use case 3	QoS mobility use case 2
	Network-initiated		QoS mobility use cases 3 and 4	QoS mobility use cases 2 and 4

Figure 9-3 shows QoS flow mobility use cases.

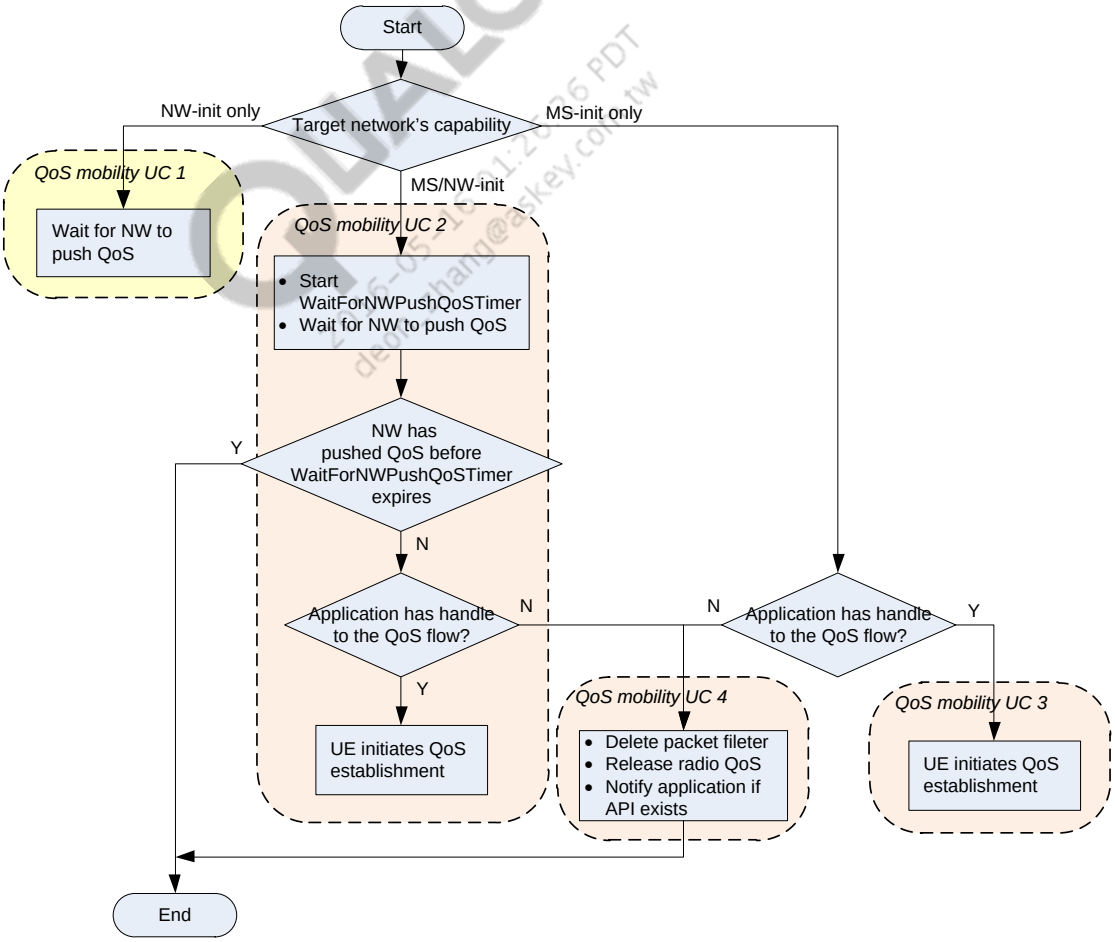

Figure 9-3 QoS flow mobility use cases

9.4.3 QoS mobility use case 2 – Target network is UE/network-initiated QoS-capable

If the UE transitions to a target network that is UE/network-initiated QoS-capable, the UE shall start a timer, WaitForNWPushQoSTimer (defined in Table 9-2), and shall wait for the network to initiate QoS setup in the target network. The use cases defined for network-initiated only QoS-capable (mobility use case 1 in Section 9.3.2) also apply here, except the UE shall start WaitForNWPushQoSTimer.

- If the target network is eHRPD, the UE shall start the timer when it learns that the target network is MS/network-initiated QoS-capable from the selected BCM during the VSNCP procedure or when it releases the radio QoS context after radio QoS renegotiation fails. See [Q2] for details.
- If the target network is E-UTRAN, the UE shall start the timer when the UE finishes the handover attach procedure.

If a network-initiated QoS setup request is received in the target network before the timer WaitForNWPushQoSTimer expires, the UE shall stop the timer.

If the timer WaitForNWPushQoSTimer expires while waiting for the network-initiated QoS setup request from the target network, the UE shall stop the timer and shall initiate the UE-initiated QoS setup procedure if the application has the handle to access the QoS flow; this is described in the following alternative scenario.

Table 9-2 Configurable WaitForNWPushQoSTimer variable

Name	Unit	Default	Description
WaitForNWPushQoSTimer	Second	30	This identifies the period of time during which the AMSS waits for the network to push the QoS. The AMSS shall not initiate QoS setup procedures before this timer expires.

9.4.4 Alternative scenario of QoS mobility UC 2 – Target network is UE/network-initiated QoS-capable and network does not initiate QoS setup

See Section 9.3.2.1 for QoS mobility use case 1.

This use case describes the scenario when the UE moves to a UE/network-initiated QoS-capable network and the target network does not initiate QoS setup procedures within a configurable period of time. In this scenario, the application has the handle to access the QoS flow.

Preconditions

- The UE is in eHRPD personality or the UE is attached to E-UTRA.
- The PPP session is established if in eHRPD.
- The UE established the PDN connection to the APN via the S-RAN and S-HSGW/S-SGW and the QoS is set up for the bearer over the PDN connection with the APN.
- The target network is UE/network-initiated QoS-capable.
- The application has the handle to access the QoS flow.
- The application specified the QoS parameters for the target network in the original network.

Assumptions

None

Trigger

The UE transitions from S-RAN to T-RAN. T-RAN selects a T-HSGW/T-SGW.

Description

The scenario is shown in Figure 9-4.

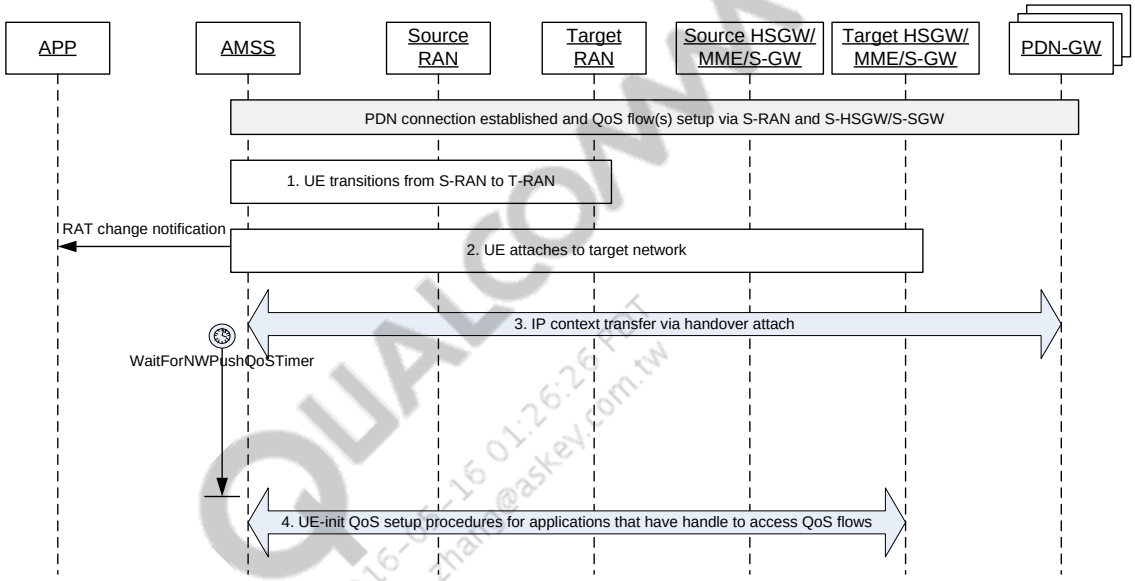

Figure 9-4 Alternative scenario of QoS mobility use case 1

The following numbered paragraphs correspond to Figure 9-4:

1. The UE transitions from S-RAN to T-RAN. The handoff could be active or dormant.
2. The UE attaches to the target network and notifies applications of a radio technology change. If the target network is eHRPD, the UE shall create the PPP session and perform EAP-AKA authentication if no partial context is available at the UE before handoff. If the target network is E-UTRA, the UE shall perform the E-UTRA Attach procedure.
3. The UE performs IP context transfer via the handover attach procedure for each PDN connection to which it has attachments within the source RAN. Upon learning that the current network is MS/network-initiated QoS-capable, not network-initiated only QoS-capable, the AMSS shall start the WaitForNWPushQoSTimer, as defined in Table 9-2. The AMSS may learn of MS/network-initiated or network-initiated only QoS-capable from the provisioned information.
4. If WaitForNWPushQoSTimer expires while the QoS setup procedure is not initiated by the network, the AMSS shall initiate the UE-init QoS setup procedures for the application that has the handle to access QoS flow.

Postconditions

The postcondition can be one of the following:

- If UE-initiated QoS succeeds, the QoS flow(s) are activated and ready to exchange packets for the application in the target network. The AMSS notifies the application of QoS Activate.
- If UE-initiated QoS fails, the AMSS releases the QoS context and notifies the application of QoS Release.

9.4.5 QoS mobility use case 3 – Target network is UE-initiated only QoS-capable and application has handle to access QoS flow

The use case describes the scenario when the UE moves to a UE-initiated only QoS-capable network. The QoS was initiated by either the UE or the network in the original network. The application has the handle to access the QoS flow.

Preconditions

- The UE is in eHRPD personality or the UE is attached to E-UTRA.
- The PPP session is established if in eHRPD.
- Suppose the UE is served by the S-RAN and S-HSGW/S-SGW before transitioning to the target network. The UE established the PDN connection to the APN via the S-RAN and S-HSGW/S-SGW and QoS is set up for the bearer over the PDN connection with the APN.
- The target network is UE-initiated only QoS-capable.
- The application has the handle to access the QoS flow.
- The application specified the QoS parameters for the target network in the original network.

Assumptions

None

Trigger

The UE transitions from S-RAN→T-RAN. T-RAN selects a T-HSGW/T-SGW.

Description

The scenario is shown in Figure 9-5.

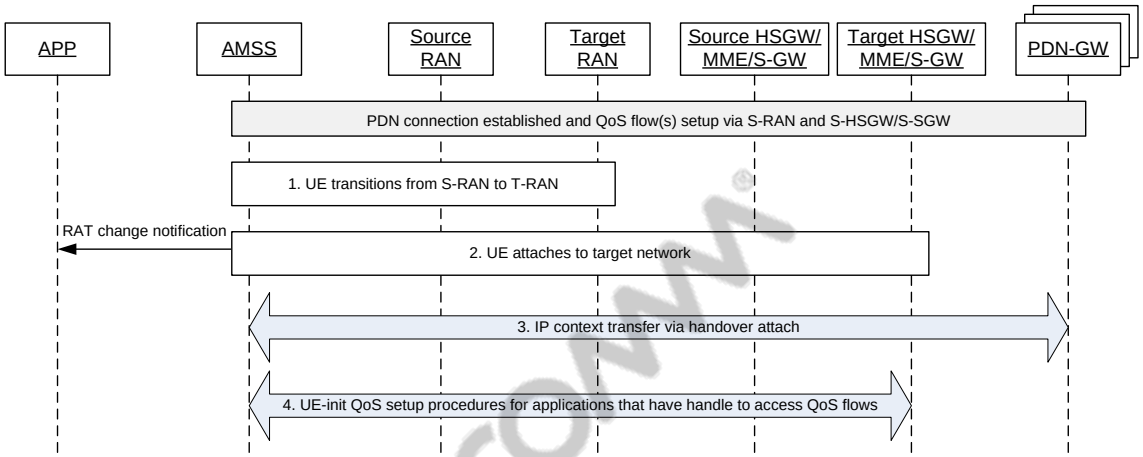

Figure 9-5 QoS mobility use case 3

The following numbered paragraphs correspond to Figure 9-5:

1. The UE transitions from S-RAN to T-RAN. The handoff could active or dormant.
2. The UE attaches to the target network and notifies the applications of a radio technology change. If the target network is eHRPD, the UE shall create the PPP session and perform EAP-AKA authentication if no partial context is available at the UE before handoff. If the target network is E-UTRA, the UE shall perform the E-UTRA Attach procedure.
3. The UE performs IP context transfer via the handover attach procedure for each PDN connection to which it has attachments within the source RAN.
4. Upon learning that the target network is UE-initiated only QoS-capable, e.g., from the selected BCM during the VSNCP procedure if the target network is eHRPD, the AMSS shall initiate the UE-initiated QoS setup procedures for the application that has the handle to access the QoS flow.

Postconditions

The postcondition can be one of the following:

- If UE-initiated QoS succeeds, the QoS flow(s) are activated and ready to exchange packets for the application in the target network. The AMSS notifies the application of QoS Activate.
- If UE-initiated QoS fails, the AMSS releases QoS context and notifies the application of QoS Release.

9.4.6 QoS mobility use case 4 – Target network is UE-initiated only QoS-capable and application has no handle to access QoS flow

This use case describes one of the following scenarios:

- The UE moves to a UE/network-initiated QoS-capable network and the QoS flow was initiated by the network in the original network. The network does not initiate QoS setup procedures within a configurable period of time. The application does not have the handle to access the QoS flow.
- The UE moves to a UE-initiated only capable network and QoS flow was initiated by the network in the original network. The application does not have the handle to access the QoS flow.

Preconditions

The preconditions are:

- The UE is in eHRPD personality or is attached to E-UTRA.
- The PPP session is established if in eHRPD.
- The UE established the PDN connection to the APN via the S-RAN and S-HSGW/S-SGW and the QoS is set up for the bearer over the PDN connection with the APN.
- The application does not have the handle to access the QoS flow.

Assumptions

None

Trigger

The trigger can be one of the following:

- The UE moves to a UE/network-initiated QoS-capable network and the WaitForNWPushQoSTimer expires while waiting for the network to initiate QoS setup procedures. See QoS mobility use case 2.
- The UE learns that the target network is UE-initiated only, e.g., from the selected BCM during the VSNCP procedure (see QoS mobility use case 5) after transitioning to the target network.

Description

The scenario is shown in Figure 9-6.

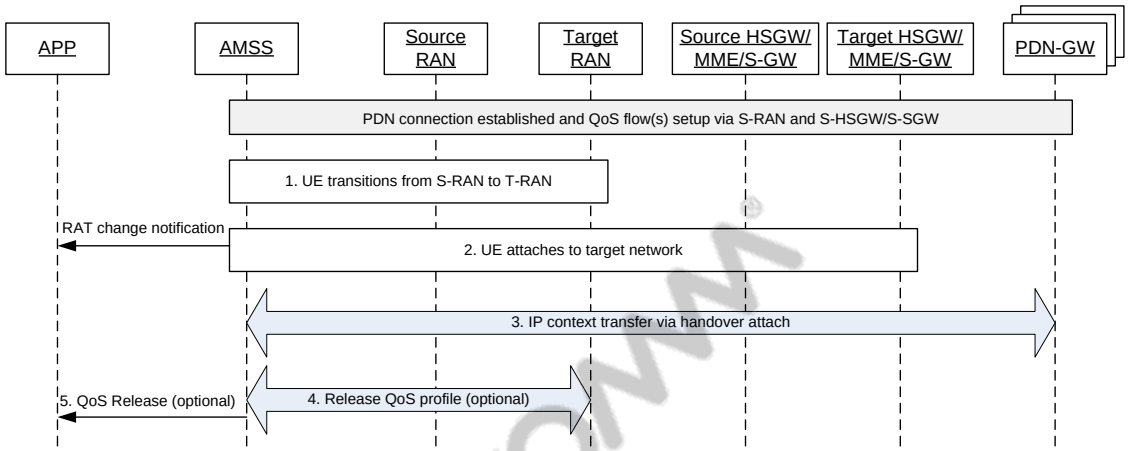

Figure 9-6 QoS mobility use case 4

The following numbered paragraphs correspond to Figure 9-6:

1. The UE transitions from S-RAN to T-RAN. This handoff could be active or dormant.
2. The UE attaches to the target network and notifies the applications of the radio technology change. If the target network is eHRPD, the UE shall create the PPP session and perform EAP-AKA authentication if no partial context is available at the UE before handoff. If the target network is E-UTRA, the UE shall the perform E-UTRA Attach procedure.
3. The UE performs an IP context transfer via the handover attach procedure for each PDN connection to which it has attachments within the source RAN. The UE shall start the WaitForNWPushQoSTimer, defined in Table 9-2, upon learning that the current network is MS/network-initiated QoS-capable. See QoS mobility UC 2 for details.
4. If the WaitForNWPushQoSTimer expires while the UE waits for the network to initiate QoS or if the UE learns that the target network is MS-initiated only QoS-capable, since the application does not have the handle to access the QoS flow, the UE shall locally delete the packet filters and may explicitly release radio QoS. See [Q5] for details about QoS release procedures.
5. The AMSS shall notify the application of QoS Release if the API exists.

Postconditions

The QoS profile is released.

10 Tethered Mode Support

This chapter details the AMSS support provided for the Tethered mode of operation. It addresses the behavior for data cards and handsets, allowing simultaneous operation over Embedded and Tethered modes.

10.1 Assumptions

eHRPD-enabled devices will not support DUN for technologies that can support mobility with IP address continuity over the EPC domain. This includes LTE, UMTS, GSM, and eHRPD.

10.2 DUN

DUN is supported only for association with the 3GPP2 packet core network. DUN is not supported for the EPC association.

For 3GPP2 DUN for both relay and network models, only one IPv4 connection is supported.

10.2.1 3GPP2 DUN

Figure 10-1 shows the 3GPP2 DUN relay model.

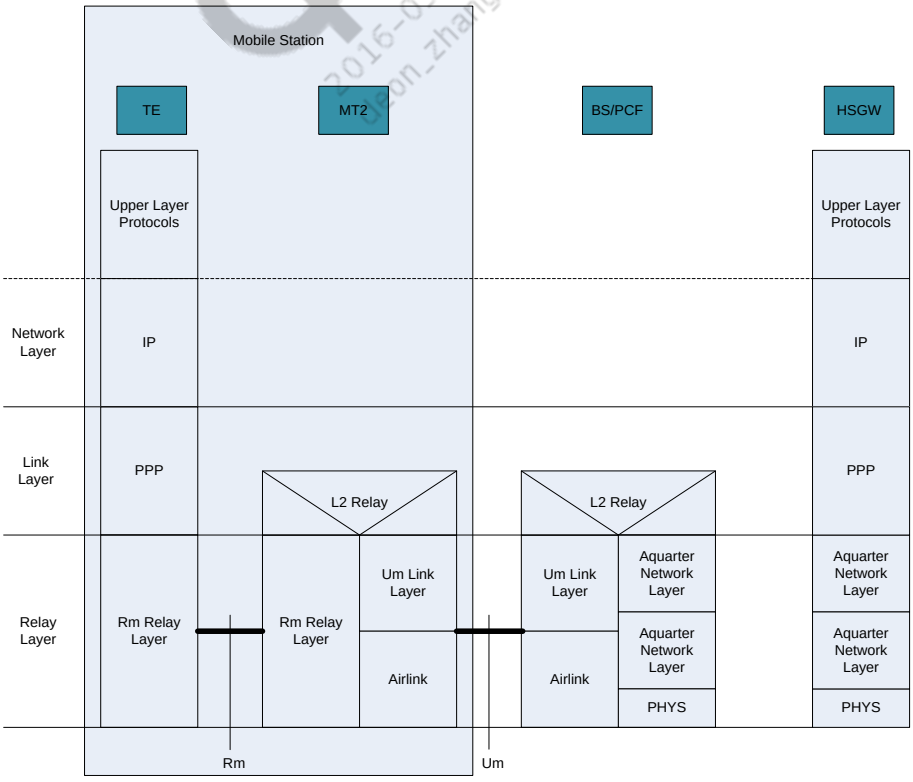

Figure 10-1 3GPP2 DUN relay model

Figure 10-2 shows 3GPP2 DUN network model – Simple IP.

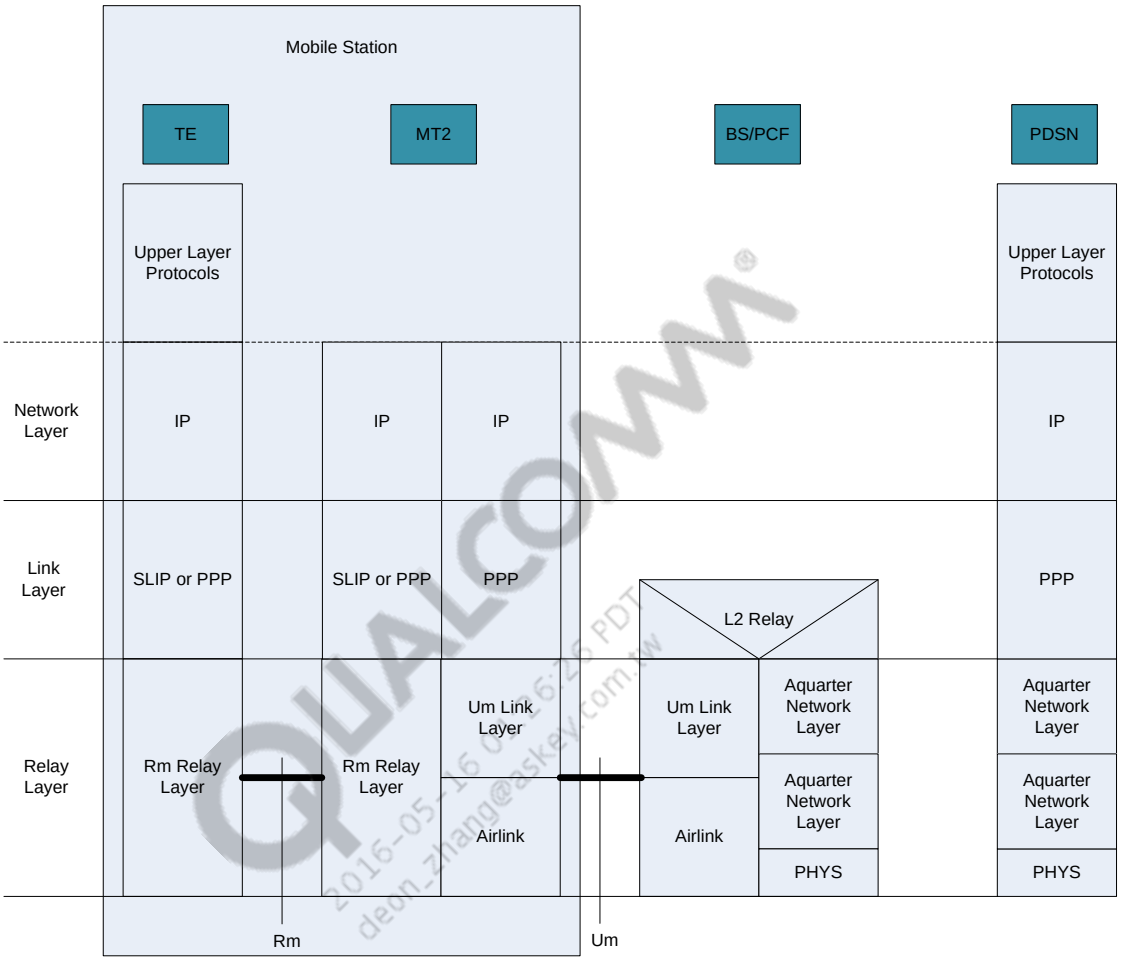

Figure 10-2 3GPP2 DUN network model – Simple IP

Figure 10-3 shows the 3GPP2 DUN network model – Mobile IP.

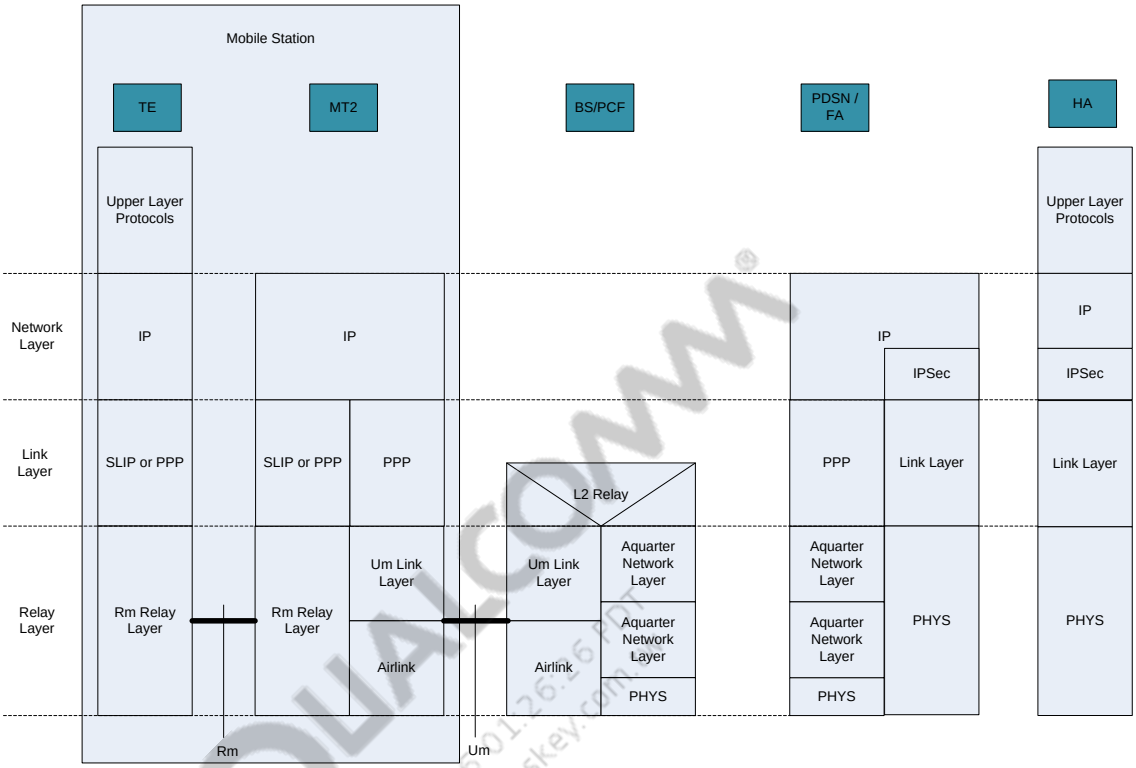

Figure 10-3 3GPP2 DUN network model – Mobile IP

Table 10-1 shows the network model vs relay model – Comparison chart.

Table 10-1 Network model vs relay model – Comparison chart

DUN relay model	DUN network model
▪ Faster for early chipsets with CPU limitations ▪ Diminishing returns with new family of chipsets that carry higher CPU processing speeds	▪ Enables transparent mobility for TE devices ▪ Supports Mobile IP (MIP) ▪ Framework for supporting advance IS-707 features ▪ Supports internal authentication for data session to address privacy and security needs for the operator's network ▪ Additional benefits with QMI ▫ EV-DO Rev-A QoS ▫ IPv6 ▫ MIPv6

10.3 RmNet

Figure 10-4 shows an RmNet model.

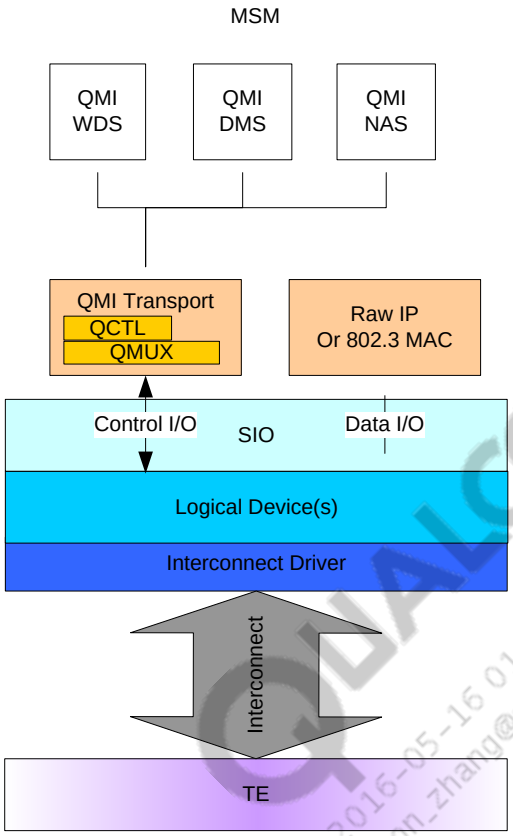

Figure 10-4 RmNet model

RmNet emulates a network interface for the connected TE that allows the MSM™ ASIC to behave like a network adapter when it is connected to the TE and provides packet data connectivity.

See [Q6] for details about RmNet. The following sections provide a brief overview, with a comparison with DUN procedures.

10.3.1 Control path

RmNet relies on a control interface for control signaling between the Tethered Equipment (TE) and the MSM. QMI (Qualcomm MSM Interface) is the recommended signaling interface for the QCT modem. It uses a control I/O channel for QMI messaging that is binary and asynchronous and always available. QMI components include QMI transport, i.e., Qmux and QCTL, QMI services, and clients.

10.3.1.1 QMI transport components

Qmux and QCTL are available on QC modems by default and must be supported via a QMI driver on the TE. A reference driver is provided.

Qmux resides on the server, MSM, and client, TE. It is the QMI message multiplexing and routing layer. On transmit, QMI messages are multiplexed via this layer. On receive, QMI messages are demultiplexed and routed to the appropriate service/client. There is one Qmux instance per QMI control channel.

QCTL is implemented as an administrative service. It performs client ID management, version control, and other administrative tasks on behalf of QMI clients/users.

QMI supports multiple services and each service can support multiple clients. QMI service resides on the modem and QMI clients reside on the TE. A QMI client can be part of the QMI driver or end-user application, such as a Connection Manager.

Examples of QMI services are:

- QMI Device Management Service (QMI_DMS) provides general device management, device identification, device, power source, charge level, etc.
- QMI Wireless Data Service (QMI_WDS) provides wireless packet data session management over all supported technologies and network interface management (start/stop), bearer management, packet statistics, etc.
- QMI Network Access Service (QMI_NAS) provides wireless network management for all supported technologies and serving systems, signal strength, network scan, register/deregister, attach/detach, etc. Different QMI services are described in [Q5].

QMI services support additional functionality that is not available through AT commands. See Table 10-2 for a comparison. AT commands can still be supported over the modem or other serial devices.

Table 10-2 Control plane comparison chart between AT commands and QMI/RmNet

Topics	AT commands	QMI/RmNet
Concurrent signaling and data	Requires separate port to support concurrent AT commands and packet data	Concurrency is supported without an additional port
Asynchronous message handling	Not supported	Supported
Concurrent signaling by multiple applications	Requires one AT port per application	QMI can facilitate multiple applications
Control channel message format	AT commands are 7-bit ASCII characters	▪ QMI uses a binary messaging format ▪ Better support of future features
CAD processing	Multiple command(s) processing on the same and different ports is serialized	▪ Completely parallel operations ▪ All command(s) processing is executed in parallel and independently
TE OS interface	▪ Requires an application on the TE to initiate the data session ▪ Microsoft Windows 7 mobile broadband access strongly discourages use of AT commands for the WWAN interface	▪ Always-On setting also supported, which allows auto data session bring-up ▪ Microsoft Windows 7 mobile broadband-compatible

10.3.2 Data path

The data path with RmNet is optimized by eliminating HDLC over Rm. HDLC incurs significant overhead on both the TE and MSM. RmNet supports 802.3 or RAW IP frames over Rm. It uses a packet-based interface, requiring packet boundary demarcation from the interconnect driver. Explicit QoS requests are supported over the RmNet interface and QoS-based packet prioritization over the RmNet interface is also supported, apart from obtaining the required resources of the radio interfaces.

Table 10-3 shows a data plane comparison between AT commands and RmNet.

Table 10-3 Data plane comparison between AT commands and RmNet

Topics	AT commands	RmNet
Performance	Incurs HDLC framing overhead for PPP	Optimized data path with 802.3 or Raw IP
TE OS interface	▪ Dial-up networking (modem) interface ▪ Not conducive for Microsoft Windows 7 mobile broadband access	▪ Network interface (NIC), such as NDIS for Windows and VED for Linux ▪ Fully capable of supporting Microsoft Windows 7 mobile broadband access
QoS	No support	Supported, both explicit QoS and packet-based prioritization

Figure 10-5 is a representation of both the Tethered and Embedded modes of operation simultaneously supported by the AMSS. The only restriction is that a given APN/PDN connection cannot be shared across the Tethered and Embedded modes of operation. This applies when only IPv4, IPv6, or both IPv4+IPv6 are assigned to the APN/PDN connection.

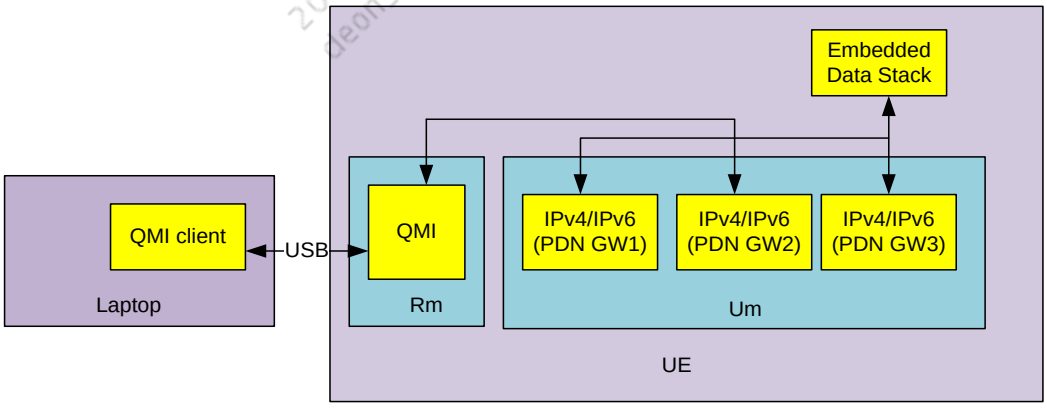

Figure 10-5 Tethered mode support over multimode devices

10.4 Recommendations

If DUN is used, the recommendation is a network model-based approach. Some key highlights of this approach are:

- Ensures operator's network security
- Meets true IP mobility requirements
- Supports seamless end-user experience

If DUN is not mandated, Qualcomm recommends the use of RmNet to accelerate the growth of new devices, with the enhanced capabilities and future proofing of the operator and OEM's product roadmaps.

11 Application Profiles

NOTE: Numerous changes were made in this chapter.

11.1 Application profile supported for eHRPD

Table 11-1 shows an application profile supported for eHRPD.

Table 11-1 Application profile supported for eHRPD

Parameter name	Parameter value
Profile_Id	▪ 0 – Default Profile ▪ 1-100 – JCDMA Profiles (currently 1 to 22 are valid profiles) ▪ 101-200 – eHRPD Profiles (currently 101 to 107 are valid profiles)
Profile_Label	This parameter can be used to categorize and refer to APNs. The actual APN Name, i.e., APN_String, can be provisioned differently for the same Profile_Label. Profile_Label can be used by the application as the index when requesting PDN connection; the UE will request to connect to the APN Name that is provisioned.
APN_String	String of maximum length 100
APN Class	Integer
APN IP Type (PDN_IP_Version_Type)	▪ V4 ▪ V6 ▪ V4V6
APN Enable/Disable	▪ 1 – APN Enable ▪ 0 – APN Disable
APN Inactivity Timer	Number of minutes
PCSCF_Addr_Needed	▪ 1 – PCSCF Address needed ▪ 0 – PCSCF Address not needed
Primary_DNS_Addr_V4	Presentation Format (dot separated) V4 address, e.g., 10.46.85.100
Secondary_DNS_Addr_V4	Presentation Format (dot separated) V4 address, e.g., 10.46.85.100
Primary_DNS_Addr_V6	Presentation Format (:: separated) V6 address, e.g., 21::17
Secondary_DNS_Addr_V6	Presentation Format (:: separated) V6 address, e.g., 21::17
RAN_Type	▪ HRPD ▪ EHRPD ▪ HRPD_EHRPD

11.2 Application profile supported for E-UTRA

Table 11-2 shows an application profile supported for eHRPD.

Table 11-2 Application profile supported for E-UTRA

Parameter name	Parameter value
Profile_Name	String of maximum length 15. This parameter can be used to categorize and refer to APNs. The actual APN Name, i.e. APN_String, can be provisioned differently for the same Profile_Name. Profile_Name can be used by the application as the index when requesting a PDN connection; the UE will request to connect to the APN Name that is provisioned.
Profile_Number	1-16 – E-UTRA profiles
APN_String	String of maximum length 100; includes NI and OI fields
APN Class	Integer
APN IP Type (PDN_IP_Version_Type)	▪ V4 ▪ V6 ▪ V4V6
APN Enable/Disable	▪ 1 – APN Enable ▪ 0 – APN Disable
APN Inactivity Timer	Number of minutes
PCSCF_Addr_Needed	▪ 1 – PCSCF Address needed ▪ 0 – PCSCF Address not needed
Primary_DNS_Addr_V4	Presentation Format (dot separated) V4 address, e.g., 10.46.85.100
Secondary_DNS_Addr_V4	Presentation Format (dot separated) V4 address, e.g., 10.46.85.100
Primary_DNS_Addr_V6	Presentation Format (:: separated) V6 address, e.g., 21::17
Secondary_DNS_Addr_V6	Presentation Format (:: separated) V6 address, e.g., 21::17
RAN_Type	▪ E-UTRA ▪ WCDMA ▪ GPRS ▪ E-UTRA_WCDMA_GPRS

12 IP Address Allocation Failure Handling

12.1 Overview

- The classification for the different throttling and blocking types are listed with the different timers that are associated in a Throttling state.
- UE behavior is dictated by the combination of the current throttling state and timer value.
- Throttling is performed to avoid repeated requests and is applied to the PDN connection, DHCP, and RS/RA procedures when a failure is encountered.
- Throttling is performed for an IP address and APN combination and is independently performed for IPv4 and IPv6 address requests.
- Blocking is performed when only one IP address is granted by the network for that APN and the allocated address is currently in use with an active PDN connection.

Table 12-1 shows throttling and blocking.

Table 12-1 Throttling and blocking

Throttling and blocking scenarios	Description
$TH_{IPv4}( )$	Throttle IPv4 requests on a given APN. This includes throttling of the PDN connection setup if it is not already up or throttling of DHCP requests.
$TH_{IPV6}( )$	Throttle IPv6 requests on a given APN. This includes throttling of the PDN connection setup if it is not already up or throttling of RS requests.
$TH_{IPv4}( )$, $TH_{IPv6}( )$	This applies when both IPv4 and IPv6 requests on a given APN are throttled and essentially results in the PDN connection being throttled for that APN.
BC_{IPv4}	When IPv6 is the only address currently allowed by the network on the APN and the PDN connection is held open by an IPv6 active application
BC_{IPv6}	When IPv4 is the only address currently allowed by the network on the APN and the PDN connection is held open by an IPv4 active application

Table 12-2 shows the throttling timers.

Table 12-2 Throttling timers

Throttling timers	Description
$TT_{Failure}$	This timer is applied to the throttling scenario when the failure is encountered to establish the IP context, e.g., DHCP or RS/RA failures. This will typically employ a back-off mechanism based on the number of attempts. The timer values may depend on IPv4 failures, IPv6 failures, or IPv4 and IPv6 failing.
$TT_{Disallowed}$	This timer is applied to the throttling scenario when the network grants only one of IPv4 or IPv6 when the application has requested another type. The PDN connection is immediately released, since no applications are associated with the currently assigned IP address. This is typically a longer timer than the TTFailure timer values. Given that IPv4 failure can be due to address exhaustion, the timer for IPv4 not granted will be different when IPv6 is not granted.

12.2 IP address allocation failures over eHRPD

Table 12-3 shows a dual-address default bearer on eHRPD.

Table 12-3 Dual-address default bearer on eHRPD

Active apps failed IP	IPv4	IPv6	IPv4 and IPv6
None	Stay connected on APN with both v4 and v6	▪ Stay connected on APN with both v4 and v6, if v4 assigned through VSNCP ▪ Stay connected on APN with only v6, if v4 assigned through DHCP	Stay connected on APN with both v4 and v6 addresses
IPv4	▪ Disconnect from APN ▪ Tear down PPP if there are no other active PDNs ▪ TH_{IPv4} ($TT_{failure}$)	Does not apply; since there is no IPv4 app, DHCP will not be attempted and, hence, IPv4 failure cannot occur	▪ Stay connected on APN with only v6; v4 apps notified of failure ▪ TH_{IPv4} ($TT_{failure}$) ▪ Reason for DHCP throttling: Radio connections are costly
IPv6	▪ Stay connected on APN with only v4 ▪ TH_{IPv6} ($TT_{failure}$) ▪ Reason for RS/RA throttling: Radio connections are costly	▪ Disconnect from APN. ▪ Tear down PPP if there are no other active PDNs. ▪ TH_{IPv6} ($TT_{failure}$)	▪ Stay connected on APN with only v4; v6 apps notified of failure ▪ TH_{IPv6} ($TT_{failure}$)

Active apps failed IP	IPv4	IPv6	IPv4 and IPv6
IPv4 and IPv6	▪ Disconnect from APN ▪ Tear down PPP if there are no other active PDNs ▪ $TH_{IPv4}(TT_{failure})$ && $TH_{IPv6}(TT_{failure})$	Does not apply; since there is no IPv4 app, DHCP will not be attempted and, hence, IPv4 failure cannot occur	▪ Disconnect from APN ▪ Tear down PPP if there are no other active PDNs ▪ $TH_{IPv4}(TT_{failure})$ && $TH_{IPv6}(TT_{failure})$

Table 12-4 shows SADB, IPv4 address.

Table 12-4 SADB, IPv4 address

Active apps failed IP	IPv4	IPv6	IPv4 and IPv6
None	▪ Stay connected on APN with v4 ▪ BC_{IPv6}	▪ Disconnect from APN ▪ Tear down PPP if there are no other active PDNs ▪ TH_{IPv6} ($TT_{disallowed}$)	▪ Stay connected on APN with v4 ▪ BC_{IPv6}
IPv4	▪ Disconnect from APN ▪ Tear down PPP if there are no other active PDN connections ▪ TH_{IPv4} ($TT_{failure}$) && TH_{IPv6} ($TT_{disallowed}$)	Does not apply; DHCP will not be performed, since there is no v4 app	▪ Disconnect from APN ▪ Tear down PPP if there are no other active PDN connections ▪ TH_{IPv4} ($TT_{failure}$) && TH_{IPv6} ($TT_{disallowed}$)

Table 12-5 shows SADB, IPv6 address.

Table 12-5 SADB (IPv6 address)

Active apps failed IP	IPv4	IPv6	IPv4 and IPv6
None	▪ Disconnect from APN ▪ Tear down PPP if there are no other active PDNs ▪ TH_{IPv4} ($TT_{disallowed}$)	▪ Stay connected on APN with v6 ▪ BC_{IPv4}	▪ Stay connected on APN with v6 ▪ BC_{IPv4}
IPv6	▪ Disconnect from APN ▪ Tear down PPP if there are no other active PDNs ▪ TH_{IPv4} ($TT_{disallowed}$) && TH_{IPv6} ($TT_{failure}$)		

12.3 IP address allocation failures over EUTRAN

Table 12-6 displays default APN – DADB.

Table 12-6 Default APN – DADB

Active apps failed IP	None	IPv4	IPv6	IPv4 and IPv6
None	▪ Stay connected on v4 v6 if v4 allocated through NAS ▪ If v4 allocated through DHCP, stay connected on v6	Stay Connected on v4 v6	▪ Stay connected on v4 v6 if v4 allocated through NAS ▪ If v4 allocated through DHCP, stay connected on v6	Stay connected on v4 v6
IPv4	▪ Stay connected on ▪ V6 ▪ DHCP not attempted	▪ Stay connected on V6 ▪ TH_{IPv4} ($TT_{Failure}$)	▪ Stay connected on ▪ V6 ▪ DHCP not attempted	▪ Stay connected on V6 ▪ TH_{IPv4} ($TT_{Failure}$)
IPv6	▪ Stay connected on v4 if v4 allocated through NAS ▪ Else, stay attached without IP ▪ DHCP not attempted ▪ TH_{IPv6} ($TT_{Failure}$)	▪ Stay connected on V4 ▪ TH_{IPv6} ($TT_{Failure}$)	▪ Stay connected on v4 if v4 allocated through NAS ▪ Else, stay attached without IP ▪ DHCP not attempted ▪ TH_{IPv6} ($TT_{Failure}$)	▪ Stay connected on V4 ▪ TH_{IPv6} ($TT_{Failure}$)
IPv4 and IPv6	▪ Stay attached without IP and ▪ Min[TH_{IPv4} ($TT_{Failure}$), TH_{IPv6} ($TT_{Failure}$)]	Stay attached without IP and Min[TH_{IPv4} ($TT_{Failure}$), TH_{IPv6} ($TT_{Failure}$)]	Stay attached without IP and Min[TH_{IPv4} ($TT_{Failure}$), TH_{IPv6} ($TT_{Failure}$)]	Stay attached without IP and Min[TH_{IPv4} ($TT_{Failure}$), TH_{IPv6} ($TT_{Failure}$)]

Table 12-7 shows nondefault APN – DADB.

Table 12-7 Nondefault APN – DADB

Active apps failed IP	IPv4	IPv6	IPv4 and IPv6
None	Stay connected on v4 v6	▪ Stay connected on v4 v6 if v4 allocated through NAS ▪ If v4 allocated through DHCP, stay connected on v6	Stay connected on v4 v6
IPv4	▪ Disconnect ▪ TH_{IPv4} ($TT_{Failure}$)	▪ Does not apply ▪ DHCP not attempted ▪ Stay connected on V6	▪ Stay connected on V6 ▪ TH_{IPv4} ($TT_{Failure}$)
IPv6	▪ Stay connected on ▪ V4 ▪ TH_{IPv6} ($TT_{Failure}$)	▪ Disconnect ▪ TH_{IPv6} ($TT_{Failure}$)	▪ Stay connected on V4 ▪ TH_{IPv6} ($TT_{Failure}$)
IPv4 and IPv6	Disconnect and Min[TH_{IPv4} ($TT_{Failure}$), TH_{IPv6} ($TT_{Failure}$)]	Disconnect and Min[TH_{IPv4} ($TT_{Failure}$), TH_{IPv6} ($TT_{Failure}$)]	Disconnect and Min[TH_{IPv4} ($TT_{Failure}$), TH_{IPv6} ($TT_{Failure}$)]

Table 12-8 shows default APN – SADB-1B, only IPv6 address assigned.

Table 12-8 Default APN – SADB-1B (only IPv6 address assigned)

Active apps failed IP	None, IPv4 Only, IPv6 Only, or both
None	▪ Stay connected on v6 bearer ▪ BC_{IPv4}
IPv6	▪ Only v6 bearer was created and RS/RA failed ▪ Stay attached without IP and Min[TH_{IPv4} ($TT_{Disallowed}$) TH_{IPv6} ($TT_{Failure}$)]

Table 12-9 shows default APN – SADB-1B, only IPv4 address assigned.

Table 12-9 Default APN – SADB-1B (only IPv4 address assigned)

Active apps failed IP	None, IPv4 Only, IPv6 Only, or both
None	▪ Stay connected on v4 bearer ▪ BC_{IPv6}
IPv4	▪ Only v4 bearer was created and DHCP failed ▪ Stay Attached without IP and Min[TH_{IPv4} ($TT_{Failure}$), TH_{IPv6} ($TT_{Disallowed}$)]

Table 12-10 shows default APN – SADB-2B, (two IP addresses, v6 first.

Table 12-10 Default APN – SADB-2B, two IP address, v6 first

Active apps failed IP	None	IPv4	IPv6	IPv4 and IPv6
None	▪ Stay connected on v6 bearer ▪ V4 not attempted	▪ Stay connected on v6 bearer ▪ Stay connected on v4 bearer	▪ Stay connected on v6 bearer ▪ V4 not attempted	▪ Stay connected on v6 bearer ▪ Stay connected on v4 bearer
IPv4	▪ Does not apply ▪ DHCP not attempted ▪ Stay connected on V6	▪ Stay connected on v6 bearer ▪ TH_{IPv4} ($TT_{Failure}$)	▪ Does not apply ▪ DHCP not attempted ▪ Stay connected on V6	▪ Stay connected on v6 bearer ▪ TH_{IPv4} ($TT_{Failure}$)
IPv6	▪ TH_{IPv6} ($TT_{Failure}$) ▪ Stay connected on v4 bearer	▪ TH_{IPv6} ($TT_{Failure}$) ▪ Stay connected on v4 bearer	▪ TH_{IPv6} ($TT_{Failure}$) ▪ Stay connected on v4 bearer	▪ TH_{IPv6} ($TT_{Failure}$) ▪ Stay connected on v4 bearer
IPv4 and IPv6	Stay attached without IP and Min[TH_{IPv4} ($TT_{Failure}$), TH_{IPv6} ($TT_{Failure}$)]	Stay attached without IP and Min[TH_{IPv4} ($TT_{Failure}$), TH_{IPv6} ($TT_{Failure}$)]	Stay attached without IP and Min[TH_{IPv4} ($TT_{Failure}$), TH_{IPv6} ($TT_{Failure}$)]	Stay attached without IP and Min[TH_{IPv4} ($TT_{Failure}$), TH_{IPv6} ($TT_{Failure}$)]

Table 12-11 shows default APN – SADB-2B, two IP address, v4 first.

Table 12-11 Default APN – SADB-2B (two IP address, v4 first)

Active apps failed IP	None	IPv4	IPv6	IPv4 and IPv6
None	▪ Stay connected on v4 bearer ▪ V6 not attempted	▪ Stay connected on v4 bearer ▪ V6 not attempted	▪ Stay connected on v6 bearer ▪ Stay connected on v4 bearer	▪ Stay Connected on v6 bearer ▪ Stay connected on v4 bearer
IPv4	▪ TH_{IPv4} ($TT_{Failure}$) ▪ Stay connected on v6 bearer	▪ TH_{IPv4} ($TT_{Failure}$) ▪ Stay connected on v6 bearer	▪ TH_{IPv4} ($TT_{Failure}$) ▪ Stay connected on v6 bearer	▪ TH_{IPv4} ($TT_{Failure}$) ▪ Stay connected on v6 bearer
IPv6	▪ Stay connected on v4 bearer ▪ TH_{IPv6} ($TT_{Failure}$)	▪ Stay connected on v4 bearer ▪ TH_{IPv6} ($TT_{Failure}$)	▪ Stay connected on v4 bearer ▪ TH_{IPv6} ($TT_{Failure}$)	▪ Stay connected on v4 bearer ▪ TH_{IPv6} ($TT_{Failure}$)
IPv4 and IPv6	▪ Stay attached without IP and Min[TH_{IPv4} ($TT_{Failure}$), TH_{IPv6} ($TT_{Failure}$)]	Stay attached without IP and Min[TH_{IPv4} ($TT_{Failure}$), TH_{IPv6} ($TT_{Failure}$)]	Stay attached without IP and Min[TH_{IPv4} ($TT_{Failure}$), TH_{IPv6} ($TT_{Failure}$)]	Stay attached without IP and Min[TH_{IPv4} ($TT_{Failure}$), TH_{IPv6} ($TT_{Failure}$)]

Table 12-12 shows nondefault APN – SADB-1B, only IPv6 address assigned.

Table 12-12 Nondefault APN – SADB-1B, only IPv6 address assigned

Active apps failed IP	IPv4	IPv6	IPv4 and IPv6
None	▪ RS/RA not attempted ▪ Disconnect ▪ TH_{IPv4} ($TT_{Disallowed}$)	▪ Stay connected on v6 bearer ▪ BC_{IPv4}	▪ Stay connected on v6 bearer ▪ BC_{IPv4}
IPv6	▪ Disconnect ▪ Min[TH_{IPv4} ($TT_{Disallowed}$) TH_{IPv6} ($TT_{Failure}$)]	▪ Only v6 bearer was created and RS/RA failed ▪ Disconnect ▪ Min[TH_{IPv4} ($TT_{Disallowed}$) TH_{IPv6} ($TT_{Failure}$)]	▪ Only v6 bearer was created and RS/RA failed ▪ Disconnect ▪ Min[TH_{IPv4} ($TT_{Disallowed}$) TH_{IPv6} ($TT_{Failure}$)]

Table 12-13 shows nondefault APN – SADB-1B, only IPv4 address assigned.

Table 12-13 Nondefault APN – SADB-1B, only IPv4 address assigned

Active apps failed IP	IPv4	IPv6	IPv4 and IPv6
None	▪ Stay connected on v4 bearer ▪ BC_{IPv6}	▪ Disconnect ▪ TH_{IPv6} ($TT_{Disallowed}$)	▪ Stay connected on v4 bearer ▪ BC_{IPv6}
IPv4	▪ Only v4 bearer was created and DHCP failed ▪ Disconnect and Min[TH_{IPv4} ($TT_{Failure}$), TH_{IPv6} ($TT_{Disallowed}$)]	▪ DHCP not attempted ▪ Disconnect ▪ TH_{IPv6} ($TT_{Disallowed}$)	▪ Only v4 bearer was created and DHCP failed ▪ Disconnect and Min[TH_{IPv4} ($TT_{Failure}$), TH_{IPv6} ($TT_{Disallowed}$)]

Table 12-14 shows nondefault APN – SADB-2B, two IP address, v6 first.

Table 12-14 Nondefault APN – SADB-2B, two IP address, v6 first

Active apps failed IP	IPv4	IPv6	IPv4 and IPv6
None	▪ Stay connected on v4 bearer ▪ Delete v6 bearer	▪ Stay connected on v6 bearer ▪ V4 not attempted	▪ Stay connected on v6 bearer ▪ Stay connected on v4 bearer
IPv4	▪ Disconnect ▪ TH_{IPv4} ($TT_{Failure}$)	▪ Does not apply ▪ DHCP not attempted ▪ Stay connected on V6	▪ Stay connected on v6 bearer ▪ TH_{IPv4} ($TT_{Failure}$)
IPv6	▪ TH_{IPv6} ($TT_{Failure}$) ▪ Stay Connected on v4 bearer	▪ Disconnect ▪ TH_{IPv6} ($TT_{Failure}$)	▪ TH_{IPv6} ($TT_{Failure}$) ▪ Stay connected on v4 bearer
IPv4 and IPv6	Disconnect and Min[TH_{IPv4} ($TT_{Failure}$), TH_{IPv6} ($TT_{Failure}$)]	Disconnect and Min[TH_{IPv4} ($TT_{Failure}$), TH_{IPv6} ($TT_{Failure}$)]	Disconnect and Min[TH_{IPv4} ($TT_{Failure}$), TH_{IPv6} ($TT_{Failure}$)]

Table 12-15 shows nondefault APN – SADB-2B, two IP address, v4 first.

Table 12-15 Nondefault APN – SADB-2B, two IP address, v4 first

Active apps failed IP	IPv4	IPv6	IPv4 and IPv6
None	▪ Stay connected on v4 bearer ▪ V6 not attempted	▪ Stay connected on v6 bearer ▪ Delete v4 bearer	▪ Stay connected on v6 bearer ▪ Stay connected on v4 bearer
IPv4	▪ Disconnect ▪ TH_{IPv4} ($TT_{Failure}$)	▪ TH_{IPv4} ($TT_{Failure}$) ▪ Stay connected on v6 bearer	▪ TH_{IPv4} ($TT_{Failure}$) ▪ Stay connected on v6 bearer
IPv6	▪ Stay connected on v6 bearer ▪ V6 not attempted	▪ Disconnect ▪ TH_{IPv6} ($TT_{Failure}$)	▪ Stay connected on v4 bearer ▪ TH_{IPv6} ($TT_{Failure}$)
IPv4 and IPv6	Disconnect and Min[TH_{IPv4} ($TT_{Failure}$), TH_{IPv6} ($TT_{Failure}$)]	Disconnect and Min[TH_{IPv4} ($TT_{Failure}$), TH_{IPv6} ($TT_{Failure}$)]	Disconnect and Min[TH_{IPv4} ($TT_{Failure}$), TH_{IPv6} ($TT_{Failure}$)]

13 Simultaneous PDN Access

NOTE: This chapter was added to this document revision.

This chapter describes the UE's behavior of simultaneously accessing a single APN from multiple applications/services running on different processors. The applications that connect to the PDN may be embedded and/or tethered.

13.1 Requirements

The UE shall support simultaneous access to a single APN from multiple applications running on different processors. The applications that connect to the APN share the same IP address assigned by the PDN-GW, which can be IPv4 or IPv6.

13.2 Problem statement

The software architecture of PDN access from applications running on multiple processors is shown in Figure 13-1. Applications that connect to the same PDN and share the same IP address (IPv4 or IPv6) are connecting to the same UM iFace, which receives services from the radio technology-specific data protocol stack, e.g., PPP and HDR protocols for CDMA2000 and LTE protocols for E-UTRA. The PC processor connects to the UM iFace through the apps processor, if it is present.

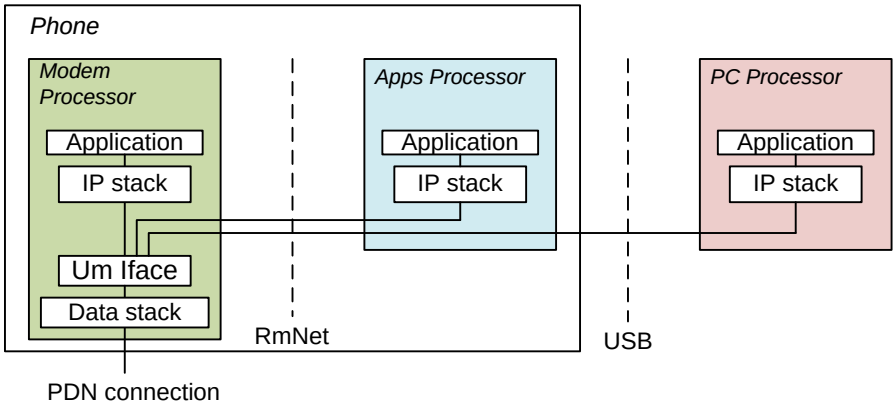

Figure 13-1 PDN access from applications running on different processors

Some simultaneous PDN access scenarios are:

- A BIP running on a UICC/modem processor and an OTADM client running on an apps processor simultaneously access the admin PDN.
- The FTP client running on a PC and a web browser running on an apps processor simultaneously access the internet PDN.
- An IMS client running on a modem processor and a location positioning service running on an apps processor simultaneously access the IMS PDN.

13.3 Hybrid port partitioning and PC-only NAT

13.3.1 Overview of hybrid solution

The proposed hybrid solution consists of port partitioning between the modem processor and the apps processor and a Network Address Translator (NAT [RFC 1631]) that provides private IP addresses to the applications running on a PC.

Based on the processors involved in the simultaneous PDN access scenario, the hybrid solution can be simplified as pure static port space partitioning or pure PC-only NAT. This is described in more detail in later chapters. The approaches are summarized in Table 13-1.

Table 13-1 Approaches for different scenarios

Applications running on PC	Applications running on AP	Applications running on MP	Approach	Example scenario
No	Yes	Yes	Static port space partitioning	BIP and OTADM access admin PDN
Yes	Yes	No	If NAT runs on AP – PC-only NAT	Access internet PDN from PC and apps processor (Android tethering)
Yes (multiple PCs)	No AP	No	PC-only NAT (NAT runs on MP)	SoftAP (applications on multiple PCs access internet PDN)
Yes	Yes	Yes	Hybrid port partitioning and PC-only NAT	Access a certain PDN from PC and apps and modem processors (Android tethering)

13.3.2 Hybrid port partitioning and PC-only NAT

In the architecture diagram shown in Figure 13-2, the NAT protocol is provided by the OS on the apps processor. For example, the diagram shown in Figure 13-2 assumes that an Android OS is running on the apps processor and the interface between the apps processor and the PC is based on RNDIS.

- Port partitioning – The available port space is partitioned into nonoverlapping ranges and assigned to the modem and apps processors. When the application requests a PDN connection, the processor on which the application is running shall assign a port from the specific range.
- The port space partitioning solution does not work in scenarios when the PDN connection is shared by the applications running on a PC. In these scenarios, NAT-based approaches can be used. The NAT module shall assign private IP addresses to the applications running on a PC. In addition, if the phone provides WiFi access to the clients through 802.11, the NAT module also assigns private IP addresses to the applications running on the WiFi clients. Additional modules required to work with the NAT module are discussed in Section 13.3.5.
- The public IP address is used by the application running on the modem and apps processors and the external interface of the NAT module. The apps processor shall assign the port number to the NAT external interface from its port range and shall ensure there is no conflict with applications running on the modem processor and the apps processor.

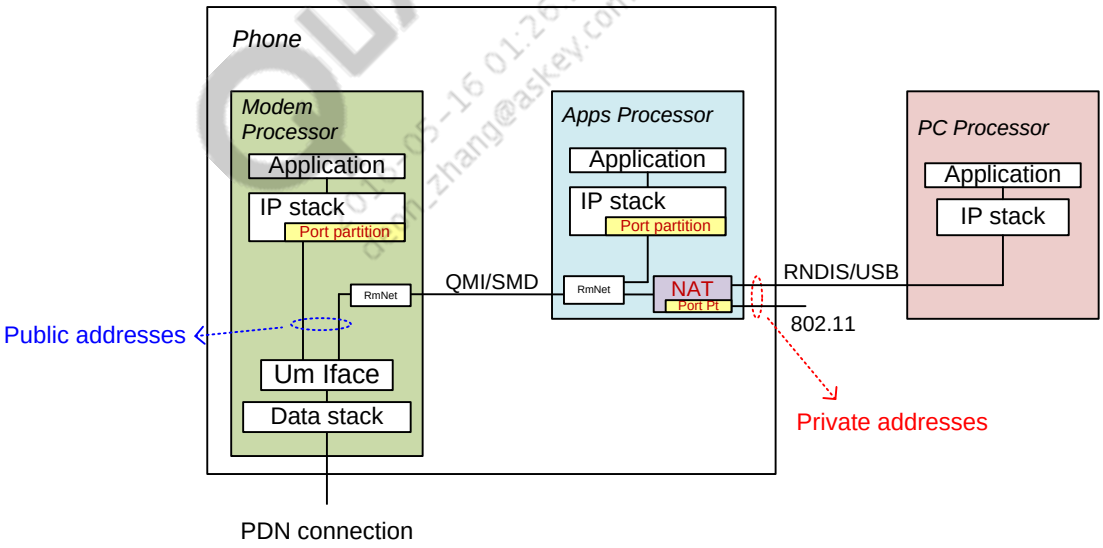

Figure 13-2 Hybrid solution, NAT running on apps processor

13.3.3 PC-only NAT

If the apps processor is not present, e.g., for data cards, the NAT module must run on the modem processor, as shown in Figure 13-3. This architecture also applies when the NAT module runs on the modem processor and no applications running on the apps processor share the PDN connection. Port partitioning is not needed.

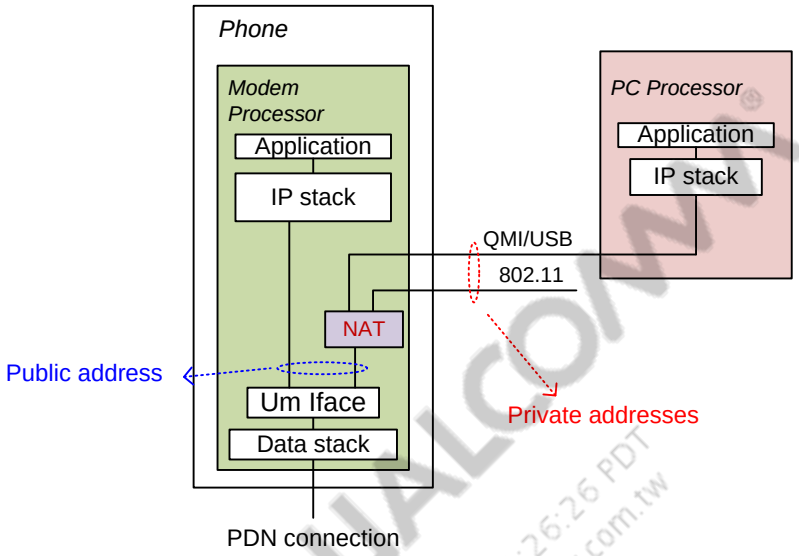

Figure 13-3 PC-only NAT – NAT running on modem processor

13.3.4 Static port-space partitioning

13.3.4.1 Assumptions/constraints

The operating systems running on different processors have the capability of selecting port numbers to the application, as specified. This approach may not be viable for applications running on a PC, as the UE does not have the capability of controlling the PC port selection.

This approach requires that the applications running on different processors do not use the same port. Therefore, it does not work when the applications running on different processors have to use the same well-known port.

13.3.4.2 Static port-partitioning solution

As shown in Figure 13-4, upon request by the application, the modem processor or apps processor selects a port number that has not been used by applications connecting to the same PDN and using the same IP address. This can be achieved by the static port-space partitioning approach, in which available port space is partitioned into nonoverlapping ranges and assigned to different processors. When the application requests a PDN connection, the processor on which the application is running shall assign a port from the specific range.

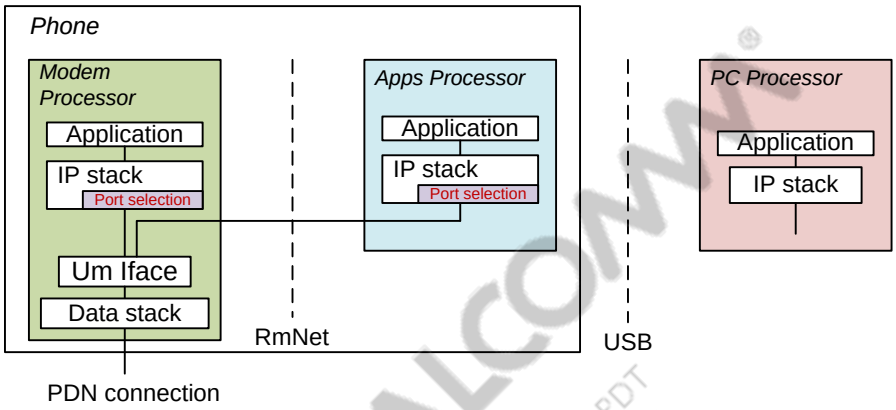

Figure 13-4 Static port-partitioning solution

13.3.5 Overloaded NAT operation

For applications running on the PC and connecting to the same PDN and that request the same IP type, the NAT router maps their private (IP address, port) pairs to the same public IP address, but with different port numbers (overloaded NAT). In particular, the NAT router shall maintain an address translation table and create an entry for each IP connectivity, indexed by the (IP address, port) of the other end point of the IP connectivity. When packets go through the NAT router:

- For uplink packets, the NAT router translates the local source (IP address, port) to the public source (IP address, port).
- For downlink packets, the NAT router translates the public destination (IP address, port) to the local destination (IP address, port).

13.3.5.1 NAT traversal problem

The NAT traversal problem arises when the application layer protocol carries IP address information in the payload data. For example, FTP uses separate connections for control traffic and data traffic. When the FTP client requests a file transfer, it identifies the connection used for data traffic by the (IP address, port) pair and notifies the FTP server.

Another example is SIP, which may use multiple ports to set up a connection and will include IP addresses and port numbers in its payload. The standalone NAT solution only translates the IP address information in the IP packet header. If the IP address and port number encoded in the payload data are not translated to the outside public IP address and port number, applications such as FTP and SIP cannot set up connections appropriately.

The following additional software modules can be used to correct the NAT traversal problem:

- Application Layer Gateway (ALG) – An ALG acts as a protocol-aware firewall, monitoring traffic and updating payload data that require extra address translation. ALGs must understand the higher-layer protocol that they need to fix. Consequently, each protocol with the NAT traversal problem requires a separate ALG. The ALG solution is not scalable as the number of the different types of services that operate over the internet PDN increases.
- Session Traversal Utilities for NAT (STUN) [RFC 5389] – The STUN protocol allows applications to discover the presence of NAT and to obtain public IP address information. The STUN client that is implemented in the application, such as an FTP client or VoIP phone, initiates queries via UDP to the STUN server running on the public side of the NAT. The STUN server responds with the mapped public (IP address, port) that will be used by the application to communicate with its peer.
- Interactive Connectivity Establishment (ICE) [RFC 5245] – ICE is a technique used for fixing the NAT traversal problem in internet applications of VoIP, video, instant messaging, and other interactive media.

Either the ALG, STUN, or ICE solution can be used with NAT.

If the ALG solution is used, the following ALG modules are required:

- FTP
- SIP
- Real Time Streaming Protocol (RTSP)

13.3.5.2 Internet packets handling

Some internet packets, e.g., Internet Control Message Protocol (ICMP) packets, do not have port numbers. There are two approaches to handle internet packets:

- For internet packets that go to the modem and apps processors, the ICMP identifier value included in the ICMP header [RFC 792] of the IP packet is used to route the ICMP packets to the correct processor.
- The internet packets of the PC go through the NAT module. The ICMP identifier value included in the ICMP header of the IP datagram is used to create the entry in the translation table. The ICMP message can normally fit in one IP packet. If the ICMP message is included in multiple fragments of the IP datagram, since only the first fragment of the IP datagram contains the ICMP header, the first fragment creates the translation[11]. The IP identification value in the IP header [RFC 791] of the first fragment is tracked. If several fragments have the same IP identification value as the first fragment, NAT translates these fragments using the same translation entry.

[11]This requires the first fragment to arrive at NAT before other fragments of the same IP datagram.

13.3.5.3 Other NAT issues

In addition to the NAT traversal problem, the following problems must be solved by extra handling:

- NAT does not directly work when IPsec encryption is applied, since encrypted IP addresses cannot be accessed and translated. The solution is IPSec-aware NAT [RFC 3947]. The IPSec-aware NAT detects NAT between IPsec hosts and negotiates the use of UDP encapsulation of IPsec packets through NAT boxes in the Internet Key Exchange (IKE).
- The connection can only be initiated from the device. To facilitate services that require initiation of a connection from the outside network, port forwarding can be used.
- NAT requires keep-alive mechanisms to retain the entry in the NAT translation table.

NOTE: Since the NAT protocol processes each IP packet, it could cause a potential performance impact. Therefore, it is better to minimize the impact of NAT. This is the motivation of the PC-only NAT solution.

13.4 IPv6 multi IID-based solution

This solution applies only to IPv6 connections. The IPv6 address is generated by using a combination of an Interface Identifier (IID) and a prefix according to the IPv6 Stateless Address Autoconfiguration [RFC 4846]. The IID can be obtained via VSNCP/NAS signaling during PDN connection establishment. The prefix allocation is via the RS/RA procedure.

The basic idea of the IPv6 multi-IID-based solution is to use different IIDs for different processors.

- The modem processor shall use the received IID and prefix to generate an IPv6 address.
- The modem processor shall send the prefix to the apps processor and the PC. The apps processor and the PC generate different IIDs. Based on the prefix and IID, the apps processor and the PC generate different IPv6 addresses. Note that the Duplicate Address Detection (DAD) must be performed.

13.5 Use case 1 – BIP and OTADM simultaneous access admin PDN

This describes the scenario when the UE simultaneously accesses the admin PDN to perform OTADM procedures from the apps processor and UICC BIP procedures from the modem processor. The approach is based on static port-space partitioning.

Preconditions

- The UE is in eHRPD personality and has a valid eHRPD session established.
- LCP and authentication phases of PPP are complete.

Assumptions

None

Triggers

Either the BIP application or the OTADM application is activated.

Description

For each combination of PDN and IP type for admin APN, the UE shall reserve the range of port numbers to be used for the embedded applications at power up. On receiving the trigger, the UE shall assign the port number that is not in the reserved range to tethered applications.

When the BIP application is activated, the OS on which it is running shall assign the port number based on the port number partitioning rule specified in Table 13-2. When the OTADM application is activated, the OS on which it is running shall assign the port number that is not in the range of the reserved numbers specified in Table 13-2. The simultaneous access to admin PDN from the BIP and OTADM applications is shown in Figure 13-5.

Table 13-2 Port numbers reserved for BIP application when accessing admin PDN

Name	Unit	Default	Description
PortNumbersBIPAdminAPN		32000 to 32007	Identifies the range of port numbers assigned to the BIP application when accessing the admin PDN

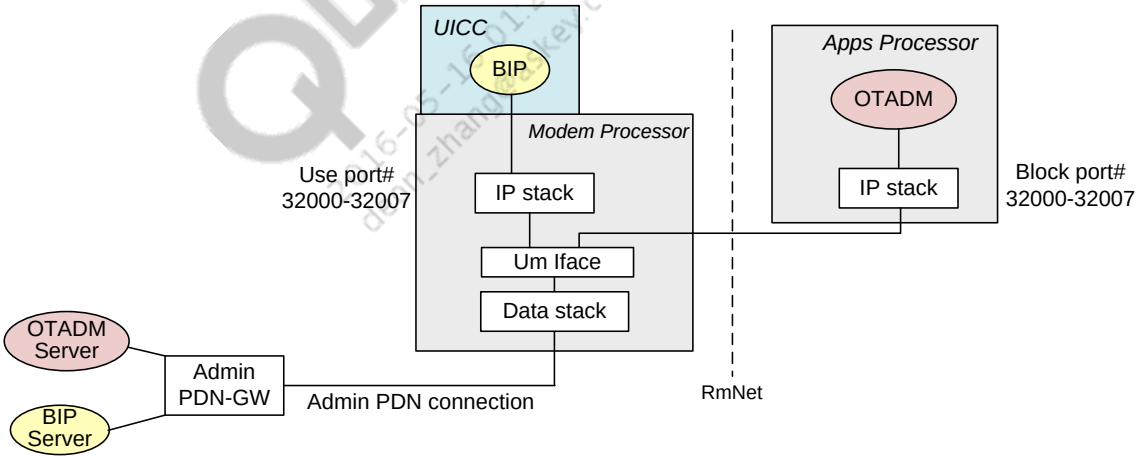

Figure 13-5 Simultaneous access to admin PDN from BIP and OTADM

If the AMSS receives an IP packet from the network on the admin PDN connection, it shall perform filtering based on the destination port number in the IP header and route the IP packet to the appropriate processor and application. Note that the filtering can be based on 4-tuple, i.e., source IP address, source port, destination IP address, and destination port.

Postcondition

Either the BIP or the OTADM application, or both, are connected to the admin PDN using the same IP address.

13.6 Use case 2 – IMS and GPS simultaneously access IMS PDN

In this use case, the IMS client that runs on the modem processor and the GPS service that runs on the apps processor simultaneously access the IMS PDN. The static port-space partitioning approach is used.

13.7 Use case 3 – Simultaneous access internet PDN

This scenario describes when the UE simultaneously accesses the internet PDN from the apps processor and the PC. The hybrid port space partitioning and PC-only NAT approach is used.

14 PDN-Level Authentication

NOTE: This chapter was added to this document revision.

This chapter describes the UE behavior for supporting PDN-level authentication using PCO. Either the PPP Authentication Protocol (PAP) [S8] or PPP Challenge Handshake Authentication Protocol (CHAP) [S9] can be used as the authentication protocol.

14.1 Assumptions

- The network should support PAP/CHAP authentication for a given APN.
- The operator should provision the UE with the PDN-level authentication protocol, e.g., None, PAP, or CHAP, to be used for each APN.
- If a PDN-level authentication protocol (PAP or CHAP) is used for a given APN, the operator should provision the UE with the username and password for this APN.

14.2 Requirements

The UE shall support PDN-level authentication over eHRPD and LTE, using PAP/CHAP during the procedure of PDN connectivity establishment. For this purpose, the UE shall include the Protocol Configuration Options (PCO) IE in the VSNCP Config-Req message and the PCO IE shall include the PAP/CHAP packet(s).

Each PAP/CHAP packet is included in the PCO IE as a unit. One unit in the PCO IE consists of the following [S10]:

- The protocol identifier, set to C023H for PAP or C223H for CHAP
- The length of the protocol identifier contents of this unit, 1 octet
- The protocol identifier contents, n octets

The protocol identifier contents field of each unit contains one PAP/CHAP packet.

- If PAP is used, the UE shall include the Authentication-Request packet in the PCO IE. The Authentication-Request packet contains the Peer-ID/Password. The PAP packet format is specified in [S8].
- If CHAP is used, the UE shall include two CHAP packets in the PCO IE, the CHAP Challenge packet and the CHAP Response packet. The CHAP packet format is specified in [S9].
  - In the Challenge packet, the UE shall include a pseudo-random number in the Value field and the username in the Name field.

- The UE shall concatenate the Identifier, the password, and the Challenge value, and shall use the concatenated stream to calculate the Response Value using the preconfigured hash function. The UE shall have a one-way hash function, MD5, preconfigured for calculating the CHAP Response Value. The UE shall include the Response Value in the Response packet.

14.3 Use case 1 – PDN connectivity establishment

This use case describes the scenario when the UE initiates a PDN connectivity establishment procedure to connect to a specific APN.

Preconditions

- The UE is in eHRPD personality and has a valid eHRPD session established.
- LCP phase and EAP-AKA authentication of PPP are complete.

Assumptions

None

Triggers

An application is activated and requests association with an APN that is not already established.

Description

Figure 14-1 shows the call flow.

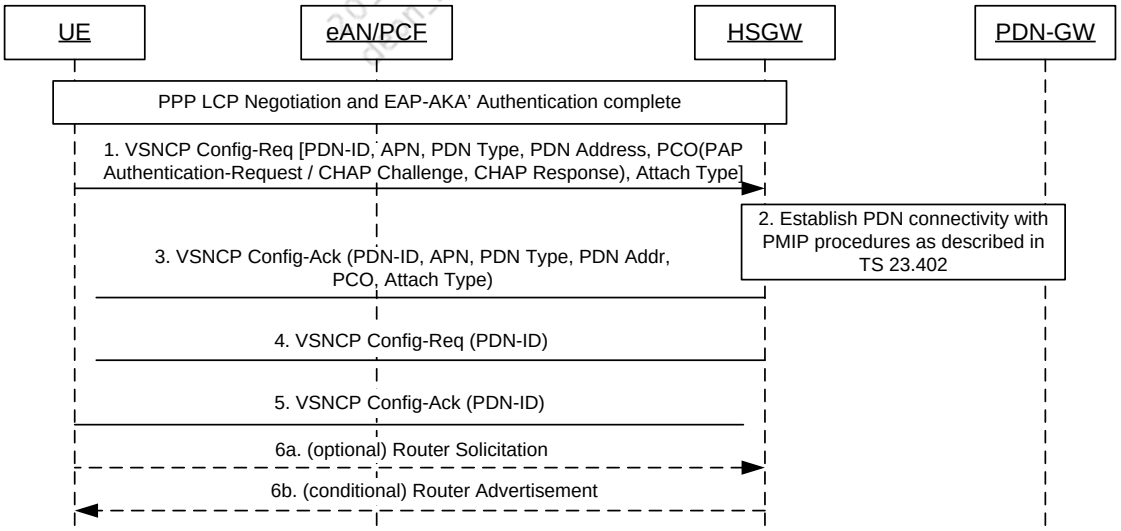

Figure 14-1 UE initiates PDN connectivity establishment procedure

The following numbered paragraphs correspond to Figure 14-1:

1. Triggered by the application's request to establish connectivity to an APN, the UE sends the VSNCP Config-Req, e.g., PDN-ID, APN, PDN Type, PDN Address, PCO, and Attach Type, message to the HSGW. The PCO IE includes a unit that indicates the Protocol Identifier PAP and the PAP Authentication-Request packet, if PAP is used. If CHAP is used, the PCO IE includes two units that indicate the Protocol Identifier CHAP and Challenge and Response packets, respectively.
2. The HSGW triggers the procedures for UE-requested additional PDN connectivity, as described [S11]. This establishes the proxy MIP bindings at the new P-GW and updates the PCRF with the indication of the new connection. The network also validates the username and password contained in the PCO IE and responds with a Success or Failure response. In this use case, the PAP/CHAP authentication succeeds and the network responds with a PAP Authentication-ACK or a CHAP Success packet.
3. After the HSGW receives the indication of completion of the PMIP procedures, it sends the VSNCP Config-ACK, e.g., PDN-ID, APN, PDN Type, PDN Address, PCO, and Attach Type, message to the UE. The PCO IE may contain a PAP Authentication-ACK or CHAP Success packet.
4. HSGW sends a VSNCP Config-Req message to complete the protocol specified in [S37].
5. The UE responds with a VSNCP Config-ACK message.
6. The UE may send a Router Solicitation message if IPv6 IID is assigned.
7. The HSGW shall send a Router Advertisement message if the P-GW sends the IPv6 prefix to the HSGW.

Postcondition

The UE and HSGW established the PDN context.

14.4 Failure scenario of use case 1 – Authentication fails

This use case describes the scenario when the UE initiates a PDN connectivity establishment procedure to connect to a specific APN.

Preconditions

- The UE is in eHRPD personality and has a valid eHRPD session established.
- LCP phase and EAP-AKA authentication of PPP are complete.

Assumptions

None

Triggers

An application is activated and requests association with an APN that is not already established.

Description

Figure 14-2 shows the call flow.

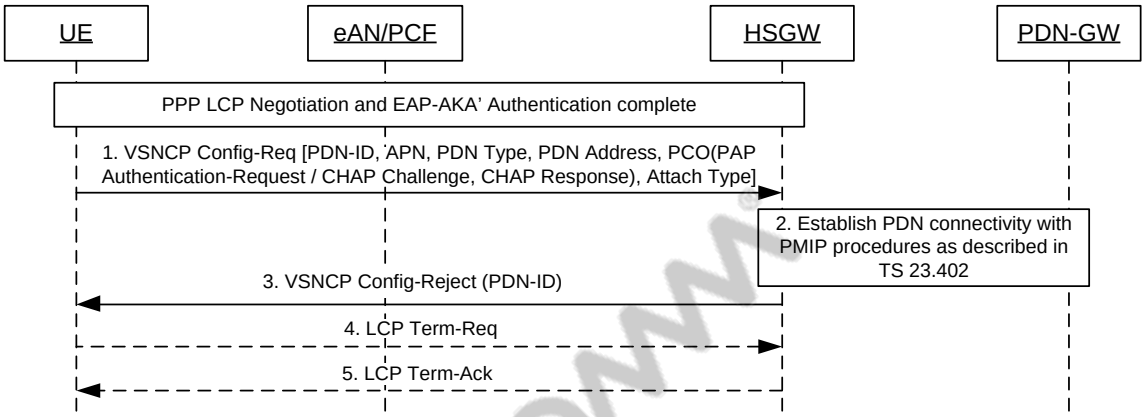

Figure 14-2 PDN-level authentication failure scenario

The following numbered paragraphs correspond to Figure 14-2:

1. Triggered by the application's request to establish connectivity to an APN, the UE sends the VSNCP Config-Req, e.g., PDN-ID, APN, PDN Type, PDN Address, PCO, and Attach Type, message to the HSGW. The PCO IE includes a unit that indicates the Protocol Identifier PAP and the PAP Authentication-Request packet, if PAP is used. If CHAP is used, the PCO IE includes two units that indicate the Protocol Identifier CHAP and Challenge and Response packets, respectively.
2. The HSGW triggers the procedures for UE-requested additional PDN connectivity, as described in [S11]. This establishes the proxy MIP bindings at the new P-GW and updates the PCRF with the indication of the new connection. The network also validates the username and password contained in the PCO IE and responds with a Success or Failure response. In this failure scenario, the PAP/CHAP authentication fails and the network responds with a PAP Authentication-NAK or a CHAP Failure packet.
3. After the HSGW receives the indication of completion of the PMIP procedures and authentication failure, it sends the VSNCP Config-Reject (PDN-ID) message to the UE.
4. If there is no other VSNCP context, the UE may start the PartialContextMaintenanceTimer. Upon expiration of the PartialContextMaintenanceTimer, the UE sends an LCP Term-Req to release LCP context.
5. The HSGW responds with an LCP Term-ACK.

Postcondition

- The PDN context is not established.
- The PDN connection reject will cause IP-level throttling, IPv4 and IPv6.
- If there is no VSNCP, PPP is torn down after the PartialContextMaintenanceTimer expires.

14.5 Use case 2 – Network-initiated PDN resynchronization

This use case describes the scenario when the network initiates a PDN resynchronization procedure, during which PDN-level authentication is performed.

Preconditions

- The UE is in eHRPD personality and has a valid eHRPD session established.
- LCP phase and EAP-AKA authentication of PPP are complete.
- The UE connected to a given APN.

Assumptions

None

Triggers

The network initiates a PDN resynchronization by sending a VSNCP Config-Req message, including a PDN-ID.

Description

Figure 14-3 shows the call flow.

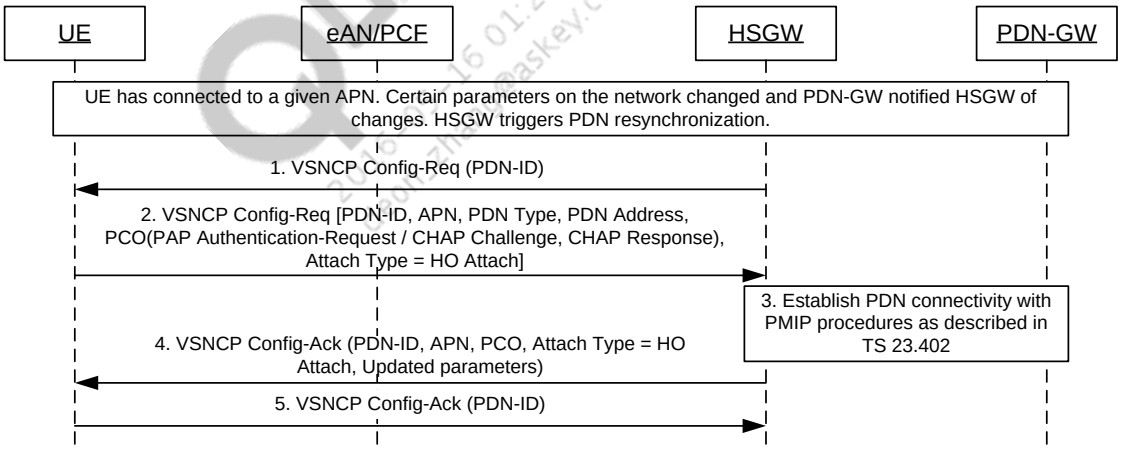

Figure 14-3 Network initiates PDN resynchronization

The following numbered paragraphs correspond to Figure 14-3:

1. The HSGW sends a VSNCP Config-Req message to the UE, identifying the PDN connection to be resynchronized by the PDN-ID included in the message.
2. The UE responds with a VSNCP Config-Req, e.g., PDN-ID, APN, PDN Type, PDN Address, PCO, and Attach Type, message to the HSGW. The PCO IE includes a unit that indicates the Protocol Identifier PAP and the PAP Authentication-Request packet, if PAP is used. If CHAP is used, the PCO IE includes two units that indicate the Protocol Identifier CHAP and Challenge and Response packets, respectively. The UE shall set Attach Type = Handoff Attach.
3. The HSGW triggers the procedures for a handover attach, as described in [S11]. This refreshes the PMIP binding at the P-GW.

4. After the HSGW receives the indication of completion of the PMIP procedures, it sends the VSNCP Config-ACK, e.g., PDN-ID, APN, PDN Address, PCO, Attach Type, message to the UE. The PCO IE may contain a PAP Authentication-ACK or CHAP Success packet.
5. The UE sends a VSNCP Config-ACK (PDN-ID) message to the HSGW.

Postconditions

- The UE and HSGW resynchronized the PDN context.
- Applications are notified of parameter updates.
- Data transfer on the resynchronized PDN connection is resumed.

14.6 Failure scenario of use case 1 – Authentication fails

This use case describes the scenario when the network initiates a PDN resynchronization procedure, during which PDN-level authentication is performed.

Preconditions

- The UE is in eHRPD personality and has a valid eHRPD session established.
- The LCP phase and EAP-AKA authentication of PPP are complete.
- The UE connected to a given APN.

Assumptions

None

Triggers

The network initiates a PDN resynchronization by sending a VSNCP Config-Req message, including a PDN-ID.

Description

Figure 14-4 shows the call flow.

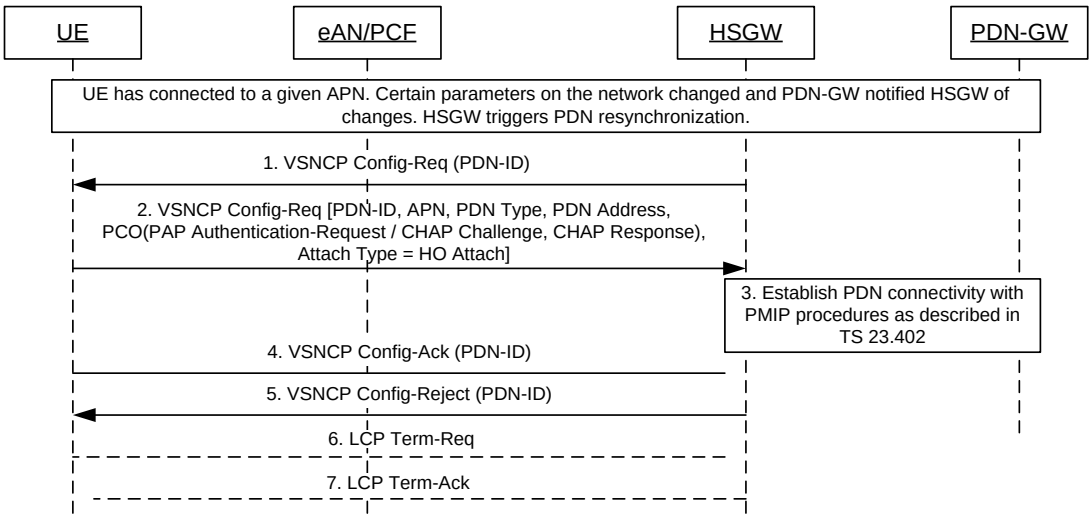

Figure 14-4 Network initiates PDN resynchronization and authentication fails

Steps 1 through 3 follow the call flow in the successful call flow in Figure 14-4.

The following numbered paragraphs correspond to Figure 14-4:

1. Before receiving the VSNCP Config-Reject message from the HSGW, the UE may send a VSNCP Config-ACK to the HSGW.
2. After the HSGW receives the indication of completion of the PMIP procedures and authentication failure, it sends the VSNCP Config-Reject (PDN-ID) message to the UE.
3. If there is no other VSNCP context, the UE may start the PartialContextMaintenanceTimer. Upon expiration of the PartialContextMaintenanceTimer, the UE sends a LCP Term-Req to release the LCP context.
4. The HSGW responds with an LCP Term-ACK.

Postcondition

- PDN resynchronization failed. PDN context is released. Applications are notified of the failure and the data transfer fails.
- A PDN connection reject will cause IP-level throttling, IPv4 and IPv6.
- If there is no VSNCP, PPP is torn down after the PartialContextMaintenanceTimer expires.

14.7 Use case 3 – PDN connectivity establishment over LTE

This use case describes the scenario when the UE initiates a PDN connectivity establishment procedure to connect to a specific APN over LTE.

Preconditions

- The UE is attached to LTE.
- If the UE requests PDN connectivity in the Idle state, the UE should first perform the service request procedure.

Assumptions

None

Triggers

An application is activated and requests association with an APN that is not already established.

Description

Figure 14-5 shows the call flow.

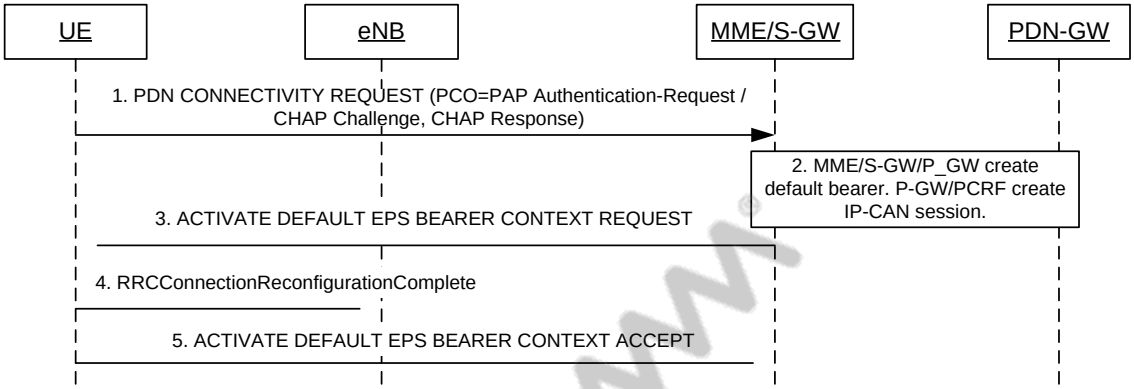

Figure 14-5 UE initiates PDN connectivity establishment procedure over LTE

The following numbered paragraphs correspond to Figure 14-5:

1. Triggered by the application's request to establish connectivity to an APN, the UE sends the NAS message PDN Connectivity Request to the MME, which is included in the RRC message ULInformationTransfer. The PCO IE includes a unit that indicates the Protocol Identifier PAP and the PAP Authentication-Request packet, if PAP is used. If CHAP is used, the PCO IE includes two units that indicate the Protocol Identifier CHAP and Challenge and Response packets, respectively.
2. The MME creates the default EPS bearer at the S-GW, which creates the default EPS bearer at the P-GW. The P-GW may establish the IP-CAN session at the PCRF.
3. The MME sends the NAS message Activate Default EPS Bearer Context Request to the UE. The MME also requests the eNB to set up the bearer.
4. The UE replies to the eNB with an RRCConnectionReconfigurationComplete message.
5. The UE replies to the MME with a NAS message Activate Default EPS Bearer Context Accept.

Postcondition

The UE and MME established the PDN context.

Failure scenario

If PDN-level authentication fails, the MME rejects the PDN connectivity request by sending a NAS message PDN Connectivity Reject. This causes IP-level throttling (IPv4 and IPv6) at the UE.

14.8 Alternative scenario of use case 3

This use case describes the scenario when the UE initiates a PDN connectivity establishment procedure to connect to a specific APN over LTE. In this alternative scenario, the PCO is transferred as security protected.

Preconditions

- The UE is attached to LTE.
- If the UE requests PDN connectivity in the Idle state, the UE should first perform the service-request procedure.

Assumptions

None

Triggers

An application is activated and requests association with an APN that is not already established.

Description

Figure 14-6 shows the call flow.

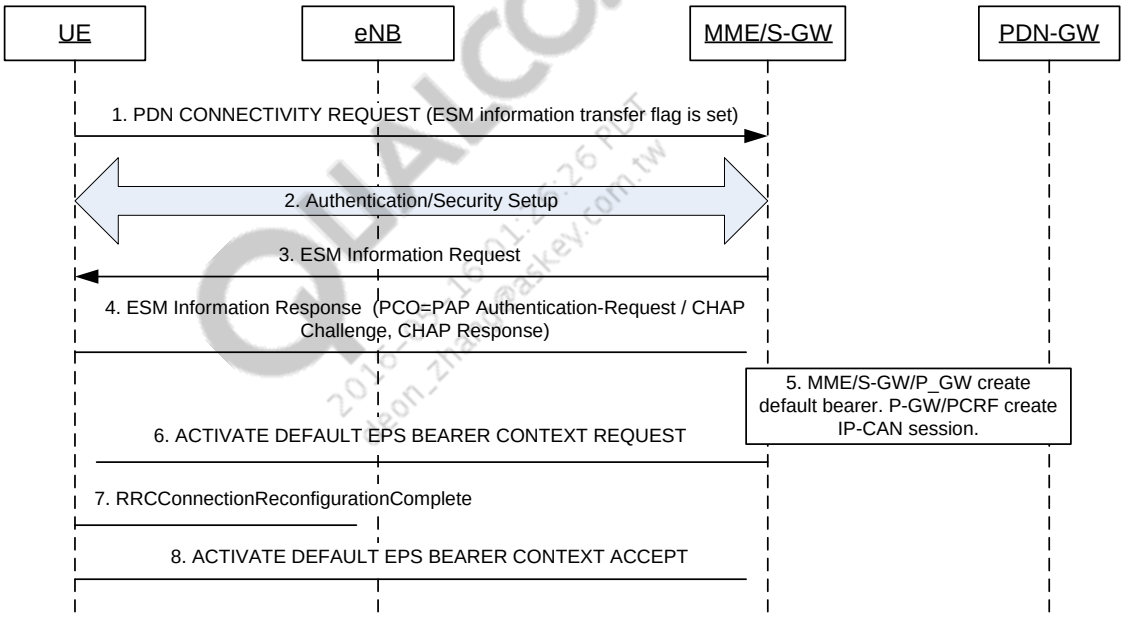

Figure 14-6 Alternative scenario of use case 3, LTE

The following numbered paragraphs correspond to Figure 14-6:

1. Triggered by the application's request to establish connectivity to an APN, the UE sends the NAS message PDN Connectivity Request to the MME, which is included in the RRC message ULInformationTransfer. The ESM information transfer flag is set to 1, indicating that PCO shall be security protected and shall not be included in this message.
2. The UE and MME perform the authentication and security procedure to set up the security to transfer PCO.
3. The MME sends the NAS message ESM Information Request to the UE.

4. The UE responds with the NAS message ESM Information Response, which includes the ciphered PCO. The PCO IE includes a unit that indicates the Protocol Identifier PAP and the PAP Authentication-Request packet, if PAP is used. If CHAP is used, the PCO IE includes two units that indicate the Protocol Identifier CHAP and Challenge and Response packets, respectively.
5. The MME creates the default EPS bearer at the S-GW, which creates the default EPS bearer at the P-GW. The P-GW may establish the IP-CAN session at the PCRF.
6. The MME sends the NAS message Activate Default EPS Bearer Context Request to the UE, with the PCO IE containing a PAP Authentication-ACK or CHAP Success packet. The MME also requests the eNB to set up the bearer.
7. The UE replies to the eNB with a RRCConnectionReconfigurationComplete message.
8. The UE replies to the MME with a NAS message Activate Default EPS Bearer Context Accept.

Postcondition

The UE and MME established the PDN context.

15 EPC Context Maintenance

NOTE: This chapter was added to this document revision.

This chapter describes the UE's behavior for maintaining EPC context when moving out of an EPC-capable region.

NOTE: This is not supported.

15.1 Overview

The UE can access the EPC network from the 3GPP E-UTRAN and the 3GPP2 eHRPD network. While it is in eHRPD radio, the UE connects to the PDN-GW through HSGW. While it is in E-UTRAN, the UE connects to the PDN-GW through S-GW. The architecture for handoffs between E-UTRAN access and cdma2000 HRPD access is shown in Figure 15-1. This architecture facilitates the interworking between E-UTRAN and eHRPD.

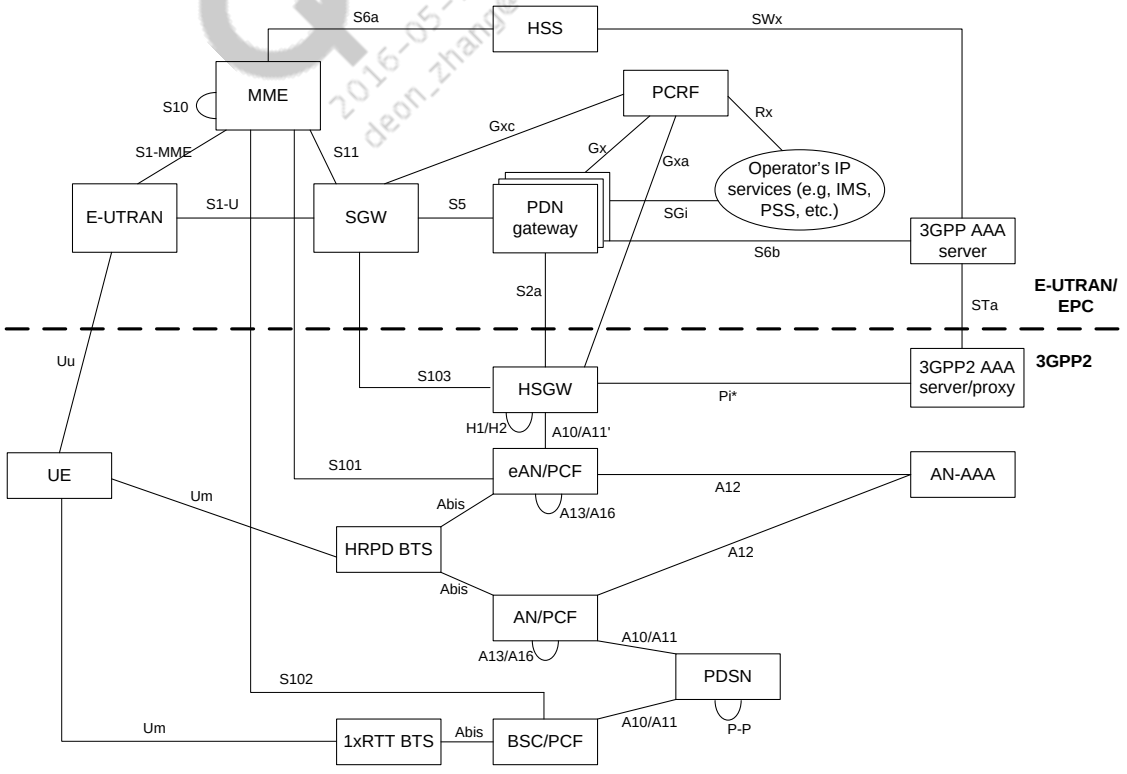

Figure 15-1 EPC access from E-UTRAN/eHRPD and nonEPC access from 1x/HRPD (nonroaming case)

There is no interworking between E-UTRAN/eHRPD and 1x/HRPD. In 1x/HRPD, the UE connects to the 3GPP2 core network to receive data services. Therefore, when the UE transitions from E-UTRAN/eHRPD to 1x/HRPD, the data session has to break and must be remade. Later, when the UE moves back to E-UTRAN/eHRPD (the denoted ECP-capable region) from 1x/HRPD (the denoted EPC noncapable region), the data session has to break and be remade again.

15.1.1 UE behavior without support of EPC context maintenance

Without support of the EPC context maintenance feature described in this chapter, when the UE loses LTE/eHRPD and declares, e.g., 1x, as the serving data system (based on data system determination logic, which is out of the scope of this feature), the UE locally releases all EPC context and notifies the applications. Consequently, the IP context breaks. Triggered by the application, the UE places the data call over 1x. Applications that can use the 1x data service receive data services over 1x.

Since EPC context is locally released at the UE, it is possible that the EPC core does not know that the UE is out of an EPC-capable region. There are three cases for mobile terminated traffic:

- For the service that supports sequential page over 1x CS followed by failing over PS, the MT traffic of such a service, e.g., SMS can finally be delivered to the UE over 1x CS.
- For some applications that can use the 1x data service, upon request of the application, after the UE sets up the data session over 1x and registers with the application server, MT traffic will be delivered over 1x CS.
- For some applications that cannot use the 1x data service, before the network context times out, MT traffic is still delivered to the ECP core and will fail.

NOTE: After the UE declares 1x as the serving data system, all applications that were connecting to the EPC core receive a failure notification. IP continuity breaks when the UE releases the EPC context, including the application that cannot use the 1x data service.

15.1.2 EPC context maintenance

Instead of releasing all EPC contexts when moving out of LTE/eHRPD, an enhanced approach is to allow the application to retain the EPC context. When moving back to LTE/eHRPD, the UE resumes the EPC context for the application. This allows the application that cannot or does not want to use the 1x data service to retain its EPC context, and, upon returning to LTE/eHRPD, to resume EPC context. In this way, IP continuity can be retained. This enhancement is especially useful for the application that cannot use nonEPC data services, or in the case when the UE temporarily moves out of an EPC-capable region.

With this new feature, the UE shall support retaining and suspending the EPC context. For applications that do not request an ECP context release, the UE will flow control the application. The UE shall also support resuming the suspended EPC context upon returning to LTE/eHRPD, such that the application can resume data transfer.

NOTE: This feature is not aimed to solve the undeliverable MT traffic problem described in Section 15.1.1.

15.2 Logical architecture and interface

Figure 15-2 shows the logical architecture of the UE, which consists of entities that are related to this feature.

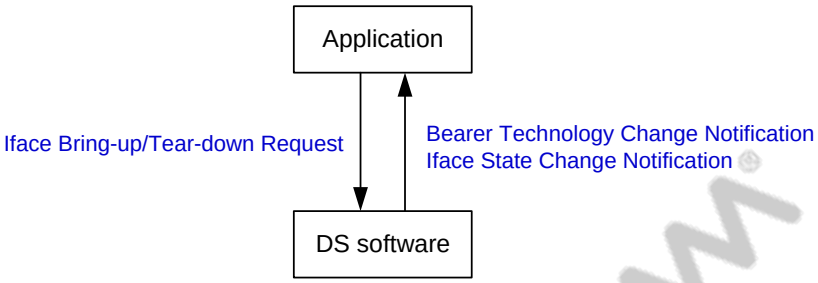

Figure 15-2 Logical architecture for EPC context maintenance

The following software entities are included in the logical architecture:

- DS software is the AMSS software manages data connections. It may include functions that manage data connections over different radio technologies, e.g., LTE, eHRPD, and 1xCS. In particular, functions of this software include maintenance of eHRPD PPP sessions, IP functionalities, and DNS functionalities. DS also determines the serving data systems. For example, the UE may camp on LTE and 1x simultaneously; if the UE loses LTE, DS will declare 1x as the serving data system based on its serving data systems logic.
- The application is any software above the DS software that requests a wireless data session. Applications do not normally belong to AMSS software.

As shown in Figure 15-2, the interfaces among these software entities are defined as follows:

- The application can invoke Iface Bring-up Request to request IP context establishment. The application can also invoke Iface Tear-Down Request to request an IP context release.
- After determining the new serving data system, DS notifies the application of Bearer Technology Change. A change of the serving data system can be caused by acquisition of a new radio technology or loss of a radio technology.
- The DS can notify the application of Iface State Change with the new Iface state.

The Iface is referred to as the interface between the application and the AMSS DS software. Each Iface is associated with a data structure that includes the assigned IP address (IPv4 or IPv6), bearer type, flows, gateway address, etc. A single Iface can be bound to multiple applications that connect to the same PDN gateway and use the same IP address. The major Iface states are:

- Coming-up – This is the transition state in which, upon request of the application, DS is trying to bring up the Iface for the application.
- Going-down – This is the transition state in which DS is releasing the Iface. It can be triggered by the last application that is bound to the Iface or can be caused by a network-initiated PDN connection release.
- Up – This is the state in which the Iface is ready for data transfer for applications.
- Down – This is the state in which the Iface is gone. The application that was requesting the data connection or that was connecting to a PDN cannot receive data services unless the DS brings up a new Iface for it.

- Configuring – This is the state in which the Iface is under configuration. For example, if the UE connected to a PDN and later the network initiates PPP resync, the Iface transitions from the Up state to the Configuring state. This can also occur if the UE, during IPv6 address assignment procedures, receives the IID and transitions from the Coming-up state to the Configuring state. Later, the UE transitions to the Up state after it receives the prefix from the network.

15.3 New requirements

The UE shall support the following new requirements:

- The UE shall support EPC iFaces and non-EPC Ifaces concurrently.
- The UE shall support suspending EPC Ifaces. The UE shall also support a new state in Iface management, Suspend, which is the state in which the Iface is still connected to applications but cannot transfer data for the application. If Iface is suspended, the AMSS shall notify the application of Iface Suspend. If the suspended Iface is resumed, the AMSS shall notify the application of Iface Resume.
- The UE shall support an instance of PPP for 1x/HRPD concurrently with PPP instances for eHRPD and AN-PPP.

15.4 Assumptions

- The application should understand the Iface Suspend state. If the application is notified of Iface Suspend, it is up to the application to decide whether to retain Iface or to release Iface. If the application decides to retain Iface, the application is allowed to transfer data only after receiving an Iface Resume notification. In this design, the focus is on applications that run on the modem processor. The feature can be extended to applications that run on HLOS with support from HLOS/RIL.
  - An application that cannot use 1x data service can retain the EPC Iface.
  - An application that can use 1x data service can request to release the EPC Iface. After the EPC Iface is released, the application can request to bring up a new Iface on 1x/HRPD to receive data service. This feature does not require the application to support both EPC and nonEPC Ifaces at the same time.
  - An application that cannot support suspended Iface can release the EPC Iface.
- It is assumed that the OS supports two technologies concurrently. That is, the OS should support simultaneous Ifaces for EPC in the Suspend state and nonEPC. Only one type of Iface is active at a time, i.e., if the nonEPC Ifaces are in the Up state, the EPC Ifaces are in the Suspend state. Since the nonEPC Ifaces do not support the Suspend state, if the EPC Ifaces are in the Up state, nonEPC Ifaces will be released.

15.5 Use case 1 – Suspend EPC context when moving to 1x/HRPD from LTE/eHRPD

This use case describes the scenario when the UE moves from LTE/eHRPD to 1x/HRPD. The UE suspends all EPC context.

The scenario of moving from LTE/eHRPD to 1x can be that the UE moves to 1x-only coverage.

The scenario of moving from LTE/eHRPD to HRPD can be one of the following:

- The UE moves from LTE to DO and the InUse personality of the EVDO session that the UE negotiates with the RAN is HRPD, or
- The UE remains in EVDO coverage and the UE falls back from eHRPD to HRPD due to any reason described in [Q2], or
- The UE remains in EVDO and the UE has an EVDO session with eHRPD as the InUse personality. Later, the session is closed and the UE and RAN negotiate a new session with HRPD as the InUse personality.

The use case uses moving to a 1x-only coverage as the example.

Preconditions

- The UE is attached to LTE or eHRPD. The UE is also registered to 1x.
- The UE established EPC context over LTE or eHRPD for the application(s).

Assumptions

None

Triggers

The UE loses LTE or eHRPD.

Description

Figure 15-3 shows the call flow.

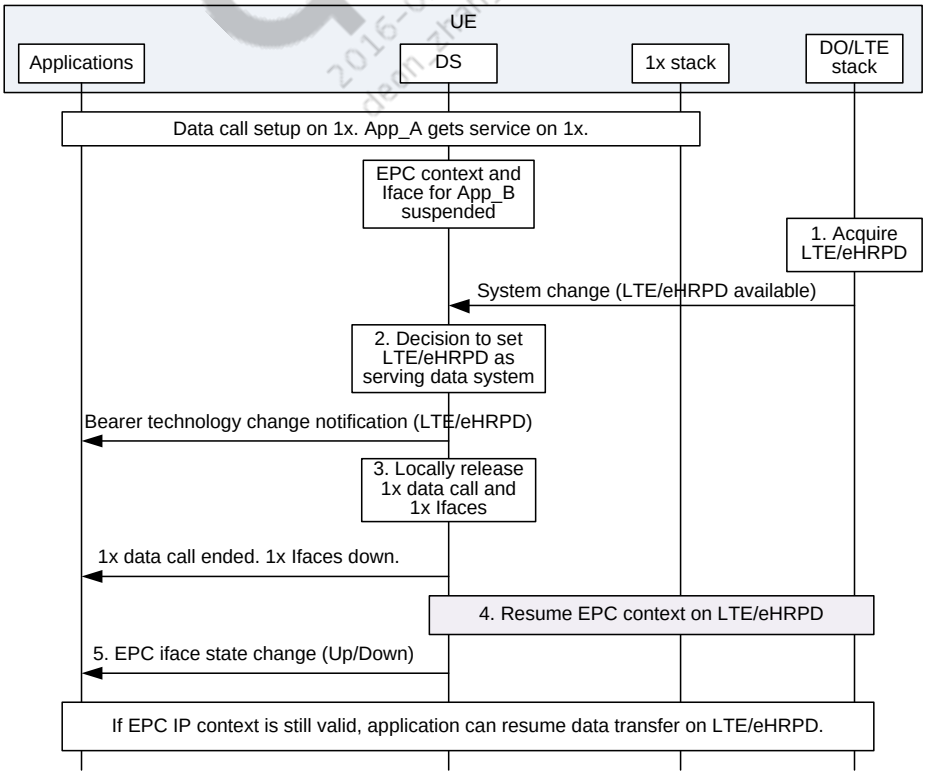

Figure 15-3 UE suspends EPC context upon moving to a 1x-only region

The following numbered paragraphs correspond to Figure 15-3:

1. When the DO/LTE stack detects a loss of LTE/eHRPD, it notifies the DS of loss of LTE/eHRPD.
2. The DS determines that 1x is the serving data system and sends the Bearer Technology Change Notification to the applications that connected to any PDN connection while the UE was on LTE/eHRPD.
3. The DS shall not release the EPC contexts. Instead, it shall suspend all existing EPC context and Ifaces that were brought up for EPC. If the PDN inactivity timer is running, it shall continue running. Upon expiration of the PDN inactivity timer, the UE shall locally clear the corresponding ECP context and release the corresponding Iface. After suspending the EPC contexts, the DS shall notify applications of EPC Iface Suspend. The UE shall also flow control the applications.
4. Upon receiving notification of Iface Suspend, it is up to the application to determine whether or not to release the suspended EPC Iface.
   - Application App_A decides to release its EPC Iface and bring up a new iface over 1x.
   - Application App_B decides to retain its EPC Iface.
   - Application App_A requests to bring up a new Iface on 1x.
5. Upon request of the application, DS places data call over 1x and set up 1x data session.

Postcondition

- The UE set up a data session over 1x. Application App_A receives data service over 1x.
- The UE suspended EPC context for application App_B.

15.6 Use case 2 – Resume EPC context when moving back to LTE/eHRPD

This use case describes the scenario when the UE moves from 1x/HRPD back to LTE/eHRPD. When moving from LTE/eHRPD to 1x/HRPD, the UE suspended EPC context and Iface. Upon moving back to LTE/eHRPD, the applications that did not request the release of EPC context are still bound to the suspended EPC Ifaces.

The use case takes the example of moving from 1x-only coverage back to LTE/eHRPD.

Preconditions

- The UE is registered to 1x. The UE set up an active or dormant data session over 1x.
- The UE suspended EPC context and Iface for the application that did not request the EPC context release.

Assumptions

None

Triggers

The UE acquires LTE or eHRPD.

Description

Figure 15-4 shows the call flow.

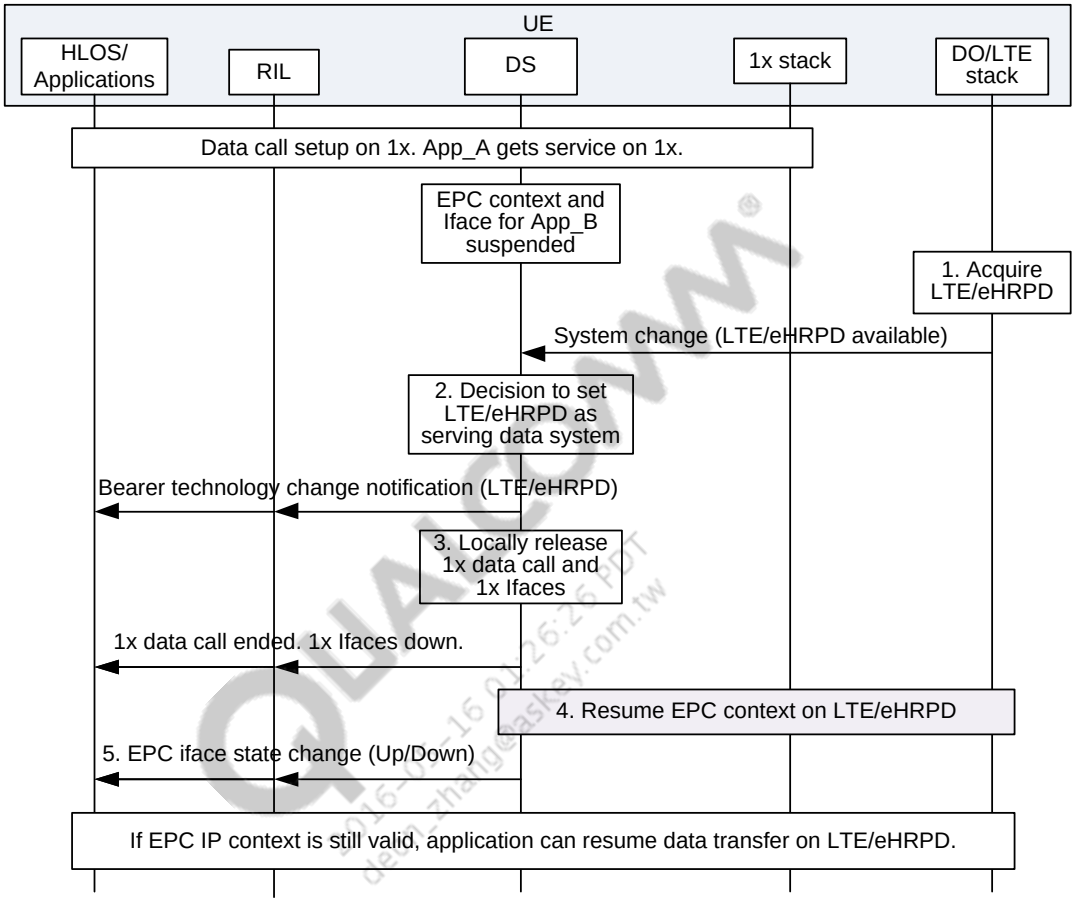

Figure 15-4 UE resumes EPC context upon moving back to LTE/eHRPD

The following numbered paragraphs correspond to Figure 15-4.

1. The UE acquires LTE or eHRPD. The DS receives notification of the system change LTE/eHRPD available.
2. The DS determines that LTE/eHRPD is the new serving data system and sends the Bearer Technology Change Notification indicating LTE or eHRPD to the applications.
3. The DS shall locally release the 1x data call and 1x Ifaces. The DS shall also notify applications of the 1x Iface Down.
4. The DS shall resume the data session on LTE or eHRPD. The resume procedures for LTE and eHRPD are, respectively:

   If the target system is LTE:

   - If the UE is EMM-Deregistered, the UE shall perform LTE HO attach. The UE performs a handover attach to each suspended EPC PDN connection.
   - If the UE is EMM-Registered, the UE performs an EPC bearer context sync-up procedure with the network, which is part of the LTE Tracking Area Update procedure.

If the target system is eHRPD:

- If the UE does not have PPP context, the UE shall create PPP context including authentication.
- If the UE does not have VSNCP context, i.e., the UE was previously attached to LTE before moving to 1x-only coverage, the UE shall perform VSNCP handover attach to each suspended EPC PDN connection.
- If the UE has at least one VSNCP context, i.e., the UE was previously attached to eHRPD before moving to 1x-only coverage:
  - If stale PDN handling is supported, the UE shall initiate the PDN sync-up procedure with the HSGW using LCP Echo packets. Based on HSGW's response, the UE shall locally release the EPC context that the HSGW does not have and shall perform VSNCP handoff attach to the PDN with which the HSGW has context but the UE does not have context.
  - If stale PDN handling is not supported, the UE shall perform a VSNCP handoff attach to each suspended EPC PDN connection.

  For each EPC IP context that is still valid, the UE shall notify applications of EPC Iface Up. Otherwise, if the IP context is invalid, the UE notifies the application of EPC Iface Down.

Postcondition

The UE resumed the data session over LTE/eHRPD. If the EPC IP context is still valid, the application can resume data transfer over LTE/eHRPD.