sysmocom
sysmocom - s.f.m.c. GmbH

OsmoMSC User Manual
by Neels Hofmeyr

Copyright © 2017 sysmocom - s.f.m.c. GmbH

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.3 or any later version published by the Free Software Foundation; with the Invariant Sections being just 'Foreword', 'Acknowledgements' and 'Preface', with no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".

The AsciiDoc source code of this manual can be found at http://git.osmocom.org/osmo-gsm-manuals/
## HISTORY

<table>
<thead>
<tr>
<th>NUMBER</th>
<th>DATE</th>
<th>DESCRIPTION</th>
<th>NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>September 18th, 2017</td>
<td>Initial version; based on OsmoNITB manual version 2.</td>
<td>NH</td>
</tr>
</tbody>
</table>
# Contents

1 Foreword 1  
  1.1 Acknowledgements ................................................................. 1  
  1.2 Endorsements ........................................................................ 2  

2 Preface 2  
  2.1 FOSS lives by contribution! .............................................................. 2  
  2.2 Osmocom and sysmocom ................................................................. 2  
  2.3 Corrections ............................................................................. 3  
  2.4 Legal disclaimers ....................................................................... 3  
    2.4.1 Spectrum License ................................................................ 3  
    2.4.2 Software License .................................................................. 3  
    2.4.3 Trademarks ....................................................................... 3  
    2.4.4 Liability ........................................................................... 3  
    2.4.5 Documentation License ....................................................... 4  

3 Introduction 4  
  3.1 Required Skills ........................................................................ 4  
  3.2 Getting assistance ..................................................................... 4  

4 Overview 4  
  4.1 About OsmoMSC ....................................................................... 5  
  4.2 Software Components ................................................................. 6  
    4.2.1 SMSC ............................................................................... 6  
    4.2.2 MSC ............................................................................... 6  
    4.2.3 VLR ............................................................................... 6  

5 Running OsmoMSC 6  
  5.1 SYNOPSIS ............................................................................... 6  
  5.2 OPTIONS ................................................................................ 6  
  5.3 Multiple instances .................................................................... 7  
  5.4 Configure primary links ............................................................... 7  
    5.4.1 Configure SCCP/M3UA to accept A and IuCS links ............... 7  
    5.4.2 Configure GSUP to reach the HLR ..................................... 8  

6 Control interface 8  
  6.1 subscriber-list-active-v1 ............................................................... 9
7 Osmocom Counters
  7.1 Osmo Counters (deprecated) .......................................................... 9
  7.2 Rate Counters ................................................................................. 9
  7.3 Stat Item ......................................................................................... 9
  7.4 Statistic Levels .............................................................................. 10
    7.4.1 Global ..................................................................................... 10
    7.4.2 Peer ......................................................................................... 10
    7.4.3 Subscriber .............................................................................. 10
  7.5 Stats Reporter .............................................................................. 10
    7.5.1 Configuring a stats reporter ..................................................... 10

8 Counters ......................................................................................... 11
  8.1 Rate Counters .............................................................................. 11

9 Osmo Stat Items ............................................................................. 12

10 Osmo Counters ................................................................................ 12

11 The Osmocom VTY Interface .......................................................... 13
  11.1 Accessing the telnet VTY ............................................................... 14
  11.2 VTY Nodes ................................................................................. 14
  11.3 Interactive help ........................................................................... 14
    11.3.1 The question-mark (?) command ........................................... 15
    11.3.2 TAB completion .................................................................... 16
    11.3.3 The list command .................................................................. 16

12 libosmocore Logging System ......................................................... 18
  12.1 Log categories ............................................................................ 18
  12.2 Log levels .................................................................................... 18
  12.3 Log printing options .................................................................... 19
  12.4 Log filters .................................................................................... 19
  12.5 Log targets ................................................................................. 20
    12.5.1 Logging to the VTY ................................................................. 20
    12.5.2 Logging to the ring buffer ..................................................... 20
    12.5.3 Logging via gsmtap ............................................................... 21
    12.5.4 Logging to a file .................................................................... 21
    12.5.5 Logging to syslog ................................................................. 22
    12.5.6 Logging to stderr ................................................................. 22
13 Configuring the Core Network .......................................................... 23
  13.1 MCC/MNC ................................................................................. 23
  13.2 Configuring MM INFO ............................................................... 23
  13.3 Authentication ........................................................................ 24
    13.3.1 Authentication on 2G ........................................................ 24
    13.3.2 Authentication on 3G ........................................................ 24
  13.4 Ciphering ................................................................................. 24
    13.4.1 Ciphering on 2G ................................................................. 24
    13.4.2 Ciphering on 3G ................................................................. 25
14 Short Message Peer to Peer (SMPP) .................................................... 25
  14.1 Global SMPP configuration ......................................................... 26
  14.2 ESME configuration ................................................................ 26
  14.3 Example configuration snippet .................................................. 26
  14.4 Osmocom SMPP protocol extensions ......................................... 26
    14.4.1 RF channel measurements ............................................... 27
    14.4.2 Equipment IMEI ............................................................... 27
15 MNCC for External Call Control ......................................................... 27
  15.1 Internal MNCC handler ............................................................... 27
    15.1.1 Internal MNCC Configuration ............................................. 28
      15.1.1.1 default-codec tch-f (fr|efr|amr) .................................... 28
      15.1.1.2 default-codec tch-h (hr|amr) ....................................... 28
  15.2 External MNCC handler ............................................................. 28
  15.3 DTMF considerations ............................................................... 28
  15.4 MNCC protocol description ...................................................... 28
    15.4.1 MNCC_HOLD_IND ............................................................. 29
    15.4.2 MNCC_HOLD_CNF ........................................................... 29
    15.4.3 MNCC_HOLD_REJ ............................................................ 29
    15.4.4 MNCC_RETRIEVE_IND ..................................................... 29
    15.4.5 MNCC_RETRIEVE_CNF .................................................... 29
    15.4.6 MNCC_RETRIEVE_REJ ..................................................... 29
    15.4.7 MNCC_USERINFO_REQ ................................................... 29
    15.4.8 MNCC_USERINFO_IND .................................................... 29
    15.4.9 MNCC_BRIDGE ............................................................... 30
    15.4.10 MNCC_FRAME_RECV ..................................................... 30
    15.4.11 MNCC_FRAME_DROP .................................................... 30
    15.4.12 MNCC_LCHAN_MODIFY .................................................. 30
    15.4.13 MNCC_RTP_CREATE ...................................................... 30

Copyright © 2017 sysmocom - s.f.m.c. GmbH
DRAFT 1.6.1-32-gc95c0, 2020-Mar-24
15.4.14 MNCC_RTP_CONNECT .................................................. 30
15.4.15 MNCC_RTP_FREE ..................................................... 30
15.4.16 GSM_TCHF_FRAME .................................................. 31
15.4.17 GSM_TCHF_FRAME_EFR .......................................... 31
15.4.18 GSM_TCHH_FRAME ................................................ 31
15.4.19 GSM_TCH_FRAE_AMR ............................................. 31
15.4.20 GSM_BAD_FRAME .................................................. 31
15.4.21 MNCC_START_DTMF_IND ....................................... 31
15.4.22 MNCC_START_DTMF_RSP ....................................... 31
15.4.23 MNCC_START_DTMF_REJ ....................................... 31
15.4.24 MNCC_STOP_DTMF_IND ........................................ 31
15.4.25 MNCC_STOP_DTMF_RSP ........................................ 32

16 Osmux ................................................................. 32

16.1 Osmux and NAT ..................................................... 32
16.2 CID allocation ....................................................... 32
16.3 3GPP AoIP network setup with Osmux ........................... 33
16.4 SCCPLite network setup with Osmux .............................. 35
16.5 SCCPLite network setup with Osmux + BSC-NAT ............... 37
16.6 Osmux and MGCP .................................................... 39
  16.6.1 X-Osmux Format ............................................... 39
  16.6.2 X-Osmux Considerations ...................................... 39
  16.6.3 X-Osmux Support .............................................. 40
16.7 Osmux Support in OsmoMSC ...................................... 40
  16.7.1 OsmoMSC in a A/IP with IPA/SCCPlite network setup ...... 40
  16.7.2 OsmoMSC in a 3GPP AoIP network setup ................... 41

17 Osmocom Control Interface ........................................ 41

17.1 Control Interface Protocol ....................................... 41
  17.1.1 GET operation ................................................ 42
  17.1.2 SET operation ................................................ 43
  17.1.3 TRAP operation .............................................. 43
17.2 Common variables ................................................ 44
17.3 Control Interface python examples ............................... 44
  17.3.1 Getting rate counters ....................................... 44
  17.3.2 Setting a value .............................................. 45
  17.3.3 Getting a value .............................................. 45
  17.3.4 Listening for traps .......................................... 45
18 Generic Subscriber Update Protocol

18.1 General .................................................. 45
18.2 Connection ............................................... 46
18.3 Using IPA ................................................. 46
18.4 Procedures .................................................. 46
  18.4.1 Authentication management ............................... 46
  18.4.2 Reporting of Authentication Failure ......................... 46
  18.4.3 Location Updating ....................................... 47
  18.4.4 Location Cancellation ................................... 47
  18.4.5 Purge MS ................................................. 48
  18.4.6 Delete Subscriber Data .................................... 48
  18.4.7 Check IMEI .............................................. 48

18.5 Procedures (E Interface) ..................................... 48
  18.5.1 E Handover ............................................. 48
  18.5.2 E Subsequent Handover ................................... 49
  18.5.3 E Forward and Process Access Signalling ..................... 49
  18.5.4 E Routing Error ......................................... 50

18.6 Message Format ............................................. 50
  18.6.1 General ............................................... 50
  18.6.2 Send Authentication Info Request .......................... 50
  18.6.3 Send Authentication Info Error ............................ 51
  18.6.4 Send Authentication Info Response ......................... 51
  18.6.5 Authentication Failure Report ............................. 51
  18.6.6 Update Location Request .................................. 51
  18.6.7 Update Location Error .................................... 51
  18.6.8 Update Location Result .................................... 51
  18.6.9 Location Cancellation Request ............................ 52
  18.6.10 Location Cancellation Result ............................. 52
  18.6.11 Purge MS Request ....................................... 52
  18.6.12 Purge MS Error ......................................... 52
  18.6.13 Purge MS Result ......................................... 52
  18.6.14 Insert Subscriber Data Request .......................... 53
  18.6.15 Insert Subscriber Data Error .............................. 53
  18.6.16 Insert Subscriber Data Result ............................ 53
  18.6.17 Delete Subscriber Data Request .......................... 53
  18.6.18 Delete Subscriber Data Error .............................. 53
  18.6.19 Delete Subscriber Data Result ............................ 54
  18.6.20 Process Supplementary Service Request .................... 54
  18.6.21 Process Supplementary Service Error ...................... 54
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>18.6.22</td>
<td>Process Supplementary Service Response</td>
<td>54</td>
</tr>
<tr>
<td>18.6.23</td>
<td>MO-forwardSM Request</td>
<td>55</td>
</tr>
<tr>
<td>18.6.24</td>
<td>MO-forwardSM Error</td>
<td>55</td>
</tr>
<tr>
<td>18.6.25</td>
<td>MO-forwardSM Result</td>
<td>55</td>
</tr>
<tr>
<td>18.6.26</td>
<td>MT-forwardSM Request</td>
<td>55</td>
</tr>
<tr>
<td>18.6.27</td>
<td>MT-forwardSM Error</td>
<td>56</td>
</tr>
<tr>
<td>18.6.28</td>
<td>MT-forwardSM Result</td>
<td>56</td>
</tr>
<tr>
<td>18.6.29</td>
<td>READY-FOR-SM Request</td>
<td>56</td>
</tr>
<tr>
<td>18.6.30</td>
<td>READY-FOR-SM Error</td>
<td>56</td>
</tr>
<tr>
<td>18.6.31</td>
<td>READY-FOR-SM Result</td>
<td>57</td>
</tr>
<tr>
<td>18.6.32</td>
<td>CHECK-IMEI Request</td>
<td>57</td>
</tr>
<tr>
<td>18.6.33</td>
<td>CHECK-IMEI Error</td>
<td>57</td>
</tr>
<tr>
<td>18.6.34</td>
<td>CHECK-IMEI Result</td>
<td>57</td>
</tr>
<tr>
<td>18.6.35</td>
<td>E Prepare Handover Request</td>
<td>57</td>
</tr>
<tr>
<td>18.6.36</td>
<td>E Prepare Handover Error</td>
<td>58</td>
</tr>
<tr>
<td>18.6.37</td>
<td>E Prepare Handover Result</td>
<td>58</td>
</tr>
<tr>
<td>18.6.38</td>
<td>E Prepare Subsequent Handover Request</td>
<td>58</td>
</tr>
<tr>
<td>18.6.39</td>
<td>E Prepare Subsequent Handover Error</td>
<td>58</td>
</tr>
<tr>
<td>18.6.40</td>
<td>E Prepare Subsequent Handover Result</td>
<td>59</td>
</tr>
<tr>
<td>18.6.41</td>
<td>E Send End Signal Request</td>
<td>59</td>
</tr>
<tr>
<td>18.6.42</td>
<td>E Send End Signal Error</td>
<td>59</td>
</tr>
<tr>
<td>18.6.43</td>
<td>E Send End Signal Result</td>
<td>59</td>
</tr>
<tr>
<td>18.6.44</td>
<td>E Process Access Signalling Request</td>
<td>59</td>
</tr>
<tr>
<td>18.6.45</td>
<td>E Forward Access Signalling Request</td>
<td>60</td>
</tr>
<tr>
<td>18.6.46</td>
<td>E Close</td>
<td>60</td>
</tr>
<tr>
<td>18.6.47</td>
<td>E Abort</td>
<td>60</td>
</tr>
<tr>
<td>18.6.48</td>
<td>E Routing Error</td>
<td>60</td>
</tr>
<tr>
<td>18.7</td>
<td>Information Elements</td>
<td>60</td>
</tr>
<tr>
<td>18.7.1</td>
<td>Message Type</td>
<td>60</td>
</tr>
<tr>
<td>18.7.2</td>
<td>IP Address</td>
<td>61</td>
</tr>
<tr>
<td>18.7.3</td>
<td>PDP Info</td>
<td>61</td>
</tr>
<tr>
<td>18.7.4</td>
<td>PDP Type</td>
<td>62</td>
</tr>
<tr>
<td>18.7.5</td>
<td>PDP Context ID</td>
<td>62</td>
</tr>
<tr>
<td>18.7.6</td>
<td>Auth tuple</td>
<td>63</td>
</tr>
<tr>
<td>18.7.7</td>
<td>RAND</td>
<td>63</td>
</tr>
<tr>
<td>18.7.8</td>
<td>SRES</td>
<td>63</td>
</tr>
<tr>
<td>18.7.9</td>
<td>Kc</td>
<td>63</td>
</tr>
<tr>
<td>18.7.10</td>
<td>IK</td>
<td>63</td>
</tr>
<tr>
<td>18.7.11</td>
<td>CK</td>
<td>63</td>
</tr>
</tbody>
</table>
18.7.12 AUTN .......................................................... 64
18.7.13 AUTS .......................................................... 64
18.7.14 RES ............................................................. 64
18.7.15 CN Domain .................................................... 64
18.7.16 Cancellation Type ........................................... 64
18.7.17 IE Identifier (informational) ................................. 65
18.7.18 Empty field ................................................... 66
18.7.19 IMSI ........................................................... 66
18.7.20 ISDN-AddressString / MSISDN / Called Party BCD Number ............................. 66
18.7.21 Access Point Name .......................................... 67
18.7.22 Quality of Service Subscribed Service ..................... 67
18.7.23 PDP-Charging Characteristics ............................... 67
18.7.24 HLR Number encoded as 3GPP TS 09.02 ISDN-AddressString .......................... 68
18.7.25 Cause .......................................................... 68
18.7.26 Supplementary Service Info ................................ 68
18.7.27 IMEI ........................................................... 68
18.7.28 IMEI Check Result ........................................... 69
18.7.29 Message Class ................................................. 69
18.7.30 Source Name .................................................. 69
18.7.31 Destination Name .............................................. 69
18.7.32 AN-APDU ..................................................... 69
18.7.33 RR Cause ....................................................... 70
18.7.34 BSSAP Cause .................................................. 70
18.7.35 Session Management Cause .................. 70

18.8 Session (transaction) management .................................. 70
18.8.1 Session ID ....................................................... 70
18.8.2 Session State .................................................... 71
18.8.3 SM-RP-MR (Message Reference) .................................. 72
18.8.4 SM-RP-DA (Destination Address) .............................. 72
18.8.5 SM-RP-OA (Originating Address) .............................. 72
18.8.6 Coding of SM-RP-DA / SM-RP-OA IEs ......................... 72
18.8.7 SM-RP-UI (SM TPDU) ........................................... 73
18.8.8 SM-RP-Cause (RP Cause value) ................................. 73
18.8.9 SM-RP-MMS (More Messages to Send) ............................ 74
18.8.10 SM Alert Reason ................................................. 74

19 Glossary .............................................................. 74
A Osmocom TCP/UDP Port Numbers ........................................ 82
1 Foreword

Digital cellular networks based on the GSM specification were designed in the late 1980ies and first deployed in the early 1990ies in Europe. Over the last 25 years, hundreds of networks were established globally and billions of subscribers have joined the associated networks.

The technological foundation of GSM was based on multi-vendor interoperable standards, first created by government bodies within CEPT, then handed over to ETSI, and now in the hands of 3GPP. Nevertheless, for the first 17 years of GSM technology, the associated protocol stacks and network elements have only existed in proprietary black-box implementations and not as Free Software.

In 2008 Dieter Spaar and I started to experiment with inexpensive end-of-life surplus Siemens GSM BTSs. We learned about the A-bis protocol specifications, reviewed protocol traces and started to implement the BSC-side of the A-bis protocol as something originally called bs11-abis. All of this was just for fun, in order to learn more and to boldly go where no Free Software developer has gone before. The goal was to learn and to bring Free Software into a domain that despite its ubiquity, had not yet seen any Free / Open Source software implementations.

bs11-abis quickly turned into bsc-hack, then OpenBSC and its OsmoNITB variant: A minimal implementation of all the required functionality of an entire GSM network, exposing A-bis towards the BTS. The project attracted more interested developers, and surprisingly quickly also commercial interest, contribution and adoption. This allowed adding support for more BTS models.

After having implemented the network-side GSM protocol stack in 2008 and 2009, in 2010 the same group of people set out to create a telephone-side implementation of the GSM protocol stack. This established the creation of the Osmocom umbrella project, under which OpenBSC and the OsmocomBB projects were hosted.

Meanwhile, more interesting telecom standards were discovered and implemented, including TETRA professional mobile radio, DECT cordless telephony, GMR satellite telephony, some SDR hardware, a SIM card protocol tracer and many others.

Increasing commercial interest particularly in the BSS and core network components has lead the way to 3G support in Osmocom, as well as the split of the minimal OsmoNITB implementation into separate and fully featured network components: OsmoBSC, OsmoMSC, OsmoHLR, OsmoMGW and OsmoSTP (among others), which allow seamless scaling from a simple "Network In The Box" to a distributed installation for serious load.

It has been a most exciting ride during the last eight-odd years. I would not have wanted to miss it under any circumstances.
— Harald Welte, Osmocom.org and OpenBSC founder, December 2017.

1.1 Acknowledgements

My deep thanks to everyone who has contributed to Osmocom. The list of contributors is too long to mention here, but I’d like to call out the following key individuals and organizations, in no particular order:

- Dieter Spaar for being the most amazing reverse engineer I’ve met in my career
- Holger Freyther for his many code contributions and for shouldering a lot of the maintenance work, setting up Jenkins - and being crazy enough to co-start sysmocom as a company with me :)
- Andreas Eversberg for taking care of Layer2 and Layer3 of OsmocomBB, and for his work on OsmoBTS and OsmoPCU
- Sylvain Munaut for always tackling the hardest problems, particularly when it comes closer to the physical layer
- Chaos Computer Club for providing us a chance to run real-world deployments with tens of thousands of subscribers every year
- Bernd Schneider of Netzing AG for funding early ip.access nanoBTS support
- On-Waves ehf for being one of the early adopters of OpenBSC and funding a never ending list of features, fixes and general improvement of pretty much all of our GSM network element implementations
- sysmocom, for hosting and funding a lot of Osmocom development, the annual Osmocom Developer Conference and releasing this manual.
• Jan Luebbe, Stefan Schmidt, Daniel Willmann, Pablo Neira, Nico Golde, Kevin Redon, Ingo Albrecht, Alexander Huemer, Alexander Chemeris, Max Suraev, Tobias Engel, Jacob Erlbeck, Ivan Kluchnikov

May the source be with you!
— Harald Welte, Osmocom.org and OpenBSC founder, January 2016.

1.2 Endorsements

This version of the manual is endorsed by Harald Welte as the official version of the manual.

While the GFDL license (see Appendix C) permits anyone to create and distribute modified versions of this manual, such modified versions must remove the above endorsement.

2 Preface

First of all, we appreciate your interest in Osmocom software.

Osmocom is a Free and Open Source Software (FOSS) community that develops and maintains a variety of software (and partially also hardware) projects related to mobile communications.

Founded by people with decades of experience in community-driven FOSS projects like the Linux kernel, this community is built on a strong belief in FOSS methodology, open standards and vendor neutrality.

2.1 FOSS lives by contribution!

If you are new to FOSS, please try to understand that this development model is not primarily about “free of cost to the GSM network operator”, but it is about a collaborative, open development model. It is about sharing ideas and code, but also about sharing the effort of software development and maintenance.

If your organization is benefitting from using Osmocom software, please consider ways how you can contribute back to that community. Such contributions can be many-fold, for example

• sharing your experience about using the software on the public mailing lists, helping to establish best practises in using/operating it,
• providing qualified bug reports, work-arounds
• sharing any modifications to the software you may have made, whether bug fixes or new features, even experimental ones
• providing review of patches
• testing new versions of the related software, either in its current “master” branch or even more experimental feature branches
• sharing your part of the maintenance and/or development work, either by donating developer resources or by (partially) funding those people in the community who do.

We’re looking forward to receiving your contributions.

2.2 Osmocom and sysmocom

Some of the founders of the Osmocom project have established sysmocom - systems for mobile communications GmbH as a company to provide products and services related to Osmocom.

sysmocom and its staff have contributed by far the largest part of development and maintenance to the Osmocom mobile network infrastructure projects.

As part of this work, sysmocom has also created the manual you are reading.

At sysmocom, we draw a clear line between what is the Osmocom FOSS project, and what is sysmocom as a commercial entity. Under no circumstances does participation in the FOSS projects require any commercial relationship with sysmocom as a company.
2.3 Corrections

We have prepared this manual in the hope that it will guide you through the process of installing, configuring and debugging your deployment of cellular network infrastructure elements using Osmocom software. If you do find errors, typos and/or omissions, or have any suggestions on missing topics, please do take the extra time and let us know.

2.4 Legal disclaimers

2.4.1 Spectrum License

As GSM and UMTS operate in licensed spectrum, please always double-check that you have all required licenses and that you do not transmit on any ARFCN or UARFCN that is not explicitly allocated to you by the applicable regulatory authority in your country.

⚠️ Warning
Depending on your jurisdiction, operating a radio transmitter without a proper license may be considered a felony under criminal law!

2.4.2 Software License

The software developed by the Osmocom project and described in this manual is Free / Open Source Software (FOSS) and subject to so-called copyleft licensing.

Copyleft licensing is a legal instrument to ensure that this software and any modifications, extensions or derivative versions will always be publicly available to anyone, for any purpose, under the same terms as the original program as developed by Osmocom.

This means that you are free to use the software for whatever purpose, make copies and distribute them - just as long as you ensure to always provide/release the complete and corresponding source code.

Every Osmocom software includes a file called COPYING in its source code repository which explains the details of the license. The majority of programs is released under GNU Affero General Public License, Version 3 (AGPLv3).

If you have any questions about licensing, don’t hesitate to contact the Osmocom community. We’re more than happy to clarify if your intended use case is compliant with the software licenses.

2.4.3 Trademarks

All trademarks, service marks, trade names, trade dress, product names and logos appearing in this manual are the property of their respective owners. All rights not expressly granted herein are reserved.

For your convenience we have listed below some of the registered trademarks referenced herein. This is not a definitive or complete list of the trademarks used.

Osmocom® and OpenBSC® are registered trademarks of Holger Freyther and Harald Welte.

sysmocom® and sysmoBTS® are registered trademarks of sysmocom - systems for mobile communications GmbH.

ip.access® and nanoBTS® are registered trademarks of ip.access Ltd.

2.4.4 Liability

The software is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the License text included with the software for more details.
2.4.5 Documentation License

Please see Appendix C for further information.

3 Introduction

3.1 Required Skills

Please note that even while the capital expenses of running mobile networks has decreased significantly due to Osmocom software and associated hardware like sysmoBTS, GSM networks are still primarily operated by large GSM operators.

Neither the GSM specification nor the GSM equipment was ever designed for networks to be installed and configured by anyone but professional GSM engineers, specialized in their respective area like radio planning, radio access network, back-haul or core network.

If you do not share an existing background in GSM network architecture and GSM protocols, correctly installing, configuring and optimizing your GSM network will be tough, irrespective whether you use products with Osmocom software or those of traditional telecom suppliers.

GSM knowledge has many different fields, from radio planning through site installation to core network configuration/administration.

The detailed skills required will depend on the type of installation and/or deployment that you are planning, as well as its associated network architecture. A small laboratory deployment for research at a university is something else than a rural network for a given village with a handful of cells, which is again entirely different from an urban network in a dense city.

Some of the useful skills we recommend are:

- general understanding about RF propagation and path loss in order to estimate coverage of your cells and do RF network planning.
- general understanding about GSM network architecture, its network elements and key transactions on the Layer 3 protocol
- general understanding about voice telephony, particularly those of ISDN heritage (Q.931 call control)
- understanding of GNU/Linux system administration and working on the shell
- understanding of TCP/IP networks and network administration, including tcpdump, tshark, wireshark protocol analyzers.
- ability to work with text based configuration files and command-line based interfaces such as the VTY of the Osmocom network elements

3.2 Getting assistance

If you do have a support package / contract with sysmocom (or want to get one), please contact support@sysmocom.de with any issues you may have.

If you don’t have a support package / contract, you have the option of using the resources put together by the Osmocom community at http://projects.osmocom.org/, checking out the wiki and the mailing-list for community-based assistance. Please always remember, though: The community has no obligation to help you, and you should address your requests politely to them. The information (and software) provided at osmocom.org is put together by volunteers for free. Treat them like a friend whom you’re asking for help, not like a supplier from whom you have bought a service.

4 Overview

This manual should help you getting started with OsmoMSC. It will cover aspects of configuring and running the OsmoMSC.
4.1 About OsmoMSC

OsmoMSC is the Osmocom implementation of a Mobile Switching Center (MSC) for 2G and 3G GSM and UMTS mobile networks. Its interfaces are:

- GSUP towards OsmoHLR (or a MAP proxy);
- A over IP towards a BSC (e.g. OsmoBSC);
- IuCS towards an RNC or HNB-GW (e.g. OsmoHNBGW) for 3G voice;
- MNCC (Mobile Network Call Control derived from GSM TS 04.07);
- SMPP 3.4 (Short Message Peer-to-Peer);
- The Osmocom typical telnet VTY and CTRL interfaces.

OsmoMSC originated from the OpenBSC project, which started as a minimalistic all-in-one implementation of the GSM Network. In 2017, OpenBSC had reached maturity and diversity (including M3UA SIGTRAN and 3G support in the form of IuCS and IuPS interfaces) that naturally lead to a separation of the all-in-one approach to fully independent separate programs as in typical GSM networks. Before it was split off, OsmoMSC originated from libmsc of the old openbsc.git. Since a true A interface and IuCS for 3G support is available, OsmoMSC exists only as a separate standalone entity.

Key differences of the new OsmoMSC compared to the old OsmoNITB are:

- The complete VLR implementation that communicates with the separate HLR (OsmoHLR) for subscriber management. In contrast to the OsmoNITB, HLR queries are fully asynchronous, and the separate HLR allows using centralized subscriber management for both circuit-switched and packet-switched domains (i.e. one OsmoHLR for both OsmoMSC and OsmoS-GSN).
- VLR and HLR brought full UMTS AKA (Authentication and Key Agreement) support, i.e. Milenage authentication in both the full 3G variant as well as the backwards compatible 2G variant.
- Addition of a true A interface for 2G voice services. Previously, OsmoBSC had an SCCPlite based A interface towards 3rd party MSC implementations. OsmoMSC features a true SCCP/M3UA A interface, which allows running OsmoBSC against this Osmocom based MSC implementation. The new SCCP/M3UA SIGTRAN for the A interface is implemented in libosmo-sccp, which is used by OsmoMSC and OsmoBSC (and others), to establish a link via an STP (e.g. OsmoSTP).
- Addition of an IuCS interface to allow operating 3G voice services, also via SCCP/M3UA SIGTRAN, for example connecting via OsmoHNBGW to a 3G small cell device.

Find the OsmoMSC issue tracker and wiki online at

- https://osmocom.org/projects/osmomsc
- https://osmocom.org/projects/osmomsc/wiki

![Figure 1: Typical GSM network architecture used with OsmoMSC](image-url)
4.2 Software Components

This is a brief description of OsmoMSC’s internal software components.

4.2.1 SMSC

A minimal store-and-forward server for SMS, supporting both MO and MT SMS service, as well as multi-part messages. The built-in SMSC also supports an external SMSC interface. For more information, see Section 14.

4.2.2 MSC

The MSC component implements the mobility management (MM) functions of the TS 04.08 and delegates to SMSC for SMS message handling and the VLR for subscriber management. Furthermore, it can handle TS 04.08 Call Control (CC), either by use of an internal MNCC handler, or by use of an external MNCC agent. For more information see Section 15.

4.2.3 VLR

A fully featured Visitor Location Register handles the subscriber management and authentication, and interfaces via GSUP to the external HLR.

5 Running OsmoMSC

The OsmoMSC executable (osmo-msc) offers the following command-line arguments:

5.1 SYNOPSIS

```
```

5.2 OPTIONS

-\textbf{-h, --help}\n
Print a short help message about the supported options

-\textbf{-V, --version}\n
Print the compile-time version number of the program

-\textbf{-d, --debug DBGMASK,DBGLEVELS}\n
Set the log subsystems and levels for logging to stderr. This has mostly been superseded by VTY-based logging configuration, see Section 12 for further information.

-\textbf{-D, --daemonize}\n
Fork the process as a daemon into background.

-\textbf{-c, --config-file CONFIGFILE}\n
Specify the file and path name of the configuration file to be used. If none is specified, use osmo-msc.cfg in the current working directory.

-\textbf{-s, --disable-color}\n
Disable colors for logging to stderr. This has mostly been deprecated by VTY based logging configuration, see Section 12 for more information.
-T, --timestamp
Enable time-stamping of log messages to stderr. This has mostly been deprecated by VTY based logging configuration, see Section 12 for more information.

-e, --log-level LOGLEVEL
Set the global log level for logging to stderr. This has mostly been deprecated by VTY based logging configuration, see Section 12 for more information.

-l, --database DATABASE
Specify the file name of the SQLite3 database to use as SMS storage

-M, --mncc-sock-path
Enable the MNCC socket for an external MNCC handler. See Section 15 for further information.

-m, --mncc-sock
Same as option -M (deprecated).

-C, --no-dbcounter
Deprecated. DB statistics and counter has been removed. This option is only valid for compatibility and does nothing.

5.3 Multiple instances

Running multiple instances of osmo-msc on the same computer is possible if all interfaces (VTY, CTRL) are separated using the appropriate configuration options. The IP based interfaces are binding to local host by default. In order to separate the processes, the user has to bind those services to specific but different IP addresses and/or ports.

The VTY and the Control interface can be bound to IP addresses from the loopback address range, for example:

```plaintext
line vty
  bind 127.0.0.2
ctrl
  bind 127.0.0.2
```

If external SMPP is enabled, you may bind it to a different interface using:

```plaintext
smpp
  local-tcp-ip 10.23.42.1 2775
```

More on SMPP configuration in [?].

The external MNCC handler is configured by the --mncc-sock commandline argument. Choose a different such socket path for each OsmoMSC instance running on the same file system. See more in Section 15.2.

For the following links, OsmoMSC acts as a client and does not listen/bind to a specific interface, and will hence not encounter conflicts for multiple instances running on the same interface:

- The SCCP/M3UA links are established by OsmoMSC contacting an STP.
- The GSUP link is established by OsmoMSC contacting an HLR.
- The MGCP link is established by OsmoMSC contacting an MGW.

5.4 Configure primary links

5.4.1 Configure SCCP/M3UA to accept A and luCS links

OsmoMSC will contact an STP instance to establish an SCCP/M3UA link. BSC and HNBGW will then reach the MSC via this link. By default, an STP instance is assumed to listen on the default M3UA port (2905) on the local host.

Establishing an SCCP/M3UA link towards an STP instance not on the local host can be configured as follows:
Note that A and Iu CS may use different SCCP instances, if so desired:

```
cs7 instance 0
  asp my-OsmoMSC-A 2905 0 m3ua
  remote-ip 10.23.42.1

cs7 instance 1
  asp my-OsmoMSC-Iu 2905 0 m3ua
  remote-ip 10.23.42.2

msc
  cs7-instance-a 0
  cs7-instance-iu 1
```

A full configuration needs an `asp` on an `as`—an Application Server Process running on an Application Server—as well as a local point code and routing configuration. The SCCP VTY automatically creates those parts that are missing, by assuming sane defaults. A complete configuration would look like this:

```
cs7 instance 0
  point-code 0.23.1
  asp my-OsmoMSC-A-Iu 2905 0 m3ua
  remote-ip 127.0.0.1
  as my-as-for-OsmoMSC-A-Iu m3ua
  asp my-OsmoMSC-A-Iu
  routing-key 0 0.23.1
```

### 5.4.2 Configure GSUP to reach the HLR

OsmoMSC will assume a GSUP server (OsmoHLR) to run on the local host and the default GSUP port (4222). Contacting an HLR at a different IP address can be configured as follows:

```
hlr
  ! IP address of the remote HLR:
  remote-ip 10.23.42.1
  ! default port is 4222, optionally configurable by:
  remote-port 1234
```

### 6 Control interface

The actual protocol is described in Section 17, the variables common to all programs using it are described in Section 17.2. This section describes the CTRL interface variables specific to OsmoMSC.

**Table 1: Variables available on OsmoMSC’s Control interface**

<table>
<thead>
<tr>
<th>Name</th>
<th>Access</th>
<th>Trap</th>
<th>Value</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>subscriber-list-active-v1</td>
<td>RO</td>
<td>No</td>
<td></td>
<td>Return list of active</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>subscribers.</td>
</tr>
</tbody>
</table>
6.1 subscriber-list-active-v1

Return a list of subscribers that are successfully attached (including full successful authentication and ciphering if those are enabled).

The reply comprises of one subscriber per line, of the format

```
<IMSI>,<MSISDN>
[<IMSI>,<MSISDN>
[...
```

For example:

```
901700000015252,22801
901700000015253,22802
```

7  Osmocom Counters

The following gives an overview of all the types of counters available:

7.1 Osmo Counters (deprecated)

Osmo counters are the oldest type of counters added to Osmocom projects. They are not grouped.

- Printed as part of VTY show stats
- Increment, Decrement
- Accessible through the control interface: `counter.<counter_name>`

7.2 Rate Counters

Rate counters count rates of events.

- Printed as part of VTY show stats
- Intervals: per second, minute, hour, day or absolute value
- Increment only
- Accessible through the control interface
- Rate counters are grouped and different instances per group can exist

The control interface command to get a counter (group) is:

```
rate_ctr.per_{sec,min,hour,day,abs}.<group_name>.<idx>.<counter_name>
```

It is possible to get all counters in a group by omitting the counter name.

7.3 Stat Item

Stat items are a grouped replacement for osmo counters.

- Printed as part of VTY show stats
- Replacement for osmo counters
- Not yet available through the control interface
- Grouped and indexed like rate counters
- Items have a unit
- Keeps a list of the last values measured, so could return an average, min, max, std. deviation. So far this is not implemented in any of the reporting options.
7.4 Statistic Levels

There are three levels on which a statistic can be aggregated in Osmocom projects: globally, per-peer and per-subscriber.

7.4.1 Global

These are global statistics.

7.4.2 Peer

These statistics relate to a peer the program connects to such as the NSVC in an SGSN.
This level also includes reporting global statistics.

7.4.3 Subscriber

These statistics are related to an individual mobile subscriber. An example would be bytes transferred in an SGSN PDP context.
This level also includes global and peer-based statistics.

7.5 Stats Reporter

The stats reporter periodically collects osmo counter, rate counter and stat item values and sends them to a backend. Currently implemented are outputting to the configured log targets and a statsd connector.

7.5.1 Configuring a stats reporter

Periodically printing the statistics to the log can be done in the following way:

Example 7.1 Log statistics

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OsmoBSC&gt; enable</td>
<td></td>
</tr>
<tr>
<td>OsmoBSC# configure terminal</td>
<td></td>
</tr>
<tr>
<td>OsmoBSC(config)# stats interval 60 1</td>
<td>The interval determines how often the statistics are reported.</td>
</tr>
<tr>
<td>OsmoBSC(config)# stats reporter log 2</td>
<td>Write the statistic information to any configured log target.</td>
</tr>
<tr>
<td>OsmoBSC(config-stats)# level global 3</td>
<td>Report only global statistics (can be global, peer, or subscriber).</td>
</tr>
<tr>
<td>OsmoBSC(config-stats)# enable 4</td>
<td>Enable the reporter, disable will disable it again.</td>
</tr>
</tbody>
</table>

The counter values can also be sent to any aggregation/visualization tool that understands the statsd format, for example a statsd server with graphite or prometheus using the statsd_exporter together with grafana.

The statsd format is specified in [https://github.com/b/statsd_spec](https://github.com/b/statsd_spec)
Example 7.2 Report statistics to statsd

OsmoBSC> enable
OsmoBSC# configure terminal
OsmoBSC(config)# stats interval 10
OsmoBSC(config)# stats reporter statsd
OsmoBSC(config-stats)# prefix BSC1
OsmoBSC(config-stats)# level subscriber
OsmoBSC(config-stats)# remote-ip 1.2.3.4
OsmoBSC(config-stats)# remote-port 8125
OsmoBSC(config-stats)# enable

Configure the statsd reporter.
Prefix the reported statistics. This is useful to distinguish statistics from multiple instances of the same service.
Report only global statistics or include peer or subscriber statistics as well.
IP address of the statsd server.
UDP port of the statsd server. Statsd by default listens to port 8125.

Setting up a statsd server and configuring the visualization is beyond the scope of this document.

8 Counters

These counters and their description based on OsmoMSC 1.4.0 (OsmoMSC).

8.1 Rate Counters

Table 2: msc - mobile switching center

<table>
<thead>
<tr>
<th>Name</th>
<th>Reference</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>loc_update_type:attach</td>
<td>[?]</td>
<td>Received Location Update (IMSI Attach) requests.</td>
</tr>
<tr>
<td>loc_update_type:normal</td>
<td>[?]</td>
<td>Received Location Update (LAC change) requests.</td>
</tr>
<tr>
<td>loc_update_type:periodic</td>
<td>[?]</td>
<td>Received (periodic) Location Update requests.</td>
</tr>
<tr>
<td>loc_update_type:detach</td>
<td>[?]</td>
<td>Received IMSI Detach indications.</td>
</tr>
<tr>
<td>loc_update_resp:failed</td>
<td>[?]</td>
<td>Rejected Location Updates requests.</td>
</tr>
<tr>
<td>loc_update_resp:completed</td>
<td>[?]</td>
<td>Successful Location Update procedures.</td>
</tr>
<tr>
<td>cm_service_request:rejected</td>
<td>[?]</td>
<td>Rejected CM Service Requests.</td>
</tr>
<tr>
<td>cm_service_request:accepted</td>
<td>[?]</td>
<td>Accepted CM Service Requests.</td>
</tr>
<tr>
<td>paging_resp:rejected</td>
<td>[?]</td>
<td>Rejected Paging Responses.</td>
</tr>
<tr>
<td>paging_resp:accepted</td>
<td>[?]</td>
<td>Accepted Paging Responses.</td>
</tr>
<tr>
<td>sms:submitted</td>
<td>[?]</td>
<td>Total MO SMS received from the MS.</td>
</tr>
<tr>
<td>sms:no_receiver</td>
<td>[?]</td>
<td>Failed MO SMS delivery attempts (no receiver found).</td>
</tr>
<tr>
<td>sms:deliver_unknown_error</td>
<td>[?]</td>
<td>Failed MO SMS delivery attempts (other reason).</td>
</tr>
<tr>
<td>sms:delivered</td>
<td>[?]</td>
<td>Total MT SMS delivery attempts.</td>
</tr>
<tr>
<td>Name</td>
<td>Reference</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>sms:rp_err_mem</td>
<td>[?]</td>
<td>Failed MT SMS delivery attempts (no memory).</td>
</tr>
<tr>
<td>sms:rp_err_other</td>
<td>[?]</td>
<td>Failed MT SMS delivery attempts (other reason).</td>
</tr>
<tr>
<td>call:mo_setup</td>
<td>[?]</td>
<td>Received MO SETUP messages (MO call establishment).</td>
</tr>
<tr>
<td>call:mo_connect_ack</td>
<td>[?]</td>
<td>Received MO CONNECT messages (MO call establishment).</td>
</tr>
<tr>
<td>call:mt_setup</td>
<td>[?]</td>
<td>Sent MT SETUP messages (MT call establishment).</td>
</tr>
<tr>
<td>call:mt_connect</td>
<td>[?]</td>
<td>Sent MT CONNECT messages (MT call establishment).</td>
</tr>
<tr>
<td>call:active</td>
<td>[?]</td>
<td>Calls that ever reached the active state.</td>
</tr>
<tr>
<td>call:complete</td>
<td>[?]</td>
<td>Calls terminated by DISCONNECT message after reaching the active state.</td>
</tr>
<tr>
<td>call:incomplete</td>
<td>[?]</td>
<td>Calls terminated by any other reason after reaching the active state.</td>
</tr>
<tr>
<td>nc_ss:mo_requests</td>
<td>[?]</td>
<td>Received MS-initiated call independent SS/USSD requests.</td>
</tr>
<tr>
<td>nc_ss:mo_established</td>
<td>[?]</td>
<td>Established MS-initiated call independent SS/USSD sessions.</td>
</tr>
<tr>
<td>nc_ss:mt_requests</td>
<td>[?]</td>
<td>Received network-initiated call independent SS/USSD requests.</td>
</tr>
<tr>
<td>nc_ss:mt_established</td>
<td>[?]</td>
<td>Established network-initiated call independent SS/USSD sessions.</td>
</tr>
<tr>
<td>bssmap:cipher_mode_reject</td>
<td>[?]</td>
<td>Number of CIPHER MODE REJECT messages processed by BSSMAP layer</td>
</tr>
<tr>
<td>bssmap:cipher_mode_complete</td>
<td>[?]</td>
<td>Number of CIPHER MODE COMPLETE messages processed by BSSMAP layer</td>
</tr>
</tbody>
</table>

### 9 Osmo Stat Items

### 10 Osmo Counters

<table>
<thead>
<tr>
<th>Name</th>
<th>Reference</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>msc.active_calls</td>
<td>[?]</td>
<td></td>
</tr>
<tr>
<td>msc.active_nc_ss</td>
<td>[?]</td>
<td></td>
</tr>
</tbody>
</table>
11 The Osmocom VTY Interface

All human interaction with Osmocom software is typically performed via an interactive command-line interface called the **VTY**.

**Note**
Integration of your programs and scripts should **not** be done via the telnet VTY interface, which is intended for human interaction only: the VTY responses may arbitrarily change in ways obvious to humans, while your scripts’ parsing will likely break often. For external software to interact with Osmocom programs (besides using the dedicated protocols), it is strongly recommended to use the Control interface instead of the VTY, and to actively request / implement the Control interface commands as required for your use case.

The interactive telnet VTY is used to
- explore the current status of the system, including its configuration parameters, but also to view run-time state and statistics,
- review the currently active (running) configuration,
- perform interactive changes to the configuration (for those items that do not require a program restart),
- store the current running configuration to the config file,
- enable or disable logging; to the VTY itself or to other targets.

The Virtual Tele Type (VTY) has the concept of **nodes** and **commands**. Each command has a name and arguments. The name may contain a space to group several similar commands into a specific group. The arguments can be a single word, a string, numbers, ranges or a list of options. The available commands depend on the current node. there are various keyboard shortcuts to ease finding commands and the possible argument values.

Configuration file parsing during program start is actually performed the VTY’s CONFIG node, which is also available in the telnet VTY. Apart from that, the telnet VTY features various interactive commands to query and instruct a running Osmocom program. A main difference is that during config file parsing, consistent indenting of parent vs. child nodes is required, while the interactive VTY ignores indenting and relies on the exit command to return to a parent node.

**Note**
In the **CONFIG** node, it is not well documented which commands take immediate effect without requiring a program restart. To save your current config with changes you may have made, you may use the write file command to **overwrite** your config file with the current configuration, after which you should be able to restart the program with all changes taking effect.

This chapter explains most of the common nodes and commands. A more detailed list is available in various programs’ VTY reference manuals, e.g. see [vty-ref-osmomsc](#).

There are common patterns for the parameters, these include IPv4 addresses, number ranges, a word, a line of text and choice. The following will explain the commonly used syntactical patterns:

<table>
<thead>
<tr>
<th>Pattern</th>
<th>Example</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.B.C.D</td>
<td>127.0.0.1</td>
<td>An IPv4 address</td>
</tr>
<tr>
<td>TEXT</td>
<td>example01</td>
<td>A single string without any spaces, tabs</td>
</tr>
<tr>
<td>.TEXT</td>
<td>Some information</td>
<td>A line of text</td>
</tr>
<tr>
<td>(OptionA</td>
<td>OptionB</td>
<td>OptionC)</td>
</tr>
<tr>
<td>&lt;0-10&gt;</td>
<td>5</td>
<td>A number from a range</td>
</tr>
</tbody>
</table>
11.1 Accessing the telnet VTY

The VTY of a given Osmocom program is implemented as a telnet server, listening to a specific TCP port. Please see Appendix A to check for the default TCP port number of the VTY interface of the specific Osmocom software you would like to connect to.

As telnet is insecure and offers neither strong authentication nor encryption, the VTY by default only binds to localhost (127.0.0.1) and will thus not be reachable by other hosts on the network.

![Warning]

By default, any user with access to the machine running the Osmocom software will be able to connect to the VTY. We assume that such systems are single-user systems, and anyone with local access to the system also is authorized to access the VTY. If you require stronger security, you may consider using the packet filter of your operating system to restrict access to the Osmocom VTY ports further.

11.2 VTY Nodes

The VTY by default has the following minimal nodes:

**VIEW**
When connecting to a telnet VTY, you will be on the VIEW node. As its name implies, it can only be used to view the system status, but it does not provide commands to alter the system state or configuration. As long as you are in the non-privileged VIEW node, your prompt will end in a > character.

**ENABLE**
The ENABLE node is entered by the enable command, from the VIEW node. Changing into the ENABLE node will unlock all kinds of commands that allow you to alter the system state or perform any other change to it. The ENABLE node and its children are signified by a # character at the end of your prompt. You can change back from the ENABLE node to the VIEW node by using the disable command.

**CONFIG**
The CONFIG node is entered by the configure terminal command from the ENABLE node. The config node is used to change the run-time configuration parameters of the system. The prompt will indicate that you are in the config node by a (config)# prompt suffix. You can always leave the CONFIG node or any of its children by using the end command. This node is also automatically entered at the time the configuration file is read. All configuration file lines are processed as if they were entered from the VTY CONFIG node at start-up.

Other
Depending on the specific Osmocom program you are running, there will be few or more other nodes, typically below the CONFIG node. For example, the OsmoBSC has nodes for each BTS, and within the BTS node one for each TRX, and within the TRX node one for each Timeslot.

11.3 Interactive help

The VTY features an interactive help system, designed to help you to efficiently navigate is commands.

---

**Note**
The VTY is present on most Osmocom GSM/UMTS/GPRS software, thus this chapter is present in all the relevant manuals. The detailed examples below assume you are executing them on the OsmoMSC VTY. They will work in similar fashion on the other VTY interfaces, while the node structure will differ in each program.
11.3.1 The question-mark (?) command

If you type a single ? at the prompt, the VTY will display possible completions at the exact location of your currently entered command.

If you type ? at an otherwise empty command (without having entered even only a partial command), you will get a list of the first word of all possible commands available at this node:

Example: Typing ? at start of OsmoMSC prompt

```
OsmoMSC> ?
show Show running system information
list Print command list
exit Exit current mode and down to previous mode
help Description of the interactive help system
enable Turn on privileged mode command
terminal Set terminal line parameters
who Display who is on vty
logging Configure logging
no Negate a command or set its defaults
sms SMS related commands
subscriber Operations on a Subscriber
```

Type ? here at the prompt, the ? itself will not be printed.

If you have already entered a partial command, ? will help you to review possible options of how to continue the command. Let’s say you remember that show is used to investigate the system status, but you don’t remember the exact name of the object. Hitting ? after typing show will help out:

Example: Typing ? after a partial command

```
OsmoMSC> show ?
version Displays program version
online-help Online help
history Display the session command history
cs7 ITU-T Signaling System 7
logging Show current logging configuration
alarms Show current logging configuration
talloc-context Show talloc memory hierarchy
stats Show statistical values
asciidoc Asciidoc generation
rate-counters Show all rate counters
fsm Show information about finite state machines
fsm-instances Show information about finite state machine instances
sgs-connections Show SGs interface connections / MMEs
subscriber Operations on a Subscriber
bsc BSC
connection Subscriber Connections
transaction Transactions
statistics Display network statistics
sms-queue Display SMSqueue statistics
smpp SMPP Interface
```

Type ? after the show command, the ? itself will not be printed.

You may pick the bsc object and type ? again:

Example: Typing ? after show bsc

```
OsmoMSC> show bsc
<cr>
```

By presenting <cr> as the only option, the VTY tells you that your command is complete without any remaining arguments being available, and that you should hit enter, a.k.a. “carriage return”.

Copyright © 2017 sysmocom - s.f.m.c. GmbH
11.3.2 TAB completion

The VTY supports tab (tabulator) completion. Simply type any partial command and press `<tab>`, and it will either show you a list of possible expansions, or completes the command if there’s only one choice.

Example: Use of `<tab>` pressed after typing only `s` as command

```
OsmoMSC> s

Type `<tab>` here.
```

At this point, you may choose `show`, and then press `<tab>` again:

Example: Use of `<tab>` pressed after typing `show` command

```
OsmoMSC> show

Type `<tab>` here.
```

11.3.3 The `list` command

The `list` command will give you a full list of all commands and their arguments available at the current node:

Example: Typing `list` at start of OsmoMSC VIEW node prompt

```
OsmoMSC> list

show version
show online-help
list
exit
help
enable
terminal length <0-512>
terminal no length
who
show history
show cs7 instance <0-15> users
show cs7 (sua|m3ua|ipa) [0-65534]
show cs7 instance <0-15> asp
show cs7 instance <0-15> as (active|all|m3ua|sua)
show cs7 instance <0-15> sccp addressbook
show cs7 instance <0-15> sccp users
show cs7 instance <0-15> sccp ssn <0-65535>
show cs7 instance <0-15> sccp connections
show cs7 instance <0-15> sccp timers
logging enable
logging disable
logging filter all (0|1)
logging color (0|1)
logging timestamp (0|1)
logging print extended-timestamp (0|1)
logging print category (0|1)
logging print category-hex (0|1)
logging print level (0|1)
logging print file (0|1|basename) [last]
```
logging set-log-mask MASK
logging level {ril|cc|mm|r|mncc|pag|msg|mcp|ho|db|ref|ctrl|smmp|ranap|vrl|iucs|bssap|←
sqs|lglobal|llapd|linp|lmux|lmi|limb|lms|ctcl|lgtp|lstats|lgss|loap|lss7|lsccp|lsua←
|lm3ua|lmgcpl|ljibuf|lrspol} (debug|info|notice|error|fatal)
logging level set-all (debug|info|notice|error|fatal)
logging level force-all (debug|info|notice|error|fatal)
no logging level force-all
show logging vty
show alarms
show talloc-context {application|all} {full|brief|DEPTH} show talloc-context {application|all} {full|brief|DEPTH} tree ADDRESS
show talloc-context {application|all} {full|brief|DEPTH} filter REGEXP
show stats
show stats level {global|peer|subscriber}
show ascidoc counters
show rate-counters
show fsm NAME
show fsm all
show fsm-instances NAME
show fsm-instances all
show sgs-connections
show subscriber {msisdn|extension|imsi|tmsi|id} ID
show subscriber cache
show bsc
show connection
show transaction
sms send pending
sms delete expired
subscriber create imsi ID
subscriber {msisdn|extension|imsi|tmsi|id} ID sms sender {msisdn|extension|imsi|tmsi|id}
SEND | SE | ID | SENDER_ID | send | LINE
subscriber {msisdn|extension|imsi|tmsi|id} ID silent-sms sender {msisdn|extension|imsi|tmsi|id} send LINE
subscriber {msisdn|extension|imsi|tmsi|id} ID silent-call start {any|tch/f|fch/any|sdccch}
subscriber {msisdn|extension|imsi|tmsi|id} ID silent-call stop
subscriber {msisdn|extension|imsi|tmsi|id} ID ussd-notify {0|1|2} TEXT
subscriber {msisdn|extension|imsi|tmsi|id} ID ms-test close-loop {a|b|c|d|e|f|i}
subscriber {msisdn|extension|imsi|tmsi|id} ID ms-test open-loop
subscriber {msisdn|extension|imsi|tmsi|id} ID paging
show statistics
show sms-queue
logging filter imsi IMSI
show smpp esme

**Tip**
Remember, the list of available commands will change significantly depending on the Osmocom program you are accessing, its software version and the current node you’re at. Compare the above example of the OsmoMSC **VIEW** node with the list of the OsmoMSC **NETWORK** config node:

**Example: Typing list at start of OsmoMSC NETWORK config node prompt**

```
OsmoMSC(config-net)# list
help
list
write terminal
write file
write memory
write
show running-config
```
exit
double country code <1-999>
mobile network code <0-999>
short name NAME
long name NAME
decryption a5 <0-3> [<=0-3>] [<=0-3>] [<=0-3>]
an authentication (optional|required)
rrlp mode (none|ms-based|ms-preferred|ass-preferred)
mm info (0|1)
timezone <-19-19> (0|15|30|45)
timezone <-19-19> (0|15|30|45) <0-2>
no timezone
periodic location update <6-1530>
no periodic location update

12 libosmocore Logging System

In any reasonably complex software it is important to understand how to enable and configure logging in order to get a better
insight into what is happening, and to be able to follow the course of action. We therefore ask the reader to bear with us while
we explain how the logging subsystem works and how it is configured.

Most Osmocom Software (like osmo-bts, osmo-bsc, osmo-nitb, osmo-sgsn and many others) uses the same common
logging system.

This chapter describes the architecture and configuration of this common logging system.

The logging system is composed of

- log targets (where to log),
- log categories (who is creating the log line),
- log levels (controlling the verbosity of logging), and
- log filters (filtering or suppressing certain messages).

All logging is done in human-readable ASCII-text. The logging system is configured by means of VTY commands that can
either be entered interactively, or read from a configuration file at process start time.

12.1 Log categories

Each sub-system of the program in question typically logs its messages as a different category, allowing fine-grained control over
which log messages you will or will not see. For example, in OsmoBSC, there are categories for the protocol layers rsl, rr,
mm, cc and many others. To get a list of categories interactively on the vty, type: logging level ?

12.2 Log levels

For each of the log categories (see Section 12.1), you can set an independent log level, controlling the level of verbosity. Log
levels include:

fatal
  Fatal messages, causing abort and/or re-start of a process. This shouldn’t happen.

teror
  An actual error has occurred, its cause should be further investigated by the administrator.
**notice**

A noticeable event has occurred, which is not considered to be an error.

**info**

Some information about normal/regular system activity is provided.

**debug**

Verbose information about internal processing of the system, used for debugging purpose. This will log the most.

The log levels are inclusive, e.g. if you select `info`, then this really means that all events with a level of at least `info` will be logged, i.e. including events of `notice`, `error` and `fatal`.

So for example, in OsmoBSC, to set the log level of the Mobility Management category to info, you can use the following command: `log level mm info`.

There is also a special command to set all categories as a one-off to a desired log level. For example, to silence all messages but those logged as notice and above issue the command: `log level set-all notice`.

Afterwards you can adjust specific categories as usual.

A similar command is `log level force-all <level>` which causes all categories to behave as if set to log level `<level>` until the command is reverted with `no log level force-all` after which the individually-configured log levels will again take effect. The difference between `set-all` and `force-all` is that `set-all` actually changes the individual category settings while `force-all` is a (temporary) override of those settings and does not change them.

### 12.3 Log printing options

The logging system has various options to change the information displayed in the log message.

**log color 1**

With this option each log message will log with the color of its category. The color is hard-coded and cannot be changed. As with other options a `0` disables this functionality.

**log timestamp 1**

Includes the current time in the log message. When logging to syslog this option should not be needed, but may come in handy when debugging an issue while logging to file.

**log print extended-timestamp 1**

In order to debug time-critical issues this option will print a timestamp with millisecond granularity.

**log print category 1**

Prefix each log message with the category name.

**log print category-hex 1**

Prefix each log message with the category number in hex (`<000b>`).

**log print level 1**

Prefix each log message with the name of the log level.

**log print file 1**

Prefix each log message with the source file and line number. Append the keyword `last` to append the file information instead of prefixing it.

### 12.4 Log filters

The default behavior is to filter out everything, i.e. not to log anything. The reason is quite simple: On a busy production setup, logging all events for a given subsystem may very quickly be flooding your console before you have a chance to set a more restrictive filter.

To request no filtering, i.e. see all messages, you may use: `log filter all 1`
In addition to generic filtering, applications can implement special log filters using the same framework to filter on particular context.

For example in OsmoBSC, to only see messages relating to a particular subscriber identified by his IMSI, you may use: `log filter imsi 262020123456789`

### 12.5 Log targets

Each of the log targets represent certain destination for log messages. It can be configured independently by selecting levels (see Section 12.2) for categories (see Section 12.1) as well as filtering (see Section 12.4) and other options like `logging timestamp` for example.

#### 12.5.1 Logging to the VTY

Logging messages to the interactive command-line interface (VTY) is most useful for occasional investigation by the system administrator.

Logging to the VTY is disabled by default, and needs to be enabled explicitly for each such session. This means that multiple concurrent VTY sessions each have their own logging configuration. Once you close a VTY session, the log target will be destroyed and your log settings be lost. If you re-connect to the VTY, you have to again activate and configure logging, if you wish.

To create a logging target bound to a VTY, you have to use the following command: `logging enable` This doesn’t really activate the generation of any output messages yet, it merely creates and attaches a log target to the VTY session. The newly-created target still doesn’t have any filter installed, i.e. all log messages will be suppressed by default

Next, you can configure the log levels for desired categories in your VTY session. See Section 12.1 for more details on categories and Section 12.2 for the log level details.

For example, to set the log level of the Call Control category to debug, you can use: `log level cc debug`

Finally, after having configured the levels, you still need to set the filter as it’s described in Section 12.4.

**Tip**

If many messages are being logged to a VTY session, it may be hard to impossible to still use the same session for any commands. We therefore recommend to open a second VTY session in parallel, and use one only for logging, while the other is used for interacting with the system. Another option would be to use different log target.

To review the current vty logging configuration, you can use: `show logging vty`

#### 12.5.2 Logging to the ring buffer

To avoid having separate VTY session just for logging output while still having immediate access to them, one can use `alarms` target. It lets you store the log messages inside the ring buffer of a given size which is available with `show alarms` command.

It’s configured as follows:

```
OsmoBSC> enable
OsmoBSC# configure terminal
OsmoBSC(config)# log alarms 98
OsmoBSC(config-log)#
```

In the example above 98 is the desired size of the ring buffer (number of messages). Once it’s filled, the incoming log messages will push out the oldest messages available in the buffer.
12.5.3 Logging via gsmtap

When debugging complex issues it’s handy to be able to reconstruct exact chain of events. This is enabled by using GSMTAP log output where frames sent/received over the air are interspersed with the log lines. It also simplifies the bug handling as users don’t have to provide separate .pcap and .log files anymore - everything will be inside self-contained packet dump.

It’s configured as follows:

```
OsmoBSC> enable
OsmoBSC# configure terminal
OsmoBSC(config)# log gsmtap 192.168.2.3
OsmoBSC(config-log)#
```

The hostname/ip argument is optional: if omitted the default 127.0.0.1 will be used. The log strings inside GSMTAP are already supported by Wireshark. Capturing for port 4729 on appropriate interface will reveal log messages including source file name and line number as well as application. This makes it easy to consolidate logs from several different network components alongside the air frames. You can also use Wireshark to quickly filter logs for a given subsystem, severity, file name etc.

```
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```

```
Frame 1: 265 bytes on wire (1640 bits), 265 bytes captured (1640 bits) on

Linux cooked capture
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
User Datagram Protocol, Src Port: 42805, Dst Port: 4729
GSMTAP libosmocore logging OsmoBSC(0): NW/5: abis.nm.c:2843 [nts=6,tx=6]
Application: OsmoBSC
Process ID: 0
Log level: NOTICE (5)
```

```
Source File Name: abis.nm.c
Source File Line Number: 2043
String: [nts=6,tx=6] Changing adm. state Unlocked -> Unlocked [vty]\n```

```
Frame 2: Wireshark with logs delivered over GSMTAP
```

Note: the logs are also duplicated to stderr when GSMTAP logging is configured because stderr is the default log target which is initialized automatically. To decrease stderr logging to absolute minimum, you can configure it as follows:

```
OsmoBSC> enable
OsmoBSC# configure terminal
OsmoBSC(config)# log stderr
OsmoBSC(config-log)# logging level force-all fatal
```

12.5.4 Logging to a file

As opposed to Logging to the VTY, logging to files is persistent and stored in the configuration file. As such, it is configured in sub-nodes below the configuration node. There can be any number of log files active, each of them having different settings.
Regarding levels/subsystems.

To configure a new log file, enter the following sequence of commands:

```bash
OsmoBSC> enable
OsmoBSC# configure terminal
OsmoBSC(config)# log file /path/to/my/file
OsmoBSC(config-log)#
```

This leaves you at the config-log prompt, from where you can set the detailed configuration for this log file. The available commands at this point are identical to configuring logging on the VTY; they include logging filter, logging level as well as logging color and logging timestamp.

**Tip**

Don’t forget to use the `copy running-config startup-config` (or its short-hand `write file`) command to make your logging configuration persistent across application re-start.

**Note**

Libosmocore provides file close-and-reopen support by SIGHUP, as used by popular log file rotating solutions such as https://github.com/logrotate/logrotate found in most GNU/Linux distributions.

### 12.5.5 Logging to syslog

Syslog is a standard for computer data logging maintained by the IETF. Unix-like operating systems like GNU/Linux provide several syslog compatible log daemons that receive log messages generated by application programs.

Libosmocore based applications can log messages to syslog by using the syslog log target. You can configure syslog logging by issuing the following commands on the VTY:

```bash
OsmoBSC> enable
OsmoBSC# configure terminal
OsmoBSC(config)# log syslog daemon
OsmoBSC(config-log)#
```

This leaves you at the config-log prompt, from where you can set the detailed configuration for this log file. The available commands at this point are identical to configuring logging on the VTY; they include logging filter, logging level as well as logging color and logging timestamp.

**Note**

Syslog daemons will normally automatically prefix every message with a time-stamp, so you should disable the libosmocore time-stamping by issuing the `logging timestamp 0` command.

### 12.5.6 Logging to stderr

If you’re not running the respective application as a daemon in the background, you can also use the stderr log target in order to log to the standard error file descriptor of the process.

In order to configure logging to stderr, you can use the following commands:

```bash
OsmoBSC> enable
OsmoBSC# configure terminal
OsmoBSC(config)# log stderr
OsmoBSC(config-log)#
```
13 Configuring the Core Network

The core network parameters are configured by the config file (as in osmo-msc -c osmo-msc.cfg). The config file is parsed by the VTY, which is also available via telnet in the running osmo-msc instance. Be aware that even though you may be able to change these parameters without restarting osmo-msc, some may not take immediate effect, and it is safest to use the config file to have these parameters set at startup time.

The core network parameters are found in the config/network.

A full reference to the available commands can be found in the OsmoMSC VTY reference manual [vty-ref-osmomsc]. This section describes only the most commonly used settings.

Here is an overview of the config items, described in more detail below:

```
network
network country code 262
mobile network code 89
mm info 1
short name OsmoMSC
long name OsmoMSC
authentication required
encryption a5 3
```

Tip
Use the telnet VTY interface to query the current configuration of a running osmo-msc process:

```
$ telnet localhost 4254
OsmoMSC> enable
OsmoMSC# show running-config
```

Some parameters may be changed without restarting osmo-msc. To reach the network node, enter:

```
OsmoMSC> enable
OsmoMSC# configure terminal
OsmoMSC(config)# network
OsmoMSC(config-net)# short name Example-Name
OsmoMSC(config-net)# exit
OsmoMSC(config)#
```

The telnet VTY features tab-completion as well as context sensitive help shown when entering a ? question mark. You can always use the list VTY command or enter ? on the blank prompt to get a list of all possible commands at the current node.

13.1 MCC/MNC

The key identities of every GSM PLMN is the Mobile Country Code and the Mobile Network Code. They are identical over the entire network. In most cases, the MCC/MNC will be allocated to the operator by the respective local regulatory authority. For example, to set the MCC/MNC of 262-89, have this in your osmo-msc.cfg:

```
network
network country code 262
mobile network code 89
```

13.2 Configuring MM INFO

The MM INFO procedure can be used after a successful LOCATION UPDATE in order to transmit the human-readable network name as well as local time zone information to the MS. By default, MM INFO is not active, i.e. 0. Set to 1 to activate this feature:
Note
Not all phones support the MM INFO procedure. If a phone is not factory-programmed to contain the name for your MCC/MNC, it will likely only provide a numeric display of the network name, such as 262-89, or show the country code transformed into a letter, such as D 89.

The time information transmitted is determined by the local system time of the operating system on which OsmoMSC is running.

13.3 Authentication

A subscriber’s IMSI must be entered in the HLR database to be able to attach. A subscriber-create-on-demand feature is also available, see the OsmoHLR reference manual [userman-osmohlr].

A known IMSI in the HLR may or may not have authentication keys associated, which profoundly affects the ability to attach and the algorithms used to negotiate authentication, as the following sections explain for 2G and 3G.

13.3.1 Authentication on 2G

If authentication tokens (such as KI for 2G, or K and OP/OPC for UMTS) are present in the HLR, OsmoMSC will only attach a subscriber after successful authentication. Note that the 3G authentication keys are also used on 2G when the MS indicates UMTS AKA capability, in which case the full UMTS style mutual authentication may indeed take place on 2G (GERAN).

On 2G, if no authentication keys are present in the HLR for a given subscriber, OsmoMSC will attach the subscriber without authentication. Subscribers that lack authentication keys can always be rejected with this setting:

network authentication required

13.3.2 Authentication on 3G

3G (UTRAN) always requires authentication (a.k.a. Integrity Protection) by specification, and hence authentication keys must be present in the HLR for a subscriber to be able to attach on 3G.

OsmoMSC always indicates UIA1 and UIA2 as permitted Integrity Protection algorithms on 3G.

13.4 Ciphering

To enable ciphering on the radio link, authentication must take place first: the Kc resulting from authentication is the key used for ciphering. Hence, to be able to use ciphering, a subscriber must have authentication tokens available in the HLR.

13.4.1 Ciphering on 2G

The MS, BTS and MSC must agree on a ciphering algorithm to use.

- The MS sends its supported ciphering algorithms via Classmark IEs during Location Updating.
- Typically the BSC needs to know which A5 ciphers are supported by connected BTSes, see the network / encryption a5 configuration item for OsmoBSC [vty-ref-osmobsc].
• Finally, OsmoMSC may impose that specific A5 ciphers shall not be considered.

It is the responsibility of the BSC to then pick an A5 cipher that satisfies all requirements.

• In OsmoMSC, A5/0 means that ciphering is turned off.

```
network
encryption a5 0
```

• A5/1 and A5/3 are currently supported by Osmocom.

```
network
encryption a5 1 3
```

• Never use A5/2: it is an "export grade cipher" and has been deprecated for its low ciphering strength.

• To allow either no encryption or any of A5/1 or A5/3 based on the presence of authentication keys and abilities of the MS, SIM and BSC configuration, it is recommended to enable all ciphers in OsmoMSC. The highest available A5 cipher will be used; the order in which the A5 options are configured does not affect the choice.

```
network
encryption a5 0 1 3
```

### 13.4.2 Ciphering on 3G

While authentication is always required on 3G, ciphering is optional.

So far OsmoMSC allows switching ciphering on 3G either on or off — the default behavior is to enable ciphering. (Individual choice of algorithms may be added in the future.)

Disable 3G ciphering:

```
network
encryption uea 0
```

Enable 3G ciphering (default):

```
network
encryption uea 1 2
```

OsmoMSC indicates UEA1 and UEA2 as permitted encryption algorithms on 3G.

### 14 Short Message Peer to Peer (SMPP)

The *Short Message Peer to Peer (SMPP) Protocol* [smpp-34] has been used for the communication with SMSCs. Osmocom implements version 3.4 of the protocol. Using this interface one can send MT-SMS to an attached subscriber or receive unrouted MO-SMS.

SMPP is served by the Osmocom MSC layer (both in the old OsmoNITB as well as the new OsmoMSC).

SMPP describes a situation where multiple ESMEs (External SMS Entities) interact with a SMSC (SMS Service Center) via the SMPP protocol. Each entity is identified by its System Id. The System ID is a character string which is configured by the system administrator.

OsmoMSC implements the SMSC side of SMPP and subsequently acts as a TCP server accepting incoming connections from ESME client programs.

Each ESME identifies itself to the SMSC with its system-id and an optional shared password.
14.1 Global SMPP configuration

There is a smpp vty node at the top level of the OsmoMSC configuration. Under this node, the global SMPP configuration is performed.

Use the local-tcp-ip command to define the TCP IP and port at which the OsmoMSC internal SMSC should listen for incoming SMPP connections. The default behaviour is to listen on all IPs (0.0.0.0), and the default port assigned to SMPP is 2775.

Use the system-id command to define the System ID of the SMSC.

Use the policy parameter to define whether only explicitly configured ESMEs are permitted to access the SMSC (closed), or whether any ESME should be accepted (accept-all).

Use the smpp-first command to define if SMPP routes have higher precedence than MSISDNs contained in the HLR (smpp-first), or if only MSISDNs found not in the HLR should be considered for routing to SMPP (no smpp-first).

14.2 ESME configuration

Under the smpp vty node, you can add any number of esme nodes, one for each ESME that you wish to configure.

Use the esme NAME command (where NAME corresponds to the system-id of the ESME to be configured) under the SMPP vty node to enter the configuration node for this given ESME.

Use the password command to specify the password (if any) for the ESME.

Use the default-route command to indicate that any MO-SMS without a more specific route should be routed to this ESME.

Use the deliver-src-imsi command to indicate that the SMPP DELIVER messages for MO SMS and the SMPP ALERT should state the IMSI (rather than the MSISDN) as source address.

Use the osmocom-extensions command to request that Osmocom specific extension TLVs shall be included in the SMPP PDUs. Those extensions include the ARFCN of the cell, the L1 transmit power of the MS, the timing advance, the uplink and downlink RxLev and RxQual, as well as the IMEI of the terminal at the time of generating the SMPP DELIVER PDU.

Use the dcs-transparent command to transparently pass the DCS value from the SMS Layer3 protocols to SMPP, instead of converting them to the SMPP-specific values.

Use the route prefix command to specify a route towards this ESME. Using routes, you specify which destination MSISDNs should be routed towards your ESME.

14.3 Example configuration snippet

The following example configuration snippet shows a single ESME galactica with a prefix-route of all national numbers stating with 2342:

```
smpp
local-tcp-port 2775
policy closed
no smpp-first
esme galactica
password SoSayWeAll
deliver-src-imsi
osmocom-extensions
route prefix national isdn 2342
```

14.4 Osmocom SMPP protocol extensions

Osmocom has implemented some extensions to the SMPP v3.4 protocol.

These extensions can be enabled using the osmocom-extensions VTY command at esme level.

The TLV definitions can be found in the `<osmocom/gsm/protocol/smpp34_osmocom.h>` header file provided by libosmocore.
14.4.1 RF channel measurements

When the Osmocom SMPP extensions are enabled, we add the following TLVs to each SMPP DELIVER PDU:

<table>
<thead>
<tr>
<th>TLV</th>
<th>IEI</th>
<th>Length (Octets)</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLVID_osmo_arfcn</td>
<td>0x2300</td>
<td>2</td>
<td>GSM ARFCN of the radio interface</td>
</tr>
<tr>
<td>TLVID_osmo_ta</td>
<td>0x2301</td>
<td>1</td>
<td>Timing Advance on the radio interface</td>
</tr>
<tr>
<td>TLVID_osmo_ms_l1_txpwr</td>
<td>0x2307</td>
<td>1</td>
<td>Uplink Power of the MS in uplink direction</td>
</tr>
<tr>
<td>TLVID_osmo_rxlev_ul</td>
<td>0x2302</td>
<td>2</td>
<td>Uplink receive level as measured by BTS in dBm (int16_t)</td>
</tr>
<tr>
<td>TLVID_osmo_rxqual_ul</td>
<td>0x2303</td>
<td>1</td>
<td>Uplink RxQual value as measured by BTS</td>
</tr>
<tr>
<td>TLVID_osmo_rxlev_dl</td>
<td>0x2304</td>
<td>2</td>
<td>Downlink receive level as measured by MS in dBm (int16_t)</td>
</tr>
<tr>
<td>TLVID_osmo_rxqual_dl</td>
<td>0x2305</td>
<td>1</td>
<td>Downlink RxQual value as measured by MS</td>
</tr>
</tbody>
</table>

All of the above values reflect the last measurement report as received via A-bis RSL from the BTS. It is thus a snapshot value (of the average within one 480ms SACCH period), and not an average over all the SACCH periods during which the channel was open or the SMS was received. Not all measurement reports contain all the values. So you might not get a TLVID_osmo_rxlev_dl IE, as that particular uplink frame might have been lost for the given snapshot we report.

14.4.2 Equipment IMEI

If we know the IMEI of the subscriber’s phone, we add the following TLV to each SMPP DELIVER PDU:

<table>
<thead>
<tr>
<th>TLV</th>
<th>IEI</th>
<th>Length</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLVID_osmo_imei</td>
<td>0x2306</td>
<td>variable</td>
<td>IMEI of the subscriber’s phone (ME)</td>
</tr>
</tbody>
</table>

15 MNCC for External Call Control

The 3GPP GSM specifications define an interface point (service access point) inside the MSC between the call-control part and the rest of the system. This service access point is called the MNCC-SAP. It is described in 3GPP TS 24.007 [3gpp-ts-24-007] Chapter 7.1.

However, like for all internal interfaces, 3GPP does not give any specific encoding for the primitives passed at this SAP.

The MNCC protocol has been created by the Osmocom community and allows to control the call handling and audio processing by an external application. The interface is currently exposed using Unix Domain Sockets. The protocol is defined in the mncc.h header file.

It is exposed by the Osmocom MSC layer (both in the old OsmoNITB as well as the new OsmoMSC.

OsmoMSC can run in two different modes:

1. with internal MNCC handler
2. with external MNCC handler

15.1 Internal MNCC handler

When the internal MNCC handler is enabled, OsmoMSC will switch voice calls between GSM subscribers internally and automatically based on the the subscribers extension number. No external software is required.

**Note**

Internal MNCC is the default behavior.
15.1.1 Internal MNCC Configuration

The internal MNCC handler offers some configuration parameters under the `mncc-int` VTY configuration node.

15.1.1.1 `default-codec tch-f (fr|efr|amr)`

Using this command, you can configure the default voice codec to be used by voice calls on TCH/F channels.

15.1.1.2 `default-codec tch-h (hr|amr)`

Using this command, you can configure the default voice codec to be used by voice calls on TCH/H channels.

15.2 External MNCC handler

When the external MNCC handler is enabled, OsmoMSC will not perform any internal call switching, but delegate all call-control handling towards the external MNCC program connected via the MNCC socket.

If you intend to operate OsmoMSC with external MNCC handler, you have to start it with the `-m` or `--mncc-sock` command line option.

At the time of this writing, the only external application implementing the MNCC interface compatible with the Osmocom MNCC socket is lcr, the Linux Call Router. More widespread integration of external call routing is available via the OsmoSIP-Connector.

15.3 DTMF considerations

In mobile networks, the signaling of DTMF tones is implemented differently, depending on the signaling direction. A mobile originated DTMF tone is signaled using START/STOP DTMF messages which are hauled through various protocols upwards into the core network.

Contrary to that, a mobile terminated DTMF tone is not transferred as an out of band message. Instead, in-band signaling is used, which means a tone is injected early inside a PBX or MGW.

When using OsmoMSC with its built in MNCC functionality a mobile originated DTMF message will not be translated into an in-band tone. Therefore, sending DTMF will not work when internal MNCC is used.

For external MNCC, the network integrator must make sure that the back-end components are configured properly in order to handle the two different signaling schemes depending on the signaling direction.

Note

osmo-sip-connector will translate MNCC DTMF signaling into sip-info messages. DTMF signaling in the opposite direction is not possible. osmo-sip-connector will reject sip-info messages that attempt to signal a DTMF tone.

15.4 MNCC protocol description

The protocol follows the primitives specified in 3GPP TS 04.07 Chapter 7.1. The encoding of the primitives is provided in the `mncc.h` header file in OsmoMSC’s source tree, which uses some common definitions from `osmocom/gsm/mncc.h` (part of libosmocore.git).

However, Osmocom’s MNCC specifies a number of additional primitives beyond those listed in the 3GPP specification.

The different calls in the network are distinguished by their callref (call reference), which is a unique unsigned 32bit integer.
15.4.1 MNCC_HOLD_IND
Direction: OsmoMSC → Handler
A CC HOLD message was received from the MS.

15.4.2 MNCC_HOLD_CNF
Direction: Handler → OsmoMSC
Acknowledge a previously-received CC HOLD message, causes the transmission of a CC HOLD ACK message to the MS.

15.4.3 MNCC_HOLD_REJ
Direction: Handler → OsmoMSC
Reject a previously-received CC HOLD message, causes the transmission of a CC HOLD REJ message to the MS.

15.4.4 MNCC_RETRIEVE_IND
Direction: OsmoMSC → Handler
A CC RETRIEVE message was received from the MS.

15.4.5 MNCC_RETRIEVE_CNF
Direction: Handler → OsmoMSC
Acknowledge a previously-received CC RETRIEVE message, causes the transmission of a CC RETRIEVE ACK message to the MS.

15.4.6 MNCC_RETRIEVE_REJ
Direction: Handler → OsmoMSC
Reject a previously-received CC RETRIEVE message, causes the transmission of a CC RETRIEVE REJ message to the MS.

15.4.7 MNCC_USERINFO_REQ
Direction: OsmoMSC → Handler
Causes a CC USER INFO message to be sent to the MS.

15.4.8 MNCC_USERINFO_IND
Direction: OsmoMSC → Handler
Indicates that a CC USER-USER message has been received from the MS.
15.4.9 MNCC_BRIDGE

Direction: Handler → OsmoMSC

Requests that the TCH (voice) channels of two calls shall be inter-connected. This is the old-fashioned way of using MNCC, historically required for circuit-switched BTSs whose TRAU frames are received via an E1 interface card, and works only when the TCH channel types match.

**Note**

Internal MNCC uses MNCC_BRIDGE to connect calls directly between connected BTSs or RNCs, in effect disallowing calls between mismatching TCH types and forcing all BTSs to be configured with exactly one TCH type and codec. This is a limitation that will probably remain for the old OsmoNITB. For the new OsmoMSC, the MNCC_BRIDGE command will instruct the separate OsmoMGW to bridge calls, which will be able to handle transcoding between different TCH as well as 3G (IuUP) payloads (but note: not yet implemented at the time of writing this). Hence an external MNCC may decide to bridge calls directly between BTSs or RNCs that both are internal to the OsmoMSC, for optimization reasons.

15.4.10 MNCC_FRAME_RECV

Direction: Handler → OsmoMSC

Enable the forwarding of TCH voice frames via the MNCC interface in OsmoMSC→Handler direction for the specified call.

15.4.11 MNCC_FRAME_DROP

Direction: Handler → OsmoMSC

Disable the forwarding of TCH voice frames via the MNCC interface in OsmoMSC→Handler direction for the specified call.

15.4.12 MNCC_LCHAN_MODIFY

Direction: Handler → OsmoMSC

Modify the current dedicated radio channel from signalling to voice, or if it is a signalling-only channel (SDCCH), assign a TCH to the MS.

15.4.13 MNCC_RTP_CREATE

Direction: Handler → OsmoMSC

Create a RTP socket for this call at the BTS/TRAU that serves this BTS.

15.4.14 MNCC_RTP_CONNECT

Direction: Handler → OsmoMSC

Connect the RTP socket of this call to the given remote IP address and port.

15.4.15 MNCC_RTP_FREE

Direction: Handler → OsmoMSC

Release a RTP connection for one given call.
15.4.16 GSM_TCHF_FRAME
Direction: both
Transfer the payload of a GSM Full-Rate (FR) voice frame between the OsmoMSC and an external MNCC handler.

15.4.17 GSM_TCHF_FRAME_EFR
Direction: both
Transfer the payload of a GSM Enhanced Full-Rate (EFR) voice frame between the OsmoMSC and an external MNCC handler.

15.4.18 GSM_TCHH_FRAME
Direction: both
Transfer the payload of a GSM Half-Rate (HR) voice frame between the OsmoMSC and an external MNCC handler.

15.4.19 GSM_TCH_FRAE_AMR
Direction: both
Transfer the payload of a GSM Adaptive-Multi-Rate (AMR) voice frame between the OsmoMSC and an external MNCC handler.

15.4.20 GSM_BAD_FRAME
Direction: OsmoMSC → Handler
Indicate that no valid voice frame, but a bad frame was received over the radio link from the MS.

15.4.21 MNCC_START_DTMF_IND
Direction: OsmoMSC → Handler
Indicate the beginning of a DTMF tone playback.

15.4.22 MNCC_START_DTMF_RSP
Direction: Handler → OsmoMSC
Acknowledge that the DTMF tone playback has been started.

15.4.23 MNCC_START_DTMF_REJ
Direction: both
Indicate that starting a DTMF tone playback was not possible.

15.4.24 MNCC_STOP_DTMF_IND
Direction: OsmoMSC → Handler
Indicate the ending of a DTMF tone playback.
15.4.25 MNCC_STOP_DTMF_RSP

Direction: Handler → OsmoMSC

Acknowledge that the DTMF tone playback has been stopped.

16 Osmux

Osmux is a protocol aimed at multiplexing and transmitting voice and signalling traffic from multiple sources in order to reduce the overall bandwidth consumption. This feature becomes specially meaningful in case of satellite based GSM systems, where the transmission cost on the back-haul is relatively expensive. In such environment, even seemingly small protocol optimizations, eg. message batching and trunking, can result in significant cost reduction.


In Osmocom satellite based GSM networks, the satellite link is envisioned to be in between the BSS and the core network, that is, between the BSC and the MSC (or BSC-NAT). Hence, Osmocom components can make use of Osmux protocol to multiplex payload audio streams from call legs between OsmoBSC and OsmoMSC (or OsmoBSCNAT). The MGW attached those components need of course also be aware of Osmux existence in order to properly set up the audio data plane.

16.1 Osmux and NAT

It is quite usual for satellite based links to use NATs, which means any or both of the two components at each side of the satellite link (BSC and MSC/BSC-NAT) may end up being behind a NAT and being unable to provide the real public address to its peer on the other side of the satellite.

As a result, upon call parameter negotiation (RTP/Osmux IP address and port), those parameters won’t be entirely useful and some specific logic needs to be introduced into the network components to circumvent the NAT under those cases.

For instance, if the BSC and its co-located MGW (BSC/MGW from now on) is under a NAT, it may end up providing its private address and port as RTP/Osmux parameters to the MSC/MGW through GSM protocols, but MSC will fail to send any message to that tuple because of the NAT or routing issues (due to IP address being a private address). In that scenario, MSC/MGW needs to be aware that there’s a NAT and wait until an RTP/Osmux message arrives from the BSC/MGW host. It then can, from that message source IP address and port (and CID in case of Osmux), discover the real public IP address and port of the peer (BSC/MGW). From that point on, the BSC/MGW punched a hole in the NAT (its connection table is updated) and MSC/MGW is able to send data back to it on that connection.

Moreover, NATs tend to drop connections from their connection tables after some inactivity time, meaning a peer may receive notice about the other end not being available while it actually is. This means the GSM network needs to be configured in a way to ensure inactivity periods are short enough that this cannot occur. That’s the reason why OsmoMGW provides the osmux dummy VTY command to enable sending dummy packets from time to time to keep the connections alive.

16.2 CID allocation

Each peer (BSC/MGW and MSC/MGW) allocates its own recvCID, and receives from the peer through the used GSM protocol the peer’s recvCID, which becomes the local sendCID for that connection.

BSC/MGW(recvCID=Y, sendCID=?) ← X → MSC/MGW(recvCID=X, sendCID=?)
BSC/MGW(recvCID=Y, sendCID=X) ↔ Y → MSC/MGW(recvCID=X, sendCID=Y)

This way each peer is responsible for allocating and managing their own local address (CID) space. This is basically the same that happens with regular IP address and port in the RTP case (and those also apply when Osmux is used, but an extra identifier, the CID, is allocated).

In an ideal scenario, without NAT, each BSC/MGW would have a public, differentiated and unique IP and port set tuple, And MSC/MGW should be able to identify messages coming from them by easily matching source IP address, port (and CID in Osmux case) against the parameters negotiated during call set up.
In this kind of scenario, MSC/MGW could easily open and manage one Osmux socket per BSC (based on SDP IPaddr and port parameters), with same \(<localIPaddr, localPort>\) tuple, allowing for 256 Osmux CIDs per BSC and hence call legs per BSC. Each of the peers could actually have more than one Osmux socket towards the other peer, by using a pool of ports or IP addresses, so there’s really not limit if required as long as there’s a way to infer the initially negotiated \(<srcIP, srcPort, dstIP, dstPort, sendCID>\) tuple from the received audio packets.

However, due to some constrains from in between NATs explained in section above, BSC/MGW IP address and port are not a priory known, and could change between different connections coming from it. As a result, it is difficult to infer the entire tuple, so for now MGW needs to allocate its Osmux \(recvCID\) in a clever way, in order to be able to identify the full tuple from it.

Hence, currently OsmoMGW CID allocation implementation shares CID between all connections, which means it can only handle up to 256 concurrent Osmux connections (call legs).

Future work in OsmoMGW (OS#4092) plans to use a set of local ports for Osmux sockets instead of only 1 currently used. This way local ports can be matched against specific \(<remoteIP, remotePort>\) tuples and have an entire 256 Osmux CID space per \(<remoteIP, remotePort>\) (aka per peer).

### 16.3 3GPP AoIP network setup with Osmux

![Diagram of 3GPP AoIP network with Osmux](image)

Figure 3: Sample node diagram of a 3GPP AoIP network with Osmux enabled
Figure 4: MO-call with Osmux enable on 3GPP AoIP
16.4 SCCPLite network setup with Osmux

Figure 5: Sample node diagram of a 3GPP AoIP using A/IP with IPA/SCCPlite network with Osmux enabled
Figure 6: MO-call with Osmux enable on 3GPP AoIP using A/IP with IPA/SCCPlite
16.5 SCCPLite network setup with Osmux + BSC-NAT

Figure 7: Sample node diagram of a 3GPP AoIP using A/IP with IPA/SCCPlite network and BSC-NAT with Osmux enabled
Figure 8: MO call with Osmux enable on 3GPP AoIP using A/IP with IPA/SCCPlite with a BSC-NAT between BSC and MSC.

Copyright © 2017 sysmocom - s.f.m.c. GmbH
16.6 Osmux and MGCP

X-Osmux indicates to OsmoMGW that a given connection of an rtpbridge endpoint has to be configured in order to handle Osmux frames instead of RTP messages on the data plane.

16.6.1 X-Osmux Format

The value part of X-Osmux must be one integer in range [0..255], or alternatively only on request messages, an asterisk (*) if the value is not yet known.

X-Osmux must be issued in the MGCP header section (typically as its last item), before the SDP section starts.

X-Osmux can be included inside CRCX and MDCX request messages, as well as their respective response messages.

In request messages, the value part of X-Osmux specifies the CID to be used by OsmoMGW to send Osmux frames to the remote peer for that connection, also known as sendCID.

In response messages, the value part of X-Osmux specifies the CID where OsmoMGW expect to receive Osmux frames from the remote peer for that connection, also known as recvCID.

Example: X-Osmux format with a known CID 3.

| X-Osmux: 3 |

Example: X-Osmux format with a wildcard (not yet known) CID.

| X-Osmux: * |

16.6.2 X-Osmux Considerations

If the MGCP client is willing to use Osmux for a given connection, it shall specify so during CRCX time, and not later. If at CRCX time the MGCP client doesn’t yet know the sendCID, it can use an asterisk (*) and provide sendCID later within MDCX messages.

All subsequent MDCX messages sent towards an Osmux connection must contain the original sendCID sent during CRCX. The same way, all MDCX response shall contain the recvCID sent during CRCX.

The other required connection address parameters, such as IP address, port, and codecs, are negotiated through MGCP and SDP as usual, but in this case the IP address and port specific the Osmux socket IP address and port to use, that together with the Osmux CID conform the entire tuple identifying a Osmux stream.

Since Osmux only supports AMR codec payloads, the SDP must specify use of AMR codec.

Example: CRCX message that instructs OsmoMGW to create an Osmux connection

```
CRCX 189 rtpbridge/1@mgw MGCP 1.0
C: 36
M: sendrecv
X-Osmux: 2
v=0
o=- 36 23 IN IP4 172.18.2.20
s=-
c=IN IP4 1.2.3.4
t=0 0
m=audio 2342 RTP/AVP 112
a=fmtp:112
a=rtpmap:112 AMR/8000/1
a=ptime:20
```

Example: response to CRCX containing the
16.6.3 X-Osmux Support

X-Osmux is known to be supported by OsmoMGW on the MGCP server side, and by OsmoBSC as well as OsmoMSC on the MGCP client side (through libosmo-mgcp-cli). No other programs supporting this feature are known or envisioned at the time of writing this document.

In OmoMGW, Osmux support is managed through VTY.

Example: Sample config file section with Osmux configuration

```
mgcp
...  
osmux on  
osmux bind-ip 172.18.1.20  
osmux port 1984  
osmux batch-factor 4  
osmux dummy on
```

1. Allow clients to set allocate Osmux connections in rtpbridge endpoints, while still allowing RTP connections
2. Bind the Osmux socket to the provided IP address
3. Bind the Osmux socket to the provided UDP port
4. Batch up to 4 RTP payloads of the same stream on each Osmux frame
5. Periodically send Osmux dummy frames, useful to punch a hole in NATs and maintain connections opened.

16.7 Osmux Support in OsmoMSC

16.7.1 OsmoMSC in a A/IP with IPA/SCCPlite network setup

In this kind of setup, the CN side of BSC co-located MGW is managed by the MSC, meaning the use of Osmux is transparent to BSC since MSC takes care of both peer MGW connections. Moreover, in this case the MSC has no dynamic information on Osmux support in the BSC co-located MGW until CRCX time, which means configuration on both nodes need to be carefully set up so they can work together.

Osmux usage in OsmoMSC in managed through the VTY command `osmux (on|off|only)`. Since there’s no dynamic information on Osmux support, it may be required in the future to have an extra VTY command which can be set per BSC to fine-tune which ones should use Osmux and which shouldn’t.

OsmoMSC will behave differently during call set up based on the VTY command presented above:
• **off:** OsmoMSC won’t include an X-Osmux extension to CRCX sent to the BSC co-located MGW when configuring the CN side of the MGW endpoint. If the MGW answers with a CRCX ACK containing an X-Osmux, OsmoMSC will cancel the call establishment.

• **on:** OsmoMSC will initially configure its co-located MGW to use Osmux, then similarly send a CRCX with an X-Osmux extension towards the BSC co-located MGW. Under this configuration, if the BSC co-located MGW didn’t support Osmux, it could send a CRCX ACK without X-Osmux extension or fail (depending on its own configuration), and OsmoMSC could choose to re-create its local connection as non-Osmux (RTP) and possibly try again against BSC co-located MGW, but this behavior is currently not implemented. As a result, currently **on** behaves the same as **only**.

• **only:** OsmoMSC will configure its co-located MGW as well as the BSC co-located MGW to use Osmux by including the X-Osmux MGCP extension. If MGW rejects to use Osmux, OsmoMSC will reject the call and the call establishment will fail.

### 16.7.2 OsmoMSC in a 3GPP AoIP network setup

Osmux usage in OsmoMSC in managed through the VTY command `osmux (on|off|only)`. Once enabled (**on** or **only**), OsmoMSC will start appending the vendor specific Osmux Support IE in BSSMAP RESET and BSSMAP RESET-ACK message towards the BSC in order to announce it supports Osmux, and BSC will do the same. This way, OsmoMSC can decide whether to use Osmux or not based on this information when setting up a call (this time using Osmux CID IE). It should be noted that this option should not be enabled unless BSCs managed by OsmoMSC support handling this extension IE (like OsmoBSC), 3rd-party BSCs might otherwise refuse the related RESET/RESET-ACK messages.

OsmoMSC will behave differently during call set up based on the VTY command presented above:

• **off:** OsmoMSC won’t use Osmux. That is, it will send a BSSMAP Assign Request without the Osmux CID IE, and will send a CRCX without X-Osmux extension towards its co-located MGW.

• **on:** If BSC announced Osmux support to OsmoMSC during BSSMAP RESET time, then OsmoMSC will set up the call to use Osmux (by adding X-Osmux to MGCP CRCX and Osmux CID IE to BSSMAP Assign Request). If the BSC didn’t announce Osmux support to OsmoMSC, then OsmoMSC will use RTP to set up the call (by avoiding addition of previously described bits).

• **only:** Same as per **on**, except that OsmoMSC will allow to set up only Osmux calls on the CN-side, this is, it will reject to set up voice calls for BSC which didn’t announce Osmux support.

### 17 Osmocom Control Interface

The VTY interface as described in Section 11 is aimed at human interaction with the respective Osmocom program.

Other programs **should not** use the VTY interface to interact with the Osmocom software, as parsing the textual representation is cumbersome, inefficient, and will break every time the formatting is changed by the Osmocom developers.

Instead, the **Control Interface** was introduced as a programmatic interface that can be used to interact with the respective program.

### 17.1 Control Interface Protocol

The control interface protocol is a mixture of binary framing with text based payload.

The protocol for the control interface is wrapped inside the IPA multiplex header with the stream identifier set to IPAC_PROTO_OSMO (0xEE).
Inside the IPA header is a single byte of extension header with protocol ID 0x00 which indicates the control interface.

After the concatenation of the two above headers, the plain-text payload message starts. The format of that plain text is illustrated for each operation in the respective message sequence chart in the chapters below.

The fields specified below follow the following meaning:

- **<id>**
  - A numeric identifier, uniquely identifying this particular operation. Value 0 is not allowed unless it’s a TRAP message. It will be echoed back in any response to a particular request.

- **<var>**
  - The name of the variable / field affected by the GET / SET / TRAP operation. Which variables/fields are available is dependent on the specific application under control.

- **<val>**
  - The value of the variable / field

- **<reason>**
  - A text formatted, human-readable reason why the operation resulted in an error.

### 17.1.1 GET operation

The GET operation is performed by an external application to get a certain value from inside the Osmocom application.
17.1.2 SET operation

The SET operation is performed by an external application to set a value inside the Osmocom application.

17.1.3 TRAP operation

The program can at any time issue a trap. The term is used in the spirit of SNMP.
17.2 Common variables

There are several variables which are common to all the programs using control interface. They are described in the following table.

<table>
<thead>
<tr>
<th>Name</th>
<th>Access</th>
<th>Value</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>counter.*</td>
<td>RO</td>
<td></td>
<td>Get counter value.</td>
</tr>
<tr>
<td>rate_ctr.*</td>
<td>RO</td>
<td></td>
<td>Get list of rate counter groups.</td>
</tr>
<tr>
<td>rate_ctr.IN.GN.GI.name</td>
<td>RO</td>
<td></td>
<td>Get value for interval IN of rate counter name which belong to group named GN with index GI.</td>
</tr>
</tbody>
</table>

Those read-only variables allow to get value of arbitrary counter using its name. For example "rate_ctr.per_hour.bsc.0.handover:timeout" is the number of handover timeouts per hour. Of course for that to work the program in question have to register corresponding counter names and groups using libosmocore functions.

In the example above, "bsc" is the rate counter group name and "0" is its index. It is possible to obtain all the rate counters in a given group by requesting "rate_ctr.per_sec.bsc.*" variable.

The list of available groups can be obtained by requesting "rateCtr.*" variable.

The rate counter group name have to be prefixed with interval specification which can be any of "per_sec", "per_min", "per_hour", "per_day" or "abs" for absolute value.

The old-style counters available via "counter.*" variables are superseded by "rate_ctr.abs" so its use is discouraged. There might still be some applications not yet converted to rate_ctr.

17.3 Control Interface python examples

In the osmo-python-tests repository, there is an example python script called scripts/osmo_ctrl.py which implements the Osmocom control interface protocol.

You can use this tool either stand-alone to perform control interface operations against an Osmocom program, or you can use it as a reference for developing your own python software talking to the control interface.

Another implementation is in scripts/osmo_rate_ctr2csv.py which will retrieve performance counters for a given Osmocom program and output it in csv format. This can be used to periodically (using systemd timer for example) retrieve data to build KPI and evaluate how it changes over time.

Internally it uses "rate_ctr.*" variable described in [?] to get the list of counter groups and than request all the counters in each group. Applications interested in individual metrics can request it directly using rate_ctr2csv.py as an example.

17.3.1 Getting rate counters

Example: Use rate_ctr2csv.py to get rate counters from OsmoBSC

```
$ ./scripts/osmo_rate_ctr2csv.py --header
Connecting to localhost:4249...
Getting rate counter groups info...
"group","counter","absolute","second","minute","hour","day"
```
17.3.2 Setting a value

Example: Use osmo_ctrl.py to set the short network name of OsmoBSC

$ ./osmo_ctrl.py -d localhost -s short-name 32C3
Got message: SET_REPLY 1 short-name 32C3

17.3.3 Getting a value

Example: Use osmo_ctrl.py to get the mnc of OsmoBSC

$ ./osmo_ctrl.py -d localhost -g mnc
Got message: GET_REPLY 1 mnc 262

17.3.4 Listening for traps

You can use osmo_ctrl.py to listen for traps the following way:

Example: Using osmo_ctrl.py to listen for traps:

$ ./osmo_ctrl.py -d localhost -m

the command will not return and wait for any TRAP messages to arrive

18 Generic Subscriber Update Protocol

18.1 General

This chapter describes the remote protocol that is used by OsmoSGSN and OsmoMSC to update and manage the local subscriber list in OsmoHLR. Functionally, it resembles the interface between the SGSN/VLR on the one hand side, and HLR/AUC on the other side.

For more information, see the specification of the Gr interface (3GPP TS 03.60).

Traditionally, the GSM MAP (Mobile Application Part) protocol is used for this purpose, running on top of a full telecom signalling protocol stack of MTP2/MTP3/SCCP/TCAP, or any of the SIGTRAN alternatives.

In order to avoid many of the complexities of MAP, which are difficult to implement in the plain C language environment of the Osmocom cellular network elements like the SGSN, we introduce the GSUP protocol.

The GSUP protocol and the messages are designed after the corresponding MAP messages (see 3GPP TS 09.02) with the following main differences:
• The encoding uses TLV structures instead of ASN.1 BER
• Segmentation is not used, i.e. we rely on the fact that the underlying transport protocol can transport signalling messages of any size.

18.2 Connection

The protocol expects that a reliable, ordered, packet boundaries preserving connection is used (e.g. IPA over TCP). The remote peer is either a service that understands the protocol natively or a wrapper service that maps the messages to/from real MAP messages that can be used to directly communicate with an HLR.

18.3 Using IPA

By default, the following identifiers should be used:

- IPA Stream ID: 0xEE (OSMO)
- IPA OSMO protocol extension: 0x05

For more information about the IPA multiplex, please see the OsmoBTS Abis/IP Specification.

18.4 Procedures

18.4.1 Authentication management

The SGSN or VLR sends a SEND_AUTHENTICATION_INFO_REQ message containing the MS’s IMSI to the peer. On errors, especially if authentication info is not available for that IMSI, the peer returns a SEND_AUTHENTICATION_INFO_ERR message. Otherwise the peer returns a SEND_AUTHENTICATION_INFO_RES message. If this message contains at least one authentication tuple, the SGSN or VLR replaces all tuples that are assigned to the subscriber. If the message doesn’t contain any tuple the SGSN or VLR may reject the Attach Request. (see 3GPP TS 09.02, 25.5.6)

![Figure 16: Send Authentication Info (Normal Case)](image)

![Figure 17: Send Authentication Info (Erroneous Case)](image)

18.4.2 Reporting of Authentication Failure

Using this procedure, the SGSN or VLR reports authentication failures to the HLR.
18.4.3 Location Updating

The SGSN or VLR sends a UPDATE_LOCATION_REQ to the peer. If the request is denied by the network, the peer returns an UPDATE_LOCATION_ERR message to the SGSN or VLR. Otherwise the peer returns an UPDATE_LOCATION_RES message containing all information fields that shall be inserted into the subscriber record. If the PDP info complete information element is set in the message, the SGSN or VLR clears existing PDP information fields in the subscriber record first. (see 3GPP TS 09.02, 19.1.1.8)

18.4.4 Location Cancellation

Using the Location Cancellation procedure, the Network Peer (HLR) can request the SGSN or VLR to remove a subscriber record.
18.4.5 Purge MS

Using the Purge MS procedure, the SGSN or VLR can request purging of MS related state from the HLR. It is used after the SGSN or VLR detects that no radio contact has been established for a prolonged duration (i.e. longer than the periodic LU timeout). See 3GPP TS 23.012 Section 3.6.1.4 for a description of this procedure.

![Figure 23: Purge MS (Normal Case)](image)

18.4.6 Delete Subscriber Data

Using the Delete Subscriber Data procedure, the Peer (HLR) can remove some of the subscriber data from the SGSN or VLR. This is used in case the subscription details (e.g. PDP Contexts / APNs) change while the subscriber is registered to that SGSN VLR.

![Figure 24: Delete Subscriber Data (Normal Case)](image)

18.4.7 Check IMEI

The VLR asks the EIR to check if a new ME’s IMEI is acceptable or not. The EIR may implement a blacklist or whitelist and reject the IMEI based on that. Against the original purpose of the Check IMEI Procedure, this could also be used to save the IMEI in the HLR DB.

![Figure 25: Check IMEI (Normal Case)](image)

18.5 Procedures (E Interface)

The E interface connects two MSCs in the traditional GSM MAP world. It is used for the inter-MSC handover. In GSUP, we don’t need that extra connection, as we route the messages over the GSUP server (OsmoHLR) instead.

Whenever MSC-A is sending to MSC-B, and vice-versa, the message needs to pass through the GSUP server. In order to make the following message sequence charts easier to read, this step has been omitted.

18.5.1 E Handover

MSC-A has an active RAN connection and hands it over to MSC-B.
18.5.2 E Subsequent Handover

MSC-B has an active RAN connection, and asks MSC-A to hand it over to MSC-B'.

18.5.3 E Forward and Process Access Signalling

MSC-A is forwarding a message from its BSS (Base Station Subsystem) to MSC-B. MSC-B forwards the message to its BSS, and answers to MSC-A with a Process Access Signalling Request.
18.5.4 E Routing Error

The GSUP server can not route any of the requests above, and responds with an E Routing Error. Possible reasons for not being able to route the message are missing routing IEs, a mismatching source name IE (Section 18.7.30), the destination not being connected to the GSUP server or a failed attempt to send the message from the GSUP sever to the destination. To figure out, what went wrong in detail, refer to the GSUP server’s logs.

In the traditional GSM MAP world, the participants of an E procedure are directly connected, hence this routing error message does not exist in MAP.

18.6 Message Format

18.6.1 General

Every message is based on the following message format

<table>
<thead>
<tr>
<th>IEI</th>
<th>IE</th>
<th>Type</th>
<th>Presence</th>
<th>Format</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>IMSI</td>
<td>Section 18.7.19</td>
<td>M</td>
<td>TLV</td>
<td>2-10</td>
</tr>
</tbody>
</table>

If a numeric range is indicated in the presence column, multiple information elements with the same tag may be used in sequence. The information elements shall be sent in the given order. Nevertheless after the generic part the receiver shall be able to received them in any order. Unknown IE shall be ignored.

Besides a numeric range, the presence column may have M (Mandatory), O (Optional) or C (Conditional). The format column holds either V (Value) or TLV (Tag Length Value).
The conditional AUTS and RAND IEs are both present in case the SIM (via UE) requests an UMTS AKA re-synchronization procedure. Either both optional IEs are present, or none of them.

### 18.6.3 Send Authentication Info Error

**Direction:** HLR ⇒ SGSN / VLR

<table>
<thead>
<tr>
<th>IEI</th>
<th>IE</th>
<th>Type</th>
<th>Presence</th>
<th>Format</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>Message Type</td>
<td>Section 18.7.1</td>
<td>M</td>
<td>V</td>
<td>1</td>
</tr>
<tr>
<td>02</td>
<td>IMSI</td>
<td>Section 18.7.19</td>
<td>M</td>
<td>TLV</td>
<td>2-10</td>
</tr>
<tr>
<td>03</td>
<td>Cause</td>
<td>Section 18.7.25</td>
<td>M</td>
<td>TLV</td>
<td>3</td>
</tr>
</tbody>
</table>

### 18.6.4 Send Authentication Info Response

**Direction:** HLR ⇒ SGSN / VLR

<table>
<thead>
<tr>
<th>IEI</th>
<th>IE</th>
<th>Type</th>
<th>Presence</th>
<th>Format</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>Message Type</td>
<td>Section 18.7.1</td>
<td>M</td>
<td>V</td>
<td>1</td>
</tr>
<tr>
<td>02</td>
<td>IMSI</td>
<td>Section 18.7.19</td>
<td>M</td>
<td>TLV</td>
<td>2-10</td>
</tr>
<tr>
<td>03</td>
<td>Auth Tuple</td>
<td>Section 18.7.6</td>
<td></td>
<td>TLV</td>
<td>36</td>
</tr>
</tbody>
</table>

### 18.6.5 Authentication Failure Report

**Direction:** SGSN / VLR ⇒ HLR

<table>
<thead>
<tr>
<th>IEI</th>
<th>IE</th>
<th>Type</th>
<th>Presence</th>
<th>Format</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>Message Type</td>
<td>Section 18.7.1</td>
<td>M</td>
<td>V</td>
<td>1</td>
</tr>
<tr>
<td>28</td>
<td>IMSI</td>
<td>Section 18.7.19</td>
<td>M</td>
<td>TLV</td>
<td>2-10</td>
</tr>
<tr>
<td>28</td>
<td>CN Domain</td>
<td>Section 18.7.15</td>
<td>O</td>
<td>TLV</td>
<td>3</td>
</tr>
</tbody>
</table>

### 18.6.6 Update Location Request

**Direction:** SGSN / VLR ⇒ HLR

<table>
<thead>
<tr>
<th>IEI</th>
<th>IE</th>
<th>Type</th>
<th>Presence</th>
<th>Format</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>Message Type</td>
<td>Section 18.7.1</td>
<td>M</td>
<td>V</td>
<td>1</td>
</tr>
<tr>
<td>02</td>
<td>IMSI</td>
<td>Section 18.7.19</td>
<td>M</td>
<td>TLV</td>
<td>2-10</td>
</tr>
<tr>
<td>28</td>
<td>CN Domain</td>
<td>Section 18.7.15</td>
<td>O</td>
<td>TLV</td>
<td>3</td>
</tr>
</tbody>
</table>

### 18.6.7 Update Location Error

**Direction:** HLR ⇒ SGSN / VLR

<table>
<thead>
<tr>
<th>IEI</th>
<th>IE</th>
<th>Type</th>
<th>Presence</th>
<th>Format</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>Message Type</td>
<td>Section 18.7.1</td>
<td>M</td>
<td>V</td>
<td>1</td>
</tr>
<tr>
<td>02</td>
<td>IMSI</td>
<td>Section 18.7.19</td>
<td>M</td>
<td>TLV</td>
<td>2-10</td>
</tr>
<tr>
<td>02</td>
<td>Cause</td>
<td>Section 18.7.25</td>
<td>M</td>
<td>TLV</td>
<td>3</td>
</tr>
</tbody>
</table>

### 18.6.8 Update Location Result

**Direction:** HLR ⇒ SGSN / VLR
If the PDP info complete IE is present, the old PDP info list shall be cleared.

### 18.6.9 Location Cancellation Request

**Direction:** HLR ⇒ SGSN / VLR

<table>
<thead>
<tr>
<th>IEI</th>
<th>IE</th>
<th>Type</th>
<th>Presence</th>
<th>Format</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>IMSI</td>
<td>Section 18.7.1</td>
<td>M</td>
<td>V</td>
<td>1</td>
</tr>
<tr>
<td>08</td>
<td>MSISDN</td>
<td>Section 18.7.20</td>
<td>O</td>
<td>TLV</td>
<td>0-9</td>
</tr>
<tr>
<td>09</td>
<td>HLR Number</td>
<td>Section 18.7.24</td>
<td>O</td>
<td>TLV</td>
<td>0-9</td>
</tr>
<tr>
<td>04</td>
<td>PDP info complete</td>
<td>Section 18.7.18</td>
<td>O</td>
<td>TLV</td>
<td>2</td>
</tr>
<tr>
<td>05</td>
<td>PDP info</td>
<td>Section 18.7.3</td>
<td>O</td>
<td>TLV</td>
<td>1-10</td>
</tr>
</tbody>
</table>

### 18.6.10 Location Cancellation Result

**Direction:** SGSN / VLR ⇒ HLR

<table>
<thead>
<tr>
<th>IEI</th>
<th>IE</th>
<th>Type</th>
<th>Presence</th>
<th>Format</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>IMSI</td>
<td>Section 18.7.19</td>
<td>M</td>
<td>TLV</td>
<td>2-10</td>
</tr>
<tr>
<td>28</td>
<td>CN Domain</td>
<td>Section 18.7.15</td>
<td>O</td>
<td>TLV</td>
<td>3</td>
</tr>
<tr>
<td>06</td>
<td>Cancellation type</td>
<td>Section 18.7.16</td>
<td>O</td>
<td>TLV</td>
<td>3</td>
</tr>
</tbody>
</table>

### 18.6.11 Purge MS Request

**Direction:** SGSN / VLR ⇒ HLR

<table>
<thead>
<tr>
<th>IEI</th>
<th>IE</th>
<th>Type</th>
<th>Presence</th>
<th>Format</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>IMSI</td>
<td>Section 18.7.19</td>
<td>M</td>
<td>TLV</td>
<td>2-10</td>
</tr>
<tr>
<td>28</td>
<td>CN Domain</td>
<td>Section 18.7.15</td>
<td>O</td>
<td>TLV</td>
<td>3</td>
</tr>
<tr>
<td>09</td>
<td>HLR Number</td>
<td>Section 18.7.24</td>
<td>M</td>
<td>TLV</td>
<td>0-9</td>
</tr>
</tbody>
</table>

### 18.6.12 Purge MS Error

**Direction:** HLR ⇒ SGSN / VLR

<table>
<thead>
<tr>
<th>IEI</th>
<th>IE</th>
<th>Type</th>
<th>Presence</th>
<th>Format</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>IMSI</td>
<td>Section 18.7.19</td>
<td>M</td>
<td>TLV</td>
<td>2-10</td>
</tr>
<tr>
<td>02</td>
<td>Cause</td>
<td>Section 18.7.25</td>
<td>M</td>
<td>TLV</td>
<td>3</td>
</tr>
</tbody>
</table>

### 18.6.13 Purge MS Result

**Direction:** HLR ⇒ SGSN / VLR
18.6.14  Insert Subscriber Data Request

Direction: HLR ⇒ SGSN / VLR

If the PDP info complete IE is present, the old PDP info list shall be cleared.

18.6.15  Insert Subscriber Data Error

Direction: SGSN / VLR ⇒ HLR

18.6.16  Insert Subscriber Data Result

Direction: SGSN / VLR ⇒ HLR

18.6.17  Delete Subscriber Data Request

Direction: HLR ⇒ SGSN / VLR

18.6.18  Delete Subscriber Data Error

Direction: SGSN / VLR ⇒ HLR
### 18.6.19 Delete Subscriber Data Result

**Direction:** HLR ⇒ SGSN / VLR

<table>
<thead>
<tr>
<th>IEI</th>
<th>IE</th>
<th>Type</th>
<th>Presence</th>
<th>Format</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>IMSI</td>
<td>Message Type</td>
<td>M</td>
<td>V</td>
<td>1</td>
</tr>
<tr>
<td>02</td>
<td>Cause</td>
<td>Section 18.7.19</td>
<td>M</td>
<td>TLV</td>
<td>2-10</td>
</tr>
</tbody>
</table>

**Section 18.6.20 Process Supplementary Service Request**

**Direction:** bidirectional

<table>
<thead>
<tr>
<th>IEI</th>
<th>IE</th>
<th>Type</th>
<th>Presence</th>
<th>Format</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>IMSI</td>
<td>Message Type</td>
<td>M</td>
<td>V</td>
<td>1</td>
</tr>
<tr>
<td>30</td>
<td>Session ID</td>
<td>Section 18.7.19</td>
<td>M</td>
<td>TLV</td>
<td>2-10</td>
</tr>
<tr>
<td>31</td>
<td>Session State</td>
<td>Section 18.8.2</td>
<td>M</td>
<td>TLV</td>
<td>3</td>
</tr>
<tr>
<td>35</td>
<td>Supplementary Service Info</td>
<td>Section 18.7.26</td>
<td>O</td>
<td>TLV</td>
<td>2-…</td>
</tr>
</tbody>
</table>

This message is used in both directions in case of USSD, because it is not known if it request or response without parsing the GSM 04.80 payload.

### 18.6.21 Process Supplementary Service Error

**Direction:** EUSE / HLR ⇒ MSC

<table>
<thead>
<tr>
<th>IEI</th>
<th>IE</th>
<th>Type</th>
<th>Presence</th>
<th>Format</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>IMSI</td>
<td>Message Type</td>
<td>M</td>
<td>V</td>
<td>1</td>
</tr>
<tr>
<td>30</td>
<td>Session ID</td>
<td>Section 18.7.19</td>
<td>M</td>
<td>TLV</td>
<td>2-10</td>
</tr>
<tr>
<td>31</td>
<td>Session State</td>
<td>Section 18.8.2</td>
<td>M</td>
<td>TLV</td>
<td>3</td>
</tr>
<tr>
<td>02</td>
<td>Cause</td>
<td>Section 18.7.25</td>
<td>M</td>
<td>TLV</td>
<td>3</td>
</tr>
</tbody>
</table>

### 18.6.22 Process Supplementary Service Response

**Direction:** EUSE / HLR ⇒ MSC

<table>
<thead>
<tr>
<th>IEI</th>
<th>IE</th>
<th>Type</th>
<th>Presence</th>
<th>Format</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>IMSI</td>
<td>Message Type</td>
<td>M</td>
<td>V</td>
<td>1</td>
</tr>
<tr>
<td>30</td>
<td>Session ID</td>
<td>Section 18.7.19</td>
<td>M</td>
<td>TLV</td>
<td>2-10</td>
</tr>
<tr>
<td>31</td>
<td>Session State</td>
<td>Section 18.8.2</td>
<td>M</td>
<td>TLV</td>
<td>3</td>
</tr>
<tr>
<td>35</td>
<td>Supplementary Service Info</td>
<td>Section 18.7.26</td>
<td>O</td>
<td>TLV</td>
<td>2-…</td>
</tr>
</tbody>
</table>

The purpose of this message is not clear yet. Probably, it can be used to notify the MSC that a structured supplementary service is successfully activated or deactivated, etc.
### 18.6.23 MO-forwardSM Request

Direction: MSC / SGSN ⇒ SMSC (via HLR)

<table>
<thead>
<tr>
<th>IEI</th>
<th>IE</th>
<th>Type</th>
<th>Presence</th>
<th>Format</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>IMSI</td>
<td>Message Type</td>
<td>Section 18.7.1</td>
<td>M</td>
<td>V</td>
</tr>
<tr>
<td>40</td>
<td>SM-RP-MR (Message Reference)</td>
<td>Section 18.8.3</td>
<td>M</td>
<td>TLV</td>
<td>1</td>
</tr>
<tr>
<td>41</td>
<td>SM-RP-DA (Destination Address)</td>
<td>Section 18.8.4</td>
<td>M</td>
<td>TLV</td>
<td>2-...</td>
</tr>
<tr>
<td>42</td>
<td>SM-RP-OA (Originating Address)</td>
<td>Section 18.8.5</td>
<td>M</td>
<td>TLV</td>
<td>2-...</td>
</tr>
<tr>
<td>43</td>
<td>SM-RP-UI (SM TPDU)</td>
<td>Section 18.8.7</td>
<td>M</td>
<td>TLV</td>
<td>1-...</td>
</tr>
</tbody>
</table>

This message is used to forward MO short messages from MSC / SGSN to an SMSC. The corresponding MAP service is MAP-MO-FORWARD-SHORT-MESSAGE, see 3GPP TS 29.002, section 12.2.

### 18.6.24 MO-forwardSM Error

Direction: SMSC (via HLR) ⇒ MSC / SGSN

<table>
<thead>
<tr>
<th>IEI</th>
<th>IE</th>
<th>Type</th>
<th>Presence</th>
<th>Format</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>IMSI</td>
<td>Message Type</td>
<td>Section 18.7.1</td>
<td>M</td>
<td>V</td>
</tr>
<tr>
<td>40</td>
<td>SM-RP-MR (Message Reference)</td>
<td>Section 18.8.3</td>
<td>M</td>
<td>TLV</td>
<td>1</td>
</tr>
<tr>
<td>41</td>
<td>SM-RP-Cause (Cause value)</td>
<td>Section 18.8.8</td>
<td>M</td>
<td>TLV</td>
<td>1</td>
</tr>
<tr>
<td>43</td>
<td>SM-RP-UI (diagnostic field)</td>
<td>Section 18.8.7</td>
<td>O</td>
<td>TLV</td>
<td>1-...</td>
</tr>
</tbody>
</table>

This message is used to indicate a negative result of an earlier MO short message delivery. The corresponding MAP service is MAP-MO-FORWARD-SHORT-MESSAGE, see 3GPP TS 29.002, section 12.2.

### 18.6.25 MO-forwardSM Result

Direction: SMSC (via HLR) ⇒ MSC / SGSN

<table>
<thead>
<tr>
<th>IEI</th>
<th>IE</th>
<th>Type</th>
<th>Presence</th>
<th>Format</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>IMSI</td>
<td>Message Type</td>
<td>Section 18.7.1</td>
<td>M</td>
<td>V</td>
</tr>
<tr>
<td>40</td>
<td>SM-RP-MR (Message Reference)</td>
<td>Section 18.8.3</td>
<td>M</td>
<td>TLV</td>
<td>1</td>
</tr>
</tbody>
</table>

This message is used to indicate a successful result of an earlier MO short message delivery. The corresponding MAP service is MAP-MO-FORWARD-SHORT-MESSAGE, see 3GPP TS 29.002, section 12.2.

### 18.6.26 MT-forwardSM Request

Direction: SMSC (via HLR) ⇒ MSC / SGSN

<table>
<thead>
<tr>
<th>IEI</th>
<th>IE</th>
<th>Type</th>
<th>Presence</th>
<th>Format</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>IMSI</td>
<td>Message Type</td>
<td>Section 18.7.1</td>
<td>M</td>
<td>V</td>
</tr>
<tr>
<td>40</td>
<td>SM-RP-MR (Message Reference)</td>
<td>Section 18.8.3</td>
<td>M</td>
<td>TLV</td>
<td>1</td>
</tr>
<tr>
<td>41</td>
<td>SM-RP-DA (Destination Address)</td>
<td>Section 18.8.4</td>
<td>M</td>
<td>TLV</td>
<td>2-...</td>
</tr>
<tr>
<td>42</td>
<td>SM-RP-OA (Originating Address)</td>
<td>Section 18.8.5</td>
<td>M</td>
<td>TLV</td>
<td>2-...</td>
</tr>
<tr>
<td>43</td>
<td>SM-RP-UI (SM TPDU)</td>
<td>Section 18.8.7</td>
<td>M</td>
<td>TLV</td>
<td>1-...</td>
</tr>
<tr>
<td>45</td>
<td>SM-RP-MMS (More Messages to Send)</td>
<td>Section 18.8.9</td>
<td>O</td>
<td>TLV</td>
<td>1</td>
</tr>
</tbody>
</table>
This message is used to forward MT short messages from an SMSC to MSC / SGSN. The corresponding MAP service is MAP-MT-FORWARD-SHORT-MESSAGE, see 3GPP TS 29.002, section 12.9.

18.6.27 MT-forwardSM Error

Direction: MSC / SGSN ⇒ SMSC (via HLR)

<table>
<thead>
<tr>
<th>IEI</th>
<th>IE</th>
<th>Type</th>
<th>Presence</th>
<th>Format</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>IMSI</td>
<td>Message Type</td>
<td>Section 18.7.1</td>
<td>M</td>
<td>V</td>
</tr>
<tr>
<td>40</td>
<td>SM-RP-MR (Message Reference)</td>
<td>Section 18.7.19</td>
<td>M</td>
<td>TLV</td>
<td>2-10</td>
</tr>
<tr>
<td>44</td>
<td>SM-RP-Cause (Cause value)</td>
<td>Section 18.8.3</td>
<td>M</td>
<td>TLV</td>
<td>1</td>
</tr>
<tr>
<td>43</td>
<td>SM-RP-UI (diagnostic field)</td>
<td>Section 18.8.7</td>
<td>O</td>
<td>TLV</td>
<td>1-...</td>
</tr>
</tbody>
</table>

This message is used to indicate a negative result of an earlier MT short message delivery. The corresponding MAP service is MAP-MT-FORWARD-SHORT-MESSAGE, see 3GPP TS 29.002, section 12.9.

18.6.28 MT-forwardSM Result

Direction: MSC / SGSN ⇒ SMSC (via HLR)

<table>
<thead>
<tr>
<th>IEI</th>
<th>IE</th>
<th>Type</th>
<th>Presence</th>
<th>Format</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>IMSI</td>
<td>Message Type</td>
<td>Section 18.7.1</td>
<td>M</td>
<td>V</td>
</tr>
<tr>
<td>40</td>
<td>SM-RP-MR (Message Reference)</td>
<td>Section 18.7.19</td>
<td>M</td>
<td>TLV</td>
<td>2-10</td>
</tr>
</tbody>
</table>

This message is used to indicate a successful result of an earlier MT short message delivery. The corresponding MAP service is MAP-MT-FORWARD-SHORT-MESSAGE, see 3GPP TS 29.002, section 12.9.

18.6.29 READY-FOR-SM Request

Direction: MSC / SGSN ⇒ SMSC (via HLR)

<table>
<thead>
<tr>
<th>IEI</th>
<th>IE</th>
<th>Type</th>
<th>Presence</th>
<th>Format</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>IMSI</td>
<td>Message Type</td>
<td>Section 18.7.1</td>
<td>M</td>
<td>V</td>
</tr>
<tr>
<td>40</td>
<td>SM-RP-MR (Message Reference)</td>
<td>Section 18.7.19</td>
<td>M</td>
<td>TLV</td>
<td>2-10</td>
</tr>
<tr>
<td>46</td>
<td>SM Alert Reason</td>
<td>Section 18.8.10</td>
<td>M</td>
<td>TLV</td>
<td>1-...</td>
</tr>
</tbody>
</table>

This message is used between the MSC / SGSN and an SMSC when a subscriber indicates memory available situation (see TS GSM 04.11, section 7.3.2). The corresponding MAP service is MAP-READY-FOR-SM, see 3GPP TS 29.002, section 12.4.

18.6.30 READY-FOR-SM Error

Direction: SMSC (via HLR) ⇒ MSC / SGSN

<table>
<thead>
<tr>
<th>IEI</th>
<th>IE</th>
<th>Type</th>
<th>Presence</th>
<th>Format</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>IMSI</td>
<td>Message Type</td>
<td>Section 18.7.1</td>
<td>M</td>
<td>V</td>
</tr>
<tr>
<td>40</td>
<td>SM-RP-MR (Message Reference)</td>
<td>Section 18.7.19</td>
<td>M</td>
<td>TLV</td>
<td>2-10</td>
</tr>
<tr>
<td>44</td>
<td>SM-RP-Cause (Cause value)</td>
<td>Section 18.8.8</td>
<td>M</td>
<td>TLV</td>
<td>1</td>
</tr>
<tr>
<td>43</td>
<td>SM-RP-UI (diagnostic field)</td>
<td>Section 18.8.7</td>
<td>O</td>
<td>TLV</td>
<td>1-...</td>
</tr>
</tbody>
</table>
This message is used to indicate a negative result of an earlier MO SMMA (Memory Available) indication. The corresponding MAP service is MAP-READY-FOR-SM, see 3GPP TS 29.002, section 12.4.

### 18.6.31 READY-FOR-SM Result

Direction: SMSC (via HLR) ⇒ MSC / SGSN

<table>
<thead>
<tr>
<th>IEI</th>
<th>IE</th>
<th>Type</th>
<th>Presence</th>
<th>Format</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>IMSI</td>
<td>Message Type</td>
<td>Section 18.7.1</td>
<td>M</td>
<td>V</td>
</tr>
<tr>
<td>00</td>
<td>SM-RP-MR (Message Reference)</td>
<td>Section 18.8.3</td>
<td>M</td>
<td>TLV</td>
<td>1</td>
</tr>
</tbody>
</table>

This message is used to indicate a successful result of an earlier MO SMMA (Memory Available) indication. The corresponding MAP service is MAP-READY-FOR-SM, see 3GPP TS 29.002, section 12.4.

### 18.6.32 CHECK-IMEI Request

Direction: VLR ⇒ EIR (via HLR)

<table>
<thead>
<tr>
<th>IEI</th>
<th>IE</th>
<th>Type</th>
<th>Presence</th>
<th>Format</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>IMSI</td>
<td>Message Type</td>
<td>Section 18.7.1</td>
<td>M</td>
<td>V</td>
</tr>
<tr>
<td>50</td>
<td>IMEI</td>
<td>Section 18.7.27</td>
<td>M</td>
<td>TLV</td>
<td>11</td>
</tr>
</tbody>
</table>

### 18.6.33 CHECK-IMEI Error

Direction: EIR (via HLR) ⇒ VLR

<table>
<thead>
<tr>
<th>IEI</th>
<th>IE</th>
<th>Type</th>
<th>Presence</th>
<th>Format</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>IMSI</td>
<td>Message Type</td>
<td>Section 18.7.1</td>
<td>M</td>
<td>V</td>
</tr>
<tr>
<td>02</td>
<td>Cause</td>
<td>Section 18.7.25</td>
<td>M</td>
<td>TLV</td>
<td>3</td>
</tr>
</tbody>
</table>

### 18.6.34 CHECK-IMEI Result

Direction: EIR (via HLR) ⇒ VLR

<table>
<thead>
<tr>
<th>IEI</th>
<th>IE</th>
<th>Type</th>
<th>Presence</th>
<th>Format</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>IMSI</td>
<td>Message Type</td>
<td>Section 18.7.1</td>
<td>M</td>
<td>V</td>
</tr>
<tr>
<td>51</td>
<td>IMEI Check Result</td>
<td>Section 18.7.28</td>
<td>M</td>
<td>TLV</td>
<td>3</td>
</tr>
</tbody>
</table>

### 18.6.35 E Prepare Handover Request

Direction: MSC-A=MSC-I ⇒ MSC-B=MSC-T (via HLR)

<table>
<thead>
<tr>
<th>IEI</th>
<th>IE</th>
<th>Type</th>
<th>Presence</th>
<th>Format</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>IMSI</td>
<td>Message Type</td>
<td>Section 18.7.1</td>
<td>M</td>
<td>V</td>
</tr>
<tr>
<td>0a</td>
<td>Message Class</td>
<td>Section 18.7.29</td>
<td>M</td>
<td>TLV</td>
<td>3</td>
</tr>
<tr>
<td>60</td>
<td>Source Name</td>
<td>Section 18.7.30</td>
<td>M</td>
<td>TLV</td>
<td>2-...</td>
</tr>
<tr>
<td>61</td>
<td>Destination Name</td>
<td>Section 18.7.31</td>
<td>M</td>
<td>TLV</td>
<td>2-...</td>
</tr>
</tbody>
</table>
IEI | IE | Type | Presence | Format | Length |
--- | --- | --- | --- | --- | --- |
62 | AN-APDU | Section 18.7.32 | M | TLV | 2-... |

### 18.6.36 E Prepare Handover Error

Direction: MSC-B=MSC-T ⇒ MSC-A=MSC-I (via HLR)

IEI | IE | Type | Presence | Format | Length |
--- | --- | --- | --- | --- | --- |
01 | Message Type | Section 18.7.1 | M | V | 1 |
0a | Message Class | Section 18.7.29 | M | TLV | 3 |
60 | Source Name | Section 18.7.30 | M | TLV | 2-... |
61 | Destination Name | Section 18.7.31 | M | TLV | 2-... |
62 | AN-APDU | Section 18.7.32 | M | TLV | 2-... |

### 18.6.37 E Prepare Handover Result

Direction: MSC-B=MSC-T ⇒ MSC-A=MSC-I (via HLR)

IEI | IE | Type | Presence | Format | Length |
--- | --- | --- | --- | --- | --- |
01 | Message Type | Section 18.7.1 | M | V | 1 |
0a | Message Class | Section 18.7.29 | M | TLV | 3 |
60 | Source Name | Section 18.7.30 | M | TLV | 2-... |
61 | Destination Name | Section 18.7.31 | M | TLV | 2-... |
62 | AN-APDU | Section 18.7.32 | M | TLV | 2-... |

### 18.6.38 E Prepare Subsequent Handover Request

Direction: MSC-B=MSC-I ⇒ MSC-A (via HLR)

IEI | IE | Type | Presence | Format | Length |
--- | --- | --- | --- | --- | --- |
01 | Message Type | Section 18.7.1 | M | V | 1 |
0a | Message Class | Section 18.7.29 | M | TLV | 3 |
60 | Source Name | Section 18.7.30 | M | TLV | 2-... |
61 | Destination Name | Section 18.7.31 | M | TLV | 2-... |
62 | AN-APDU | Section 18.7.32 | M | TLV | 2-... |

### 18.6.39 E Prepare Subsequent Handover Error

Direction: MSC-A ⇒ MSC-B=MSC-I (via HLR)

IEI | IE | Type | Presence | Format | Length |
--- | --- | --- | --- | --- | --- |
01 | Message Type | Section 18.7.1 | M | V | 1 |
0a | Message Class | Section 18.7.29 | M | TLV | 3 |
60 | Source Name | Section 18.7.30 | M | TLV | 2-... |
61 | Destination Name | Section 18.7.31 | M | TLV | 2-... |
62 | AN-APDU | Section 18.7.32 | M | TLV | 2-... |
### 18.6.40 E Prepare Subsequent Handover Result

**Direction:** MSC-A $\Rightarrow$ MSC-B=MSC-I (via HLR)

<table>
<thead>
<tr>
<th>IEI</th>
<th>IE</th>
<th>Type</th>
<th>Presence</th>
<th>Format</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>IMSI</td>
<td>Message Type</td>
<td>M</td>
<td>V</td>
<td>1</td>
</tr>
<tr>
<td>0a</td>
<td>Message Class</td>
<td>Section 18.7.19</td>
<td>M</td>
<td>TLV</td>
<td>2-10</td>
</tr>
<tr>
<td>60</td>
<td>Source Name</td>
<td>Section 18.7.30</td>
<td>M</td>
<td>TLV</td>
<td>2-…</td>
</tr>
<tr>
<td>61</td>
<td>Destination Name</td>
<td>Section 18.7.31</td>
<td>M</td>
<td>TLV</td>
<td>2-…</td>
</tr>
<tr>
<td>62</td>
<td>AN-APDU</td>
<td>Section 18.7.32</td>
<td>M</td>
<td>TLV</td>
<td>2-…</td>
</tr>
</tbody>
</table>

### 18.6.41 E Send End Signal Request

**Direction:** MSC-B=MSC-T $\Rightarrow$ MSC-A=MSC-I (via HLR)

<table>
<thead>
<tr>
<th>IEI</th>
<th>IE</th>
<th>Type</th>
<th>Presence</th>
<th>Format</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>IMSI</td>
<td>Message Type</td>
<td>M</td>
<td>V</td>
<td>1</td>
</tr>
<tr>
<td>0a</td>
<td>Message Class</td>
<td>Section 18.7.29</td>
<td>M</td>
<td>TLV</td>
<td>3</td>
</tr>
<tr>
<td>60</td>
<td>Source Name</td>
<td>Section 18.7.30</td>
<td>M</td>
<td>TLV</td>
<td>2-…</td>
</tr>
<tr>
<td>61</td>
<td>Destination Name</td>
<td>Section 18.7.31</td>
<td>M</td>
<td>TLV</td>
<td>2-…</td>
</tr>
<tr>
<td>62</td>
<td>AN-APDU</td>
<td>Section 18.7.32</td>
<td>M</td>
<td>TLV</td>
<td>2-…</td>
</tr>
</tbody>
</table>

### 18.6.42 E Send End Signal Error

**Direction:** MSC-A=MSC-I $\Rightarrow$ MSC-B=MSC-T (via HLR)

<table>
<thead>
<tr>
<th>IEI</th>
<th>IE</th>
<th>Type</th>
<th>Presence</th>
<th>Format</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>IMSI</td>
<td>Message Type</td>
<td>M</td>
<td>V</td>
<td>1</td>
</tr>
<tr>
<td>0a</td>
<td>Message Class</td>
<td>Section 18.7.29</td>
<td>M</td>
<td>TLV</td>
<td>3</td>
</tr>
<tr>
<td>60</td>
<td>Source Name</td>
<td>Section 18.7.30</td>
<td>M</td>
<td>TLV</td>
<td>2-…</td>
</tr>
<tr>
<td>61</td>
<td>Destination Name</td>
<td>Section 18.7.31</td>
<td>M</td>
<td>TLV</td>
<td>2-…</td>
</tr>
<tr>
<td>62</td>
<td>AN-APDU</td>
<td>Section 18.7.32</td>
<td>M</td>
<td>TLV</td>
<td>2-…</td>
</tr>
</tbody>
</table>

### 18.6.43 E Send End Signal Result

**Direction:** MSC-A $\Rightarrow$ MSC-B=MSC-I (via HLR)

<table>
<thead>
<tr>
<th>IEI</th>
<th>IE</th>
<th>Type</th>
<th>Presence</th>
<th>Format</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>IMSI</td>
<td>Message Type</td>
<td>M</td>
<td>V</td>
<td>1</td>
</tr>
<tr>
<td>0a</td>
<td>Message Class</td>
<td>Section 18.7.29</td>
<td>M</td>
<td>TLV</td>
<td>3</td>
</tr>
<tr>
<td>60</td>
<td>Source Name</td>
<td>Section 18.7.30</td>
<td>M</td>
<td>TLV</td>
<td>2-…</td>
</tr>
<tr>
<td>61</td>
<td>Destination Name</td>
<td>Section 18.7.31</td>
<td>M</td>
<td>TLV</td>
<td>2-…</td>
</tr>
<tr>
<td>62</td>
<td>AN-APDU</td>
<td>Section 18.7.32</td>
<td>M</td>
<td>TLV</td>
<td>2-…</td>
</tr>
</tbody>
</table>

### 18.6.44 E Process Access Signalling Request

**Direction:** MSC-B=MSC-T $\Rightarrow$ MSC-A=MSC-I (via HLR)

<table>
<thead>
<tr>
<th>IEI</th>
<th>IE</th>
<th>Type</th>
<th>Presence</th>
<th>Format</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>IMSI</td>
<td>Message Type</td>
<td>M</td>
<td>V</td>
<td>1</td>
</tr>
</tbody>
</table>

Copyright © 2017 sysmocom - s.f.m.c. GmbH

DRAFT 1.6.1-32-ge95c0, 2020-Mar-24
### 18.6.45 E Forward Access Signalling Request

Direction: MSC-A ⇒ MSC-B=MSC-I (via HLR)

<table>
<thead>
<tr>
<th>IEI</th>
<th>IE</th>
<th>Type</th>
<th>Presence</th>
<th>Format</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>IMSI</td>
<td>Section 18.7.19</td>
<td>M</td>
<td>TLV</td>
<td>2-10</td>
</tr>
<tr>
<td>0a</td>
<td>Message Class</td>
<td>Section 18.7.29</td>
<td>M</td>
<td>TLV</td>
<td>3</td>
</tr>
<tr>
<td>60</td>
<td>Source Name</td>
<td>Section 18.7.30</td>
<td>M</td>
<td>TLV</td>
<td>2-…</td>
</tr>
<tr>
<td>61</td>
<td>Destination Name</td>
<td>Section 18.7.31</td>
<td>M</td>
<td>TLV</td>
<td>2-…</td>
</tr>
<tr>
<td>62</td>
<td>AN-APDU</td>
<td>Section 18.7.32</td>
<td>M</td>
<td>TLV</td>
<td>2-…</td>
</tr>
</tbody>
</table>

### 18.6.46 E Close

Direction: MSC-A ⇒ MSC-B (via HLR)

<table>
<thead>
<tr>
<th>IEI</th>
<th>IE</th>
<th>Type</th>
<th>Presence</th>
<th>Format</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>IMSI</td>
<td>Section 18.7.19</td>
<td>M</td>
<td>TLV</td>
<td>2-10</td>
</tr>
<tr>
<td>0a</td>
<td>Message Class</td>
<td>Section 18.7.29</td>
<td>M</td>
<td>TLV</td>
<td>3</td>
</tr>
<tr>
<td>60</td>
<td>Source Name</td>
<td>Section 18.7.30</td>
<td>M</td>
<td>TLV</td>
<td>2-…</td>
</tr>
<tr>
<td>61</td>
<td>Destination Name</td>
<td>Section 18.7.31</td>
<td>M</td>
<td>TLV</td>
<td>2-…</td>
</tr>
</tbody>
</table>

### 18.6.47 E Abort

This message was added to GSUP for the inter-MSC handover. But so far it is not used yet.

### 18.6.48 E Routing Error

Direction: GSUP Server (HLR) ⇒ GSUP Client (MSC)

<table>
<thead>
<tr>
<th>IEI</th>
<th>IE</th>
<th>Type</th>
<th>Presence</th>
<th>Format</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>IMSI</td>
<td>Section 18.7.19</td>
<td>M</td>
<td>TLV</td>
<td>2-10</td>
</tr>
<tr>
<td>0a</td>
<td>Message Class</td>
<td>Section 18.7.29</td>
<td>M</td>
<td>TLV</td>
<td>3</td>
</tr>
<tr>
<td>60</td>
<td>Source Name</td>
<td>Section 18.7.30</td>
<td>M</td>
<td>TLV</td>
<td>2-…</td>
</tr>
<tr>
<td>61</td>
<td>Destination Name</td>
<td>Section 18.7.31</td>
<td>M</td>
<td>TLV</td>
<td>2-…</td>
</tr>
<tr>
<td>30</td>
<td>Session ID</td>
<td>Section 18.8.1</td>
<td>O</td>
<td>TLV</td>
<td>6</td>
</tr>
<tr>
<td>31</td>
<td>Session State</td>
<td>Section 18.8.2</td>
<td>O</td>
<td>TLV</td>
<td>3</td>
</tr>
</tbody>
</table>

### 18.7 Information Elements

#### 18.7.1 Message Type
<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x04</td>
<td>Update Location Request</td>
</tr>
<tr>
<td>0x05</td>
<td>Update Location Error</td>
</tr>
<tr>
<td>0x06</td>
<td>Update Location Result</td>
</tr>
<tr>
<td>0x08</td>
<td>Send Auth Info Request</td>
</tr>
<tr>
<td>0x09</td>
<td>Send Auth Info Error</td>
</tr>
<tr>
<td>0x0a</td>
<td>Send Auth Info Result</td>
</tr>
<tr>
<td>0x0c</td>
<td>Authentication Failure Report</td>
</tr>
<tr>
<td>0x0d</td>
<td>Purge MS Request</td>
</tr>
<tr>
<td>0x0e</td>
<td>Purge MS Error</td>
</tr>
<tr>
<td>0x0f</td>
<td>Purge MS Result</td>
</tr>
<tr>
<td>0x10</td>
<td>Insert Subscriber Data Request</td>
</tr>
<tr>
<td>0x11</td>
<td>Insert Subscriber Data Error</td>
</tr>
<tr>
<td>0x12</td>
<td>Insert Subscriber Data Result</td>
</tr>
<tr>
<td>0x14</td>
<td>Delete Subscriber Data Request</td>
</tr>
<tr>
<td>0x15</td>
<td>Delete Subscriber Data Error</td>
</tr>
<tr>
<td>0x16</td>
<td>Delete Subscriber Data Result</td>
</tr>
<tr>
<td>0x1c</td>
<td>Location Cancellation Request</td>
</tr>
<tr>
<td>0x1d</td>
<td>Location Cancellation Error</td>
</tr>
<tr>
<td>0x1e</td>
<td>Location Cancellation Result</td>
</tr>
<tr>
<td>0x20</td>
<td>Supplementary Service Request</td>
</tr>
<tr>
<td>0x21</td>
<td>Supplementary Service Error</td>
</tr>
<tr>
<td>0x22</td>
<td>Supplementary Service Result</td>
</tr>
<tr>
<td>0x24</td>
<td>MO-forwardSM Request</td>
</tr>
<tr>
<td>0x25</td>
<td>MO-forwardSM Error</td>
</tr>
<tr>
<td>0x26</td>
<td>MO-forwardSM Result</td>
</tr>
<tr>
<td>0x28</td>
<td>MT-forwardSM Request</td>
</tr>
<tr>
<td>0x29</td>
<td>MT-forwardSM Error</td>
</tr>
<tr>
<td>0x2a</td>
<td>MT-forwardSM Result</td>
</tr>
<tr>
<td>0x2c</td>
<td>READY-FOR-SM Request</td>
</tr>
<tr>
<td>0x2d</td>
<td>READY-FOR-SM Error</td>
</tr>
<tr>
<td>0x2e</td>
<td>READY-FOR-SM Result</td>
</tr>
<tr>
<td>0x30</td>
<td>CHECK-IMEI Request</td>
</tr>
<tr>
<td>0x31</td>
<td>CHECK-IMEI Error</td>
</tr>
<tr>
<td>0x32</td>
<td>CHECK-IMEI Result</td>
</tr>
</tbody>
</table>

The category of the message is indicated by the last two bits of the type. Request, Error and Result messages only differ in these last two bits, so it is trivial to transform them.

<table>
<thead>
<tr>
<th>Ending Bits</th>
<th>Message Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>Request</td>
</tr>
<tr>
<td>01</td>
<td>Error</td>
</tr>
<tr>
<td>10</td>
<td>Result</td>
</tr>
<tr>
<td>11</td>
<td>Other</td>
</tr>
</tbody>
</table>

**18.7.2 IP Address**

The value part is encoded like in the Packet data protocol address IE defined in 3GPP TS 04.08, Chapter 10.5.6.4. PDP type organization must be set to *IETF allocated address*.

**18.7.3 PDP Info**

This is a container for information elements describing a single PDP.
The conditional IE are mandatory unless mentioned otherwise.

### 18.7.4 PDP Type

The PDP type value consists of 2 octets that are encoded like octet 4-5 of the End User Address defined in 3GPP TS 09.60, 7.9.18.

The spare bits are left undefined. While 09.60 defines them as 1 1 1 1, there are MAP traces where these bits are set to 0 0 0 0. So the receiver shall ignore these bits.

Examples:

- IPv4: PDP type org: 1 (IETF), PDP type number: 0x21
- IPv6: PDP type org: 1 (IETF), PDP type number: 0x57

### 18.7.5 PDP Context ID

The PDP type context ID IE consists of a single integer byte wrapped in a TLV.
18.7.6 Auth tuple

This is a container for information elements describing a single authentication tuple.

<table>
<thead>
<tr>
<th>IEI</th>
<th>IE</th>
<th>Type</th>
<th>Presence</th>
<th>Format</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auth Tuple IEI</td>
<td>Section 18.7.17</td>
<td>M</td>
<td>V</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Length of Auth Tuple IE</td>
<td></td>
<td>M</td>
<td>V</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>RAND</td>
<td>Section 18.7.7</td>
<td>M</td>
<td>TLV</td>
<td>18</td>
</tr>
<tr>
<td>21</td>
<td>SRES</td>
<td>Section 18.7.8</td>
<td>M</td>
<td>TLV</td>
<td>6</td>
</tr>
<tr>
<td>22</td>
<td>Kc</td>
<td>Section 18.7.9</td>
<td>M</td>
<td>TLV</td>
<td>10</td>
</tr>
<tr>
<td>23</td>
<td>IK</td>
<td>Section 18.7.10</td>
<td>C</td>
<td>TLV</td>
<td>18</td>
</tr>
<tr>
<td>24</td>
<td>CK</td>
<td>Section 18.7.11</td>
<td>C</td>
<td>TLV</td>
<td>18</td>
</tr>
<tr>
<td>25</td>
<td>AUTN</td>
<td>Section 18.7.12</td>
<td>C</td>
<td>TLV</td>
<td>18</td>
</tr>
<tr>
<td>27</td>
<td>RES</td>
<td>Section 18.7.14</td>
<td>C</td>
<td>TLV</td>
<td>2-18</td>
</tr>
</tbody>
</table>

The conditional IEs IK, CK, AUTN and RES are only present in case the subscriber supports UMTS AKA.

18.7.7 RAND

The 16-byte Random Challenge of the GSM Authentication Algorithm.

18.7.8 SRES

The 4-byte Authentication Result of the GSM Authentication Algorithm.

18.7.9 Kc

The 8-byte Encryption Key of the GSM Authentication and Key Agreement Algorithm.

18.7.10 IK

The 16-byte Integrity Protection Key generated by the UMTS Authentication and Key Agreement Algorithm.

18.7.11 CK

The 16-byte Ciphering Key generated by the UMTS Authentication and Key Agreement Algorithm.
18.7.12 AUTN

The 16-byte Authentication Nonce sent from network to USIM in the UMTS Authentication and Key Agreement Algorithm.

18.7.13 AUTS

The 14-byte Authentication Synchronization Nonce generated by the USIM in case the UMTS Authentication and Key Agreement Algorithm needs to re-synchronize the sequence counters between AUC and USIM.

18.7.14 RES

The (variable length, but typically 16 byte) Authentication Result generated by the USIM in the UMTS Authentication and Key Agreement Algorithm.

18.7.15 CN Domain

This single-byte information element indicates the Core Network Domain, i.e. if the message is related to Circuit Switched or Packet Switched services.

For backwards compatibility reasons, if no CN Domain IE is present within a request, the PS Domain is assumed.

Table 6: CN Domain Number

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x01</td>
<td>PS Domain</td>
</tr>
<tr>
<td>0x02</td>
<td>CS Domain</td>
</tr>
</tbody>
</table>

18.7.16 Cancellation Type

Table 7: Cancellation Type Number

<table>
<thead>
<tr>
<th>Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x00</td>
<td>Update Procedure</td>
</tr>
<tr>
<td>0x01</td>
<td>Subscription Withdrawn</td>
</tr>
</tbody>
</table>
### 18.7.17 IE Identifier (informational)

These are the standard values for the IEI. See the message definitions for the IEI that shall be used for the encoding.

Table 8: GSUP IE Identifiers

<table>
<thead>
<tr>
<th>IEI</th>
<th>Info Element</th>
<th>Type / Encoding</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x01</td>
<td>IMSI</td>
<td>Mobile Identity, 3GPP TS 04.08 Ch. 10.5.1.4</td>
</tr>
<tr>
<td>0x02</td>
<td>Cause</td>
<td>Section 18.7.25</td>
</tr>
<tr>
<td>0x03</td>
<td>Auth Tuple</td>
<td>Section 18.7.6</td>
</tr>
<tr>
<td>0x04</td>
<td>PDP Info Compl</td>
<td>Section 18.7.18</td>
</tr>
<tr>
<td>0x05</td>
<td>PDP Info</td>
<td>Section 18.7.3</td>
</tr>
<tr>
<td>0x06</td>
<td>Cancel Type</td>
<td>Section 18.7.16</td>
</tr>
<tr>
<td>0x07</td>
<td>Freeze P-TMSI</td>
<td>Section 18.7.18</td>
</tr>
<tr>
<td>0x08</td>
<td>MSISDN</td>
<td>ISDN-AddressString/octet, Section 18.7.20</td>
</tr>
<tr>
<td>0x09</td>
<td>HLR Number</td>
<td>Section 18.7.24</td>
</tr>
<tr>
<td>0x0a</td>
<td>Message Class</td>
<td>Section 18.7.29</td>
</tr>
<tr>
<td>0x10</td>
<td>PDP Context ID</td>
<td>Section 18.7.5</td>
</tr>
<tr>
<td>0x11</td>
<td>PDP Type</td>
<td>Section 18.7.4</td>
</tr>
<tr>
<td>0x12</td>
<td>Access Point Name</td>
<td>Section 18.7.21</td>
</tr>
<tr>
<td>0x13</td>
<td>QoS</td>
<td>Section 18.7.22</td>
</tr>
<tr>
<td>0x14</td>
<td>PDP-Charging Characteristics</td>
<td>Section 18.7.23</td>
</tr>
<tr>
<td>0x20</td>
<td>RAND</td>
<td>Section 18.7.7</td>
</tr>
<tr>
<td>0x21</td>
<td>SRES</td>
<td>Section 18.7.8</td>
</tr>
<tr>
<td>0x22</td>
<td>Kc</td>
<td>Section 18.7.9</td>
</tr>
<tr>
<td>0x23</td>
<td>IK</td>
<td>Section 18.7.10</td>
</tr>
<tr>
<td>0x24</td>
<td>CK</td>
<td>Section 18.7.11</td>
</tr>
<tr>
<td>0x25</td>
<td>AUTN</td>
<td>Section 18.7.12</td>
</tr>
<tr>
<td>0x26</td>
<td>AUTS</td>
<td>Section 18.7.13</td>
</tr>
<tr>
<td>0x27</td>
<td>RES</td>
<td>Section 18.7.14</td>
</tr>
<tr>
<td>0x28</td>
<td>CN Domain</td>
<td>Section 18.7.15</td>
</tr>
<tr>
<td>0x30</td>
<td>Session ID</td>
<td>Section 18.8.1</td>
</tr>
<tr>
<td>0x31</td>
<td>Session State</td>
<td>Section 18.8.2</td>
</tr>
<tr>
<td>0x35</td>
<td>Supplementary Service Info</td>
<td>Section 18.7.26</td>
</tr>
<tr>
<td>0x40</td>
<td>SM-RP-MR (Message Reference)</td>
<td>Section 18.8.3</td>
</tr>
<tr>
<td>0x41</td>
<td>SM-RP-DA (Destination Address)</td>
<td>Section 18.8.4</td>
</tr>
<tr>
<td>0x42</td>
<td>SM-RP-OA (Originating Address)</td>
<td>Section 18.8.5</td>
</tr>
<tr>
<td>0x43</td>
<td>SM-RP-UI (SM TPDU)</td>
<td>Section 18.8.7</td>
</tr>
<tr>
<td>0x44</td>
<td>SM-RP-Cause (RP Cause value)</td>
<td>Section 18.8.8</td>
</tr>
<tr>
<td>0x45</td>
<td>SM-RP-MMS (More Messages to Send)</td>
<td>Section 18.8.9</td>
</tr>
<tr>
<td>0x46</td>
<td>SM Alert Reason</td>
<td>Section 18.8.10</td>
</tr>
<tr>
<td>0x50</td>
<td>IMEI</td>
<td>Section 18.7.27</td>
</tr>
<tr>
<td>0x51</td>
<td>IMEI Check Result</td>
<td>Section 18.7.28</td>
</tr>
<tr>
<td>0x60</td>
<td>Source Name</td>
<td>Section 18.7.30</td>
</tr>
<tr>
<td>0x61</td>
<td>Destination Name</td>
<td>Section 18.7.31</td>
</tr>
<tr>
<td>0x62</td>
<td>AN-APDU</td>
<td>Section 18.7.32</td>
</tr>
<tr>
<td>0x63</td>
<td>RK Cause</td>
<td>Section 18.7.33</td>
</tr>
<tr>
<td>0x64</td>
<td>BSSAP Cause</td>
<td>Section 18.7.34</td>
</tr>
<tr>
<td>0x65</td>
<td>Session Management Cause</td>
<td>Section 18.7.35</td>
</tr>
</tbody>
</table>
18.7.18 Empty field

This is used for flags, if and only if this IE is present, the flag is set. The semantics depend on the IEI and the context.

18.7.19 IMSI

The IMSI is encoded like in octet 4-N of the Called Party BCD Number defined in 3GPP TS 04.08, 10.5.4.7.

Note

Either 1 1 1 1 | Number digit N (N odd) or Number digit N | Number digit N-1 (N even), where N is the number of digits.

18.7.20 ISDN-AddressString / MSISDN / Called Party BCD Number

The MSISDN is encoded as an ISDN-AddressString in 3GPP TS 09.02 and Called Party BCD Number in 3GPP TS 04.08. It will be stored by the SGSN or VLR and then passed as is to the GGSN during the activation of the primary PDP Context.
18.7.21 Access Point Name

This encodes the Access Point Name of a PDP Context. The encoding is defined in 3GPP TS 23.003.

18.7.22 Quality of Service Subscribed Service

This encodes the subscribed QoS of a subscriber. It will be used by the SGSN during the PDP Context activation. If the length of the QoS data is 3 (three) octets it is assumed that these are octets 3-5 of the TS 3GPP TS 24.008 Quality of Service Octets. If it is more than three then it is assumed that the first octet is the Allocation/Retention Priority and the reset are encoded as octets 3-N of 24.008.

18.7.23 PDP-Charging Characteristics

This encodes the ChargingCharacteristics of 3GPP TS 32.215. A HLR may send this as part of the InsertSubscriberData or within a single PDP context definition. If the HLR supplies this information it must be used by the SGSN or VLR when activating a PDP context.
18.7.24  HLR Number encoded as 3GPP TS 09.02 ISDN-AddressString

The HLR Number is encoded as an ISDN-AddressString in 3GPP TS 09.02. It will be stored by the SGSN or VLR can be used by the CDR module to keep a record.

18.7.25  Cause

This IE shall be encoded according to the GMM Cause as described in Chapter 10.5.5.14 of 3GPP TS 04.08.

18.7.26  Supplementary Service Info

This IE shall be used together with both Section 18.8.2 and Section 18.8.1 IEs. It is used to carry the payload of Supplementary Services encoded according to GSM TS 04.80.

18.7.27  IMEI

The IMEI encoded as Called Party BCD Number in 3GPP TS 04.08.
18.7.28 IMEI Check Result

Result of the Check IMEI request. A NACK could be sent in theory, if the ME is not permitted on the network (e.g. because it is on a blacklist).

Table 9: IMEI Check Result

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x01</td>
<td>ACK</td>
</tr>
<tr>
<td>0x02</td>
<td>NACK</td>
</tr>
</tbody>
</table>

18.7.29 Message Class

Indicate, which kind of message is being sent. This allows to trivially dispatch incoming GSUP messages to the right code paths, and should make writing a GSUP to MAP converter easier.

This IE was introduced together with inter-MSC handover code. Inter-MSC messages must include this IE and set it to the appropriate type. The intention of creating this IE was to use it with all GSUP messages eventually.

<table>
<thead>
<tr>
<th>Type</th>
<th>Always present</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>no</td>
<td>Subscriber Management</td>
</tr>
<tr>
<td>2</td>
<td>no</td>
<td>SMS</td>
</tr>
<tr>
<td>3</td>
<td>no</td>
<td>USSD</td>
</tr>
<tr>
<td>4</td>
<td>yes</td>
<td>Inter-MSC</td>
</tr>
</tbody>
</table>

18.7.30 Source Name

When the GSUP server is asked to forward a message between two GSUP clients, the source name is the IPA name of the client where the message is coming from. The source name IE is present, when the GSUP server forwards the message to the destination. Although redundant, the source name IE is also sent from the source to the GSUP server (so it is easier to follow the network traces).

Source and destination names are sent as nul-terminated strings.

![Figure 30: Message forwarding example](image)

18.7.31 Destination Name

The receiving counterpart to source name (Section 18.7.30).

18.7.32 AN-APDU

This IE encodes the AN-APDU parameter described in 3GPP TS 29.002 7.6.9.1.
### Table 10: Access Network Protocol

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x01</td>
<td>BSSAP</td>
</tr>
<tr>
<td>0x02</td>
<td>RANAP</td>
</tr>
</tbody>
</table>

18.7.33 **RR Cause**

This IE contains the reason for release or completion of an assignment or handover. See 3GPP TS 44.018 10.5.2.31 for reference.

18.7.34 **BSSAP Cause**

This IE indicates why an event is happening on the BSSAP interface. See 3GPP TS 48.008 3.2.2.5 for reference.

18.7.35 **Session Management Cause**

This IE contains the reason for rejecting a session management request. See 3GPP TS 24.008 10.5.6.6 / Table 10.5.157 for reference.

18.8 **Session (transaction) management**

Unlike TCAP/MAP, GSUP is just a transport layer without the dialogue/context. All communication is usually happening over a single connection. In order to fill this gap, there is a few optional IEs, which allow both communication sides to establish and terminate TCAP-like transactions over GSUP.

18.8.1 **Session ID**

This auxiliary IE shall be used together with Section 18.8.2. The purpose of this IE is to identify a particular transaction using the 4-byte unique identifier.
18.8.2 Session State

This auxiliary IE shall be used together with Section 18.8.1. The purpose of this IE is to indicate a state of a particular transaction, i.e. initiate, continue or terminate it.
### Table 11: Session state

<table>
<thead>
<tr>
<th>State</th>
<th>TCAP alternative</th>
<th>Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0x00</td>
<td>Undefined</td>
<td>Used when session management is not required</td>
<td></td>
</tr>
<tr>
<td>0x01</td>
<td>BEGIN</td>
<td>Used to initiate a new session</td>
<td></td>
</tr>
<tr>
<td>0x02</td>
<td>CONTINUE</td>
<td>Used to continue an existing session</td>
<td></td>
</tr>
<tr>
<td>0x03</td>
<td>END</td>
<td>Used to terminate an existing session</td>
<td></td>
</tr>
</tbody>
</table>

#### 18.8.3 SM-RP-MR (Message Reference)

According to TS GSM 04.11, section 8.2.3, every single message on the SM-RL (SM Relay Layer) has a unique message reference, that is used to link an RP-ACK or RP-ERROR message to the associated (preceding) RP-DATA or RP-SMMA message transfer attempt.

In case of TCAP/MAP, this message reference is being mapped to the Invoke ID. But since GSUP has no Invoke ID IE, and it is not required for other applications (other than SMS), a special Section 18.8.3 is used to carry the message reference value ’as-is’ (i.e. in range 0 through 255).

#### 18.8.4 SM-RP-DA (Destination Address)

This IE represents the destination address used by the short message service relay sub-layer protocol. It can be one of the following:

- IMSI (see 3GPP TS 29.002, clause 7.6.2.1);
- MSISDN (see 3GPP TS 29.002, clause 7.6.2.17);
- service centre address (see 3GPP TS 29.002, clause 7.6.2.27).

Coding of this IE is described in Section 18.8.6. See 3GPP TS 29.002, section 7.6.8.1 for details.

#### 18.8.5 SM-RP-OA (Originating Address)

This IE represents the originating address used by the short message service relay sub-layer protocol. It can be either of the following:

- MSISDN (see 3GPP TS 29.002, clause 7.6.2.17);
- service centre address (see 3GPP TS 29.002, clause 7.6.2.27).

Coding of this IE is described in Section 18.8.6. See 3GPP TS 29.002, section 7.6.8.2 for details.

#### 18.8.6 Coding of SM-RP-DA / SM-RP-OA IEs

Basically, both Section 18.8.4 / Section 18.8.5 IEs contain a single TV of the following format:

<table>
<thead>
<tr>
<th>Field</th>
<th>Presence</th>
<th>Length</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>M</td>
<td>1</td>
<td>Identity type</td>
</tr>
<tr>
<td>V</td>
<td>O</td>
<td>1</td>
<td>ToN/NPI header</td>
</tr>
<tr>
<td>V</td>
<td>O</td>
<td>...</td>
<td>BCD encoded (or alphanumeric) identity</td>
</tr>
</tbody>
</table>
where the identity type can be one of the following:

<table>
<thead>
<tr>
<th>Type</th>
<th>ToN/NPI Header</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x01</td>
<td>No</td>
<td>IMSI (see 3GPP TS 29.002, clause 7.6.2.1)</td>
</tr>
<tr>
<td>0x02</td>
<td>Yes</td>
<td>MSISDN (see 3GPP TS 29.002, clause 7.6.2.17)</td>
</tr>
<tr>
<td>0x03</td>
<td>Yes</td>
<td>Service centre address (see 3GPP TS 29.002, clause 7.6.2.27)</td>
</tr>
<tr>
<td>0xff</td>
<td>No</td>
<td>Omit value for noSM-RP-DA and noSM-RP-OA</td>
</tr>
</tbody>
</table>

Coding of the optional ToN/NPI header, as well as all possible ToN/NPI values, is described in 3GPP TS 129.002, section 17.7.8 "Common data types", and can be summarized as follows:

![Figure 31: ToN/NPI header coding (as per 3GPP TS 129.002, MSB first)](image)

Please note that unlike both Section 18.7.19 and Section 18.7.20, where the value part is encoded as LV (i.e. contains an additional length), an identity in both Section 18.8.4 / Section 18.8.5 IEs shall not contain the redundant length octet.

18.8.7 SM-RP-UI (SM TPDU)

This IE represents the user data field carried by the short message service relay sub-layer (i.e. SM-TL (Transfer Layer)) protocol. In case of errors (i.e. MO/-MT-forwardSM Error messages), this IE may contain optional diagnostic field payload from RP-ERROR message.

See 3GPP TS 29.002, section 7.6.8.4 for details.

18.8.8 SM-RP-Cause (RP Cause value)

According to TS GSM 04.11, RP-Cause is a variable length element always included in the RP-ERROR message, conveying a negative result of an RP-DATA message transfer attempt or RP-SMMA notification attempt.

The mapping between error causes in TS GSM 04.11 and TS GSM 09.02 (MAP) is specified in TS GSM 03.40. But since GSUP has no generic User Error IE, and it is not required for other applications (other than SMS), a special Section 18.8.8 is used to carry the cause value 'as-is'.
18.8.9 SM-RP-MMS (More Messages to Send)

This is an optional IE of MT-ForwardSM-Req message, that is used by SMSC to indicate that there are more MT SMS messages to be sent, so the network should keep the RAN connection open. See 3GPP TS 29.002, section 7.6.8.7.

18.8.10 SM Alert Reason

According to 3GPP TS 29.002, section 7.6.8.8, Alert Reason is used to indicate the reason why the service centre is alerted, e.g. the MS has got some memory to store previously rejected incoming SMS.

It can take one of the following values:

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x01</td>
<td>MS present</td>
</tr>
<tr>
<td>0x02</td>
<td>Memory Available</td>
</tr>
</tbody>
</table>

Table 14: SM Alert Reason values

19 Glossary

2FF  
2nd Generation Form Factor; the so-called plug-in SIM form factor

3FF  
3rd Generation Form Factor; the so-called microSIM form factor

3GPP 
3rd Generation Partnership Project

4FF  
4th Generation Form Factor; the so-called nanoSIM form factor

A Interface  
Interface between BTS and BSC, traditionally over E1 (3GPP TS 48.008 [3gpp-ts-48-008])

A3/A8  
Algorithm 3 and 8; Authentication and key generation algorithm in GSM and GPRS, typically COMP128v1/v2/v3 or MILLENAGE are typically used

A5  
Algorithm 5; Air-interface encryption of GSM; currently only A5/0 (no encryption), A5/1 and A5/3 are in use

Abis Interface  
Interface between BTS and BSC, traditionally over E1 (3GPP TS 48.058 [3gpp-ts-48-058] and 3GPP TS 52.021 [3gpp-ts-52-021])

ACC  
Access Control Class; every BTS broadcasts a bit-mask of permitted ACC, and only subscribers with a SIM of matching ACC are permitted to use that BTS

AGCH  
Access Grant Channel on Um interface; used to assign a dedicated channel in response to RACH request

AGPL  
GNU Affero General Public License, a copyleft-style Free Software License
ARFCN
Absolute Radio Frequency Channel Number; specifies a tuple of uplink and downlink frequencies

AUC
Authentication Center; central database of authentication key material for each subscriber

BCCH
Broadcast Control Channel on Um interface; used to broadcast information about Cell and its neighbors

BCC
Base Station Color Code; short identifier of BTS, lower part of BSIC

BTS
Base Transceiver Station

BSC
Base Station Controller

BSIC
Base Station Identity Code; 16bit identifier of BTS within location area

BSSGP
Base Station Subsystem Gateway Protocol (3GPP TS 48.018 [3gpp-ts-48-018])

BVCI
BSSGP Virtual Circuit Identifier

CBCH
Cell Broadcast Channel; used to transmit Cell Broadcast SMS (SMS-CB)

CC
Call Control; Part of the GSM Layer 3 Protocol

CCCH
Common Control Channel on Um interface; consists of RACH (uplink), BCCH, PCH, AGCH (all downlink)

Cell
A cell in a cellular network, served by a BTS

CEPT
Conférence européenne des administrations des postes et des télécommunications; European Conference of Postal and Telecommunications Administrations.

CGI
Cell Global Identifier comprised of MCC, MNC, LAC and BSIC

CSFB
Circuit-Switched Fall Back; Mechanism for switching from LTE/EUTRAN to UTRAN/GERAN when circuit-switched services such as voice telephony are required.

dB
deci-Bel; relative logarithmic unit

dBm
deci-Bel (milliwatt); unit of measurement for signal strength of radio signals

DHCP
Dynamic Host Configuration Protocol (IETF RFC 2131 [ietf-rfc2131])

downlink
Direction of messages / signals from the network core towards the mobile phone

DSP
Digital Signal Processor
dvnxload
Tool to program UBL and the Bootloader on a sysmoBTS

EDGE
Enhanced Data rates for GPRS Evolution; Higher-speed improvement of GPRS; introduces 8PSK

EGPRS
Enhanced GPRS; the part of EDGE relating to GPRS services

EIR
Equipment Identity Register; core network element that stores and manages IMEI numbers

ESME
External SMS Entity; an external application interfacing with a SMSC over SMPP

ETSI
European Telecommunications Standardization Institute

FPGA
Field Programmable Gate Array; programmable digital logic hardware

Gb
Interface between PCU and SGSN in GPRS/EDGE network; uses NS, BSSGP, LLC

GERAN
GPRS/EDGE Radio Access Network

GFDL
GNU Free Documentation License; a copyleft-style Documentation License

GGSN
GPRS Gateway Support Node; gateway between GPRS and external (IP) network

GMSK
Gaussian Minimum Shift Keying; modulation used for GSM and GPRS

GPL
GNU General Public License, a copyleft-style Free Software License

Gp
Gp interface between SGSN and GGSN; uses GTP protocol

GPRS
General Packet Radio Service; the packet switched 2G technology

GPS
Global Positioning System; provides a highly accurate clock reference besides the global position

GSM
Global System for Mobile Communications. ETSI/3GPP Standard of a 2G digital cellular network

GSMTAP
GSM tap; pseudo standard for encapsulating GSM protocol layers over UDP/IP for analysis

GSUP
Generic subscriber Update Protocol. Osmocom-specific alternative to TCAP/MAP

GT
Global Title; an address in SCCP

GTP
GPRS Tunnel Protocol; used between SGSN and GGSN

HLR
Home Location Register; central subscriber database of a GSM network
HNB-GW
Home NodeB Gateway. Entity between femtocells (Home NodeB) and CN in 3G/UMTS.

HPLMN
Home PLMN; the network that has issued the subscriber SIM and has his record in HLR

IE
Information Element

IMEI
International Mobile Equipment Identity; unique 14-digit decimal number to globally identify a mobile device, optionally with a 15th checksum digit

IMEISV
IMEI software version; unique 14-digit decimal number to globally identify a mobile device (same as IMEI) plus two software version digits (total digits: 16)

IMSI
International Mobile Subscriber Identity; 15-digit unique identifier for the subscriber/SIM; starts with MCC/MNC of issuing operator

IP
Internet Protocol (IETF RFC 791 [?])

IPA
ip.access GSM over IP protocol; used to multiplex a single TCP connection

Iu
Interface in 3G/UMTS between RAN and CN

IuCS
Iu interface for circuit-switched domain. Used in 3G/UMTS between RAN and MSC

IuPS
Iu interface for packet-switched domain. Used in 3G/UMTS between RAN and SGSN

LAC
Location Area Code; 16bit identifier of Location Area within network

LAPD
Link Access Protocol, D-Channel (ITU-T Q.921 [itu-t-q921])

LAPDm
Link Access Protocol Mobile (3GPP TS 44.006 [3gpp-ts-44-006])

LLC
Logical Link Control; GPRS protocol between MS and SGSN (3GPP TS 44.064 [3gpp-ts-44-064])

Location Area
Location Area; a geographic area containing multiple BTS

LU
Location Updating; can be of type IMSI-Attach or Periodic. Procedure that indicates a subscriber’s physical presence in a given radio cell.

M2PA
MTP2 Peer-to-Peer Adaptation; a SIGTRAN Variant (RFC 4165 [ietf-rfc4165])

M2UA
MTP2 User Adaptation; a SIGTRAN Variant (RFC 3331 [ietf-rfc3331])

M3UA
MTP3 User Adaptation; a SIGTRAN Variant (RFC 4666 [ietf-rfc4666])
**MCC**  
Mobile Country Code; unique identifier of a country, e.g. 262 for Germany

**MFF**  
Machine-to-Machine Form Factor; a SIM chip package that is soldered permanently onto M2M device circuit boards.

**MGW**  
Media Gateway

**MM**  
Mobility Management; part of the GSM Layer 3 Protocol

**MNC**  
Mobile Network Code; identifies network within a country; assigned by national regulator

**MNCC**  
Mobile Network Call Control; Unix domain socket based Interface between MSC and external call control entity like osmo-sip-connector

**MNO**  
Mobile Network Operator; operator with physical radio network under his MCC/MNC

**MO**  
Mobile Originated. Direction from Mobile (MS/UE) to Network

**MS**  
Mobile Station; a mobile phone / GSM Modem

**MSC**  
Mobile Switching Center; network element in the circuit-switched core network

**MSISDN**  
Mobile Subscriber ISDN Number; telephone number of the subscriber

**MT**  
Mobile Terminated. Direction from Network to Mobile (MS/UE)

**MTP**  
Message Transfer Part; SS7 signaling protocol ([ITU-T Q.701](https://www.itu.int/rec/T-REC-Q.701))

**MVNO**  
Mobile Virtual Network Operator; Operator without physical radio network

**NCC**  
Network Color Code; assigned by national regulator

**NITB**  
Network In The Box; combines functionality traditionally provided by BSC, MSC, VLR, HLR, SMSC functions; see OsmoNITB

**NSEI**  
NS Entity Identifier

**NVCI**  
NS Virtual Circuit Identifier

**NWL**  
Network Listen; ability of some BTS to receive downlink from other BTSs

**NS**  
Network Service; protocol on Gb interface ([3GPP TS 48.016](https://www.3gpp.org/technologies-and-standards/standards/tds-48-016))

**OCXO**  
Oven Controlled Crystal Oscillator; very high precision oscillator, superior to a VCTCXO
OML
Operation & Maintenance Link (ETSI/3GPP TS 52.021 [3gpp-ts-52-021])

OpenBSC
Open Source implementation of GSM network elements, specifically OsmoBSC, OsmoNITB, OsmoSGSN

OpenGGSN
Open Source implementation of a GPRS Packet Control Unit

OpenVPN
Open-Source Virtual Private Network; software employed to establish encrypted private networks over untrusted public networks

Osmocom
Open Source MOBILE COMMUNICATIONS; collaborative community for implementing communications protocols and systems, including GSM, GPRS, TETRA, DECT, GMR and others

OsmoBSC
Open Source implementation of a GSM Base Station Controller

OsmoNITB
Open Source implementation of a GSM Network In The Box, combines functionality traditionally provided by BSC, MSC, VLR, HLR, AUC, SMSC

OsmoSGSN
Open Source implementation of a Serving GPRS Support Node

OsmoPCU
Open Source implementation of a GPRS Packet Control Unit

OTA
Over-The-Air; Capability of operators to remotely reconfigure/reprogram ISM/USIM cards

PC
Point Code; an address in MTP

PCH
Paging Channel on downlink Um interface; used by network to page an MS

PCU
Packet Control Unit; used to manage Layer 2 of the GPRS radio interface

PDCH
Packet Data Channel on Um interface; used for GPRS/EDGE signalling + user data

PIN
Personal Identification Number; a number by which the user authenticates to a SIM/USIM or other smart card

PLMN
Public Land Mobile Network; specification language for a single GSM network

PUK
PIN Unblocking Code; used to unblock a blocked PIN (after too many wrong PIN attempts)

RAC
Routing Area Code; 16bit identifier for a Routing Area within a Location Area

RACH
Random Access Channel on uplink Um interface; used by MS to request establishment of a dedicated channel

RAM
Remote Application Management; Ability to remotely manage (install, remove) Java Applications on SIM/USIM Card
RF
Radio Frequency

RFM
Remote File Management; Ability to remotely manage (write, read) files on a SIM/USIM card

Roaming
Procedure in which a subscriber of one network is using the radio network of another network, often in different countries; in some countries national roaming exists

Routing Area
Routing Area; GPRS specific sub-division of Location Area

RR
Radio Resources; Part of the GSM Layer 3 Protocol

RSL
Radio Signalling Link ([3GPP TS 48.058 [3gpp-ts-48-058]])

RTP
Real-Time Transport Protocol ([IETF RFC 3550 [ietf-rfc3550]]); Used to transport audio/video streams over UDP/IP

SACCH
Slow Associate Control Channel on Um interface; bundled to a TCH or SDCCH, used for signalling in parallel to active dedicated channel

SCCP
Signaling Connection Control Part; SS7 signaling protocol ([ITU-T Q.711 [itu-t-q711]])

SDCCH
Slow Dedicated Control Channel on Um interface; used for signalling and SMS transport in GSM

SDK
Software Development Kit

SGs
Interface between MSC (GSM/UMTS) and MME (LTE/EPC) to facilitate CSFB and SMS.

SGSN
Serving GPRS Support Node; Core network element for packet-switched services in GSM and UMTS.

SIGTRAN
Signaling Transport over IP ([IETF RFC 2719 [ietf-rfc2719]])

SIM
Subscriber Identity Module; small chip card storing subscriber identity

Site
A site is a location where one or more BTSs are installed, typically three BTSs for three sectors

SMPP
Short Message Peer-to-Peer; TCP based protocol to interface external entities with an SMSC

SMSC
Short Message Service Center; store-and-forward relay for short messages

SS7
Signaling System No. 7; Classic digital telephony signaling system

SS
Supplementary Services; query and set various service parameters between subscriber and core network (e.g. USSD, 3rd-party calls, hold/retrieve, advice-of-charge, call deflection)
SSH
Secure Shell; *IETF RFC 4250* [ietf-rfc4251] to 4254

SSN
Sub-System Number; identifies a given SCCP Service such as MSC, HLR

STP
Signaling Transfer Point; A Router in SS7 Networks

SUA
SCCP User Adaptation; a SIGTRAN Variant (*RFC 3868* [ietf-rfc3868])

syslog
System logging service of UNIX-like operating systems

**System Information**
A set of downlink messages on the BCCH and SACCH of the Um interface describing properties of the cell and network

TCH
Traffic Channel; used for circuit-switched user traffic (mostly voice) in GSM

TCP
Transmission Control Protocol; *(IETF RFC 793* [ietf-rfc793])

TFTP
Trivial File Transfer Protocol; *(IETF RFC 1350* [ietf-rfc1350])

TRX
Transceiver; element of a BTS serving a single carrier

TS
Technical Specification

u-Boot
Boot loader used in various embedded systems

UBI
An MTD wear leveling system to deal with NAND flash in Linux

UBL
Initial bootloader loaded by the TI Davinci SoC

UDP
User Datagram Protocol *(IETF RFC 768* [ietf-rfc768])

UICC
Universal Integrated Chip Card; A smart card according to *ETSI TR 102 216* [etsi-tr102216]

Um interface
U mobile; Radio interface between MS and BTS

uplink
Direction of messages: Signals from the mobile phone towards the network

USIM
Universal Subscriber Identity Module; application running on a UICC to provide subscriber identity for UMTS and GSM networks

USSD
Unstructured Supplementary Service Data; textual dialog between subscriber and core network, e.g. *100 → Your extension is 1234*

VCTCXO
Voltage Controlled, Temperature Compensated Crystal Oscillator; a precision oscillator, superior to a classic crystal oscillator, but inferior to an OCXO
VLR
Visitor Location Register; volatile storage of attached subscribers in the MSC

VPLMN
Visited PLMN; the network in which the subscriber is currently registered; may differ from HPLMN when on roaming

VTY
Virtual Teletype; a textual command-line interface for configuration and introspection, e.g. the OsmoBSC configuration file as well as its telnet link on port 4242

A Osmocom TCP/UDP Port Numbers

The Osmocom GSM system utilizes a variety of TCP/IP based protocols. The table below provides a reference as to which port numbers are used by which protocol / interface.

<table>
<thead>
<tr>
<th>L4 Protocol</th>
<th>Port Number</th>
<th>Purpose</th>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDP</td>
<td>2427</td>
<td>MGCP GW</td>
<td>osmo-bsc_mgcp, osmo-mgw</td>
</tr>
<tr>
<td>TCP</td>
<td>2775</td>
<td>SMPP (SMS interface for external programs)</td>
<td>osmo-nitb</td>
</tr>
<tr>
<td>TCP</td>
<td>3002</td>
<td>A-bis/IP OML</td>
<td>osmo-bts, osmo-bsc, osmo-nitb</td>
</tr>
<tr>
<td>TCP</td>
<td>3003</td>
<td>A-bis/IP RSL</td>
<td>osmo-bts, osmo-bsc, osmo-nitb</td>
</tr>
<tr>
<td>TCP</td>
<td>4236</td>
<td>Control Interface</td>
<td>osmo-trx</td>
</tr>
<tr>
<td>TCP</td>
<td>4237</td>
<td>telnet (VTY)</td>
<td>osmo-trx</td>
</tr>
<tr>
<td>TCP</td>
<td>4238</td>
<td>Control Interface</td>
<td>osmo-bts</td>
</tr>
<tr>
<td>TCP</td>
<td>4239</td>
<td>telnet (VTY)</td>
<td>osmo-stp</td>
</tr>
<tr>
<td>TCP</td>
<td>4240</td>
<td>telnet (VTY)</td>
<td>osmo-pcu</td>
</tr>
<tr>
<td>TCP</td>
<td>4241</td>
<td>telnet (VTY)</td>
<td>osmo-bts</td>
</tr>
<tr>
<td>TCP</td>
<td>4242</td>
<td>telnet (VTY)</td>
<td>osmo-nitb, osmo-bsc, cellmgr-ng</td>
</tr>
<tr>
<td>TCP</td>
<td>4243</td>
<td>telnet (VTY)</td>
<td>osmo-bsc_mgcp, osmo-mgw</td>
</tr>
<tr>
<td>TCP</td>
<td>4244</td>
<td>telnet (VTY)</td>
<td>osmo-bsc_nat</td>
</tr>
<tr>
<td>TCP</td>
<td>4245</td>
<td>telnet (VTY)</td>
<td>osmo-sgsn</td>
</tr>
<tr>
<td>TCP</td>
<td>4246</td>
<td>telnet (VTY)</td>
<td>osmo-gbproxy</td>
</tr>
<tr>
<td>TCP</td>
<td>4247</td>
<td>telnet (VTY)</td>
<td>OsmocomBB</td>
</tr>
<tr>
<td>TCP</td>
<td>4249</td>
<td>Control Interface</td>
<td>osmo-nitb, osmo-bsc</td>
</tr>
<tr>
<td>TCP</td>
<td>4250</td>
<td>Control Interface</td>
<td>osmo-bsc_nat</td>
</tr>
<tr>
<td>TCP</td>
<td>4251</td>
<td>Control Interface</td>
<td>osmo-sgsn</td>
</tr>
<tr>
<td>TCP</td>
<td>4252</td>
<td>telnet (VTY)</td>
<td>sysmobts-mgr</td>
</tr>
<tr>
<td>TCP</td>
<td>4253</td>
<td>telnet (VTY)</td>
<td>osmo-gplhub</td>
</tr>
<tr>
<td>TCP</td>
<td>4254</td>
<td>telnet (VTY)</td>
<td>osmo-msc</td>
</tr>
<tr>
<td>TCP</td>
<td>4255</td>
<td>Control Interface</td>
<td>osmo-msc</td>
</tr>
<tr>
<td>TCP</td>
<td>4256</td>
<td>telnet (VTY)</td>
<td>osmo-sip-connector</td>
</tr>
<tr>
<td>TCP</td>
<td>4257</td>
<td>Control Interface</td>
<td>osmo-ggsn, ggsn (OpenGGSN)</td>
</tr>
<tr>
<td>TCP</td>
<td>4258</td>
<td>telnet (VTY)</td>
<td>osmo-hlr</td>
</tr>
<tr>
<td>TCP</td>
<td>4259</td>
<td>Control Interface</td>
<td>osmo-hlr</td>
</tr>
<tr>
<td>TCP</td>
<td>4260</td>
<td>telnet (VTY)</td>
<td>osmo-ggsn</td>
</tr>
<tr>
<td>TCP</td>
<td>4261</td>
<td>telnet (VTY)</td>
<td>osmo-hnbgw</td>
</tr>
<tr>
<td>TCP</td>
<td>4262</td>
<td>Control Interface</td>
<td>osmo-hnbgw</td>
</tr>
<tr>
<td>TCP</td>
<td>4263</td>
<td>Control Interface</td>
<td>osmo-gbproxy</td>
</tr>
<tr>
<td>TCP</td>
<td>4264</td>
<td>telnet (VTY)</td>
<td>osmo-cbc</td>
</tr>
<tr>
<td>TCP</td>
<td>4265</td>
<td>Control Interface</td>
<td>osmo-cbc</td>
</tr>
<tr>
<td>TCP</td>
<td>4266</td>
<td>D-GSM MS Lookup: mDNS serve</td>
<td>osmo-hlr</td>
</tr>
<tr>
<td>TCP</td>
<td>4267</td>
<td>Control Interface</td>
<td>osmo-mgw</td>
</tr>
<tr>
<td>UDP</td>
<td>4729</td>
<td>GSMTAP</td>
<td>Almost every osmocom project</td>
</tr>
</tbody>
</table>
Table 15: (continued)

<table>
<thead>
<tr>
<th>L4 Protocol</th>
<th>Port Number</th>
<th>Purpose</th>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>5000</td>
<td>A/IP</td>
<td>osmo-bsc, osmo-bsc_nat</td>
</tr>
<tr>
<td>UDP</td>
<td>23000</td>
<td>GPRS-NS over IP default port</td>
<td>osmo-pcu, osmo-sgsn, osmo-gbproxy</td>
</tr>
</tbody>
</table>

B Bibliography / References

B.0.0.0.1 References


[18] [3gpp-ts-23-048] 3GPP TS 23.048: Security mechanisms for the (U)SIM application toolkit; Stage 2 http://www.3gpp.org/DynaReport/23048.htm


[26] [3gpp-ts-35-205] 3GPP TS 35.205: 3G Security; Specification of the MILENAGE algorithm set; General


[28] [3gpp-ts-44-006] 3GPP TS 44.006: Mobile Station - Base Station System (MS - BSS) interface; Data Link (DL) layer specification http://www.3gpp.org/DynaReport/44006.htm

[29] [3gpp-ts-44-018] 3GPP TS 44.018: Mobile radio interface layer 3 specification; Radio Resource Control (RRC) protocol http://www.3gpp.org/DynaReport/44018.htm


[31] [3gpp-ts-48-008] 3GPP TS 48.008: Mobile Switching Centre - Base Station system (MSC-BSS) interface; Layer 3 specification http://www.3gpp.org/DynaReport/48008.htm


[33] [3gpp-ts-48-018] 3GPP TS 48.018: General Packet Radio Service (GPRS); Base Station System (BSS) - Serving GPRS Support Node (SGSN); BSS GPRS protocol (BSSGP) http://www.3gpp.org/DynaReport/48018.htm

[34] [3gpp-ts-48-056] 3GPP TS 48.056: Base Station Controller - Base Transceiver Station (BSC - BTS) interface; Layer 2 specification http://www.3gpp.org/DynaReport/48056.htm


[38] [3gpp-ts-52-021] 3GPP TS 52.021: Network Management (NM) procedures and messages on the A-bis interface http://www.3gpp.org/DynaReport/52021.htm
[39] [etsi-tr102216] ETSI TR 102 216: Smart cards http://www.etsi.org/deliver/etsi_tr/102200_102299/102216/-03.00.00_60/tr_102216v030000p.pdf

[40] [etsi-ts102221] ETSI TS 102 221: Smart Cards; UICC-Terminal interface; Physical and logical characteristics http://www.etsi.org/deliver/etsi_ts/102200_102299/102221/13.01.00_60/ts_102221v130100p.pdf

[41] [etsi-ts101220] ETSI TS 101 220: Smart Cards; ETSI numbering system for telecommunication application providers http://www.etsi.org/deliver/etsi_ts/101200_101299/101220/12.00.00_60/ts_101220v120000p.pdf


[58] [itu-t-q713] ITU-T Q.713: Signalling connection control part formats and codes https://www.itu.int/rec/T-REC-Q.713/en/


[60] [itu-t-q921] ITU-T Q.921: ISDN user-network interface - Data link layer specification https://www.itu.int/rec/T-REC-Q.921/en


[63] [freeswitch_pbx] FreeSWITCH SIP PBX https://freeswitch.org
C GNU Free Documentation License

Version 1.3, 3 November 2008


Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

C.1 PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document “free” in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of “copyleft”, which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals: it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

C.2 APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The “Document”, below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as “you”. You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A “Modified Version” of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A “Secondary Section” is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document’s overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The “Invariant Sections” are certain Secondary Section whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The “Cover Texts” are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The “Cover Texts” are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A “Transparent” copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not Transparent is called “Opaque”.

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary...
formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The “Title Page” means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, Title Page means the text near the most prominent appearance of the work’s title, preceding the beginning of the body of the text.

The “publisher” means any person or entity that distributes copies of the Document to the public.

A section “Entitled XYZ” means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as “Acknowledgements”, “Dedications”, “Endorsements”, or “History”.) To “Preserve the Title” of such a section when you modify the Document means that it remains a section “Entitled XYZ” according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

C.3 VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section Section C.4.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

C.4 COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document’s license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

C.5 MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:
a. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

b. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

c. State on the Title Page the name of the publisher of the Modified Version, as the publisher.

d. Preserve all the copyright notices of the Document.

e. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

f. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

g. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document’s license notice.

h. Include an unaltered copy of this License.

i. Preserve the section Entitled “History”, Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled “History” in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

j. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the “History” section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

k. For any section Entitled “Acknowledgements” or “Dedications”, Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

l. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

m. Delete any section Entitled “Endorsements”. Such a section may not be included in the [?].

n. Do not retitle any existing section to be Entitled “Endorsements” or to conflict in title with any Invariant Sections.

o. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Section and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version’s license notice. These titles must be distinct from any other section titles.

You may add a section Entitled “Endorsements”, provided it contains nothing but endorsements of your Modified Version by various parties—for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.
C.6 COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled “History” in the various original documents, forming one section Entitled “History”; likewise combine any sections Entitled “Acknowledgements”; and any sections Entitled “Dedications”. You must delete all sections Entitled “Endorsements”.

C.7 COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

C.8 AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an “aggregate” if the copyright resulting from the compilation is not used to limit the legal rights of the compilation’s users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document’s Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

C.9 TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled “Acknowledgements”, “Dedications”, or “History”, the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

C.10 TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, or distribute it is void, and will automatically terminate your rights under this License.
However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, receipt of a copy of some or all of the same material does not give you any rights to use it.

C.11 FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License “or any later version” applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation. If the Document specifies that a proxy can decide which future versions of this License can be used, that proxy’s public statement of acceptance of a version permanently authorizes you to choose that version for the Document.

C.12 RELICENSING

“Massive Multiauthor Collaboration Site” (or “MMC Site”) means any World Wide Web server that publishes copyrightable works and also provides prominent facilities for anybody to edit those works. A public wiki that anybody can edit is an example of such a server. A “Massive Multiauthor Collaboration” (or “MMC”) contained in the site means any set of copyrightable works thus published on the MMC site.

“CC-BY-SA” means the Creative Commons Attribution-Share Alike 3.0 license published by Creative Commons Corporation, a not-for-profit corporation with a principal place of business in San Francisco, California, as well as future copyleft versions of that license published by that same organization.

“Incorporate” means to publish or republish a Document, in whole or in part, as part of another Document.

An MMC is “eligible for relicensing” if it is licensed under this License, and if all works that were first published under this License somewhere other than this MMC, and subsequently incorporated in whole or in part into the MMC, (1) had no cover texts or invariant sections, and (2) were thus incorporated prior to November 1, 2008.

The operator of an MMC Site may republish an MMC contained in the site under CC-BY-SA on the same site at any time before August 1, 2009, provided the MMC is eligible for relicensing.

C.13 ADDENDUM: How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

```
Copyright (c) YEAR YOUR NAME.
Permission is granted to copy, distribute and/or modify this document
under the terms of the GNU Free Documentation License, Version 1.3
or any later version published by the Free Software Foundation;
with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.
A copy of the license is included in the section entitled `GNU
Free Documentation License'.
```

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the “with . . . Texts.” line with this:
with the Invariant Sections being LIST THEIR TITLES, with the
Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit
the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your
choice of free software license, such as the GNU General Public License, to permit their use in free software.