

# Expected Differences Between QCAT Version 4 and QCAT Version 5 Output

80-VB261-1 A

February 14, 2006

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

### **QUALCOMM®** Proprietary

**Restricted Distribution:** This document contains critical information about QUALCOMM products and may not be distributed to anyone that is not an employee of QUALCOMM, its affiliates or subsidiaries without the approval of Configuration Management.

All data and information contained in or disclosed by this document is confidential and proprietary information of QUALCOMM Incorporated and all rights therein are expressly reserved. By accepting this material the recipient agrees that this material and the information contained therein is to be held in confidence and in trust and will not 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 Incorporated.

QUALCOMM Incorporated 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 proprietary information and must be shredded when discarded.

QUALCOMM is a registered trademark and registered service mark of QUALCOMM Incorporated. CDMA2000 is a registered certification mark of the Telecommunications Industry Association, used under license. ARM is a registered trademark of ARM Limited. QDSP is a registered trademark of QUALCOMM Incorporated in the United States and other countries. Other product and brand names may be trademarks or registered trademarks of their respective owners.

Export of this technology may be controlled by the United States Government. Diversion contrary to U.S. law prohibited.

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

# Contents

1 Introduction	4
1.1 Purpose	4
1.2 Scope	4
1.3 Conventions	
1.4 Revision history	4
1.5 References	5
1.6 Technical assistance	5
1.7 Acronyms	
2 QCAT4 vs. QCAT5	6
2.1 General	6
2.2 BT	13
3 Previous QCAT5 vs. Current QCAT5	14
3.1 QCAT5.00.01 vs. QCAT5.01.00	
3.2 QCAT5.01.00 vs. QCAT5.01.01	22
3.3 QCAT5.01.01 vs. QCAT5.02.00	

## **Tables**

Table 1-1	Revision history	4
Table 1-2	Reference documents and standards	5

## 1 Introduction

## 1.1 Purpose

The purpose of this document is to show the Over the Air (OTA) message parser difference between QCAT4 and QCAT5.

## **5** 1.2 Scope

14

15

16

This document provides guidance for testers about the OTA message structure or field naming change. Therefore, testers need to update their automation scripts accordingly.

#### 1.3 Conventions

- Function declarations, function names, type declarations, and code samples appear in a different font, e.g., #include.
- 11 Code variables appear in angle brackets, e.g., <number>.
- Commands and command variables appear in a different font, e.g., copy a:\*.\* b:.\

## 1.4 Revision history

The revision history for this document is shown in Table 1-1.

#### **Table 1-1 Revision history**

Version	Date	Description
Α	Feb 2006	Initial release

80-VB261-1 A QUALCOMM Proprietary

## 1.5 References

3

5

6

9

10

11

12

13

14

Reference documents, which may include QUALCOMM<sup>®</sup>, 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	
QUAL	СОММ	
Q1	Application Note: Software Glossary for Customers	CL93-V3077-1

## 1.6 Technical assistance

For assistance or clarification on information in this guide, submit a Service Request to QUALCOMM CDMA Technologies at <a href="https://support.cdmatech.com/">https://support.cdmatech.com/</a>.

If you do not have access to Internet web browsing, you may send email to <a href="mailto:support.cdmatech@qualcomm.com">support.cdmatech@qualcomm.com</a>.

## 1.7 Acronyms

For definitions of terms and abbreviations, refer to [Q1].

80-VB261-1 A 5 QUALCOMM Proprietary

#### 2.1 General

5

6

24

25

26

37

- New data sections can be preceded by a new infer\_incl field.
- Pretty printing enhancements have been made, but these changes should not affect your tests in any way. However, we have attempted to make this additional data more useful for visual inspection, but not for fixed script use. It is not guaranteed to remain fixed or unchanged.
- Two-line [HI][LO] field conversion into a single 64-bit field.

```
8
          Example of Previous Format:
10
          11
          system_time[HI] = 6 (0x6)
          system_time[LO] = 4116258630 (0xf5591f46)
12
13
          Example of Current Format:
14
          _____
15
          system_time = 0x06f5591f46
16
17
          The LO/HI segments have been combined, and I noticed also that they are only
18
          presented in hex. Would you also like the decimal version?
19
20
          system_time = 29886062406 (0x06f5591f46)
21
22
```

#### **GSM**

■ The GSM RR Signaling Message (System Information Type 6) has the field appended after the se\_6\_rest structure name (this is where FAILED CSN1 PARSE used to be). Two cases will appear as:

```
27
            si 6 rest
28
              padding bits L = 0 (L)
29
30
            and
31
32
            si 6 rest
33
              padding bits H = 1 (H)
              PCH and NCH info
35
                paging channel restructuring
36
```

Some completely new GPRS messages have been added. Other messages have been modified, but we have no log files with the enhanced packet to test against. This document will be updated as soon as data becomes available.

- The Old SILK interpreter would output to strings at the end of a message that are no longer printed by the New SILK interpreter.
  - □ FAILED CSN1 PARSE
  - □ (no CSN.1 output)

1

6

10

12

■ The contents of 0x512F.GSM\_RR\_MANAGEMENT.ASSIGNMENT\_COMMAND.multi\_rate\_conf have been changed as shown below:

```
Old SILK Output
                                              New SILK Output
In File: \perforce\QCAT\TestLogs\Mix_Test3.dlf
Day 354 23:43:23.460 [D2]
                              0x512F GSM RR
                                               Day 354 23:43:23.460 [D2]
                                                                              0x512F GSM RR
Signaling Message
                                               Signaling Message
       Channel Type = DCCH (0)
                                                      Channel Type = DCCH (0)
       Direction = Downlink
                                                      Direction = Downlink
       Message Type = Assignment Command
                                                      Message Type = Assignment Command
(46)
                                               (46)
       Message Length in bytes = 15
                                                      Message Length in bytes = 15
       L3 Message in Hex:
                                                      L3 Message in Hex:
                                                        06 2E 0F 02 CO 00 63 41 03 05 20
         06 2E 0F 02 CO 00 63 41 03 05 20
A4 0D 45 D0
                                               A4 0D 45 D0
                                               Decoded Message:
Decoded Message:
chan_type = 0
                                               chan_{type} = 0 (0x0)
trans_id_or_skip_ind = 0
                                               trans_id_or_skip_ind = 0 (0x0)
prot_disc = 6 (GSM_RR_MANAGEMENT)
                                               prot_disc = 6 (0x6) (GSM_RR_MANAGEMENT)
                                               msg\_type = 46 (0x2e)
msg\_type = 46
prot
                                               prot
  rr man prot
                                                rr man prot
    ASSIGNMENT_COMMAND
                                                  ASSIGNMENT_COMMAND
      first_chan_desc_after
                                                     first_chan_desc_after
                                                       chan_type_tdma_offset = 1 (0x1)
        chan_type_tdma_offset = 1
        timeslot_num = 7
                                                       timeslot_num = 7 (0x7)
        train_seq_code = 0
                                                      train_seq_code = 0 (0x0)
                                                      hopping\_chan = 0 (0x0)
        hopping\_chan = 0
        abs_rf_chan_num = 704 (0x2c0)
                                                       abs_rf_chan_num = 704 (0x2c0)
      multi_rate_conf_incl = 1
                                                     multi_rate_conf_incl = 1 (0x1)
      multi_rate_conf
                                                     multi_rate_conf
        alloc_len = 5
                                                       length = 5 (0x5)
        alloc[0] = 32
                                                       mr_version = 1 (0x1)
        alloc[1] = 164
                                                       ncsb = 0 (0x0)
                                                       icmi = 0 (0x0)
        alloc[2] = 13
                                                       start_mode = 0 (0x0)
        alloc[3] = 69
                                                       multirate_params[0] = 164 (0xa4)
        alloc[4] = 208
                                                       multirate_params[1] = 13 (0xd)
                                                       multirate_params[2] = 69 (0x45)
                                                       . . .
```

80-VB261-1 A 7 QUALCOMM Proprietary

#### **UMTS NAS**

2

The bearer\_cap\_1 structure has been changed, as shown in the following examples:

```
Old SILK Output
                                               New SILK Output
In File: \perforce\QCAT\TestLogs\0x4142_0x4143.dlf
Day 0
      00:00:33.184 [D5]
                              0x713A UMTS
                                               Day 0
                                                       00:00:33.184 [D5]
                                                                              0x713A UMTS
UE OTA
                                               UE OTA
       Message Direction = From UE
                                                       Message Direction = From UE
       NAS OTA Message Contents:
                                                       NAS OTA Message Contents:
chan_type = 0
                                               chan_{type} = 0 (0x0)
trans_id_or_skip_ind = 0
                                               trans_id_or_skip_ind = 0 (0x0)
prot_disc = 3 (GSM_CALL_CONTROL)
                                               prot_disc = 3 (0x3) (GSM_CALL_CONTROL)
                                               msg\_type = 5 (0x5)
msg\_type = 5
prot
                                               prot
  call_ctrl_prot
                                                 call_ctrl_prot
    SETUP
                                                   SETUP
      bc_repeat_ind_incl = 0
                                                     bc\_repeat\_ind\_incl = 0 (0x0)
                                                     bearer_cap_1_incl = 1 (0x1)
      bearer_cap_1_incl = 1
      bearer_cap_1
                                                     bearer_cap_1
        num\_cap = 1
                                                       ext_1 = 1 (0x1)
        cap[0] = 160
                                                       rad_chan_req = 1 (0x1)
      bearer_cap_2_incl = 0
                                                       coding_std = 0 (0x0)
                                                       xfer_mode = 0 (0x0)
                                                       info_xfer_cap = 0 (0x0)
                                                     bearer_cap_2_incl = 0 (0x0)
In File: \perforce\QCAT\TestLogs\0x4142_0x4143.dlf
       00:01:27.908 [2D]
                                                       00:01:27.908 [2D]
                                                                              0x713A UMTS
Day 0
                              0x713A UMTS
                                               Day 0
UE OTA
                                               UE OTA
       Message Direction = From UE
                                                       Message Direction = From UE
       NAS OTA Message Contents:
                                                       NAS OTA Message Contents:
chan_type = 0
                                               chan_type = 0 (0x0)
                                               trans_id_or_skip_ind = 0 (0x0)
trans_id_or_skip_ind = 0
prot_disc = 3 (GSM_CALL_CONTROL)
                                               prot_disc = 3 (0x3) (GSM_CALL_CONTROL)
msg\_type = 5
                                               msg\_type = 5 (0x5)
prot
                                               prot
  call_ctrl_prot
                                                 call_ctrl_prot
    SETUP
                                                   SETUP
      bc_repeat_ind_incl = 0
                                                     bc\_repeat\_ind\_incl = 0 (0x0)
                                                     bearer\_cap\_1\_incl = 1 (0x1)
      bearer_cap_1_incl = 1
      bearer_cap_1
                                                     bearer_cap_1
        num_cap = 3
                                                       ext_1 = 0 (0x0)
        cap[0] = 32
                                                       rad_chan_req = 1 (0x1)
        cap[1] = 0
                                                       coding_std = 0 (0x0)
        cap[2] = 130
                                                       xfer_mode = 0 (0x0)
                                                       info_xfer_cap = 0 (0x0)
      bearer_cap_2_incl = 0
                                                       ext_2 = 0 (0x0)
                                                       coding1 = 0 (0x0)
                                                       ctm = 0 (0x0)
                                                       spare_bit0 = 0 (0x0)
                                                       speech_vers_ind1 = 0 (0x0)
                                                       ext_3 = 1 (0x1)
                                                       coding2 = 0 (0x0)
                                                       spare_bit1 = 0 (0x0)
                                                       speech_vers_ind2 = 2 (0x2)
                                                     bearer_cap_2_incl = 0 (0x0)
```

80-VB261-1 A 8 QUALCOMM Proprietary

- The supp\_codecs\_incl field has been appended to 0x713A.GSM\_CALL\_CONTROL.SETUP
- The emer\_num\_list\_incl field has been appended to 0x713A.GSM\_MOB\_MANAGEMENT.LOCATION\_UPDATE\_ACCEPT
  - The prot\_conf\_opt\_incl field has been appended to 0x713A.GSM\_SM\_MESSAGES.SM\_DEACTIVATE\_PDP\_CONTEXT\_REQUEST
  - The ps\_lcs\_cap\_incl field has been appended to 0x713A.GSM GMM MESSAGES.GMM ATTACH REQUEST
  - Both the net\_feat\_supp\_incl and emer\_num\_list\_incl fields are appended to 0x713A.GSM\_GMM\_MESSAGES.GMM\_ATTACH\_ACCEPT
  - The rad\_pri\_tom8 structure has been added just before rad\_pri\_sms in 0x713A.GSM\_GMM\_MESSAGES.gprs\_mob\_man\_prot.GMM\_ATTACH\_ACCEPT
  - An array of tmsi\_ident[] values has been removed, after num\_tmsi\_ident in
     0x713A.GSM\_GMM\_MESSAGES.GMM\_ROUTING\_AREA\_UPDATE\_REQUEST

#### **HDR**

10

11

12

13

15

17 18

19

20

21

22

23 24

25

26

27

28

29 30 31

32

33

34

35

36 37

38 39

40

41

42

43 44 Additional message header information has been added to the beginning of the HDR signaling output. All fields between header\_rev and subtype (inclusive) are new and can be ignored by older test scripts.

```
Example of Previous Format:
_____
>>> New header info here...See below. <<<
protocol_instance = 0 (0x0) (In Use)
protocol_type = 11 (0xb) (Initialization State Protocol)
init_state
  message_id = 0 (0x0) (Sync)
  sync
    maximum\_revision = 1 (0x1)
    minimum_revision = 1 (0x1)
    pilot_pn = 104 (0x68)
Example of Current Format:
_____
header rev = 1 (0x1)
num_options = 0 (0x0)
subtype = 0 (0x0)
protocol_instance = 0 (0x0) (In Use)
protocol_type = 11 (0xb) (Initialization State Protocol)
message_id = 0 (0x0) (Sync)
init_state
  sync
    maximum\_revision = 1 (0x1)
    minimum_revision = 1 (0x1)
    pilot_pn = 104 (0x68)
```

80-VB261-1 A 9 QUALCOMM Proprietary

message\_id accounting in different modes, PIDs, and MIDs. Lines from either file will have to be smartly read in and skipped or compared depending on the rules and examples specified below. Some structure names are different but unless otherwise stated field name/value pairs will be identical. message\_id is the only field that is known to be out of the old parse order, and it has been swapped only with structure names which, we are told, are ignored by QCT's test environment.

```
6
7
8
```

10

5

```
if ((MID >= 80 and MID <= 84)or((ProtInst=="In
Config")and(PID!=15) and(PID!=5)))
{
    OLK SILK</pre>
```

```
protocol_instance = 1 (0x1) (In Config)
protocol_type = 14 (0xe) (Route Update
Protocol)
route_update
message_id = 80 (0x50)
(ConfigurationRequest)
config_req
}
protocol_instance = 1 (0x1) (In Config)
protocol_type = 14 (0xe) (Route Update Protocol)
message_id = 80 (0x50)
(ConfigurationRequest)
ConfigurationRequest
```

```
11 }
12 else
13 {
```

OLK SILK	NEW SILK
<pre>protocol_instance = 0 (0x0) (In Use)</pre>	<pre>protocol_instance = 0 (0x0) (In Use)</pre>
$protocol\_type = 18 (0x12) (Session$	$protocol\_type = 18 (0x12) (Session$
Configuration Protocol)	Configuration Protocol)
session_config	$message_id = 0 (0x0)$
	(ConfigurationComplete)
$message_id = 0 (0x0)$	session_config
(ConfigurationComplete)	
config_comp	config_comp
}	

14 15

16

17

18

19

20

21

22 23

24

- Structure name differences So far it's a small list, and according to QCT, the tests look at the name/value pairs of fields and do not pay attention to structure names.
- rec\_0[?] and rec\_1[?] in the Configuration Request Message have been reorganized so that they are contained in a recs[?]struct array.
- For any ConfigurationRequest (only found in Route Update In Config, but the test is general) that is a combination of an array of recs with generic value\_id fields is replaced with an array of appropriately named values (the one example found follows).

OLK SILK	NEW SILK
recs[0] value id = 1	override_allowed[0] = 1 (0x1)
value_iu = i	

80-VB261-1 A 10 QUALCOMM Proprietary

2

10 11 12

13 14 Pre-SILK log packet header information has two additional fields.

```
NEW SILK
```

```
22:32:41.408 [35]
                                   0x107C 1xEV Signaling Control Channel
2002 Aug 1
Broadcast -- QuickConfig Msg
                  = 1
                            Chan Num
                                            = 1124
                                                      Pilot PN
                                                                      = 136
  Band
  HSTR
                  = 0
                            Reliable
                                            = 0
                                                     Fragmented
                                                                      = 0
  Ack Seq # Valid = 0
                             Seq # Valid
                                            = 0
                                                      SyncCCFlag
                                                                      = 1
   Ack Seq No
                  = 255
                             Seq No
                                            = 255
                                                      App SubType
                                                                      = 6
  IS890 (TAPP)
                  = 0
```

• For ConfigurationRequests that have their attribute records in arrays of recs or rec\_0 or rec\_1, more appropriate names have been given. Examples are given below.

```
OLK SILK
                                                            NEW SILK
attribute_id = 1
                                            attribute_id = 1
num\_recs = 1
                                            num\_recs = 1
recs[0]
                                            chan_params[0]
                                               value_id = ...
   value_id = ...
                                               pilot_add = ...
   pilot_add = ...
   pilot_compare = ...
                                               pilot_compare = ...
attribute_id = 0
                                            attribute_id = 0
num\_recs = 1
                                            num\_recs = 1
rec_0[0]
                                            power_params[0]
   value_id = ...
                                               value_id = ...
   data_offset_nom = ...
                                               data_offset_nom = ...
attribute_id = 1
                                            attribute_id = 1
num\_recs = 1
                                            num\_recs = 1
                                            rate_params[0]
rec_1[0]
   value_id = ...
                                               value_id = ...
   transition009k6_019k2 = ...
                                               transition009k6_019k2 = ...
```

15 16

17 18 • For ConfigurationResponses that have a num\_recs field, the New SILK removes it; there is only supposed to be one response value\_id per attribute response.

 OLK SILK
 NEW SILK

 attrib[0]
 attrib[0]

 attribute\_id = 1
 attribute\_id = 1 (0x1)

 num\_recs = 1
 value\_id = 1 (0x1)

 attrib value[0] = 1
 value\_id = 1 (0x1)

19

80-VB261-1 A 11 QUALCOMM Proprietary

■ In some cases, field name changes were also necessary. They are listed as follows:

Old SILK Field Name	New SILK Field Name	Conditions
smp_close	smp_close_time	"In Config", PID=16,
		MID=80, AID=255
recs	num_recs	"In Use", PID=18,
		MID=80, AID=All
protocol_type_value	protocol_subtype	"In Use", PID=18,
		MID=80, AID=5,6,8
		(Others?)

Actually, for the lines below, all Config responses are now formatted as an array of attribute\_id/value\_id pairs. For simple attributes, the value\_id contains the actual value. For complex attributes, the value\_id contains just the ID of the agreed upon attribute value. Specific examples found follow below.

DCIOW:		
attrib_value	value_id	"In Config", PID=24,
1 1 55		MID=81, AID=All
ran_handoff	value_id	"In Config", PID=22, MID=81, AID=255
value	value id	"In Use", PID=18,
Value	varac_ra	MID=81, AID=5,6,8
		(Others?)
session_key_length_value	value_id	"In Config", PID=5,
		MID=81, AID=0
ac_auth_key_length	value_id	"In Config", PID=6,
		MID=81, AID=0
<pre>pref_con_chn_cycle</pre>	pref_cc_cycle_attrib	"In Config", PID=12,
		MID=80, AID=0
recs_1	rate_params	"In Config", PID=4,
		MID=80, AID=1

- There is support for additional protocol\_types in the CC\_MAC packets. Specifically, we found bcast\_msgs and packet\_Applications in the MsgPayload structure that will be fully parsed in QCAT5, whereas QCAT4 would stop parsing at MsgPayload. The user normally would never see bcast\_msgs or packet\_Applications, because they were never supported.
- Also, protocol\_type=21 (Stream 1 Application Protocol) has a new subtype=5 (Multi-Flow Packet Application), and the message\_id=20 (DataOverSignalling) is now supported and parsed...message\_id=20 (unknown) is no longer valid.
- protocol\_type =12 (Enhanced Idle State and messag\_id=80(ConfigurationRequest) with a new attribute id (255) is now supported and parsed. attribute\_id=255 (unknown) is no longer valid)

3

8

10

11

12

13

80-VB261-1 A 12 QUALCOMM Proprietary

## 2.2 BT

5

6

8

- The [HI][LO] conversion can be found in the BT output as well. Refer to Section 2.1 for a more detailed description.
- There are a few BT mismatches from the file VariousBlueTooth.txt. It appears, however, that Old SILK is the culprit. It is incorrectly parsing the BT buffer and printing clearly incorrect data. In these cases, we favor using the more correct New SILK output as the master.

OLD SILK NEW SILK cid = 1 (0x1)cid = 1 (0x1) $num\_cmds = 2 (0x2)$  $num\_cmds = 1 (0x1)$ 12cap\_cmd[0] 12cap\_cmd[0] code = 8 (0x8)code = 8 (0x8)12cap\_echo\_request 12cap\_echo\_request identifier = 0 (0x0)identifier = 0 (0x0)length = 1 (0x1)length = 1 (0x1)data[0] = 4 (0x4)data[0] = 4 (0x4)12cap\_cmd[1] code = 3 (0x3)/\* Remaining buffer data "03 04 00 b2 00" is 12cap\_connection\_response left unparsed. \*/ identifier = 4 (0x4)length = 45568 (0xb200) $destination\_cid = 0 (0x0)$  $source\_cid = 64768 (0xfd00)$  $bt_12_result = 52477 (0xccfd) (unknown)$ bt\_12\_status = 52428 (0xcccc) (unknown) Length: 28 Length: Header: 1C 00 4D 10 CC CC 6C 6D C8 36 92 Header: 1C 00 4D 10 CC CC 6C 6D C8 36 92 00 Payload: 0C 00 01 00 08 00 01 00 04 03 04 00 Payload: 0C 00 01 00 08 00 01 00 04 03 04 B2 00 00 00 B2 00 00 00 fd fd cc cc cc

80-VB261-1 A 13 QUALCOMM Proprietary

#### 3.1 QCAT5.00.01 vs. QCAT5.01.00

#### GSM

3

Container in Packet Neighbor Cell Data message or Packet Serving Cell Data message (from fix)

Ocat5.00.01 Ocat5.01.00 MESSAGE TYPE 001101 = 13 (0xd) $MESSAGE_TYPE_001101 = 13 (0xd)$ Packet Serving Cell Data message content Packet Serving Cell Data message content  $PAGE\_MODE = 0 (0x0)$  $PAGE\_MODE = 0 (0x0)$  $const_0 = 0 (0x0)$  $const_0 = 0 (0x0)$ Global TFI Global TFI  $const_0 = 0 (0x0)$  $const_0 = 0 (0x0)$  $UPLINK\_TFI = 0 (0x0)$  $UPLINK\_TFI = 0 (0x0)$ spare = 0 (0x0)spare = 0 (0x0)CONTAINER\_INDEX = 1 (0x1)CONTAINER\_INDEX = 1 (0x1)CONTATNER CONTAINER  $struct0\_count = 2 (0x2)$  $struct0\_count = 2 (0x2)$ struct0[0] struct0[0] PD = 0 (0x0)PD = 0 (0x0) $CD_LENGTH = 3 (0x3)$  $CD\_LENGTH = 3 (0x3)$ CONTAINER\_DATA[0] = 189 (0xbd) CONTAINER\_DATA[0] = 189 (0xbd)CONTAINER\_DATA[1] = 0 (0x0)CONTAINER\_DATA[1] = 0 (0x0)CONTAINER\_DATA[2] = 1 (0x1)CONTAINER\_DATA[2] = 1 (0x1)struct0[1] struct0[1] PD = 0 (0x0)PD = 0 (0x0) $CD_LENGTH = 31 (0x1f)$  $CD_LENGTH_111111 = 31 (0x1f)$ CONTAINER\_DATA[0] = 0 (0x0)container\_data\_count = 14 (0xe) CONTAINER\_DATA[1] = 3 (0x3)CONTAINER\_DATA[0] = 3 (0x3)CONTAINER\_DATA[2] = 16 (0x10)CONTAINER\_DATA[1] = 16 (0x10)CONTAINER\_DATA[3] = 132 (0x84)CONTAINER\_DATA[2] = 132 (0x84)CONTAINER\_DATA[4] = 0 (0x0)CONTAINER\_DATA[3] = 0 (0x0)CONTAINER\_DATA[4] = 0 (0x0)CONTAINER\_DATA[5] = 0 (0x0)CONTAINER\_DATA[6] = 0 (0x0)CONTAINER DATA[5] =  $0 (0 \times 0)$ CONTAINER\_DATA[7] = 0 (0x0)CONTAINER\_DATA[6] = 0 (0x0)CONTAINER\_DATA[8] = 0 (0x0)CONTAINER\_DATA[7] = 0 (0x0)CONTAINER\_DATA[9] = 0 (0x0)CONTAINER\_DATA[8] = 0 (0x0)CONTAINER\_DATA[10] = 4 (0x4)CONTAINER\_DATA[9] = 4 (0x4)CONTAINER\_DATA[10] = 0 (0x0)CONTAINER\_DATA[11] = 0 (0x0)CONTAINER\_DATA[11] = 0 (0x0)CONTAINER\_DATA[12] = 0 (0x0)CONTAINER\_DATA[13] = 0 (0x0)CONTAINER DATA[12] = 0 (0x0) CONTAINER\_DATA[14] = 0 (0x0)CONTAINER\_DATA[13] = 0 (0x0)CONTAINER\_DATA[15] = 0 (0x0)padding bits CONTAINER\_DATA[16] = 0 (0x0)CONTAINER DATA[17] = 0 (0x0)CONTAINER\_DATA[18] = 0 (0x0)CONTAINER\_DATA[19] = 0 (0x0)CONTAINER\_DATA[20] = 0 (0x0)CONTAINER\_DATA[21] = 0 (0x0)CONTAINER\_DATA[22] = 0 (0x0)CONTAINER\_DATA[23] = 0 (0x0)CONTAINER\_DATA[24] = 0 (0x0)

80-VB261-1 A 14 QUALCOMM Proprietary

```
CONTAINER_DATA[25] = 0 (0x0)
     CONTAINER_DATA[26] = 0 (0x0)
      CONTAINER_DATA[27] = 0 (0x0)
     CONTAINER_DATA[28] = 0 (0x0)
      CONTAINER_DATA[29] = 0 (0x0)
     CONTAINER_DATA[30] = 0 (0x0)
 padding bits
Length: 37
                                             Length: 37
Header: 25 00 26 52 00 04 AF AB 13 90 C9
                                             Header: 25 00 26 52 00 04 AF AB 13 90 C9 00
                                             Payload: FF 0D 16 34 00 01 03 BD 00 01 1F 03
Payload: FF 0D 16 34 00 01 03 BD 00 01 1F
                                                      10 84 00 00 00 00 00 04 00 00 00
        10 84 00 00 00 00 00 00 04 00 00
00
        0.0
```

Qcat5.01.00

Payload: FF 0D 0C 34 00 02 07 00 00 00 2B 2B

2B 2B 00

Qcat5.00.01

Payload: FF 0D 0C 34 00 02 07 00 00 00 2B

2B 2B 00

Packet Serving Cell Data message content  $MESSAGE_TYPE_001101 = 13 (0xd)$  $PAGE\_MODE = 0 (0x0)$ Packet Serving Cell Data message content  $PAGE\_MODE = 0 (0x0)$  $const_0 = 0 (0x0)$ Global TFI  $const_0 = 0 (0x0)$ const 0 = 0 (0x0)Global TFI  $UPLINK\_TFI = 0 (0x0)$  $const_0 = 0 (0x0)$ spare = 0 (0x0) $UPLINK\_TFI = 0 (0x0)$ CONTAINER\_INDEX = 2 (0x2)spare = 0 (0x0)CONTAINER\_INDEX = 2 (0x2)CONTAINER  $struct0\_count = 2 (0x2)$ CONTATNER struct0[0]  $struct0\_count = 1 (0x1)$ PD = 0 (0x0)struct0[0]  $CD\_LENGTH = 7 (0x7)$ PD = 0 (0x0)CONTAINER\_DATA[0] = 0 (0x0) $CD\_LENGTH = 7 (0x7)$ CONTAINER\_DATA[0] = 0 (0x0) CONTAINER\_DATA[1] = 0 (0x0)CONTAINER\_DATA[2] = 0 (0x0)CONTAINER\_DATA[1] = 0 (0x0)CONTAINER\_DATA[3] = 43 (0x2b)CONTAINER\_DATA[2] = 0 (0x0)CONTAINER\_DATA[4] = 43 (0x2b)CONTAINER\_DATA[3] = 43 (0x2b)CONTAINER DATA[5] = 43 (0x2b)CONTAINER DATA[4] = 43 (0x2b)CONTAINER\_DATA[6] = 43 (0x2b)CONTAINER\_DATA[5] = 43 (0x2b)CONTAINER\_DATA[6] = 43 (0x2b)struct0[1] PD = 0 (0x0) $spare\_bit0 = 0 (0x0)$  $CD\_LENGTH = 0 (0x0)$  $CD\_LENGTH = 0 (0x0)$ padding bits padding bits Length: 27 Length: 27 Header: 1B 00 26 52 00 3C BE AB 13 90 C9 Header: 1B 00 26 52 00 3C BE AB 13 90 C9 00

3

2В

2

#### PSI1 message (from fix)

Qcat5.00.01 Qcat5.01.00  $MESSAGE\_TYPE\_110001 = 49 (0x31)$  $MESSAGE_TYPE_110001 = 49 (0x31)$ PSI1 message content PSI1 message content distribution\_part\_error\_count = 1024  $PAGE\_MODE = 0 (0x0)$  $PBCCH\_CHANGE\_MARK = 4 (0x4)$  $(0 \times 400)$ Distribution part error =  $PSI\_CHANGE\_FIELD = 0 (0x0)$  $PSI1_REPEAT_PERIOD = 5 (0x5)$  $PSI_COUNT_LR = 3 (0x3)$  $psi\_count\_hr\_present = 1 (0x1)$  $PSI\_COUNT\_HR = 1 (0x1)$ MEASUREMENT\_ORDER = 0 (0x0)GPRS Cell Options 00001010101000000ffff00010105010 NMO = 0 (0x0)T3168 = 0 (0x0)402010106010007070000000101030500 T3192 = 7 (0x7) $DRX\_TIMER\_MAX = 7 (0x7)$  $ACCESS_BURST_TYPE = 0 (0x0)$  $CONTROL\_ACK\_TYPE = 1 (0x1)$  $BS_CV_MAX = 6 (0x6)$  $pan_dec_present = 1 (0x1)$  $PAN_DEC = 1 (0x1)$  $PAN_INC = 2 (0x2)$  $PAN_MAX = 4 (0x4)$  $extension_length_present = 1 (0x1)$ Extension Length = 5(0x5)Extension Information struct egprs\_packet\_channel\_request\_present = 0 (0x0) $PFC_FEATURE_MODE = 0 (0x0)$ DTM SUPPORT = 0 (0x0)BSS\_PAGING\_COORDINATION = 0 (0x0) $CCN\_ACTIVE = 1 (0x1)$  $NW\_EXT\_UTBF = 1 (0x1)$  $spare0\_count = 0 (0x0)$ PRACH Control Parameters  $ACC\_CONTR\_CLASS = 1 (0x1)$ struct0[0]  $MAX_RETRANS = 2 (0x2)$ struct0[1]  $MAX_RETRANS = 2 (0x2)$ struct0[2]  $MAX_RETRANS = 2 (0x2)$ struct0[3]  $MAX_RETRANS = 2 (0x2)$ S = 0 (0x0) $TX_INT = 6 (0x6)$  $option0_present = 0 (0x0)$ PCCCH Organization Parameters  $BS\_PCC\_REL = 0 (0x0)$  $BS_PBCCH_BLKS = 0 (0x0)$  $BS_PAG_BLKS_RES = 10 (0xa)$  $BS_PRACH_BLKS = 0 (0x0)$ Global Power Control Parameters ALPHA = 0 (0x0) $T_AVG_W = 12 (0xc)$  $T_AVG_T = 10 (0xa)$ Pb = 0 (0x0) $PC\_MEAS\_CHAN = 0 (0x0)$  $INT\_MEAS\_CHANNEL\_LIST\_AVAIL = 0 (0x0)$  $N_AVG_I = 2 (0x2)$  $PSI\_STATUS\_IND = 1 (0x1)$  $const_1 = 1 (0x1)$ MSCR = 1 (0x1)SGSNR = 1 (0x1)BAND\_INDICATOR = 0 (0x0)padding bits

80-VB261-1 A 16 QUALCOMM Proprietary

```
Length: 33

Header: 21 00 26 52 00 64 E0 01 14 90 C9

00

Payload: 83 31 12 C4 80 A1 C4 0F D6 95 22

86

00 03 54 0C 14 00 C5 00 5E
```

#### ■ PSI2 message (from fix)

3

```
Qcat5.00.01
                                                                Qcat5.01.00
MESSAGE\_TYPE\_110010 = 50 (0x32)
                                               MESSAGE TYPE 110010 = 50 (0 \times 32)
PSI2 message content
                                               PSI2 message content
  PAGE MODE = 0 (0x0)
                                                 PAGE MODE = 0 (0x0)
  PSI2\_CHANGE\_MARK = 0 (0x0)
                                                 PSI2\_CHANGE\_MARK = 0 (0x0)
  PSI2\_INDEX = 0 (0x0)
                                                 PSI2\_INDEX = 0 (0x0)
  PSI2\_COUNT = 1 (0x1)
                                                 PSI2\_COUNT = 1 (0x1)
  cell_identification_present = 1 (0x1)
                                                 cell_identification_present = 1 (0x1)
                                                 Cell Identification
  Cell Identification
    Location Area Identification IE[0] =
                                                   Location Area Identification IE[0] = 114
                                               (0x72)
114 (0x72)
    Location Area Identification IE[1] =
                                                   Location Area Identification IE[1] = 242
242 (0xf2)
                                               (0xf2)
    Location Area Identification IE[2] = 57
                                                   Location Area Identification IE[2] = 57
(0x39)
                                               (0x39)
    Location Area Identification IE[3] = 0
                                                   Location Area Identification IE[3] = 0
(0x0)
    Location Area Identification IE[4] = 2
                                                   Location Area Identification IE[4] = 2
(0x2)
                                               (0x2)
    RAC = 1 (0x1)
                                                   RAC = 1 (0x1)
    Cell Identity IE[0] = 0 (0x0)
                                                   Cell Identity IE[0] = 0 (0x0)
                                                   Cell Identity IE[1] = 64 (0x40)
    Cell Identity IE[1] = 64 (0x40)
                                                 non\_gprs\_cell\_options\_present = 1 (0x1)
  non_gprs_cell_options_present = 1 (0x1)
  Non GPRS Cell Options
                                                 Non GPRS Cell Options
    ATT = 1 (0x1)
                                                   ATT = 1 (0x1)
    t3212\_present = 1 (0x1)
                                                   t3212\_present = 1 (0x1)
    T3212 = 0 (0x0)
                                                   T3212 = 0 (0x0)
    NECI = 0 (0x0)
                                                   NECI = 0 (0x0)
    PWRC = 0 (0x0)
                                                   PWRC = 0 (0x0)
                                                   DTX = 2 (0x2)
    DTX = 2 (0x2)
    RADIO-LINK-TIMEOUT = 3 (0x3)
                                                   RADIO-LINK-TIMEOUT = 3 (0x3)
    BS-AG-BLKS-RES = 1 (0x1)
                                                   BS-AG-BLKS-RES = 1 (0x1)
    CCCH-CONF = 1 (0x1)
                                                   CCCH-CONF = 1 (0x1)
    BS-PA-MFRMS = 2 (0x2)
                                                   BS-PA-MFRMS = 2 (0x2)
    MAX-RETRANS = 2 (0x2)
                                                   MAX-RETRANS = 2 (0x2)
    TX-INTEGER = 15 (0xf)
                                                   TX-INTEGER = 15 (0xf)
                                                   EC = 0 (0x0)
    EC = 0 (0x0)
    MS-TXPWR-MAX-CCCH = 6 (0x6)
                                                   MS-TXPWR-MAX-CCCH = 6 (0x6)
    extension_length_present = 1 (0x1)
                                                   extension_length_present = 1 (0x1)
    Extension Length = 1 (0x1)
                                                   Extension Length = 1 (0x1)
                                                   Extension Information struct
    Extension Information struct
      ECSC = 1 (0x1)
                                                     ECSC = 1 (0x1)
      3G ECSR = 0 (0x0)
                                                     3G ECSR = 0 (0x0)
      spare0\_count = 0 (0x0)
                                                     spare0\_count = 0 (0x0)
  Reference Frequency Lists
                                                 Reference Frequency Lists
    struct0\_count = 0 (0x0)
                                                   struct0\_count = 0 (0x0)
    const_0 = 0 (0x0)
                                                   const_0 = 0 (0x0)
  Cell Allocation
                                                 Cell Allocation
    struct0\_count = 1 (0x1)
                                                   struct0\_count = 1 (0x1)
    const_0 = 0 (0x0)
                                                   struct0[0]
  GPRS Mobile Allocations
                                                     const_1 = 1 (0x1)
    struct0\_count = 0 (0x0)
                                                     Cell Allocation struct
    const_0 = 0 (0x0)
                                                       RFL_NUMBER = 0 (0x0)
                                                    const_0 = 0 (0x0)
  PCCCH Description
                                                 GPRS Mobile Allocations
    struct0 count = 1 (0x1)
    const_0 = 0 (0x0)
                                                   struct0\_count = 0 (0x0)
  const_1 = 1 (0x1)
                                                   const_0 = 0 (0x0)
  compact_control_information_present = 0
                                                 PCCCH Description
                                                   struct0\_count = 1 (0x1)
  additional_psi_messages_present = 0 (0x0)
                                                   struct0[0]
```

80-VB261-1 A 17 QUALCOMM Proprietary

```
padding bits
                                                    const_1 = 1 (0x1)
                                                    PCCCH Description struct
    const_0 = 0 (0x0)
    spare_padding0_count = 0 (0x0)
                                                      TSC = 1 (0x1)
                                                      const_0 = 0 (0x0)
                                                      Non-hopping PCCCH carriers
                                                        struct0\_count = 1 (0x1)
                                                        struct0[0]
                                                          const_1 = 1 (0x1)
                                                          Non-Hopping PCCCH Carriers
                                              struct
                                                            ARFCN = 525 (0x20d)
                                                            TIMESLOT\_ALLOCATION = 8 (0x8)
                                                        const_0 = 0 (0x0)
                                                  const_0 = 0 (0x0)
                                                const_1 = 1 (0x1)
                                                compact_control_information_present = 0
                                                additional_psi_messages_present = 0 (0x0)
                                                padding bits
                                                  const_0 = 0 (0x0)
                                                  spare_padding0_count = 0 (0x0)
Length: 36
                                              Length: 36
Header: 24 00 26 52 00 0C A1 02 14 90 C9
                                              Header: 24 00 26 52 00 0C A1 02 14 90 C9 00
                                              Payload: 83 32 15 C8 01 B9 79 1C 80 01 00 80
Payload: 83 32 15 C8 01 B9 79 1C 80 01 00
                                                       20 70 02 32 55 E3 41 90 25 83 42
         20 70 02 32 55 E3 41 90 25 83 42
80
```

#### Output format of undefined msg (from standard upgrade)

2

Qcat5.00.01	Qcat5.01.00
bits0 = 0 (0x0)	Unknown downlink message type = 0 (0x0)
Default downlink message content	downlink_message_count = 22 (0x16)
$PAGE\_MODE = 0 (0x0)$	Downlink message[0] = $0 (0x0)$
bits0_count = 176 (0xb0)	Downlink message[1] = $0 (0x0)$
bits0 =	Downlink message[2] = $0 (0x0)$
$0 \times 000010100040000000000000000000000000$	Downlink message[3] = $64 (0x40)$
	Downlink message[4] = $64 (0x40)$
	Downlink $message[5] = 1 (0x1)$
	Downlink message[6] = $0 (0x0)$
	Downlink message[7] = $0 (0x0)$
	Downlink message[8] = $0 (0x0)$
	Downlink message[9] = $0 (0x0)$
	Downlink message[10] = 0 $(0x0)$
	Downlink message[11] = $0 (0x0)$
	Downlink message[12] = $0 (0x0)$
	Downlink message[13] = $0 (0x0)$
	Downlink message[14] = $0 (0x0)$
	Downlink message[15] = $0 (0x0)$
	Downlink message[16] = $0 (0x0)$
	Downlink message[17] = $0 (0x0)$
	Downlink message[18] = $0 (0x0)$
	Downlink message[19] = $0 (0x0)$
	Downlink message[20] = $0 (0x0)$
	Downlink message[21] = $0 (0x0)$
Length: 35	Length: 35
Header: 23 00 2C 52 00 00 1F A3 9C 08 00 00	Header: 23 00 2C 52 00 00 1F A3 9C 08 00
Payload: 00 00 00 01 01 00 04 00 00 00 00	00
00 00 00 00 00 00 00 00 00 00	Payload: 00 00 00 01 01 00 04 00 00 00
	00
	00 00 00 00 00 00 00 00 00 00

80-VB261-1 A 18 QUALCOMM Proprietary

#### HDR

2

8

- New messages and attribute IDs from Rel A 2.0 (from standard update); for example, attribute\_id = 5634 (0x1602) (T2PTransFuncNN) in Subtype 3 Reverse Traffic Channel MAC Protocol is recognized by qcat5.01.00
- SectorParameters message in Overhead Messages Protocol (mid = 1, pid =15)
- Existing field name change and adding new fields

```
Qcat5.00.01
                                                                 Qcat5.01.00
header rev = 1 (0x1)
                                               header_rev = 1 (0x1)
num\_options = 0 (0x0)
                                               num\_options = 0 (0x0)
subtype = 0 (0x0)
                                               subtype = 0 (0x0)
protocol_instance = 0 (0x0) (In Use)
                                               protocol_instance = 0 (0x0) (In Use)
protocol_type = 15 (0xf) (Overhead Messages
                                               protocol_type = 15 (0xf) (Overhead Messages
                                               Protocol)
message_id = 1 (0x1) (SectorParameters)
                                               message_id = 1 (0x1) (SectorParameters)
ovhd msgs
                                               ovhd_msgs
  sec_parms
                                                 sec_parms
  reverse_link_silence_dur = 0 (0x0)
                                                 reverse_link_silence_duration = 0 (0x0)
  reverse_link_silence_per = 3 (0x3)
                                                 reverse_link_silence_period = 3 (0x3)
  infer_incl = 1 (0x1)
                                                 infer_incl4 = 1 (0x1)
  route\_update\_trig\_color\_incl = 0 (0x0)
                                                 ext\_chan\_incl = 0 (0x0)
  infer_incl2 = 1 (0x1)
                                                 infer_incl5 = 1 (0x1)
                                                 hash\_chan\_mask\_incl = 0 (0x0)
  PriorSessionGAUP = 0 (0x0)
  infer_incl3 = 1 (0x1)
                                                 infer_incl = 1 (0x1)
  fpdch\_supported\_incl = 0 (0x0)
                                                 route_update_trig_color_incl = 0 (0x0)
                                                 infer_incl2 = 1 (0x1)
                                                 PriorSessionGAUP = 0 (0x0)
                                                 infer_incl3 = 1 (0x1)
                                                 fpdch\_supported\_incl = 0 (0x0)
                                               Length:
                                                        87
Length:
         87
Header:
         57 00 7C 10 40 04 B9 4A 17 69 95
                                               Header:
                                                        57 00 7C 10 40 04 B9 4A 17 69 95 00
                                               Payload: 00 72 02 68 00 00 00 00 FF FF 01 0F
Payload: 00 72 02 68 00 00 00 00 FF FF 01
                                                         01 00 10 00 00 00 00 00 00 00 00
          01 00 10 00 00 00 00 00 00 00 00
                                                         00 00 00 00 00 07 16 80 00 11 1D
                                               ΑO
          00 00 00 00 00 07 16 80 00 11 1D
                                                         B3 1F D5 00 00 DC 40 60 A9 B0 E0
                                               74
Α0
          B3 1F D5 00 00 DC 40 60 A9 B0 E0
                                                         3C 1F 10 08 44 42 31 20 94 4C 27
74
                                               14
          3C 1F 10 08 44 42 31 20 94 4C 27
                                                         0A 45 42 B1 60 B4 5C 2F 00 00 02
                                               0.0
14
          0A 45 42 B1 60 B4 5C 2F 00 00 02
                                                         13 E8 00
0.0
          13 E8 00
```

80-VB261-1 A 19 QUALCOMM Proprietary

- DOS message in Multi-Flow Packet Application protocol (mid =20 and pid =21)
- rlpflow field is removed (from standard update)

Qcat5.00.01	Qcat5.01.00
header_rev = 1 (0x1)	header_rev = 1 (0x1)
$num\_options = 0 (0x0)$	num_options = 0 (0x0)
subtype = 5 (0x5)	subtype = 5 (0x5)
<pre>protocol_instance = 0 (0x0) (In Use)</pre>	<pre>protocol_instance = 0 (0x0) (In Use)</pre>
<pre>protocol_type = 21 (0x15) (Multi-Flow</pre>	<pre>protocol_type = 21 (0x15) (Multi-Flow Packet</pre>
Packet Application (Service Network))	Application (Service Network))
<pre>message_id = 20 (0x14) (DataOverSignalling)</pre>	message_id = 20 (0x14) (DataOverSignalling)
packet_Applications	packet_Applications
dos	dos
rlpflow = 0 (0x0)	$ack\_required = 0 (0x0)$
$ack\_required = 0 (0x0)$	Reset = $0 (0x0)$
Reset = $0 (0x0)$	$msg\_seq = 0 (0x0)$
$msg\_seq = 0 (0x0)$	
Length: 69	Length: 69
Header: 45 00 76 10 80 03 41 69 17 69 95	Header: 45 00 76 10 80 03 41 69 17 69 95 00
00	Payload: 00 72 02 68 00 00 00 22 FF 00 00 15
Payload: 00 72 02 68 00 00 00 22 FF 00 00	14 00 00 7E 21 45 00 00 25 01 00 00
15	00 FF 11 35 51 0A 2E 60 74 81 2E 99
14 00 00 7E 21 45 00 00 25 01 00	A6 OF A7 OO O7 OO 11 BA 68 53 44 42
00	20 54 65 73 74 53 FC F8 7E
00 FF 11 35 51 0A 2E 60 74 81 2E	
99	
A6 OF A7 OO O7 OO 11 BA 68 53 44	
42	
20 54 65 73 74 53 FC F8 7E	

- ConfigurationRequest message in Session Configuration Protocol (mid =80 and pid =18)
- Field name change (prior\_session -> prior\_session\_attrib)

```
Qcat5.00.01
                                                               Qcat5.01.00
header_rev = 1 (0x1)
                                              header_rev = 1 (0x1)
num_options = 0 (0x0)
                                              num\_options = 0 (0x0)
subtype = 0 (0x0)
                                              subtype = 0 (0x0)
protocol_instance = 0 (0x0) (In Use)
                                              protocol_instance = 0 (0x0) (In Use)
protocol\_type = 18 (0x12) (Session
                                              protocol\_type = 18 (0x12) (Session
Configuration Protocol)
                                              Configuration Protocol)
message_id = 80 (0x50)
                                              message_id = 80 (0x50)
(ConfigurationRequest)
                                               (ConfigurationRequest)
ConfigurationRequest
                                              ConfigurationRequest
  transaction_id = 39 (0x27)
                                                transaction_id = 39 (0x27)
  num\_attribs = 1 (0x1)
                                                num_attribs = 1 (0x1)
  attribs[0]
                                                attribs[0]
    attribute_id = 4096 (0x1000)
                                                  attribute_id = 4096 (0x1000)
(PriorSession Attribute)
                                               (PriorSession Attribute)
    num\_recs = 1 (0x1)
                                                  num\_recs = 1 (0x1)
    prior_session[0]
                                                   prior_session_attrib[0])
Length:
         52
                                              Length:
                                                        52
Header: 34 00 77 10 00 01 52 54 C8 86 94
                                                        34 00 77 10 00 01 52 54 C8 86 94 00
                                              Header:
                                              Payload: 01 2C 01 78 00 00 00 0F 00 00 00 12
Payload: 01 2C 01 78 00 00 00 0F 00 00 00
                                                        50 27 19 10 00 10 80 00 00 00 00
                                               00
         50 27 19 10 00 10 80 00 00 00 00
                                                        00 00 00 00 00 00 00 00 2D E0 F3
00
                                              04
         00 00 00 00 00 00 00 00 2D E0 F3
                                                        02 E3 8D 47
04
         02 E3 8D 47
```

80-VB261-1 A 20 QUALCOMM Proprietary

4

2

7

8

- ConfigurationRequest message in Idle State Protocol (mid =80 and pid =12)
- Field name change (pref\_con\_chn\_cyc\_en\_ -> pref\_con\_chn\_cyc\_enable)

1

4

 $header_rev = 1 (0x1)$  $header_rev = 1 (0x1)$  $num\_options = 0 (0x0)$  $num\_options = 0 (0x0)$ subtype = 0 (0x0)subtype = 0 (0x0)protocol\_instance = 1 (0x1) (In Config) protocol\_instance = 1 (0x1) (In Config)  $protocol\_type = 12 (0xc) ()$ protocol\_type = 12 (0xc) (Idle State  $message_id = 80 (0x50)$ Protocol) (ConfigurationRequest)  $message_id = 80 (0x50)$ (ConfigurationRequest) ConfigurationRequest  $transaction_id = 17 (0x11)$ ConfigurationRequest  $num\_attribs = 1 (0x1)$  $transaction_id = 17 (0x11)$ attribs[0]  $num_attribs = 1 (0x1)$  $attribute_id = 0 (0x0)$ attribs[0] (PreferredControlChannelCycle)  $attribute_id = 0 (0x0)$ (PreferredControlChannelCycle) num recs = 1 (0x1)pref\_con\_chn\_cycle[0]  $num\_recs = 1 (0x1)$  $value_id = 17 (0x11)$ pref\_con\_chn\_cycle[0]  $pref_con_chn_cyc_en = 1 (0x1)$  $value_id = 17 (0x11)$  $pref_con_chn_cycle = 0 (0x0)$ pref\_con\_chn\_cyc\_enable = 1 (0x1)  $pref_con_chn_cycle = 0 (0x0)$ Length: Length: 31 Header: 1F 00 77 10 00 01 CE 37 F4 6D 94 1F 00 77 10 00 01 CE 37 F4 6D 94 00 Header: Payload: 01 2C 01 68 00 00 00 09 01 00 00 8C Payload: 01 2C 01 68 00 00 00 09 01 00 00 50 11 04 00 11 80 00 8C 50 11 04 00 11 80 00

80-VB261-1 A 21 QUALCOMM Proprietary

#### 3.2 QCAT5.01.00 vs. QCAT5.01.01

#### **HDR**

10

11

 Message name change for RevReservationOn/Off message in Multi-Flow Packet Application Protocol (mid =26/27 and pid = 21/22/23). (ReservationOn → RevReservationOn, ReservationOff → RevReservationOff)

Qcat5.01.00	Qcat5.01.01
header_rev = 1 (0x1) num_options = 0 (0x0) subtype = 5 (0x5) protocol_instance = 0 (0x0) (In Use) protocol_type = 22 (0x16) (Multi-Flow Packet Application (Service Network)) message_id = 27 (0x1b) (ReservationOff) packet_Applications   reservation_off     transaction_id = 53 (0x35)   reservation_count = 3 (0x3)   reservation_label[0] = 0 (0x0)   reservation_label[1] = 1 (0x1) reservation_label[2] = 2 (0x2)	header_rev = 1 (0x1) num_options = 0 (0x0) subtype = 5 (0x5) protocol_instance = 0 (0x0) (In Use) protocol_type = 22 (0x16) (Multi-Flow Packet Application (Service Network)) message_id = 27 (0x1b) (RevReservationOff) packet_Applications   reservation_off   transaction_id = 53 (0x35)   reservation_count = 3 (0x3)   reservation_label[0] = 0 (0x0)   reservation_label[1] = 1 (0x1)   reservation_label[2] = 2 (0x2)
Length: 30 Header: 1E 00 79 10 00 02 3B D9 7F 73 98 00 Payload: 01 2C 01 68 00 00 00 20 FF FF 00 16 1B 35 03 00 01 02	Length: 30 Header: 1E 00 79 10 00 02 3B D9 7F 73 98 00 Payload: 01 2C 01 68 00 00 00 20 FF FF 00 16 1B 35 03 00 01 02

■ Add missing transaction\_id field in FwdReservationOn/Off message in Multi-Flow Packet Application Protocol (mid = 26/27 and pid = 34/35) (bug fix)

Qcat5.01.00 Ocat5.01.01 header rev = 1 (0x1)header rev = 1 (0x1)num options = 0 (0x0)num options = 0 (0x0)subtype = 5(0x5)subtype = 5 (0x5)protocol\_instance = 0 (0x0) (In Use) protocol\_type = 22 (0x16) (Multi-Flow protocol\_instance = 0 (0x0) (In Use)
protocol\_type = 22 (0x16) (Multi-Flow Packet
Application (Service Network)) Packet Application (Service Network)) message id = 35 (0x23) (FwdReservationOn) packet\_Applications message id = 35 (0x23) (FwdReservationOn) packet\_Applications fwd reservation on fwd reservation on  $\overline{\text{transaction}}_{id} = 55 (0x37)$ reservation\_count = 55 (0x37) reservation\_label[0] = 3 (0x3) reservation\_label[1] = 0 (0x0) reservation\_count = 3 (0x3) reservation label[0] = 0 (0x0) reservation\_label[1] = 1 (0x1) reservation\_label[2] = 2 (0x2) reservation\_label[2] = 1 (0x1)
reservation\_label[3] = 2 (0x2)  $reservation\_label[4] = 0 (0x0)$ Length: 30 Length: 30 Header: 1E 00 79 10 C0 01 A3 DA 7F Header: 1E 00 79 10 C0 01 A3 DA 7F 73 98 00 73 98 00 Payload: 01 2C 01 68 00 00 00 20 FF FF 00 Payload: 01 2C 01 68 00 00 00 20 FF FF 00 16 23 37 03 00 01 02 23 37 03 00 01 02

80-VB261-1 A 22 QUALCOMM Proprietary

#### 3.3 QCAT5.01.01 vs. QCAT5.02.00

#### GSM

5

- si6\_rest\_incl is added to indicate whether si\_6\_rest IE exists in SYSTEM\_INFORMATION\_6, GSM\_RR\_MANAGEMENT protocol
- Silk will not display garbage if si\_6\_rest IE does not exist in the log file

Qcat5.01.01  $chan_type = 4 (0x4)$ chan type = 4(0x4)trans\_id\_or\_skip\_ind = 0 (0x0) prot\_disc = 6 (0x6) (GSM\_RR\_MANAGEMENT) trans\_id\_or\_skip\_ind = 0 (0x0) prot\_disc = 6 (0x6) (GSM\_RR\_MANAGEMENT)  $msg\_type = 30 (0x1e)$  $msg\_type = 30 (0x1e)$ prot prot rr man prot rr man prot SYSTEM\_INFORMATION 6 SYSTEM\_INFORMATION\_6 cell\_ident
 cell\_ident\_val = 1 (0x1) cell\_ident
 cell ident val = 1 (0x1) loc\_area\_ident loc\_area\_ident  $mcc_1 = 0 (0x0)$   $mcc_2 = 0 (0x0)$  $mcc_1 = 0 (0x0)$   $mcc_2 = 0 (0x0)$  $mcc^{-}3 = 2 (0x2)$  $mcc^{-}3 = 2 (0x2)$  $mnc_3 = 15 (0xf)$   $mnc_1 = 0 (0x0)$  $mnc_3 = 15 (0xf)$   $mnc_1 = 0 (0x0)$  $mnc^2 = 1 (0x1)$  $mnc^2 = 1 (0x1)$  $loc_area_code = 101 (0x65)$  $loc_area_code = 101 (0x65)$ cell\_options cell\_options  $dtx_high = 0 (0x0)$  $dtx_high = 0 (0x0)$ pwrc = 0 (0x0)pwrc = 0 (0x0) $dtx_low = 2 (0x2)$ dtx low = 2 (0x2)radio link timeout = 4 (0x4)radio link timeout = 4 (0x4) $\operatorname{ncc\_permitted}$ ncc\_permitted  $\overline{ncc}$  permitted = 255 (0xff)  $\overline{\text{ncc}}$  permitted = 255 (0xff) si 6 rest si6 rest incl = 0 (0x0) $\overline{padding}$  bits H = 1 (H) PCH and NCH info Length: Length: 26 26 1A 00 2F 51 00 00 CA 5F DD 8C 00 00 1A 00 2F 51 00 00 CA 5F DD 8C 00 00 Header: Header: Payload: 84 1E 0B 06 1E 00 01 00 F2 10 00 65 Payload: 84 1E 0B 06 1E 00 01 00 F2 10 00 65 24 FF 24 FF

80-VB261-1 A 23 QUALCOMM Proprietary

#### HDR

2

3

5

8

• subtype 1 is mapped to subtype 0 for Broadcast Protocol. Now subtype 1, same as subtype 0 is supported for Broadcast Protocol.

Qcat5.01.01	Qcat5.01.02
header_rev = 1 (0x1) num_options = 0 (0x0) subtype = 1 (0x1) protocol_instance = 0 (0x0) (In Use) protocol_type = 24 (0x18) (SID (1) OoRuse '0'(Broadcast Protocol)) message_id = 0 (0x0) (SID (1) OoRuse '0'(BroadcastFlowRegistration))	header_rev = 1 (0x1) num_options = 0 (0x0) subtype = 0 (0x0) (subtype 0) protocol_instance = 0 (0x0) (In Use) protocol_type = 24 (0x18) (Broadcast Protocol) message_id = 0 (0x0) (BroadcastFlowRegistration)

- QoS attribute updated from latest IS835D. Since num\_qos\_attribute\_sets field length is changed, Silk might have a totally different output with old QoS log.
- Pretty printing function is added/changed for subtype/ protocol\_type

```
Qcat5.01.01
                                                                                    Qcat5.01.02
header rev = 1 (0x1)
                                                             header rev = 1 (0x1)
num\_options = 0 (0x0)
                                                             num options = 0 (0x0)
subtype = 5 (0x5)
                                                             subtype = 5 (0x5) ((subtype 4 or 5 if protocol
protocol_instance = 0 (0x0) (In Use)
protocol_type = 21 (0x15) (Multi-Flow Packet
Application (Service Network))
message_id = 82 (0x52)
                                                             type is 0x15-0x17)
                                                             protocol_instance = 0 (0x0) (In Use)
protocol_type = 21 (0x15) (Multi-Flow Packet
(AttributeUpdateRequest)
                                                             Application (Access or Service Network)
AttributeUpdateRequest
                                                             Network))
  transaction_id = 2 (0x2)
num_attribs = 1 (0x1)
                                                             message_id = 82 (0x52) (AttributeUpdateRequest)
                                                             AttributeUpdateRequest
                                                               transaction_id = 2 (0x2)
  attribs[0]
     attribute id = 2049 (0x801)
                                                               num attribs = 1 (0x1)
(Reservation KKQoSRequestRev)
                                                               attribs[0]
                                                                  attribute id = 2049 (0x801)
     num recs = 1 (0x1)
     ReservationKKQosReqRev[0]
                                                             (ReservationKKQoSRequestRev)
       value id = 0 (0x0)
                                                                  num recs = 1 (0x1)
       profile_type = 1 (0x1)
profile_len = 6 (0x6)
                                                                  ReservationKKQosReqRev[0]
                                                                    value id = 0 (0x0)
                                                                    profile_type = 1 (0x1)
profile_len = 6 (0x6)
       flow_priority = 9 (0x9)
       num_qos_attribute_sets = 1 (0x1)
       qos attribute set[0]
                                                                    flow priority = 9(0x9)
          qos_attribute_set_len = 4 (0x4)
qos_attibute_set_id = 0 (0x0)
                                                                    num_qos_attribute_sets = 0 (0x0)
         verbose = 0 (0x0)
profile_id = 15 (0xf)
Length:
                                                             Length:
                                                                        39
           39
Header:
           27 00 77 10 40 05 B8 A3 C5 70 96 00
                                                                        27 00 77 10 40 05 B8 A3 C5 70 96 00
                                                             Header:
Payload: 01 2C 01 68 00 00 00 2B 03 00 00 15 52 02 0C 08 01 00 01 00 06 91 04 00
                                                             Payload: 01 2C 01 68 00 00 00 2B 03 00 00 15
                                                                         52 02 0C 08 01 00 01 00 06 91 04 00
            00 07 80
                                                                         00 07 80
```

10

80-VB261-1 A 24 QUALCOMM Proprietary

2

6

■ FlowNNTransmitAbortTimer attribute (in multiflow protocol) length is corrected from 8 bit to 16 bit

Qcat5.01.01	Qcat5.01.02
attribute_id = 63232 (0xf700) FlowNNTransmitAbortTimerRev) num_recs = 2 (0x2) flow_nn_transm_abort_timer_rev[0] = 1 (0x1)	<pre>attribute_id = 63232 (0xf700) (FlowNNTransmitAbortTimerRev) num_recs = 1 (0x1) flow_nn_transmit_abort_timer_rev[0] = 300</pre>
FlowNNTransmitAbortTimerRev) num_recs = 2 (0x2)	(FlowNNTransmitAbortTimerRev) num recs = 1 (0x1)

- radius\_add attribute length in route update protocol is corrected from 8 bit to 16 bit
- Profile Type 4 in attribute id 0x0002 and 0x0003 is further parsed for multiflow protocol

80-VB261-1 A 25 QUALCOMM Proprietary