ACKNOWLEDGEMENT

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

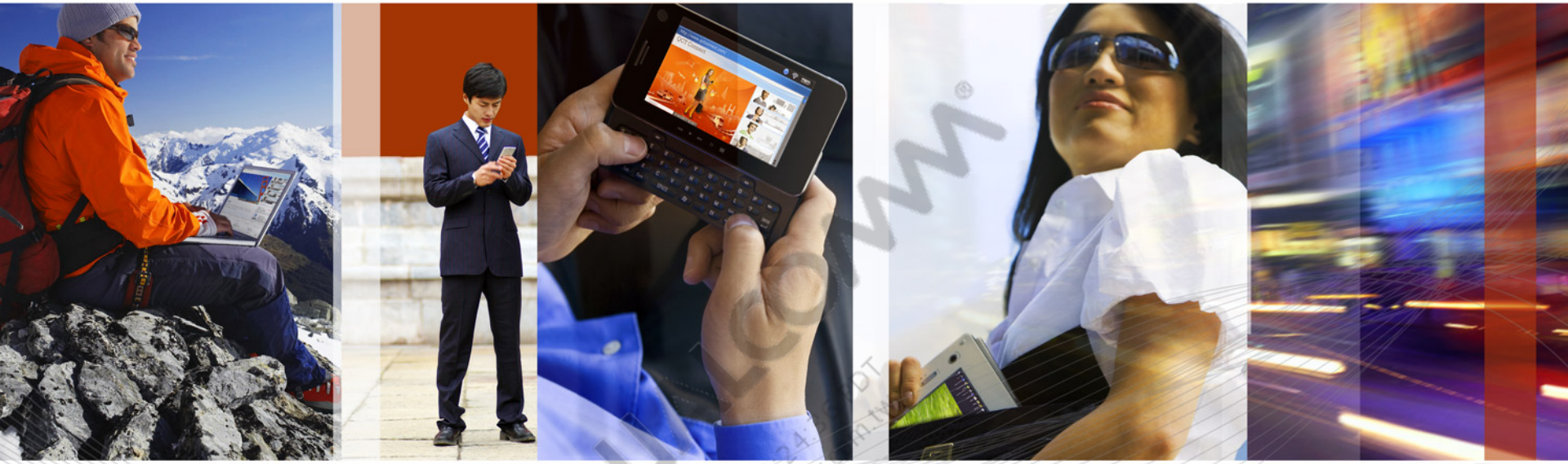
Effective October 1, 2012, QUALCOMM Incorporated completed a corporate reorganization in which the assets of certain of its businesses and groups, as well as the stock of certain of its direct and indirect subsidiaries, were contributed to Qualcomm Technologies, Inc. (QTI), a wholly-owned subsidiary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



QUALCOMM CDMA Technologies

REDEFINING MOBILITY

Introduction to eHRPD

80-VR815-1 D

Qualcomm Confidential and Proprietary

Restricted Distribution. Not to be distributed to anyone who is not an employee of either Qualcomm or a subsidiary of Qualcomm without the express approval of Qualcomm's Configuration Management.

Not to be used, copied, reproduced in whole or in part, nor its contents revealed in any manner to others without the express written permission of Qualcomm.

Qualcomm reserves the right to make changes to the product(s) or information contained herein without notice. No liability is assumed for any damages arising directly or indirectly by their use or application. The information provided in this document is provided on an "as is" basis.

This document contains Qualcomm confidential and proprietary information and must be shredded when discarded.

This technical data may be subject to U.S. and international export, re-export, or transfer ("export") laws. Diversion contrary to U.S. and international law is strictly prohibited.

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

Revision History

Version	Date	Description
A	Sep 2009	Initial release
B	Jan 2010	eHRPD Call Flow and Log update
C	Aug 2010	Added Dual IP bearer support
D	Sep 2010	Updated eHRPD-LTE Comparison Table (slide 15) and Dual IP Address, PDN Context Release Call Flows (slides 62-67)

Contents

eHRPD Overview

REDEFINING MOBILITY

eHRPD Overview

- enhanced High Rate Packet Data (eHRPD) is a bridging technology between EV-DO and LTE
  - Based on EV-DO Rev A air interface
  - Evolved Packet Core (EPC) network can be accessed by EV-DO network
  - Provides seamless interworking between EV-DO and LTE networks
  - Operational modes supported by eHRPD Evolved Access Terminal (eAT)
    - 1xRTT only
    - HRPD only
    - eHRPD only
    - 1xRTT and HRPD Hybrid mode
    - 1xRTT and eHRPD Hybrid mode
- eHRPD personality negotiation
  - eHRPD is another EV-DO personality
  - Supports connectivity to EPC

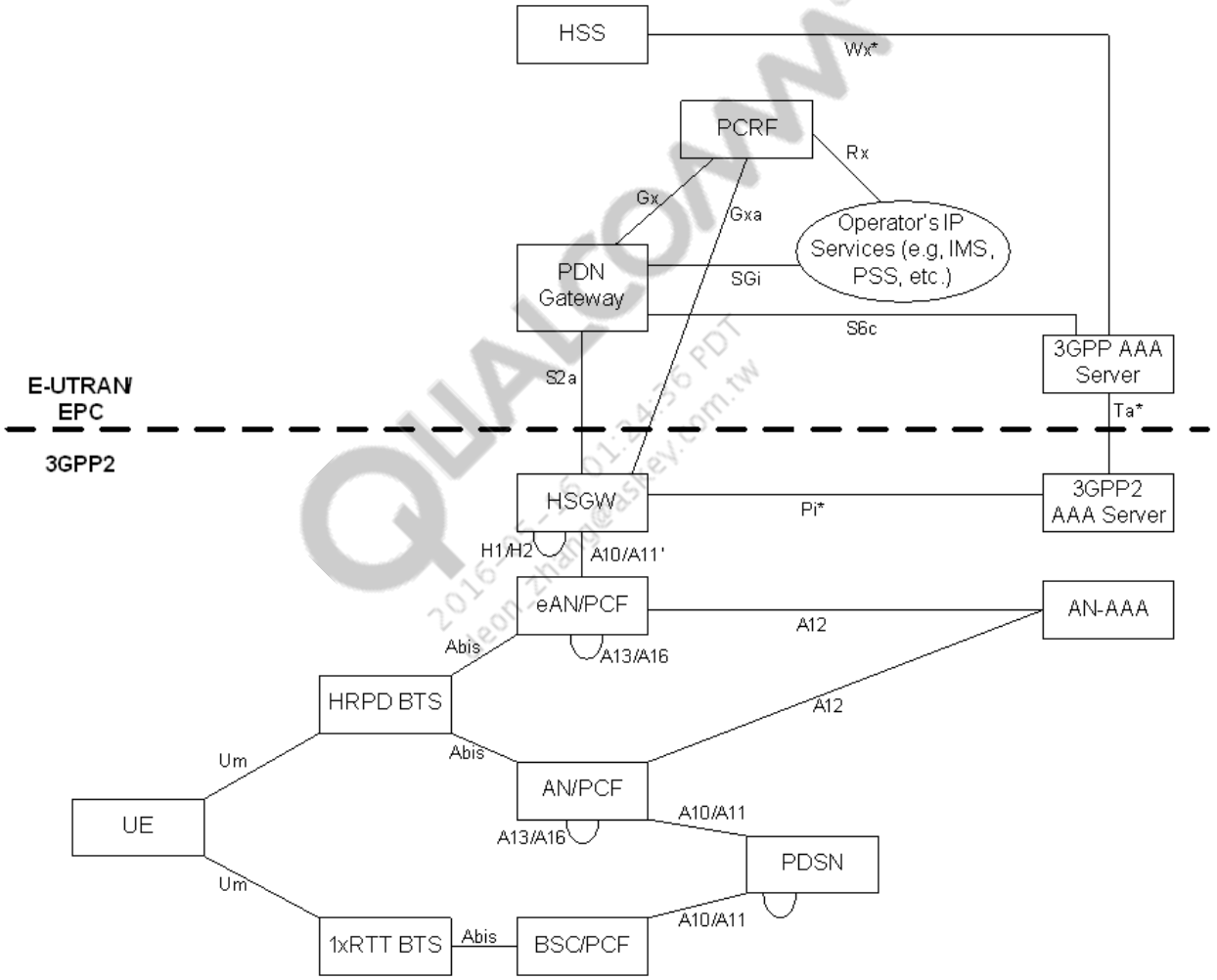
eHRPD Overview (cont.)

- Authentication
  - SN stream authentication
    - EAP-AKA'-based service authentication is used for eHRPD mode
    - Legacy Password Authentication Protocol (PAP) and authentication based on Challenge Handshake Authentication Protocol (CHAP) will still be supported for non-eHRPD mode
  - Access Network (AN) stream authentication
    - CHAP authentication is used for eHRPD and HRPD
- IP address allocation
  - Attach procedures based on Vendor-Specific Network Control Protocol (VSNCP)
  - Capable of supporting both address types, e.g., IPv4 and IPv6
  - Simple IP only support over eHRPD personality
  - Client MIP or simple IP support over non-eHRPD personality

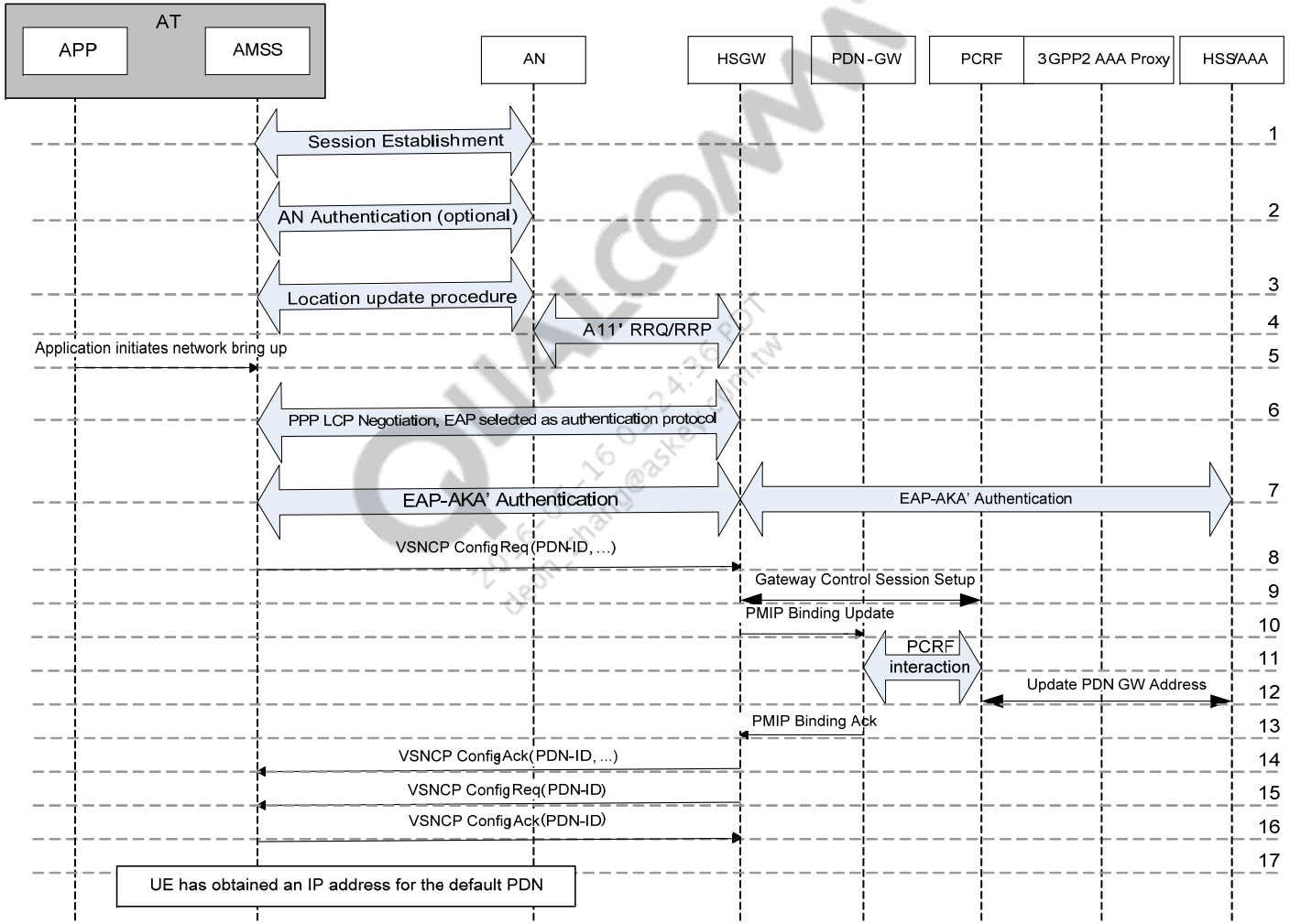
eHRPD Overview (cont.)

- Protocol Configuration Option (PCO) within VSNCP
  - Used for negotiating
    - DNS address
    - Authentication credentials associated with Packet Data Network (PDN) instance
    - P-CSCF address option, used for VoIP service
- Multiple PDN support
  - VSNP enables multiplexing multiple PDN streams on 0xFF (best effort) flow
- Service options supported
  - SO59 and SO67
- Quality of Service (QoS)
  - AMSS current implementation supports User Equipment (UE)-initiated QoS only
  - QoS is available over IPv4 and IPv6

eHRPD Architecture



eHRPD Call Flow Overview



eHRPD Call Flow Overview (cont.)

- Steps are as follows:
  1. The UE and Evolved Access Network (eAN) initiate eHRPD session establishment.
  2. The UE and eAN perform device-level authentication procedures (optional).
  3. If the eAN supports the Location Update procedure, eAN updates the Access Network ID (ANID) in the UE using the Location Update procedure. The eAN may also retrieve the Previous Network Access Identifier (PANID) from the UE, if necessary.
  4. PCF sends an A11-Registration Request message to the HRPD Serving Gateway (HSGW) to set up the main A10 connection with SO59, and to optionally set up the Best Effort (BE) auxiliary service connection with SO72. The A11-Registration Request is validated and HSGW accepts the connection by returning an A11-Registration Reply message.
  5. When the application starts sending data, the AMSS triggers PPP establishment procedures, if the PPP is not already established.
  6. The UE and HSGW perform Link Control Protocol (LCP) negotiation and select EAP as the authentication protocol.

eHRPD Call Flow Overview (cont.)

- Steps are as follows: (cont.)
  7. The authentication procedures are initiated and performed involving the UE, HSGW, 3GPP2 AAA, and 3GPP AAA server. In this step, the P-GW address is determined and the subscription profile of the UE from the HSS/AAA is updated to the HSGW.
  8. The UE sends a VSNCP Config-Req message that contains the PDN-ID, type of connection, UE network capability, PDN address, protocol configuration options, and attach type over the main signaling connection.
  9. The HSGW may perform the Gateway Control Session Establishment procedure with the PCRF.
  10. The HRPD Serving GW sends a Proxy Binding Update (MN NAI, Lifetime, Access Technology Type option, APN, IP address allocation request, and additional parameters) to the P-GW to establish the new registration after a P-GW is selected using the associated APN.
  11. The P-GW performs a PCRF interaction to retrieve the QoS policy parameter.

eHRPD Call Flow Overview (cont.)

- Steps are as follows: (cont.)
  12. The P-GW sends an update message to the 3GPP AAA server to update the UE profile with its address. The 3GPP AAA server acknowledges the updated P-GW address.
  13. The P-GW responds with a PMIP Binding Acknowledgement (MN NAI, Lifetime, UE address information, PCO, additional parameters) message to the HRPD serving GW.
  14. The HSGW sends a VSNCP Config-ACK (APN, PDN address, PCO) message to the UE over the main service connection.
  15. The HSGW sends a VSNCP Config-Req message to complete the protocol specified in RFC 3772.
  16. The UE responds with a VSNCP Config-ACK message.
  17. For IPv6, the UE uses the interface identifier from Step 14 and the prefix from the RS/RA procedures.

eHRPD vs. LTE Comparison

	eHRPD	LTE
Dual IP bearer (IPv4/IPv6)	Yes	Yes
IP address assignment	VSNCP	Upon attach procedure
Default bearer	No	Yes
Number of PDN connections	4	4
Data session termination	From PPP layer	From IP layer
Max down/uplink throughput (Mbps)	3.1/1.8 (EV-DO Rev A)	326.4/86.4 (20 MHz)

eHRPD Session Management

REDEFINING MOBILITY

eHRPD Session Management

- eHRPD operation mode setting
  - See [Q2]
- The UE is operating in eHRPD Session mode, if
  - UE has negotiated an Enhanced Multiflow Packet Application (EMPA) session with the eAN
  - RLP0 flow protocol = 0x07 is configured

eHRPD Session Management Procedures

- UE shall propose 0xFFFE (alternate EMPA) in SCP ATSupportedApplicationSubtype attribute to the eAN
- UE will not propose alternate EMPA during stream protocol negotiation
- During EMPA session negotiation, UE shall propose ATSupportedFlowProtocolParametersPP attribute with ProtocolSupported values 0x07
- Along with other EMPA session attributes, eAN and UE shall negotiate Flow00FlowProtocolFwd/Flow00FlowProtocolRev = 0x07

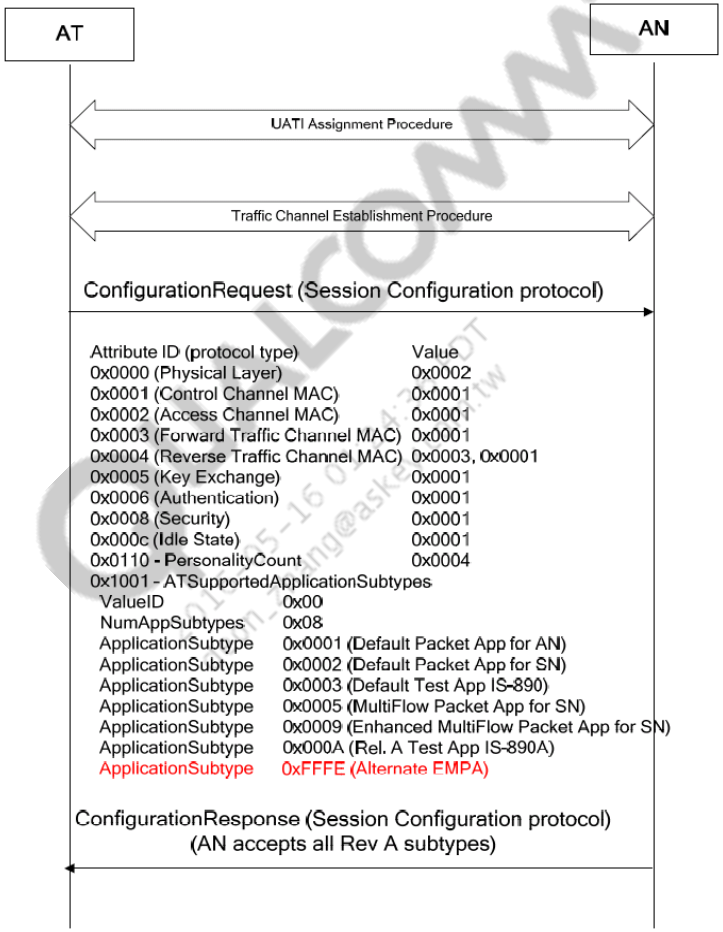
Types of UE Personalities

- UE is allowed to maintain separate personalities for eHRPD and HRPD
- UE and AN do not need a separate personality for HRPD and eHRPD if
  - Both HRPD and eHRPD regions support EMPA and GAUP-ing of attributes FlowNNFlowProtocolParametersFwd and FlowNNFlowProtocolParametersRev
  - During handoff, AN can GAUP to bind and unbind flow protocols 0x00 through 0x08 to and from RLP flows

Mobility Between HRPD and eHRPD Personalities

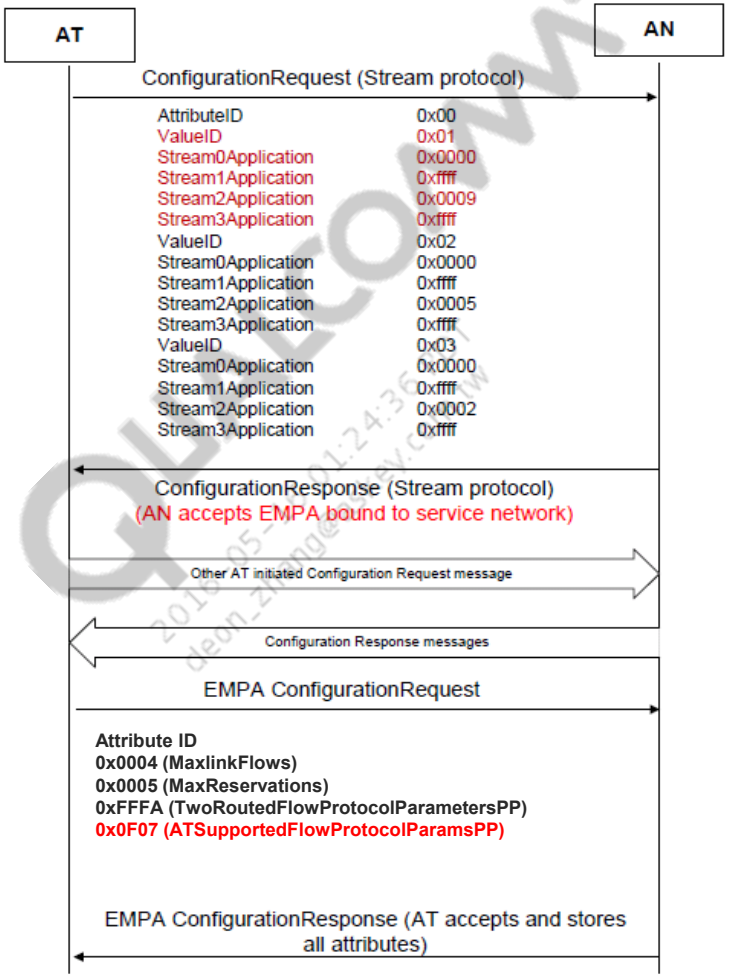
- Handoff from HRPD to eHRPD
  - If AT HRPD session with source AN does not include compatible personality with that of the target eAN, then
    - eAN can close the HRPD session and force AT to renegotiate a new eHRPD session
    - During th eHRPD session configuration, eAN reconfigures the AT using a configuration start mechanism
  - If AT HRPD session with source AN includes compatible personality with that of the target eAN, then
    - eAN can switch AT personality to eHRPD
    - eAN can GAUP Flow protocol attributes to upgrade AT personality to eHRPD.
- Handoff from eHRPD to HRPD will follow similar call flow

eHRPD Personality Negotiation Call Flow



Note: Attributes specific to eHRPD personality are highlighted in red.

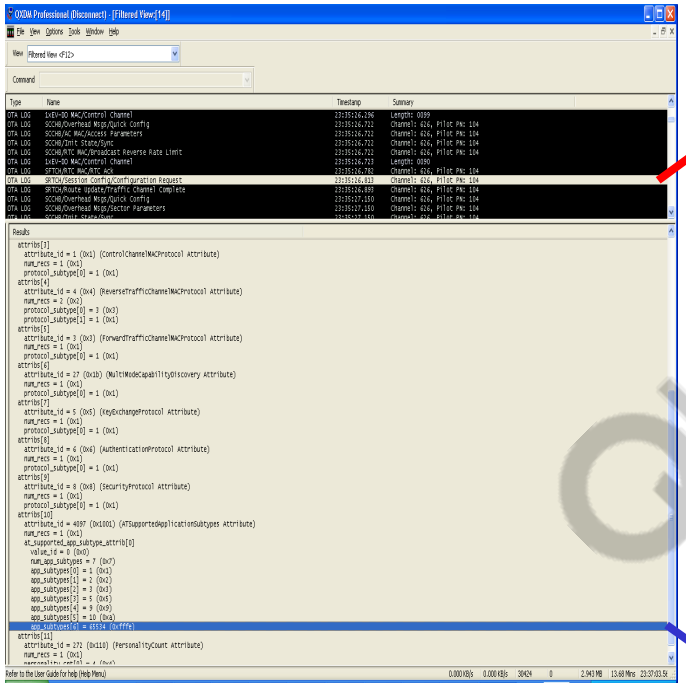
eHRPD Personality Negotiation Call Flow (cont.)



Note: Attributes specific to eHRPD personality are highlighted in red.

eHRPD Personality Negotiation Log

QXDM Log



Session Configuration Request Message

```
OTA LOG     SCCHB/RTC MAC/Broadcast Reverse Rate Limit
OTA LOG     1xEV-DO MAC/Control Channel
OTA LOG     SFTCH/RTC MAC/RTC Ack
OTA LOG     SRTCH/Session Config/Configuration Request
OTA LOG     SRTCH/Route Update/Traffic Channel Complete
OTA LOG     SCCHB/Overhead Msgs/Quick Config
OTA LOG     SCCHB/Overhead Msgs/Sector Parameters
OTA LOG     SCCHB/Init State/Sync
OTA LOG     1xEV-DO MAC/Control Channel
OTA LOG     SRTCH/Session Config/Configuration Request
OTA LOG     SRTCH/Route Update/Traffic Channel Complete
```

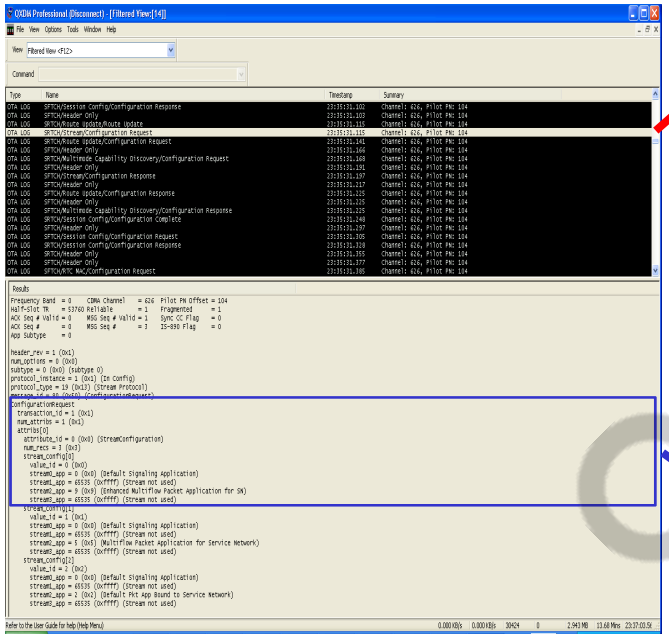
Message body

```
attribs[10]
  attribute_id = 4097 (0x1001) (ATSupportedApplicationSubtypes Attribute)
  num_recs = 1 (0x1)
  at_supported_app_subtype_attrib[0]
    value_id = 0 (0x0)
    num_app_subtypes = 7 (0x7)
    app_subtypes[0] = 1 (0x1)
    app_subtypes[1] = 2 (0x2)
    app_subtypes[2] = 3 (0x3)
    app_subtypes[3] = 5 (0x5)
    app_subtypes[4] = 9 (0x9)
    app_subtypes[5] = 10 (0xa)
    app_subtypes[6] = 65534 (0xfffe)
attribs[11]
  attribute_id = 272 (0x110) (PersonalityCount Attribute)
  num_recs = 1 (0x1)
  personality_cnt[0] = 4 (0x4)
```

Alternate EMPA(0xFFFE) is proposed

eHRPD Personality Negotiation Log (cont.)

QXDM Log



Stream Configuration Request Message

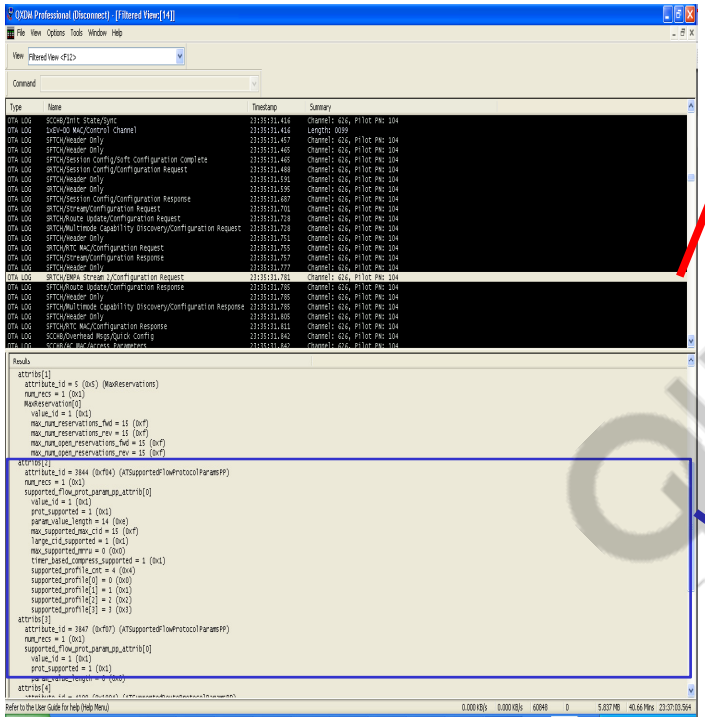
```
OTA LOG     SRTCH/Route Update/Route Update
OTA LOG     SRTCH/Stream/Configuration Request
OTA LOG     SRTCH/Route Update/Configuration Request
OTA LOG     SFTCH/Header Only
OTA LOG     SRTCH/Multimode Capability Discovery/Configuration Request
OTA LOG     SFTCH/Header Only
OTA LOG     SFTCH/Stream/Configuration Response
OTA LOG     SFTCH/Header Only
OTA LOG     SFTCH/Route Update/Configuration Response
```

Message body

```
ConfigurationRequest
  transaction_id = 1 (0x1)
  num_attribs = 1 (0x1)
  attribs[0]
    attribute_id = 0 (0x0) (StreamConfiguration)
    num_recs = 3 (0x3)
    stream_config[0]
      value_id = 0 (0x0)
      stream0_app = 0 (0x0) (Default Signaling Application)
      stream1_app = 65535 (0xffff) (Stream not used)
      stream2_app = 9 (0x9) (Enhanced Multiflow Packet Application for SN)
      stream3_app = 65535 (0xffff) (Stream not used)
```

eHRPD Personality Negotiation Log (cont.)

QXDM Log



EMPA Configuration Request Message

```
OTA LOG     SFTCH/Header Only
OTA LOG     SRTCH/EMPA Stream 2/Configuration Request
OTA LOG     SFTCH/Route Update/Configuration Response
OTA LOG     SFTCH/Header Only
OTA LOG     SFTCH/Multimode Capability Discovery/Configuration Response
OTA LOG     SFTCH/Header Only
OTA LOG     SFTCH/RTC MAC/Configuration Response
OTA LOG     SCCHB/Overhead Msgs/Quick Config
OTA LOG     SCCHB/AC MAC/Access Parameters
OTA LOG     SCCHB/Init State/Sync
OTA LOG     SCCHB/RTC MAC/Broadcast Reverse Rate Limit
OTA LOG     1xEV-DO MAC/Control Channel
OTA LOG     SFTCH/Header Only
OTA LOG     SFTCH/EMPA Stream 2/Configuration Response
```

Message body

```
attribs[2]
  attribute_id = 3844 (0xf04) (ATSupportedFlowProtocolParamsPP)
  num_recs = 1 (0x1)
  supported_flow_prot_param_pp_attrib[0]
    value_id = 1 (0x1)
    prot_supported = 1 (0x1)
    param_value_length = 14 (0xe)
    max_supported_max_cid = 15 (0xf)
    large_cid_supported = 1 (0x1)
    max_supported_mrru = 0 (0x0)
    timer_based_compress_supported = 1 (0x1)
    supported_profile_cnt = 4 (0x4)
    supported_profile[0] = 0 (0x0)
    supported_profile[1] = 1 (0x1)
    supported_profile[2] = 2 (0x2)
    supported_profile[3] = 3 (0x3)
attribs[3]
  attribute_id = 3847 (0xf07) (ATSupportedFlowProtocolParamsPP)
  num_recs = 1 (0x1)
  supported_flow_prot_param_pp_attrib[0]
    value_id = 1 (0x1)
    prot_supported = 1 (0x1)
    param_value_length = 0 (0x0)
```

PPP Session Establishment

REDEFINING MOBILITY

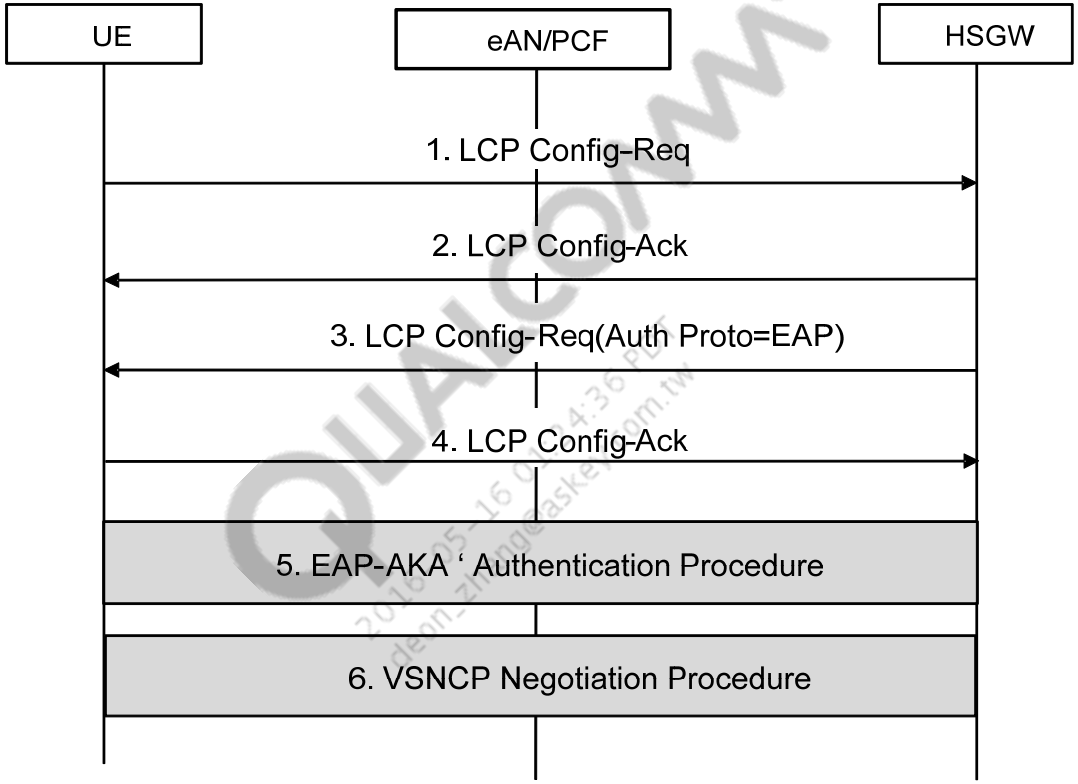
PPP

- PPP session negotiation includes three phases
  - Link establishment negotiation
    - LCP used for establishing, configuring, and testing data-link connection
  - Authentication negotiation
    - Authentication negotiation is mandatory for eHRPD
      - » EAP-AKA' is used as authentication protocol
  - Network-layer protocol negotiation
    - VSNCP is used as network control protocol

LCP Negotiation

- Defined in [S1]
- Protocol number C021
- Most LCP options to be negotiated are same as before
  - Maximum-Receive-Unit (MRU)
  - Async Character Control Map (ACCM)
  - Protocol Field Compression (PFC)
  - Magic Number
  - Address Control Field Compression (ACFC)
- eHRPD-specific changes
  - SN stream
    - EAP (C227) is mandatory authentication protocol for eHRPD

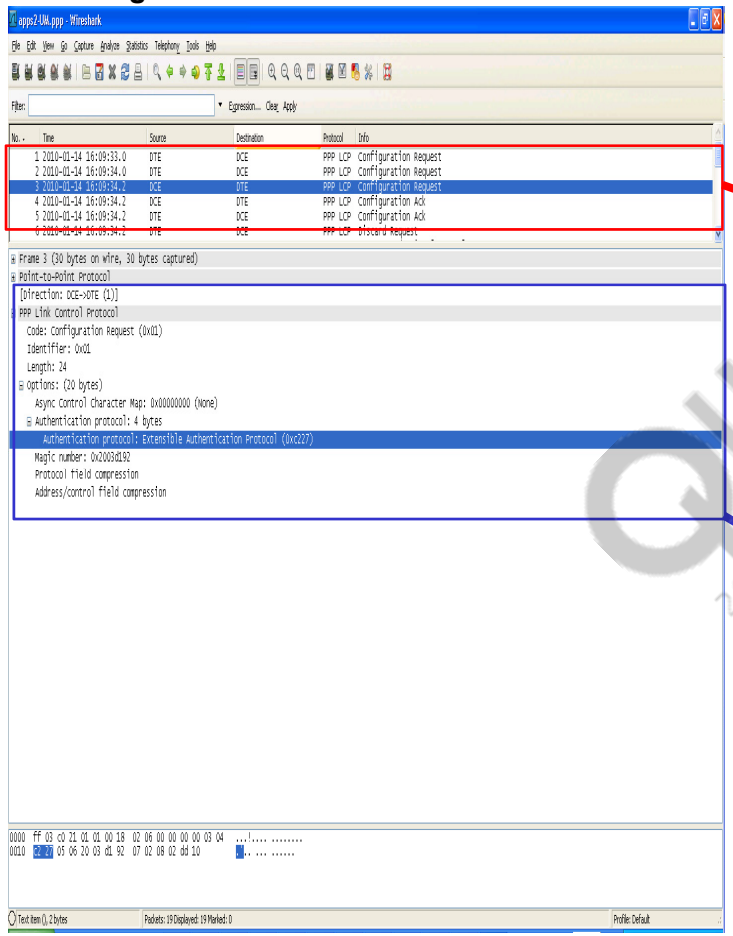
LCP Negotiation Call Flow



Note: In the LCP configuration-request message, the EAP option is proposed by the network HSGW via setting the authentication protocol option to C227.

eHRPD LCP Negotiation Log

PPP Log



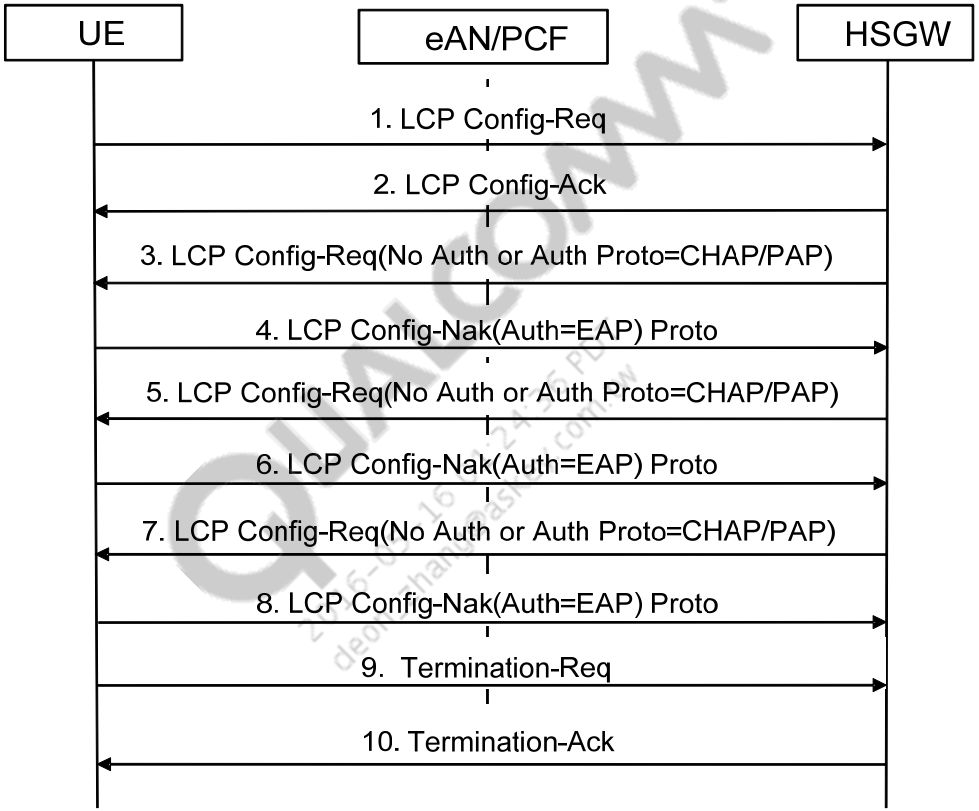
LCP Negotiation Messages

Time	Source	Destination	Protocol	Info	
0.0	DTE	DCE	PPP LC	Configuration Request	1
1.0	DTE	DCE	PPP LC	Configuration Request	
1.2	DCE	DTE	PPP LC	Configuration Request	3
1.2	DCE	DTE	PPP LC	Configuration Ack	2
1.2	DTE	DCE	PPP LC	Configuration Ack	4

LCP Config-Req Message(DCE to DTE)

```
PPP Link Control Protocol
  Code: Configuration Request (0x01)
  Identifier: 0x01
  Length: 24
⊟ Options: (20 bytes)
    Async Control Character Map: 0x00000000 (None)
  ⊟ Authentication protocol: 4 bytes
      Authentication protocol: Extensible Authentication Protocol
    Magic number: 0x2003d192
    Protocol field compression
    Address/control field compression
```

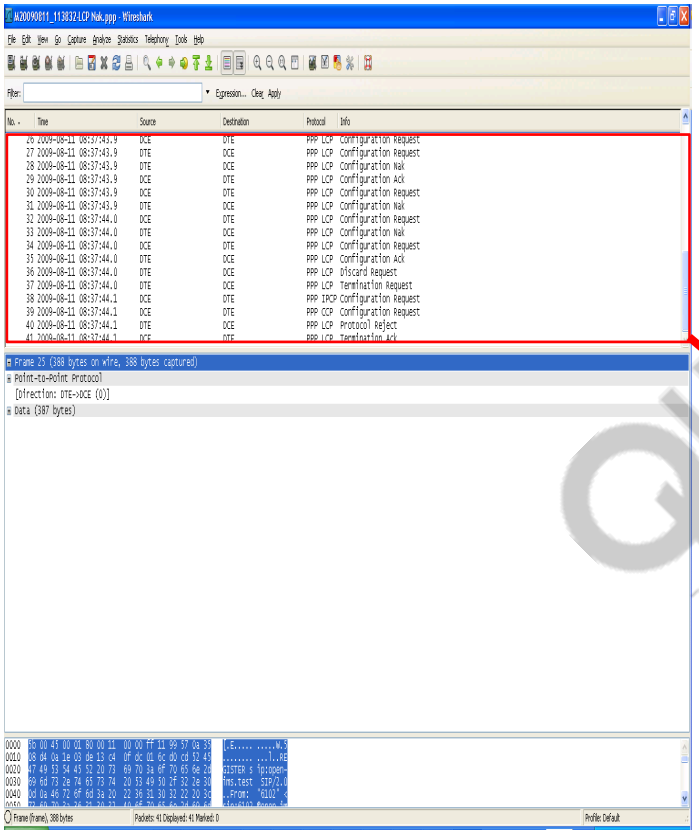
LCP Negotiation Call Flow – Error Scenario



Note: HSGW may not correctly respond with a Cfg-Req with the authentication protocol as EAP. The UE will try NAK-ing a configurable number of times with the EAP before terminating the connection.

LCP Negotiation – Error Scenario Log

PPP Log



LCP Negotiation Messages for error case

Time	Source	Destination	Protocol	Info	
167.3	DCE	DTE	PPP LC	Configuration Request	3
167.3	DTE	DCE	PPP LC	Configuration Request	1
167.3	DTE	DCE	PPP LC	Configuration Nak	4
167.3	DCE	DTE	PPP LC	Configuration Ack	2
167.3	DCE	DTE	PPP LC	Configuration Request	5
167.3	DTE	DCE	PPP LC	Configuration Nak	6
167.4	DCE	DTE	PPP LC	Configuration Request	7
167.4	DTE	DCE	PPP LC	Configuration Nak	8
167.4	DCE	DTE	PPP LC	Configuration Request	
167.4	DTE	DCE	PPP LC	Configuration Ack	
167.4	DTE	DCE	PPP LC	Discard Request	
167.4	DTE	DCE	PPP LC	Termination Request	9
167.5	DCE	DTE	PPP IP	Configuration Request	
167.5	DCE	DTE	PPP CC	Configuration Request	
167.5	DTE	DCE	PPP LC	Protocol Reject	
167.5	DCE	DTE	PPP LC	Termination Ack	10

Authentication Procedures

REDEFINING MOBILITY

Authentication Procedures

- eHRPD UE uses EAP-AKA' for authentication
- EAP
  - Provides authentication framework
  - Allows selection of specific authentication mechanism
    - eHRPD will use EAP-AKA'
- AKA'
  - Provides authentication and session key distribution
  - Uses EAP framework for signaling procedures

EAP

- EAP
  - Defined in [S2]
  - Protocol number C227
- EAP packet type
  - Request (1)
  - Response (2)
  - Success (3)
  - Failure (4)
- EAP Request types
  - Identity (1)
    - Permanent IMSI-based root-NAI for initial authentication
    - Pseudonym-based NAI for subsequent full authentication(s)
    - Reauthentication identity for fast reauthentication
  - EAP-AKA' authentication (50)

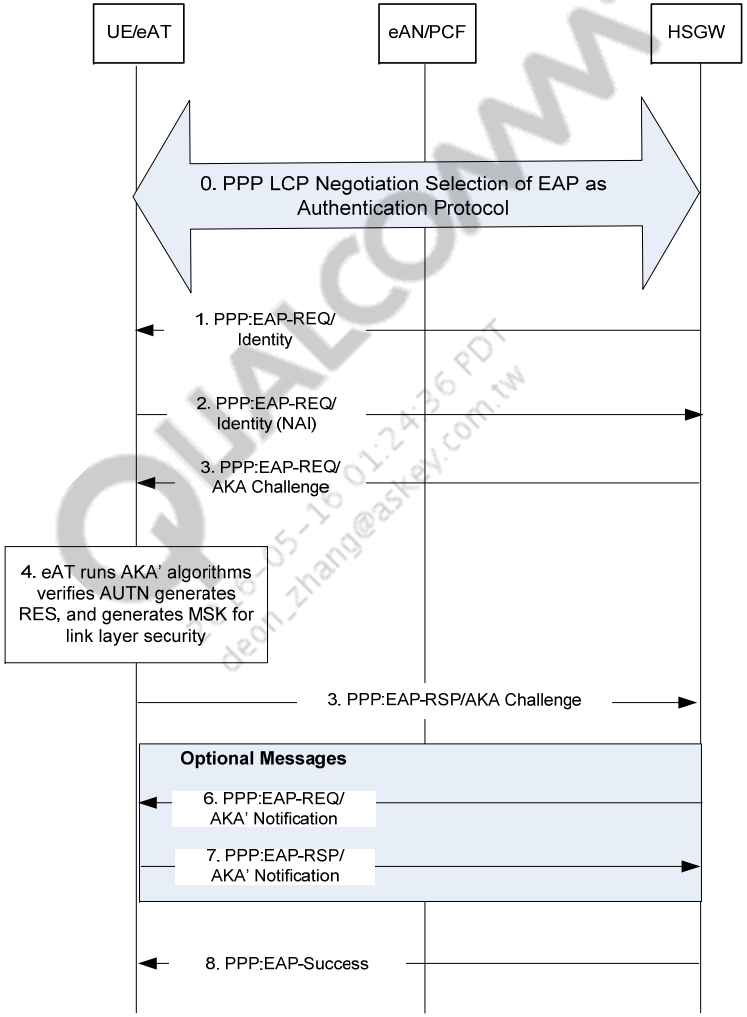
EAP-AKA'

- EAP-AKA'
  - Defined in [S5]
- Message types used in EAP-AKA'
  - Challenge (1)
  - Authentication-Reject (2)
  - Synchronization-Failure (4)
  - Identity (5)
  - Notification (12)
  - Reauthentication (13)
  - Client-Error (14)

EAP-AKA' Authentication Types

- Two types of EAP-AKA' authentication
  - Full authentication
    - Initial authentication will always be full authentication
    - UE and HSGW/AAA must mutually authenticate each other before UE can attach itself to the network
    - Permanent IMSI-based root-NAI is used for full authentication
  - Fast reauthentication
    - Performed only if UE has done full authentication before and received a fast reauthentication ID
    - More efficient as it reduces signaling overhead

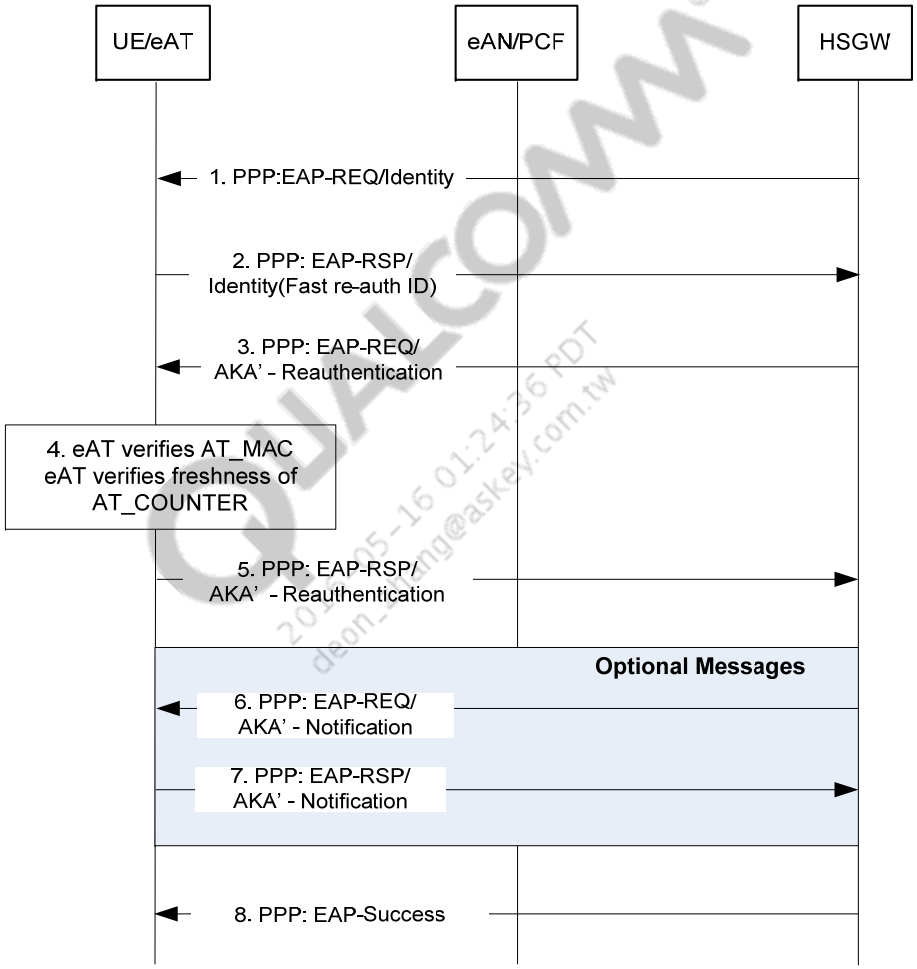
Sample Call Flow of Initial EAP-AKA' Authentication



Sample Call Flow of Initial EAP-AKA' Authentication (cont.)

- Steps are as follows:
  1. EAP is selected as authentication protocol as part of PPP LCP negotiation procedure
  2. HSGW sends EAP-Request/Identity message to UE
  3. UE responds with EAP-Response/Identity (NAI) to HSGW
  4. HSGW sends EAP-Request/AKA'-Challenge to UE
  5. UE runs AKA' algorithms and verifies authentication value (AUTN); if correct, it generates authentication result value (RES) and a Master Session Key (MSK)
  6. UE formats EAP Response/AKA'-Challenge response that contains RES and Message Authentication Code (MAC)
  7. HSGW sends EAP Request/AKA'-Notification to UE (optional)
  8. UE sends EAP Response/AKA'-Notification to HSGW (optional)
  9. HSGW signals EAP-Success to UE

Sample Call Flow of Fast Reauthentication

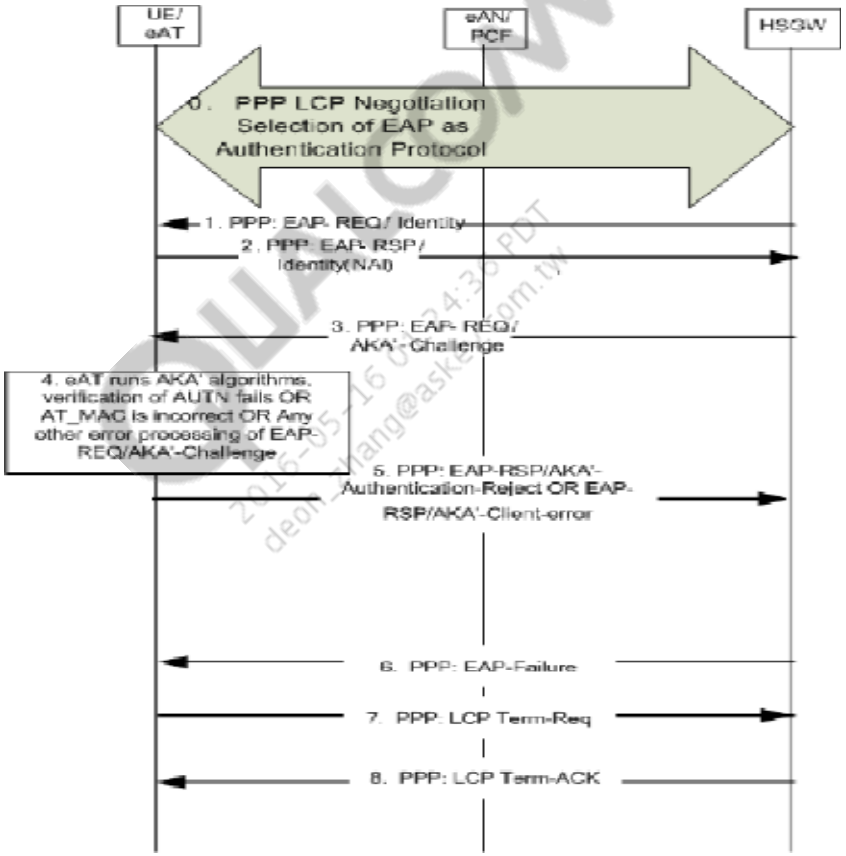


Sample Call Flow of Fast Reauthentication (cont.)

- Steps are as follows:
  1. HSGW sends EAP-Request/Identity message to UE
  2. UE responds with EAP-Response/Identity (fast reauthentication ID) to HSGW
  3. HSGW sends EAP-Request/AKA'-Reauthentication to UE
  4. UE verifies AT_MAC and AT_COUNTER
  5. UE sends EAP Response/AKA'-Reauthentication containing new MAC and AT_COUNTER to HSGW
  6. HSGW sends EAP Request/AKA'-Notification to UE (optional)
  7. UE sends EAP Response/AKA'-Notification to HSGW (optional)
  8. HSGW signals EAP-Success to UE

Sample Failure Scenario Call Flow of Initial EAP-AKA' Authentication

- Authentication vectors from the network are invalid.

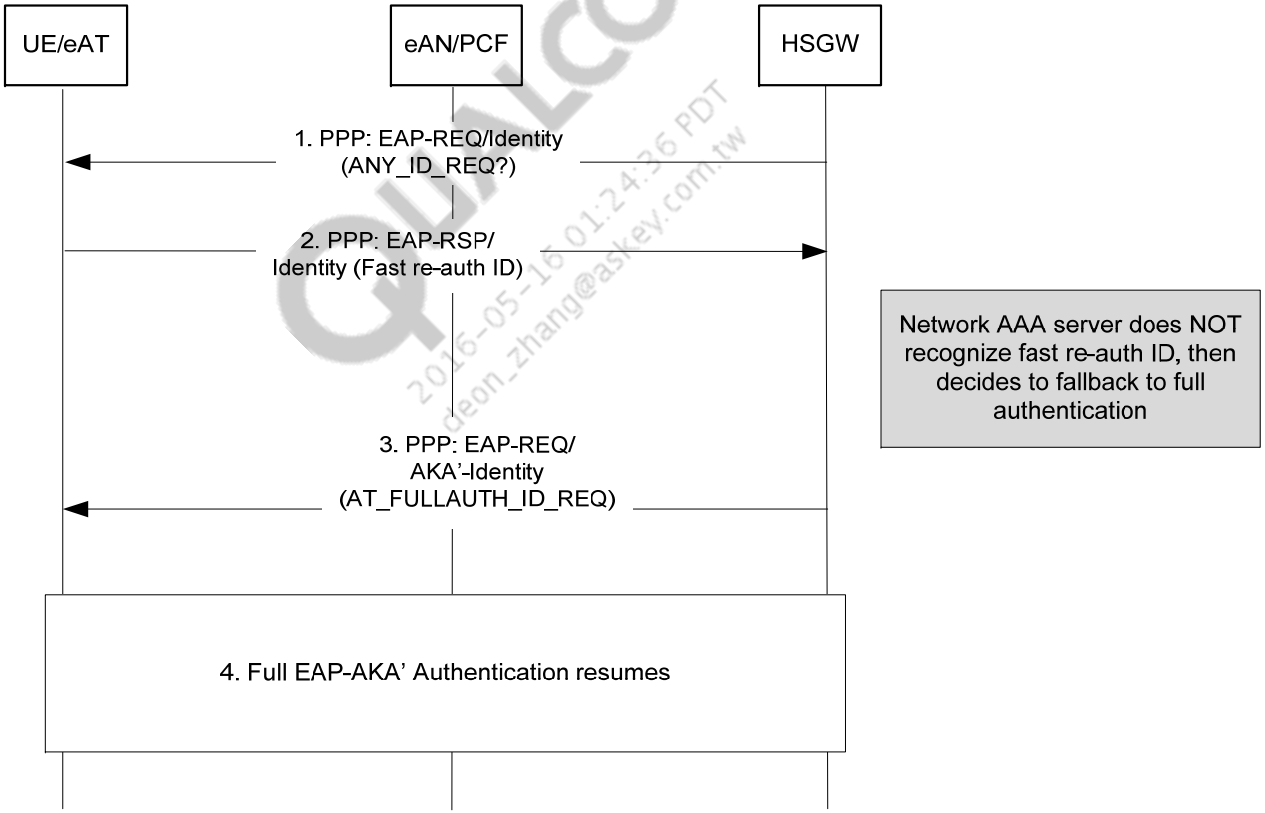


Sample Failure Scenario Call Flow of Initial EAP-AKA' Authentication (cont.)

- Authentication vectors from the network are invalid.
- Steps are as follows:
  4. UE runs AKA' algorithms and verifies authentication vectors to determine if they are invalid
     - If AUTN is invalid, UE creates an EAP-Response/ AKA'-Authentication-Reject packet
     - If AT_MAC failure or failure in any other attributes, UE creates an EAP-Response/AKA' Client-Error packet
  5. UE encapsulates EAP-Response in PPP packet and sends it to HSGW
  6. HSGW sends EAP-Failure to UE
  7. Since authentication has failed, UE terminates PPP session by sending LCP Term-Request to HSGW
  8. HSGW responds with LCP Term-ACK

Sample Call Flow for Fallback to Full Authentication

- Fallback to full authentication due to reauthentication ID is not recognized at EAP server



Sample Call Flow for Fallback to Full Authentication (cont.)

- Fallback to full authentication due to reauthentication ID is not recognized at EAP server
  - Network AAA server – Fast reauthentication ID is sent to EAP server, but EAP server does not recognize it and decides to fall back to full authentication
    3. HSGW sends EAP-Request/AKA' Identity (AT_FULLAUTH_ID_REQ) message to UE
    4. Full EAP-AKA' authentication resumes from this point with UE sending full authentication ID to HSGW

IP Address Management Procedures

REDEFINING MOBILITY

VSNCP Negotiation

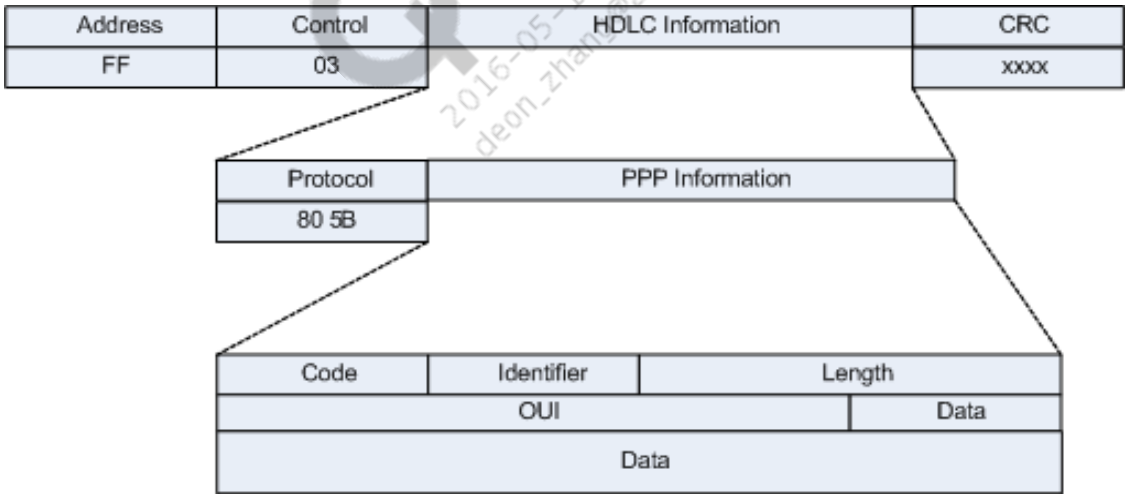
- VSNCP is used to obtain IP address from the PDN
- One-to-one relationship exists between PDN instance and VSNCP instance
- Defined in [S3]
- Protocol number 805B
- VSNCP packet type
  - Configure-Request (1)
  - Configure-Ack (2)
  - Configure-Reject (4)
  - Terminate-Request (5)
  - Terminate-Ack (6)
  - Code-Reject (7)
  - Protocol-Reject (8)

VSNCP Negotiation (cont.)

- Configuration options presented in VSNCP packet
  - PDN-ID – Identify PDN, in the range of 0x00-0x0f
  - Access Point Name (APN)
  - PDN-TYPE – IPv4 or IPv6 or both
  - PDN-ADDRESS
  - PCO – May include DNS address, P-CSCF address
  - ATTACH-TYPE
    - Initial attach does not require PDN IP address
    - PDN IP address is required for handoffs and handover scenarios

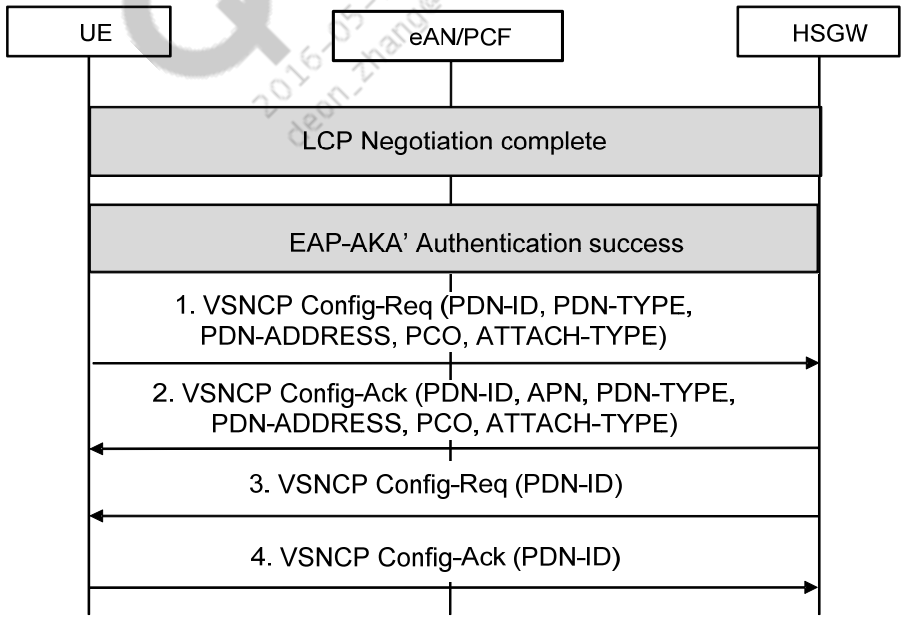
VSNCP Packet Format

- Protocol – 0x805b as defined in [S3]
- Code – VSNCP packet type (i.e., VSNCP Configure-Request)
- Identifier, Length – As defined for LCP
- OUI – 3GPP2 organizationally unique identifier, 0xCF0002
- Data – Zero or more configuration options (i.e., PDN-ID)



VSNCP Negotiation – Sample Call Flow – PDN Context Creation and IP Address Allocation

- Preconditions
  - UE has valid eHRPD session established
  - LCP and authentication phase of PPP are complete
- Triggers
  - Application is activated and requests association with PDN that is not already established

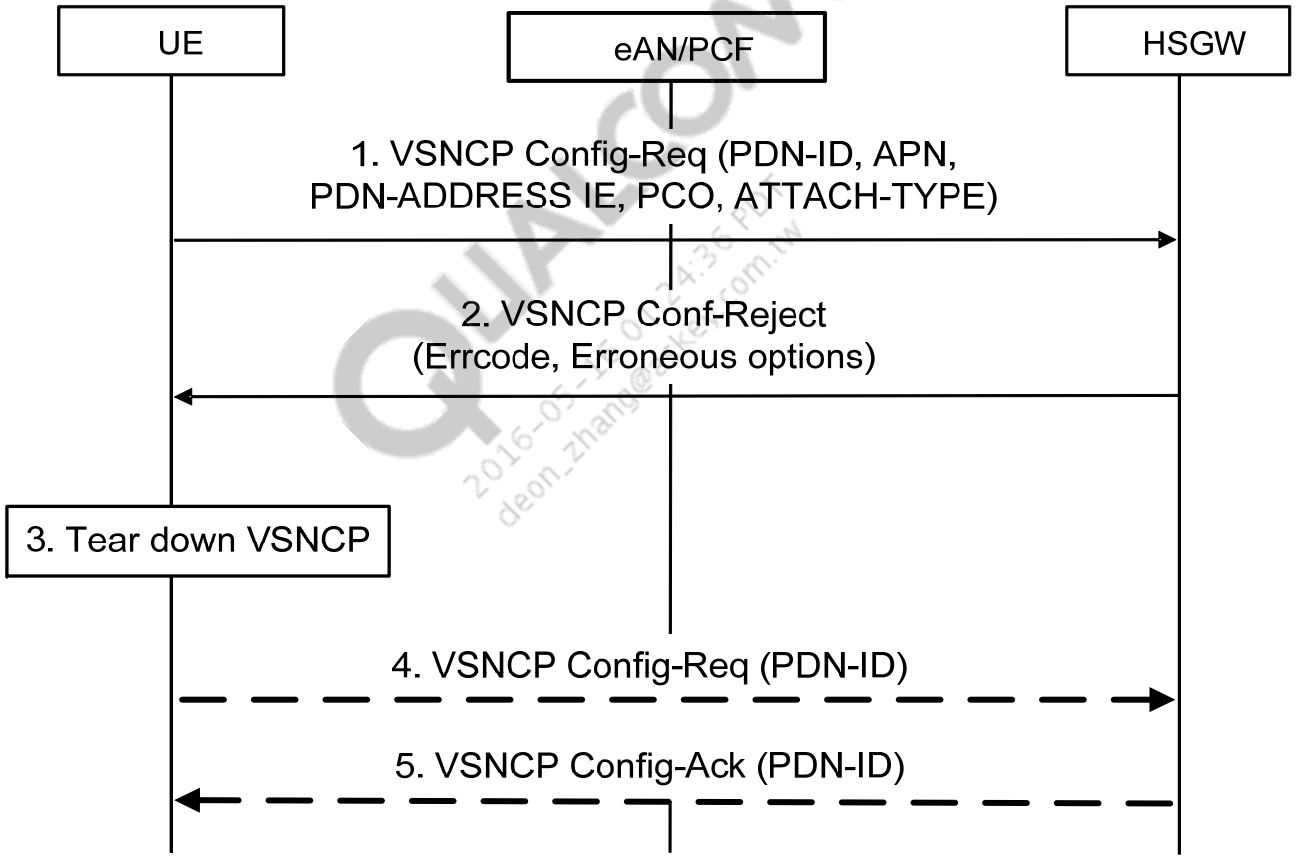


VSNCP Negotiation – Sample Call Flow – PDN Context Creation and IP Address Allocation (cont.)

- Steps are as follows:
  1. The UE sends the VSNCP Config-Req (PDN-ID, APN, PDN Type, PDN Address, PCO, Attach Type) message. The HSGW verifies that the APN provided by the UE is allowed by subscription. Protocol Configuration Options (PCO) are used to transfer parameters between the UE and the P-GW, and are sent transparently through the HSGW.
  2. After the HSGW receives the indication of the completion of PMIP procedures, it sends the VSNCP Config-ACK (PDN-ID, APN, PDN type, PDN Address, PCO, attach type) message to the UE.
  3. The HSGW sends a VSNCP Config-Req message to complete the protocol specified in RFC1661 [S21].
  4. The UE responds with a VSNCP Config-ACK message.

Sample Failure Scenario Call Flow of VSNCP Negotiation

- UE receives VSNCP Config-Reject from HSGW

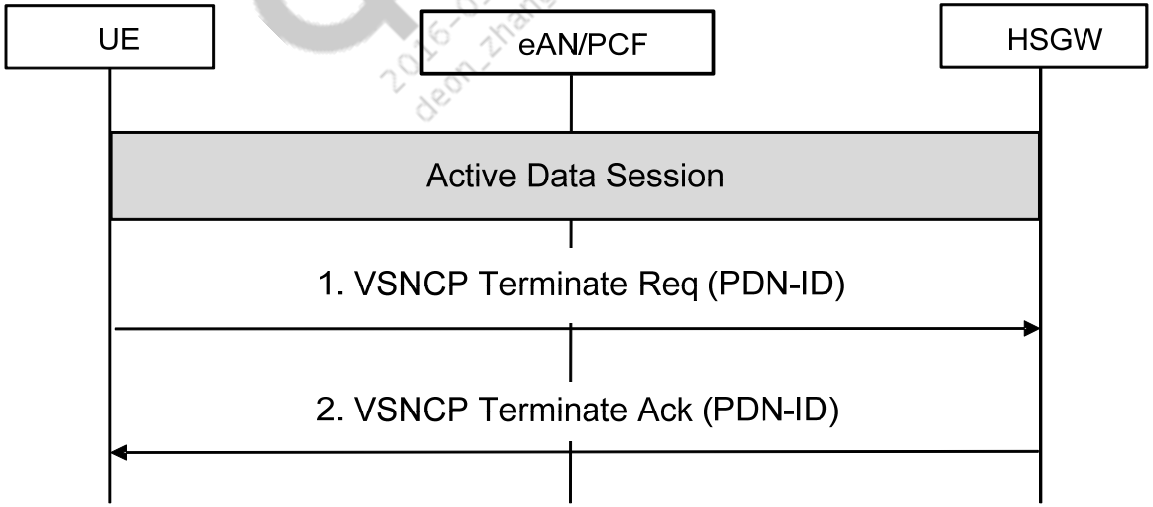


Sample Failure Scenario Call Flow of VSNCP Negotiation (cont.)

- Steps are as follows:
  1. When the UE wants to establish connectivity to a PDN, it sends the VSNCP Config-Req (PDN-ID, APN, PDN Address Allocation, and Protocol Configuration options, Attach Type) message.
  2. The HSGW responds to the request with a VSNCP Config-Reject message to reject specific options within the message.
  3. The UE tears down the VSNCP connection.
  4. If this was the last VSNCP instance, the UE terminates the call by sending an LCP Term-Req.
  5. The HSGW responds with an LCP Term-ACK.

VSNCP Negotiation – Sample Call Flow – PDN Context Release and IP Address Release (UE-Initiated PDN Release)

- Preconditions
  - UE has a valid eHRPD session
  - UE has established PDN context and IP address (IPv4 and IPv6 addresses)
- Triggers
  - Last application using the APN closes



IPv6 Overview

- IPv6 introduces enhancements over IPv4
- Expanded addressing capabilities
  - Larger address space (128 bits vs. 32 bits)
  - Simpler address autoconfiguration
  - Addresses have different scope link, site and global
- Simplified header
  - Some v4 header fields dropped or made optional
  - No header options – Extension headers instead
- Refer to the following documents for further details regarding IPv6:
  - FDD [Q3]
  - IPv6 Overview [Q4]

IPv6 Overview (cont.)

Items	IPv4	IPv6
Address size	32 bits	128 bits
Header size	≥ 20 bytes	40 bytes
Header fields	12	8
Header options	Yes	No (extra header)
Router fragmentation	Yes	No
QoS	TOS field	Class/flow field
Header checksum	Yes	No
Path MTU discovery	Optional	Mandatory (> min)
Minimum MTU	576 bytes	1280 bytes

Multiple PDN Support

REDEFINING MOBILITY

PDN ID Management

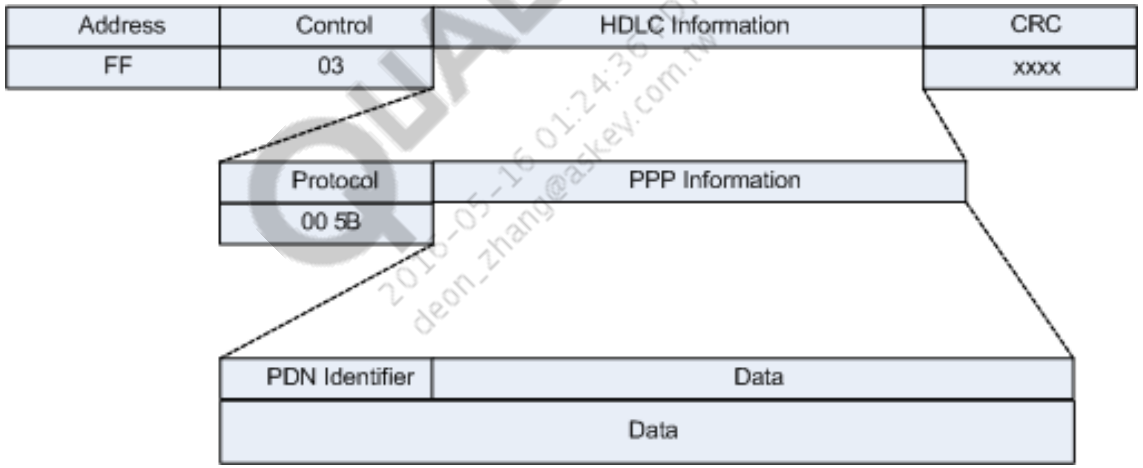
- Unique ID for identifying PDNs
- Internal to AMSS
- One PDN to many application profile IDs mapping
- PDN ID is carried in VSNP protocol

VSNP Support for Multiple PDNs

- UE currently supports up to four PDNs simultaneously
  - PDN multiplexing is supported using VSNP
- VSNP
  - Defined in [S3]
  - Protocol number 005B
  - Runs on top of PPP
  - Carries PDN ID information associated with each packet
  - Supports IPv4 and IPv6

VSNP Packet Format

- Protocol – 0x005b as defined in [S3]
- PDN identifier – PDN identifier of PDN for which user data is sent
- Data – IPv4 or IPv6 datagram



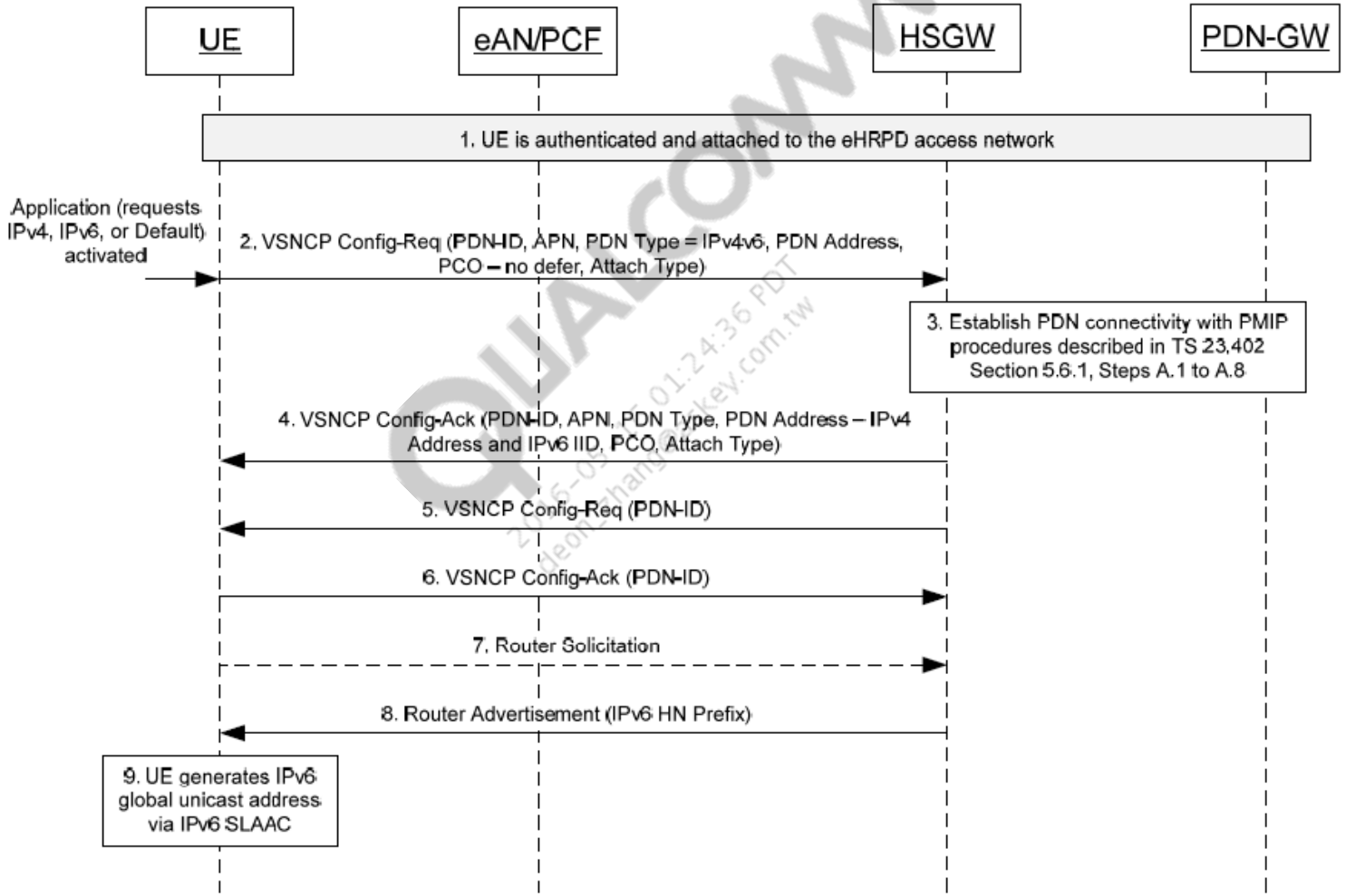
Dual IP Bearer Support

REDEFINING MOBILITY

Dual IP Bearer Support

- Feature allows UE to support IPv4 and IPv6 address assignment over single PDN connection
- IPv4 address and IPv6 IID on single VSNCP signaling message

Sample Call Flow for Dual-IP Address Assignment During PDN Connection Establishment



Sample Call Flow for Dual-IP Address Assignment During PDN Connection Establishment (cont.)

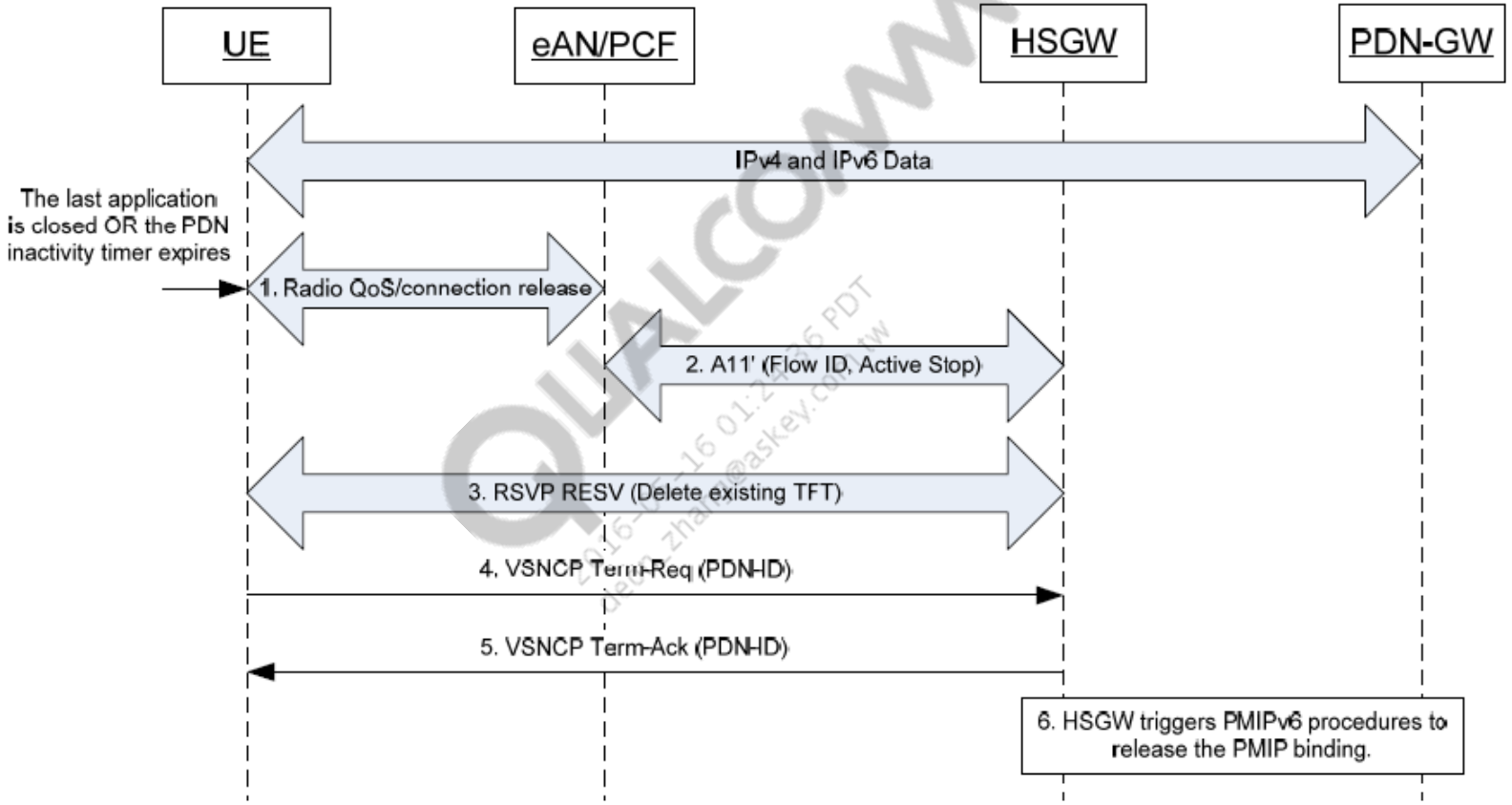
- Steps
  1. UE performed successful authentication and is attached to eHRPD access network.
  2. UE sends VSNCP Configure-Request message over main service connection, including PDN-ID, APN, PDN Type, PDN Address PCO, and Attach Type
  3. HSGW triggers PMIP procedures, as described in TS 23.402, Section 5.6.1, steps A.1 through A.8, inclusive.
  4. HSGW sends VSNCP Config-Ack (PDN-ID, APN, PDN Type, PDN Address, PCO, and Attach Type) message to UE over main service connection, after it receives indication of completion of PMIP procedures.

     UE shall accept both IPv4 address and IPv6 Interface ID. UE shall proceed with IPv6 address generation procedures.
  5. HSGW sends VSNCP Config-Req message to complete protocol specified in RFC 3772.

Sample Call Flow for Dual-IP Address Assignment During PDN Connection Establishment (cont.)

- Steps (cont.)
  6. UE responds with VSNCP Config-Ack message.
  7. UE may send Router Solicitation (RS) message to HSGW via eAN (optional).
  8. HSGW sends IPv6 Router Advertisement message (see RFC 4862) to UE, which includes UE's home network prefix.
  9. UE generates IPv6 global unicast address via IPv6 SLAAC or IPv6 privacy extensions; UE may use interface ID received from step 4 to configure its link to local IPv6 address; UE shall be able to maintain both IPv4 and IPv6 addresses assigned by same PDN-GW in single VSNCP instance.

Sample Call Flow for PDN Context Release (UE-Initiated)



Sample Call Flow for PDN Context Release (UE-Initiated) (cont.)

- Steps
  1. When last application using specified APN is closed or PDN inactivity timer expires, UE/eAN may initiate radio QoS/connection release for connections associated with released PDN.
  2. AN sends A11' Registration Request message to HSGW, indicating removed flow ID.
  3. Steps 3 through 5 occur in parallel with steps 1 and 2; UE sends RSVP RESV message to HSGW to indicate removed flows; HSGW clears TFTs associated with PDN and responds with RESVConf message.
  4. UE sends VSNCP Term-Req message to HSGW; message contains PDN-ID of PDN with which UE is closing connection.
  5. HSGW sends VSNCP Term-Ack to UE to indicate that it received request to terminate connection to PDN.
  6. HSGW triggers PMIPv6 procedures to release PMIP bindings.

QoS

REDEFINING MOBILITY

HRPD QoS Overview

- QoS allows for different application layer requirements to be met via priority settings; specifically, different data flows are conditioned independently of one another so various traffic characteristics, such as jitter, latency, etc., are controlled per flow, rather than flatly across all data.
  - Requires 1xEV-DO Rev A
  - Refer to QoS FDD [Q5]
- HRPD QoS
  - Reservation request
  - RLP configuration
  - RTCMAC configuration
  - Reservation activation
  - Reservation deactivation/teardown

eHRPD QoS Overview

- Changes in reservation label semantics
- Addition of new procedure QoS check
- Change in QoS DSS API
  - Extension of bearer technology change IOCTL to notify registered applications about eHRPD modes of operation

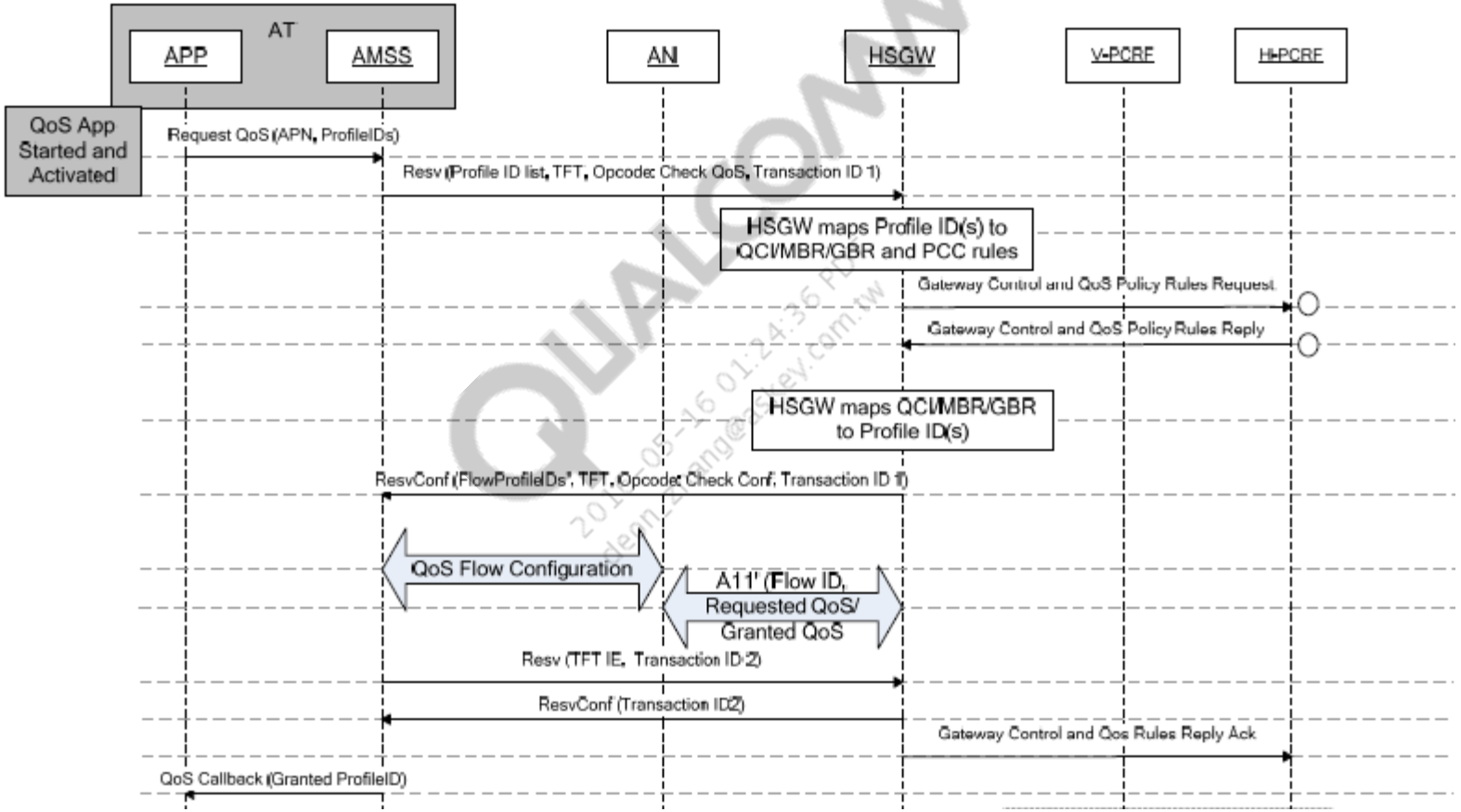
Reservation Label Changes

- Reservation labels used to indicate PDN_ID, i.e., PDN flow association
  - Higher-order 4-bits are PDN_ID
  - Lower-order 4-bits represent reservation label
- 0xFF flow is for BE traffic
  - In this case, higher-order 4-bits do not indicate PDN_ID

QoS Check

- New IE within the RESV message between UE and HSGW
- Purpose of QoS check procedure is to authorize QoS profile-ID and QoS filters, before UE-requested QoS is configured/activated
- Procedure is internally activated using the following methods:
  - By calling either of the following APIs:
    - QoS request
    - QoS modify
    - QoS configure
  - PPP resync occurs within eHRPD system(s)

eHRPD QoS Call Flow



Packet Data Models

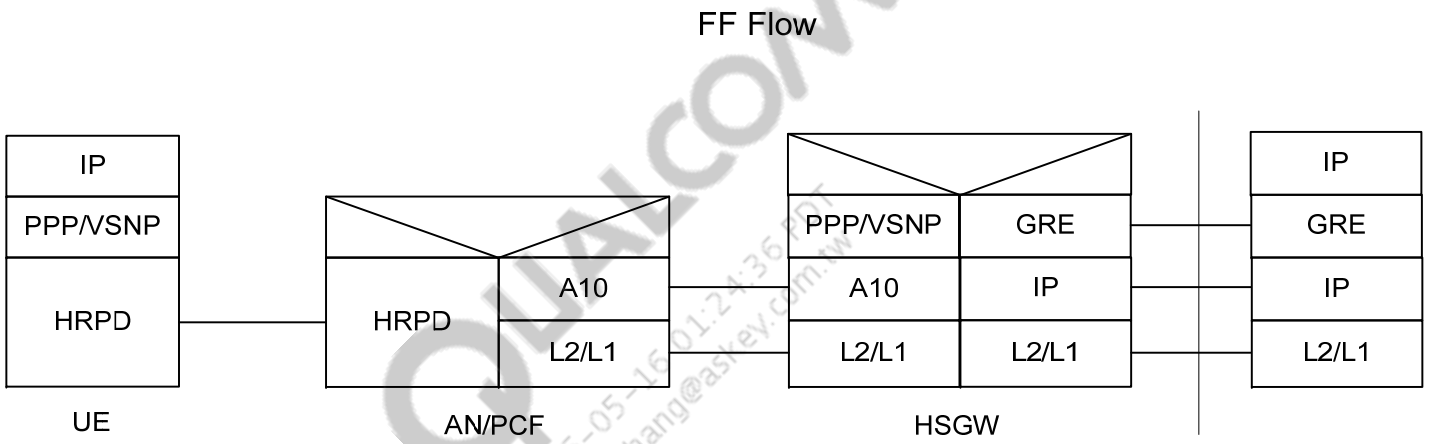
REDEFINING MOBILITY

Packet Data Models

- UE supports
  - Embedded data calls
  - Tethered data calls
    - QMI/RmNet calls
      - » IP mode
      - » Ethernet mode
    - DUN calls will not be supported while UE is operating on eHRPD
- Simultaneous embedded and tethered calls can be supported as long as they are on separate PDN connections
- Two PDN connections with IP or one PDN with dual IP is supported

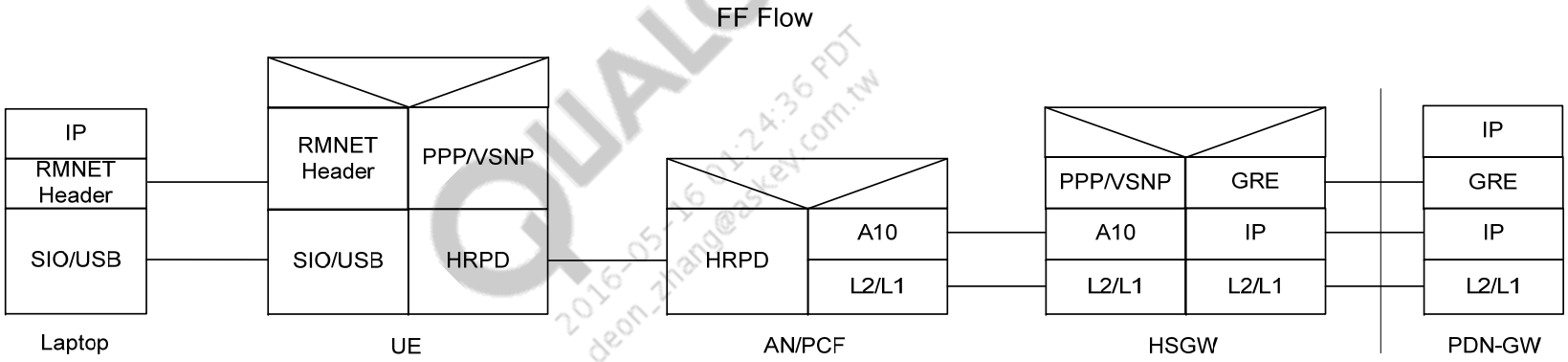
Packet Data Models – Embedded Model

- Packet data model for embedded calls over main BE flow



Packet Data Models – QMI IP Mode

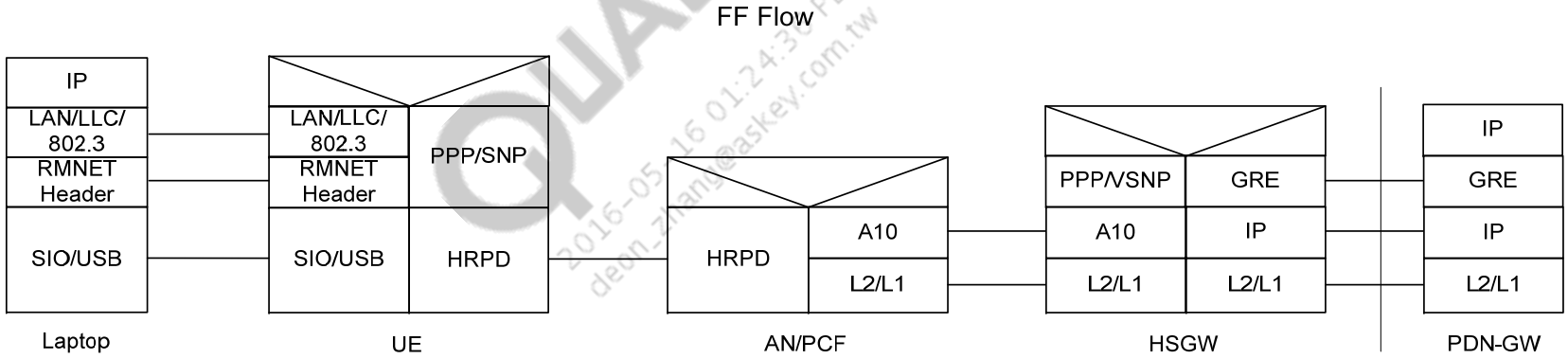
- The QMI/RmNet interface on the laptop receives native IP packets from the application to be transferred to the UE.
- The packets arriving on the UE on the RmNet interface can directly be sent to the HSGW.



- The diagram illustrates the packet data model for QMI-based network model laptop calls in IP mode, over the main BE flow.

Packet Data Models – QMI Ethernet Mode

- IP packets are encapsulated in an Ethernet frame before being handed over to the QMI/RmNet interface.
- Packets arriving on the UE on the RmNet interface must be unframed in the LAN/LLC/802.3 layer from the Ethernet frame, before they are sent to the HSGW.



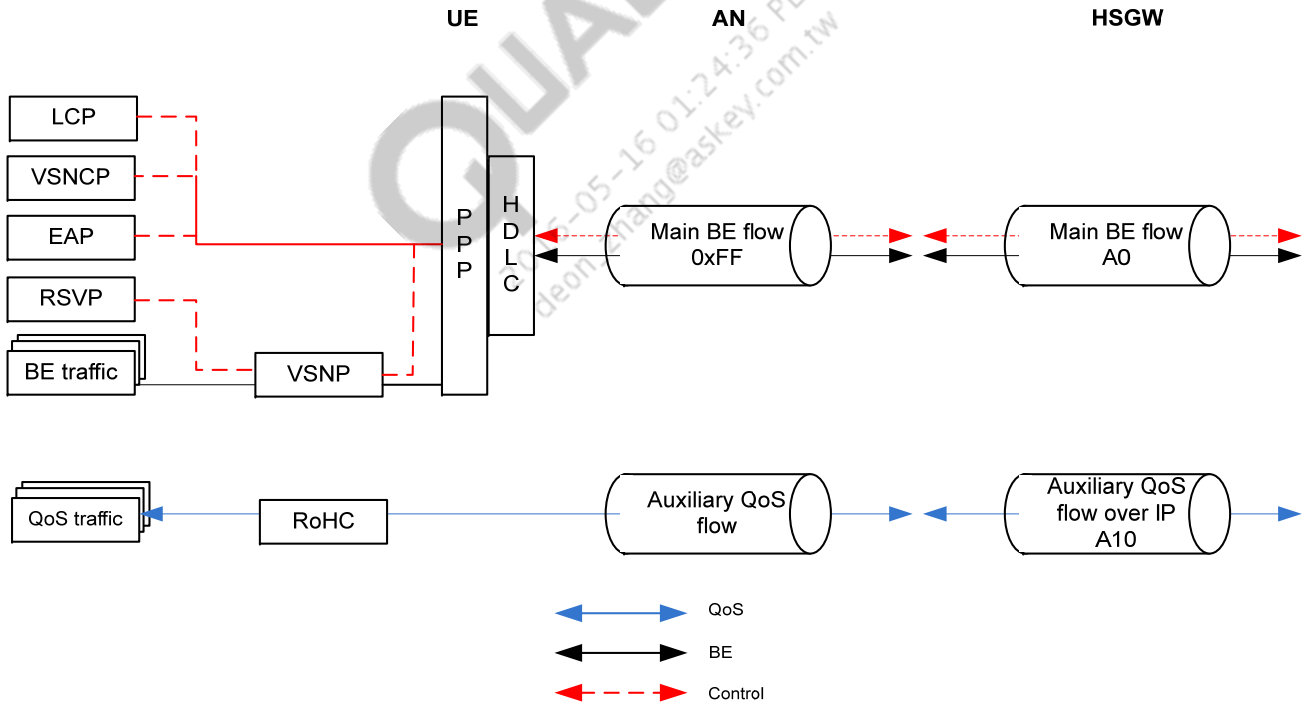
- The diagram illustrates the packet data model for QMI-based network model laptop calls in Ethernet mode, over the main BE flow.

Supported eHRPD Flows

REDEFINING MOBILITY

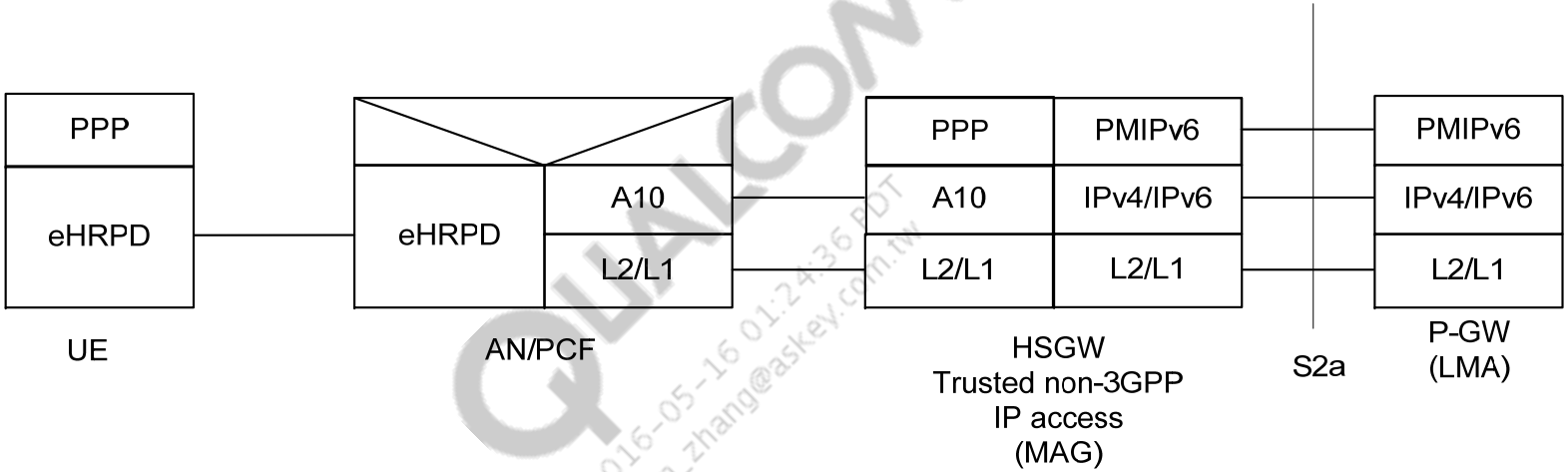
eHRPD Flows

- End-to-end connectivity
- eHRPD modes of operations
  - With PPP – SO59
  - Without PPP – SO67



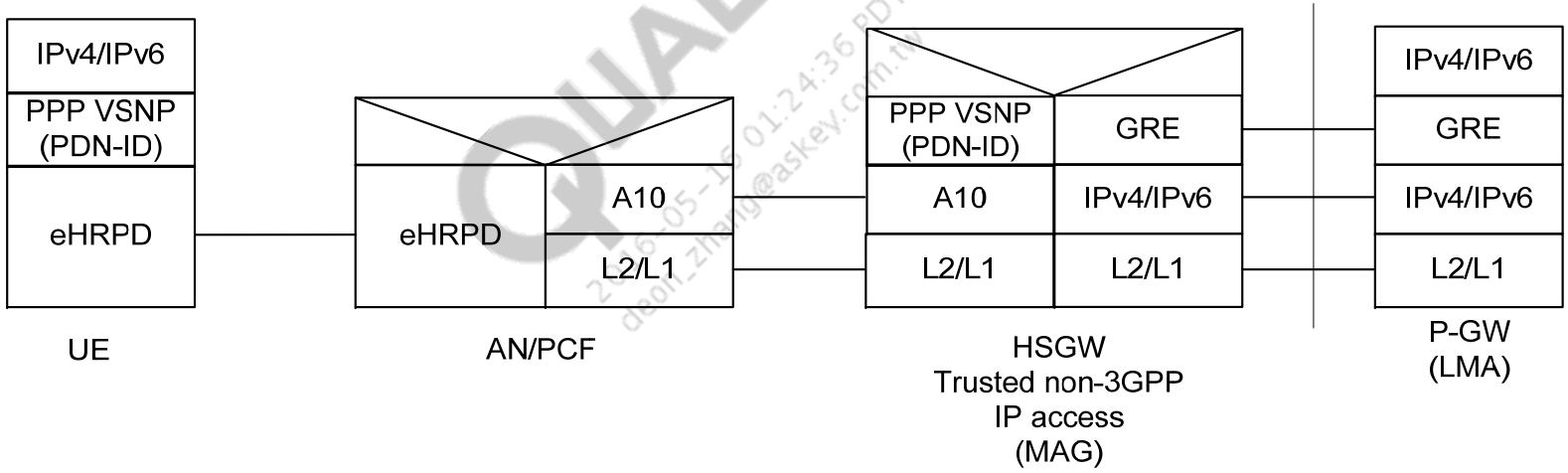
Main Best Effort Flow (0xFF flow) – Control Protocol Stack

- Control signaling uses PPP over main BE flow



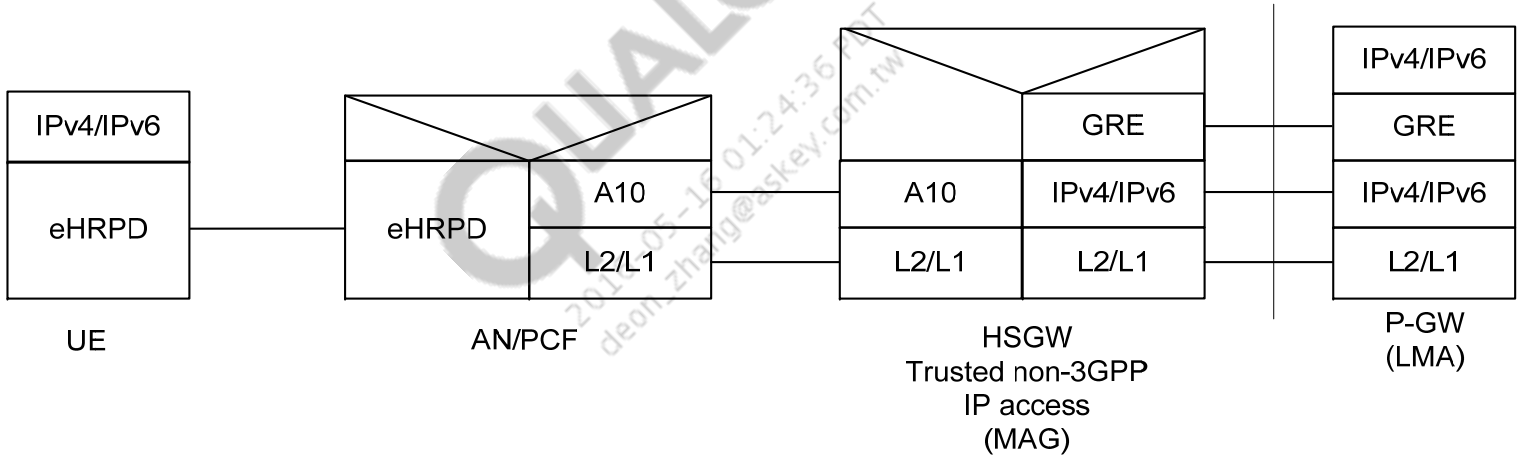
Main Best Effort Flow (0xFF flow) – Data Protocol Stack

- Traffic from different PDNs may share main BE flow
- Packets are separated with PDN-ID within VSNP
- RSVP control signaling is carried as IP traffic, which associates with specific PDN context



Auxiliary QoS Flow – Data Protocol Stack Without PPP

- Real-time traffic (i.e., VoIP) will traverse dedicated service connections and, therefore, not require the addition of explicit PDN-ID information in the payload.



Modifications to Existing Data Services Software Components

REDEFINING MOBILITY

DS Mode Handler Software Components

- DSSNET
  - Added support for multiple PDNs
    - Each PDN has its own DSSNET instance
    - Each DSSNET instance is capable of supporting any of the IP address family, i.e., IPv4 or IPv6
- PS_IFACE
  - eHRPD UE makes use of existing CDMA_SN_IFACE
  - CDMA_SN_IFACE now supports multiple instances to cover multiple PDNs
- One-to-one mapping exists among each instance of DSSNET, PS_IFACE and PDN

DS Mode Handler Software Components (cont.)

- RMSM
  - DUN calls using RMSM are not supported when UE operational mode is eHRPD
  - Instead, eHRPD tethered-data calls will be supported using QMI/RmNet
- ACL
  - ACL related to CDMA_SN_IFACE is updated to facilitate eHRPD interface
- Application profiles
  - eHRPD has new set of application profiles stored on UE EFS, such as
    - APN name, PDN IP version type, RAN type, etc.
  - Default profile
    - Carriers and/or licensees are required to provision the default profile
    - Can be used by legacy applications that do not support application profiles
    - Default profile should have PDN IP version type set to IPv4

DS CDPS Software Components

- PPP
  - VSNP
    - Processing/parsing of messages and preparing responses
  - Multiple VSNCP
    - Processing/parsing of messages and preparing responses
    - Interfaces with Mode Handler (MH) have changed
    - New NCP API is added for configuration-related changes
  - Support M-PDN
    - Currently supports three PDNs
    - Each PDN tied to a type of IP address, i.e., IPv4 or IPv6
- EAP
  - Addition of new authentication framework
    - EAP-AKA' software module delivered in library to customers

Log Mask for eHRPD Data Call Analysis

- Use the QXDM log mask located in the following location for eHRPD data call analysis
  - C:\Documents and Settings\All Users\Documents\Qualcomm\QXDM\Extensions\eHRPD_Data_DMC.dmc

References

Ref.	Document	
Qualcomm		
Q1	*Application Note: Software Glossary for Customers*	CL93-V3077-1
Q2	eHRPD Provisioning Guide	80-VL069-1
Q3	AMSS Support for Internet Protocol Version 6 (IPv6) Feature Description Document	80-VD229-1
Q4	Presentation: IPv6 Overview	80-VA952-1
Q5	Quality of Service (QoS) Feature for 1xEV-DO Revision A	80-VB296-1
Standards		
S1	The Point-to-Point Protocol (PPP)	IETF: RFC 1661
S2	Extensible Authentication Protocol (EAP)	IETF: RFC 3748
S3	Point-to-Point Protocol (PPP) Vendor Protocol	IETF: RFC 3772
S4	Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)	IETF: RFC 4187
S5	Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')	IETF: RFC 5448
S6	E-UTRAN-eHRPD Connectivity and Interworking Core Network Aspects	3GPP2 X.S0057-0

Questions?

https://support.cdmatech.com

REDEFINING MOBILITY