sysmocom

sysmocom - s.f.m.c. GmbH



OsmoHLR User Manual

by Neels Hofmeyr

DRAFT

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			
NUMBER	DATE	DESCRIPTION	NAME
1	September 18th, 2017	Initial version; based on OsmoNITB manual version 2.	NH

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

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 . . . 3
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 . . . 4
2.4.5 Documentation License . . . 4

3 Introduction **4**
3.1 Required Skills . . . 4
3.2 Getting assistance . . . 5

4 Overview **5**
4.1 About OsmoHLR . . . 5

5 Running OsmoHLR **6**
5.1 SYNOPSIS . . . 6
5.2 OPTIONS . . . 6
5.3 Bootstrap the Database . . . 6
5.4 Multiple instances . . . 7

6 Managing Subscribers **7**
6.1 Example: Add/Update/Delete Subscriber via VTY . . . 7
6.2 Subscriber Parameters . . . 8
6.3 Configuring the Subscribers Create on Demand Feature . . . 9
6.4 Import Subscriber Data . . . 10
6.4.1 Scripted Import . . . 10
6.4.2 Import OsmoNITB database . . . 11

7 Unstructured Supplementary Services Data (USSD) **11**
7.1 USSD in Osmocom . . . 11
7.2 USSD Configuration . . . 12
7.3 Built-in USSD handlers . . . 12
7.4 Example EUSE program . . . 12

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

8 The Osmocom VTY Interface **12**
8.1 Accessing the telnet VTY . . . 14
8.2 VTY Nodes . . . 14
8.3 Interactive help . . . 14
8.3.1 The question-mark (?) command . . . 15
8.3.2 TAB completion . . . 16
8.3.3 The list command . . . 16
8.3.4 The attribute system . . . 18
8.3.5 The expert mode . . . 19

9 libosmocore Logging System **20**
9.1 Log categories . . . 20
9.2 Log levels . . . 20
9.3 Log printing options . . . 21
9.4 Log filters . . . 21
9.5 Log targets . . . 22
9.5.1 Logging to the VTY . . . 22
9.5.2 Logging to the ring buffer . . . 22
9.5.3 Logging via gsmtap . . . 22
9.5.4 Logging to a file . . . 24
9.5.5 Logging to syslog . . . 24
9.5.6 Logging to systemd-journal . . . 25
9.5.7 Logging to stderr . . . 26

10 Control interface **26**
10.1 subscriber.by-*.info, info-aud, info-all . . . 27
10.2 subscriber.by-*.ps-enabled, cs-enabled . . . 28
10.3 subscriber.by-*.msisdn . . . 30
10.4 subscriber.by-*.aud2g . . . 30
10.5 subscriber.by-*.aud3g . . . 31

11 Osmocom Control Interface **31**
11.1 Control Interface Protocol . . . 32
11.1.1 GET operation . . . 33
11.1.2 SET operation . . . 33
11.1.3 TRAP operation . . . 33
11.2 Common variables . . . 34
11.3 Control Interface python examples . . . 34
11.3.1 Getting rate counters . . . 34
11.3.2 Setting a value . . . 35
11.3.3 Getting a value . . . 35
11.3.4 Listening for traps . . . 35

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

12 Distributed GSM / Multicast MS Lookup **35**
12.1 Finding Subscribers: mslookup Clients . . . 36
12.1.1 Find the Current Location of an MSISDN . . . 36
12.1.2 Find the Home HLR for an IMSI . . . 37
12.2 mslookup Configuration . . . 37
12.2.1 Example . . . 38
12.2.2 mDNS . . . 38
12.2.3 Server: Site Services . . . 39
12.2.4 Server: Own GSUP Address . . . 39
12.2.5 Client IPA Naming . . . 40
12.3 Queries . . . 40
12.4 Service Client Implementation . . . 41
12.4.1 mslookup Library . . . 41
12.4.2 osmo-mslookup-client . . . 41
12.4.3 SIP Service Client . . . 42
12.4.3.1 FreeSwitch dialplan.py . . . 42
12.4.4 SMS Service Client . . . 42
12.4.4.1 SMS via SMPP Port . . . 42
12.4.4.2 SMS-Over-GSUP . . . 43

13 Generic Subscriber Update Protocol **43**
13.1 General . . . 43
13.2 Connection . . . 44
13.3 Using IPA . . . 44
13.4 Procedures . . . 44
13.4.1 Authentication management . . . 44
13.4.2 Reporting of Authentication Failure . . . 44
13.4.3 Location Updating . . . 45
13.4.4 Location Cancellation . . . 45
13.4.5 Purge MS . . . 45
13.4.6 Delete Subscriber Data . . . 46
13.4.7 Check IMEI . . . 46
13.5 Procedures (E Interface) . . . 46
13.5.1 E Handover . . . 46
13.5.2 E Subsequent Handover . . . 47
13.5.3 E Forward and Process Access Signalling . . . 47
13.5.4 E Routing Error . . . 48
13.6 Message Format . . . 48
13.6.1 General . . . 48

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

13.6.2 Send Authentication Info Request . . . 48
13.6.3 Send Authentication Info Error . . . 49
13.6.4 Send Authentication Info Response . . . 49
13.6.5 Authentication Failure Report . . . 49
13.6.6 Update Location Request . . . 49
13.6.7 Update Location Error . . . 49
13.6.8 Update Location Result . . . 49
13.6.9 Location Cancellation Request . . . 50
13.6.10 Location Cancellation Error . . . 50
13.6.11 Location Cancellation Result . . . 50
13.6.12 Purge MS Request . . . 50
13.6.13 Purge MS Error . . . 50
13.6.14 Purge MS Result . . . 51
13.6.15 Insert Subscriber Data Request . . . 51
13.6.16 Insert Subscriber Data Error . . . 51
13.6.17 Insert Subscriber Data Result . . . 51
13.6.18 Delete Subscriber Data Request . . . 51
13.6.19 Delete Subscriber Data Error . . . 52
13.6.20 Delete Subscriber Data Result . . . 52
13.6.21 Process Supplementary Service Request . . . 52
13.6.22 Process Supplementary Service Error . . . 52
13.6.23 Process Supplementary Service Response . . . 52
13.6.24 MO-forwardSM Request . . . 53
13.6.25 MO-forwardSM Error . . . 53
13.6.26 MO-forwardSM Result . . . 53
13.6.27 MT-forwardSM Request . . . 54
13.6.28 MT-forwardSM Error . . . 54
13.6.29 MT-forwardSM Result . . . 54
13.6.30 READY-FOR-SM Request . . . 54
13.6.31 READY-FOR-SM Error . . . 55
13.6.32 READY-FOR-SM Result . . . 55
13.6.33 CHECK-IMEI Request . . . 55
13.6.34 CHECK-IMEI Error . . . 55
13.6.35 CHECK-IMEI Result . . . 55
13.6.36 E Prepare Handover Request . . . 56
13.6.37 E Prepare Handover Error . . . 56
13.6.38 E Prepare Handover Result . . . 56
13.6.39 E Prepare Subsequent Handover Request . . . 56
13.6.40 E Prepare Subsequent Handover Error . . . 56

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

13.6.41 E Prepare Subsequent Handover Result . . . 57
13.6.42 E Send End Signal Request . . . 57
13.6.43 E Send End Signal Error . . . 57
13.6.44 E Send End Signal Result . . . 57
13.6.45 E Process Access Signalling Request . . . 58
13.6.46 E Forward Access Signalling Request . . . 58
13.6.47 E Close . . . 58
13.6.48 E Abort . . . 58
13.6.49 E Routing Error . . . 58
13.6.50 ePDG Tunnel Request . . . 59
13.6.51 ePDG Tunnel Error . . . 59
13.6.52 ePDG Tunnel Result . . . 59
13.7 Information Elements . . . 59
13.7.1 Message Type . . . 59
13.7.2 IP Address . . . 62
13.7.3 PDP Info . . . 62
13.7.4 PDP Address . . . 62
13.7.5 PDP Context ID . . . 64
13.7.6 Auth tuple . . . 64
13.7.7 RAND . . . 64
13.7.8 SRES . . . 64
13.7.9 Kc . . . 64
13.7.10 IK . . . 64
13.7.11 CK . . . 65
13.7.12 AUTN . . . 65
13.7.13 AUTS . . . 65
13.7.14 RES . . . 65
13.7.15 CN Domain . . . 65
13.7.16 Cancellation Type . . . 65
13.7.17 IE Identifier (informational) . . . 66
13.7.18 Empty field . . . 67
13.7.19 IMSI . . . 67
13.7.20 ISDN-AddressString / MSISDN / Called Party BCD Number . . . 67
13.7.21 Access Point Name . . . 68
13.7.22 Quality of Service Subscribed Service . . . 68
13.7.23 PDP-Charging Characteristics . . . 68
13.7.24 Protocol Configuration Options (PCO) . . . 69
13.7.25 HLR Number encoded as 3GPP TS 09.02 ISDN-AddressString . . . 69
13.7.26 Cause . . . 69

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

13.7.27 Supplementary Service Info . . . 69
13.7.28 IMEI . . . 69
13.7.29 IMEI Check Result . . . 69
13.7.30 Message Class . . . 70
13.7.31 Source Name . . . 70
13.7.32 Destination Name . . . 70
13.7.33 AN-APDU . . . 70
13.7.34 RR Cause . . . 71
13.7.35 BSSAP Cause . . . 71
13.7.36 Current RAT Type . . . 71
13.7.37 Session Management Cause . . . 71
13.8 Session (transaction) management . . . 71
13.8.1 Session ID . . . 71
13.8.2 Session State . . . 72
13.8.3 SM-RP-MR (Message Reference) . . . 72
13.8.4 SM-RP-DA (Destination Address) . . . 72
13.8.5 SM-RP-OA (Originating Address) . . . 72
13.8.6 Coding of SM-RP-DA / SM-RP-OA IEs . . . 72
13.8.7 SM-RP-UI (SM TPDU) . . . 73
13.8.8 SM-RP-Cause (RP Cause value) . . . 73
13.8.9 SM-RP-MMS (More Messages to Send) . . . 74
13.8.10 SM Alert Reason . . . 74

14 VTY Process and Thread management **74**
14.1 Scheduling Policy . . . 74
14.2 CPU-Affinity Mask . . . 74

15 Glossary **76**

A Osmocom TCP/UDP Port Numbers **84**

B Bibliography / References **85**
B.0.0.0.1 References . . . 85

C GNU Free Documentation License **90**
C.1 PREAMBLE . . . 90
C.2 APPLICABILITY AND DEFINITIONS . . . 90
C.3 VERBATIM COPYING . . . 91
C.4 COPYING IN QUANTITY . . . 91
C.5 MODIFICATIONS . . . 91
C.6 COMBINING DOCUMENTS . . . 93

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

C.7 COLLECTIONS OF DOCUMENTS . . . 93
C.8 AGGREGATION WITH INDEPENDENT WORKS . . . 93
C.9 TRANSLATION . . . 93
C.10 TERMINATION . . . 93
C.11 FUTURE REVISIONS OF THIS LICENSE . . . 94
C.12 RELICENSING . . . 94
C.13 ADDENDUM: How to use this License for your documents . . . 94

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

1 Foreword

Digital cellular networks based on the GSM specification were designed in the late 1980s and first deployed in the early 1990s 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.

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

- 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
- NLnet Foundation, for providing funding for a number of individual work items within the Osmocom universe, such as LTE support in OsmoCBC or GPRS/EGPRS support for Ericsson RBS6000.
- WaveMobile Ltd, for many years of sponsoring.

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 benefiting 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, workarounds
- 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.

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

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.

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

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 https://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.

If you would like to obtain professional/commercial support on Osmocom CNI, you can always reach out to sales@sysmocom.de to discuss your support needs. Purchasing support from sysmocom helps to cover the ongoing maintenance of the Osmocom CNI software stack.

4 Overview

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

4.1 About OsmoHLR

OsmoHLR is Osmocom's minimal implementation of a Home Location Register (HLR) for 2G and 3G GSM and UMTS mobile core networks. Its interfaces are:

- GSUP, serving towards OsmoMSC and OsmoSGSN;
- A local SQLite database;
- The Osmocom typical telnet VTY and CTRL interfaces.

Originally, the OpenBSC project's OsmoNITB all-in-one implementation had an integrated HLR, managing subscribers and SMS in the same local database. Along with the separate OsmoMSC and its new VLR component, OsmoHLR was implemented from scratch to alleviate various shortcomings of the internal HLR:

- The separate HLR allows using centralized subscriber management for both circuit-switched and packet-switched domains (i.e. one OsmoHLR for both OsmoMSC and OsmoSGSN).
- 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.
- In contrast to the OsmoNITB, the specific way the new OsmoMSC's VLR accesses OsmoHLR brings fully asynchronous subscriber database access.

Find the OsmoHLR issue tracker and wiki online at

- https://osmocom.org/projects/osmo-hlr
- https://osmocom.org/projects/osmo-hlr/wiki

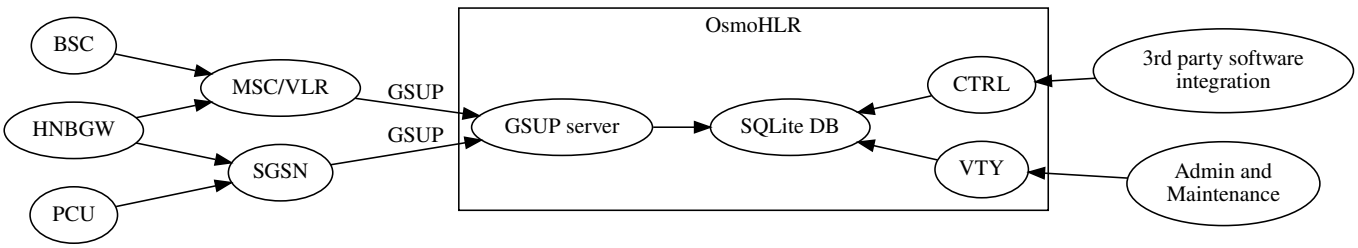


Figure 1: Typical GSM network architecture used with OsmoHLR

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

5 Running OsmoHLR

The OsmoHLR executable (`osmo-hlr`) offers the following command-line arguments:

5.1 SYNOPSIS

osmo-hlr [-h] [-c *CONFIGFILE*] [-l *DATABASE*] [-d *DBGMASK*] [-D] [-s] [-T] [-e *LOGLEVEL*] [-U] [-V]

5.2 OPTIONS

-h, --help
Print a short help message about the supported options

-c, --config-file *CONFIGFILE*
Specify the file and path name of the configuration file to be used. If none is specified, use `osmo-hlr.cfg` in the current working directory.

-l, --database *DATABASE*
Specify the file name of the SQLite3 database to use as HLR/AUC storage

-d, --debug *DBGMASK,DBGLEVELS*
Set the log subsystems and levels for logging to stderr. This has mostly been superseded by VTY-based logging configuration, see Section 9 for further information.

-D, --daemonize
Fork the process as a daemon into background.

-s, --disable-color
Disable colors for logging to stderr. This has mostly been deprecated by VTY based logging configuration, see Section 9 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 9 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 9 for more information.

-U, --db-upgrade
Allow HLR database schema upgrades. If OsmoHLR was updated and requires a newer database schema, it will refuse to start unless this option is specified. The updated database can not be downgraded, make backups as necessary.

-V, --version
Print the compile-time version number of the OsmoHLR program

5.3 Bootstrap the Database

If no database exists yet, OsmoHLR will automatically create and bootstrap a database file with empty tables. If no `-l` command-line option is provided, this database file will be created in the current working directory.

Alternatively, you may use the `osmo-hlr-db-tool`, which is installed along with `osmo-hlr`, to bootstrap an empty database, or to migrate subscriber data from an old *OsmoNITB* database. See Section 6.4.2.

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

5.4 Multiple instances

Running multiple instances of `osmo-hlr` 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:

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

The GSUP interface can be bound to a specific IP address by the following configuration options:

```
hlr
 gsup
  bind ip 10.23.42.1
```

Note
At the time of writing, OsmoHLR lacks a config option to change the GSUP port, which is by default TCP port 4222.

6 Managing Subscribers

Subscribers are kept in a local SQLite database file and can be managed via VTY and CTRL interfaces.

This section provides some examples; also refer to the OsmoHLR VTY reference manual [vty-ref-osmohlr] as well as the Control interface described in Section 10.

6.1 Example: Add/Update/Delete Subscriber via VTY

The following telnet VTY session adds a subscriber complete with GSM (2G) and UMTS (3G and 2G) authentication tokens, and finally removes the subscriber again; it assumes that osmo-hlr is running and listening for telnet VTY connections on localhost:

```
$ telnet localhost 4258
OsmoHLR> enable
OsmoHLR# subscriber imsi 123456789023000 create
% Created subscriber 123456789023000
    ID: 1
    IMSI: 123456789023000
    MSISDN: none

OsmoHLR# subscriber imsi 123456789023000 update msisdn 423
% Updated subscriber IMSI='123456789023000' to MSISDN='423'

OsmoHLR# subscriber msisdn 423 update aud3g milenage k deaf0ff1ced0d0dabbedd1ced1cef00d opc ↩
     cededeffacedacefacedbadfadedbeef
OsmoHLR# subscriber msisdn 423 show
    ID: 1
    IMSI: 123456789023000
    MSISDN: 423
    3G auth: MILENAGE
             K=deaf0ff1ced0d0dabbedd1ced1cef00d
             OPC=cededeffacedacefacedbadfadedbeef
             IND-bitlen=5

OsmoHLR# subscriber msisdn 423 update aud2g comp128v3 ki beefedcafefaceacedaddeddecadefee
```

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

```
OsmoHLR# subscriber msisdn 423 show
    ID: 1
    IMSI: 123456789023000
    MSISDN: 423
    2G auth: COMP128v3
             KI=beefedcafefaceacedaddeddecadefee
    3G auth: MILENAGE
             K=deaf0ff1ced0d0dabbedd1ced1cef00d
             OPC=cededeffacedacefacedbadfadedbeef
             IND-bitlen=5

OsmoHLR# subscriber imsi 123456789023000 delete
% Deleted subscriber for IMSI '123456789023000'
```

6.2 Subscriber Parameters

The following parameters are managed for each subscriber of the HLR, modelled roughly after 3GPP TS 23.008, version 13.3.0; note that not all of these parameters are necessarily in active use.

The `aud3g` table also applies to 2G networks: it provides UMTS AKA tokens for Milenage authentication, which is available both on 3G and 2G networks. On 2G, when both MS and network are R99 capable (like OsmoMSC and OsmoSGSN are), the full UMTS AKA with Milenage keys from `aud_3g`, using AUTN and extended RES tokens, is available. With pre-R99 MS or network configurations, the GSM AKA compatible variant of Milenage, still using the Milenage keys from `aud_3g` but transceiving only RAND and SRES, may be applicable. (See 3GPP TS 33.102, chapter 6.8.1, Authentication and key agreement of UMTS subscribers.)

Table 2: OsmoHLR's subscriber parameters

Name	Example	Description
imsi	901700000014701	identity of the SIM/USIM, 3GPP TS 23.008 chapter 2.1.1.1
msisdn	2342123	number to dial to reach this subscriber (multiple MSISDNs can be stored per subscriber), 3GPP TS 23.008 chapter 2.1.2
imeisv	4234234234234275	identity of the mobile device and software version, 3GPP TS 23.008 chapter 2.2.3
aud2g.algo	comp128v3	Authentication algorithm ID for GSM AKA, corresponds to enum osmo_auth_algo
aud2g.ki		Subscriber's secret key (128bit)
aud3g.algo	milenage	Authentication algorithm ID for UMTS AKA (applies to both 3G and 2G networks), corresponds to enum osmo_auth_algo
aud3g.k	(32 hexadecimal digits)	Subscriber's secret key (128bit)
aud3g.op	(32 hexadecimal digits)	Operator's secret key (128bit)
aud3g.opc	(32 hexadecimal digits)	Secret key derived from OP and K (128bit), alternative to using OP which does not disclose OP to subscribers
aud3g.sqn	123	Sequence number of last used key (64bit unsigned)
aud3g.ind_bitlen	5	Nr of index bits at lower SQN end
apn		
vlr_number		3GPP TS 23.008 chapter 2.4.5
msc_number		3GPP TS 23.008 chapter 2.4.6
sgsn_number		3GPP TS 23.008 chapter 2.4.8.1
sgsn_address		3GPP TS 23.008 chapter 2.13.10
ggsn_number		3GPP TS 23.008 chapter 2.4.8.2
gmlc_number		3GPP TS 23.008 chapter 2.4.9.2
smsc_number		3GPP TS 23.008 chapter 2.4.23
periodic_lu_tmr		3GPP TS 23.008 chapter 2.4.24

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

Table 2: (continued)

Name	Example	Description
periodic_rau_tau_tmr		3GPP TS 23.008 chapter 2.13.115
nam_cs	1	Enable/disable voice access (3GPP TS 23.008 chapter 2.1.1.2: network access mode)
nam_ps	0	Enable/disable data access (3GPP TS 23.008 chapter 2.1.1.2: network access mode)
lmsi		3GPP TS 23.008 chapter 2.1.8
ms_purged_cs	0	3GPP TS 23.008 chapter 2.7.5
ms_purged_ps	1	3GPP TS 23.008 chapter 2.7.6

6.3 Configuring the Subscribers Create on Demand Feature

Usually a HLR will only allow mobile equipment (ME) on the network, if the HLR has a subscriber entry with the ME's IMSI. But OsmoHLR can also be configured to automatically create new entries for new IMSIs, with the `subscriber-create-on-demand` VTY option. The obvious use case is creating the new subscriber entry and then allowing the ME to use both the CS (Circuit Switched) and PS (Packet Switched) NAM (Network Access Mode).

osmo-hlr.cfg

```
hlr
 subscriber-create-on-demand 5 cs+ps
```

On the other hand, operators might only want to give network access to IMSIs, of which they know the owner. In order to do that, one can set the default NAM to `none` and manually approve new subscribers by changing the NAM (e.g. over the VTY, see the example below).

Oftentimes it is hard to know, which IMSI belongs to which ME, but the IMEI is readily available. If you configure your MSC to send IMEI checking requests to the HLR, before sending location update requests, the subscribers created on demand can also have the IMEI stored in the HLR database. With OsmoMSC, this is done by writing `check-imei-rqd early` in the `msc` section of osmo-msc.cfg. Then enable storing the IMEI when receiving check IMEI requests with `store-imei` in the OsmoHLR configuration.

osmo-msc.cfg

```
msc
 check-imei-rqd early
```

osmo-hlr.cfg

```
hlr
 subscriber-create-on-demand 5 none
 store-imei
```

Example: Enabling CS and PS NAM via VTY for a known IMEI

```
OsmoHLR> enable
OsmoHLR# subscriber imei 35761300444848 show
    ID: 1
    IMSI: 123456789023000
    MSISDN: 58192 ❶
    IMEI: 35761300444848
    CS disabled ❷
    PS disabled ❸
OsmoHLR# subscriber imei 35761300444848 update network-access-mode cs+ps
OsmoHLR# subscriber imei 35761300444848 show
    ID: 1
```

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

```
    IMSI: 123456789023000
    MSISDN: 58192
    IMEI: 35761300444848
```

❶ Randomly generated 5 digit MSISDN

❷, ❸ Disabled CS and PS NAM prevent the subscriber from accessing the network

6.4 Import Subscriber Data

6.4.1 Scripted Import

Warning
It is not generally a good idea to depend on the HLR database's internal table structure, but in the lack of an automated import procedure, this example is provided as an ad-hoc method to aid automated subscriber import. This is not guaranteed to remain valid.

Note
We may add CSV and other import methods to the `osmo-hlr-db-tool`, but so far that is not implemented. Contact the community if you are interested in such a feature being implemented.

Note
`sqlite3` is available from your distribution packages or `sqlite.org`.

Currently, probably the easiest way to automatically import subscribers to OsmoHLR is to write out a text file with SQL commands per subscriber, and feed that to `sqlite3`, as described below.

A difficulty is to always choose subscriber IDs that are not yet in use. For an initial import, the subscriber ID may be incremented per subscriber record. If adding more subscribers to an existing database, it is necessary to choose subscriber IDs that are not yet in use. Get the highest ID in use with:

```
sqlite3 hlr.db 'select max(id) from subscriber'
```

A full SQL example of adding a single subscriber with id 23, IMSI 001010123456789, MSISDN 1234, Ki for COMP128v1, and K and OPC for Milenage:

```
INSERT subscriber (id, imsi, msisdn) VALUES (23, '001010123456789', '1234');

INSERT INTO auc_2g (subscriber_id, algo_id_2g, ki)
VALUES(23, 1, '0123456789abcdef0123456789abcdef');

INSERT INTO auc_3g (subscriber_id, algo_id_3g, k, op, opc)
VALUES(23, 5, '0123456789abcdef0123456789abcdef',NULL,'0123456789abcdef0123456789abcdef');
```

Table entries to `auc_2g` and/or `auc_3g` may be omitted if no such key material is required.

UMTS Milenage auth (on both 2G and 3G RAN) is configured by the `auc_3g` table. `algo_id_3g` must currently always be 5 (MILENAGE).

The algorithm IDs for `algo_id_2g` and `algo_id_3g` are:

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

Table 3: Algorithm IDs in OsmoHLR's database

algo_id_2g / algo_id_3g	**Authentication Algorithm**
1	COMP128v1
2	COMP128v2
3	COMP128v3
4	XOR
5	MILENAGE

Create an empty HLR database with

```
osmo-hlr-db-tool -l hlr.db create
```

Repeat above SQL commands per subscriber, incrementing the subscriber ID for each block, then feed the SQL commands for the subscribers to be imported to the `sqlite3` command line tool:

```
sqlite3 hlr.db < subscribers.sql
```

6.4.2 Import OsmoNITB database

To upgrade from old OsmoNITB to OsmoHLR, use `osmo-hlr-db-tool`:

```
osmo-hlr-db-tool -l hlr.db import-nitb-db nitb.db
```

Be aware that the import is lossy, only the IMSI, MSISDN, nam_cs/ps and 2G auth data are set.

7 Unstructured Supplementary Services Data (USSD)

The *Unstructured Supplementary Services Data (USSD)* is one service within 2G/3G networks next to other services such as circuit-switched voice, packet-switched data and SMS (Short Message Service).

It is on an abstract level quite similar to SMS in that USSD can be used to send textual messages. However, there are the following differences:

- USSD is between the MS (phone) and an USSD application on the network, while SMS is primarily between two subscribers identified by their MSISDN
- USSD is faster, as it doesn't suffer from the complicated three-layer CP/RP/TP protocol stack of SMS with it's acknowledgement of the acknowledged acknowledgement.
- USSD is session-oriented, i.e. a dialogue/session between subscriber and application can persist for the transfer of more than one message. The dedicated radio channel on the RAN remains established throughout that dialogue.

7.1 USSD in Osmocom

Until August 2018, OsmoMSC contained some minimalistic internal USSD handling with no ability to attach/extend it with external USSD applications.

From August 2018 onwards, OsmoMSC doesn't contain any internal USSD handlers/applications anymore. Instead, all USSD is transported to/from OsmoHLR via the GSUP protocol.

OsmoHLR contains some intenal USSD handlers and can route USSD messages to any number of external USSD entities (EUSEs). The EUSE also use GSUP to communicate USSD from/to OsmoHLR.

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

Each EUSE is identified by its name. The name consists of a single-word string preceding a currently fixed ("-00-00-00-00-00-00") suffix. There is no authentication between EUSE and OsmoHLR: Any client program able to connect to the GSUP port of OsmoHLR can register as any EUSE (name).

NOTE
We plan to remove the requirement for this suffix as soon as we are done resolving all more important issues.

7.2 USSD Configuration

USSD configuration in OsmoHLR happens within the `hlr` VTY node.

`euse foobar-00-00-00-00-00-00` defines an EUSE with the given name `foobar`

`ussd route prefix *123 external foobar-00-00-00-00-00-00` installs a prefix route to the named EUSE. All USSD short codes starting with *123 will be routed to the named EUSE.

`ussd route prefix *#100# internal own-msisdn` installs a prefix route to the named internal USSD handler. The above command will restore the old behavior, in which *100 will return a text message containing the subscribers own phone number. More information on internal USSD handlers can be found in Section 7.3.

`ussd default-route external foobar-00-00-00-00-00-00` installs a default route to the named EUSE. This means that all USSD codes for which no more specific route exists will be routed to the named EUSE.

7.3 Built-in USSD handlers

OsmoHLR has an Internal USSD Entity (IUSE) that allows to handle some USSD requests internally. It features a set of simple handlers, which can be assigned to one or more USSD request prefixes:

- `own-msisdn` returns subscriber's MSISDN (if assigned);
- `own-imsi` returns subscriber's IMSI;
- `test-idle` keeps the session idle until the MS terminates it, or the guard timer expires (may be useful for testing).

Additional handlers can be added on request.

7.4 Example EUSE program

We have provided an example EUSE developed in C language using existing Osmocom libraries for GSUP protocol handling and USSD encoding/decoding. It will register as `foobar` EUSE to OsmoHLR on localhost. You can run it on a different machine by specifying e.g. `osmo-euse-demo 1.2.3.4 5678` to make it connect to OsmoHLR on IP address 1.2.3.4 and GSUP/TCP port 5678.

The idea is that you can use this as a template to develop your own USSD applications, or any gateways to other protocols or interfaces.

You can find it in `osmo-hlr/src/osmo-euse-demo.c` or online by following the link to http://git.osmocom.org/osmo-hlr/tree/src/osmo-euse-demo.c

This demonstration program will echo back any USSD message sent/routed to it, quoted like *You sent "..."*.

8 The Osmocom VTY Interface

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

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

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 4: VTY Parameter Patterns

Pattern	Example	Explanation
`A.B.C.D`	`127.0.0.1`	An IPv4 address
`A.B.C.D/M`	`192.168.1.0/24`	An IPv4 address and mask
`X:X::X:X`	`::1`	An IPv6 address
`X:X::X:X/M`	`::1/128`	An IPv6 address and mask
`TEXT`	`example01`	A single string without any spaces, tabs
`.TEXT`	`Some information`	A line of text
`(OptionA|OptionB|OptionC)`	`OptionA`	A choice between a list of available options
`<0-10>`	`5`	A number from a range

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

8.1 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.

8.2 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.

8.3 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.

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

8.3.1 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> ❶
  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
```

❶ 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 ❶
  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
```

❶ 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

8.3.2 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> s❶
show       sms        subscriber
```

❶ 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 ❶
version    online-help history    cs7        logging    alarms
talloc-context stats      asciidoc   rate-counters fsm        fsm-instances
sgs-connections subscriber bsc        connection transaction statistics
sms-queue smpp
```

❶ Type `<tab>` here.

8.3.3 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]
```

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

```
  logging set-log-mask MASK
  logging level (rll|cc|mm|rr|mncc|pag|msc|mgcp|ho|db|ref|ctrl|smpp|ranap|vlr|iucs|bssap| ↩
      sgs|lglobal|llapd|linp|lmux|lmi|lmib|lsms|lctrl|lgtp|lstats|lgsup|loap|lss7|lsccp|lsua ↩
      |lm3ua|lmgcp|ljibuf|lrspro) (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 asciidoc 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)  ↩
      SENDER_ID send .LINE
  subscriber (msisdn|extension|imsi|tmsi|id) ID silent-sms sender (msisdn|extension|imsi| ↩
      tmsi|id) SENDER_ID send .LINE
  subscriber (msisdn|extension|imsi|tmsi|id) ID silent-call start (any|tch/f|tch/any|sdcch)
  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
```

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

```
  exit
  end
  network country code <1-999>
  mobile network code <0-999>
  short name NAME
  long name NAME
  encryption a5 <0-3> [<0-3>] [<0-3>] [<0-3>]
  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
```

8.3.4 The attribute system

The VTY allows to edit the configuration at runtime. For many VTY commands the configuration change is immediately valid but for some commands a change becomes valid on a certain event only. In some cases it is even necessary to restart the whole process.

To give the user an overview, which configuration change applies when, the VTY implemets a system of attribute flags, which can be displayed using the `show` command with the parameter `vty-attributes`

Example: Typing show vty-attributes at the VTY prompt

```
OsmoBSC> show vty-attributes
  Global attributes:
    ^  This command is hidden (check expert mode)
    !  This command applies immediately
    @  This command applies on VTY node exit
  Library specific attributes:
    A  This command applies on ASP restart
    I  This command applies on IPA link establishment
    L  This command applies on E1 line update
  Application specific attributes:
    o  This command applies on A-bis OML link (re)establishment
    r  This command applies on A-bis RSL link (re)establishment
    l  This command applies for newly created lchans
```

The attributes are symbolized through a single ASCII letter (flag) and do exist in three levels. This is more or less due to the technical aspects of the VTY implementation. For the user, the level of an attribute has only informative purpose.

The global attributes, which can be found under the same attribute letter in every osmocom application, exist on the top level. The Library specific attributes below are used in various osmocom libraries. Like with the global attributes the attribute flag letter stays the same throughout every osmocom application here as well. On the third level one can find the application specific attributes. Those are unique to each osmocom application and the attribute letters may have different meanings in different osmocom applications. To make the user more aware of this, lowercase letters were used as attribute flags.

The `list` command with the parameter `with-flags` displays a list of available commands on the current VTY node, along with attribute columns on the left side. Those columns contain the attribute flag letters to indicate to the user how the command behaves in terms of how and when the configuration change takes effect.

Example: Typing list with-flags at the VTY prompt

```
OsmoBSC(config-net-bts)# list with-flags
  . ...  help
  . ...  list [with-flags]
  . ...  show vty-attributes
  . ...  show vty-attributes (application|library|global)
```

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

```
  . ...  write terminal
  . ...  write file [PATH]
  . ...  write memory
  . ...  write
  . ...  show running-config ❶
  . ...  exit
  . ...  end
  . o..  type (unknown|bs11|nanobts|rbs2000|nokia_site|sysmobts) ❷
  . ...  description .TEXT
  . ...  no description
  . o..  band BAND
  . .r.  cell_identity <0-65535> ❸
  . .r.  dtx uplink [force]
  . .r.  dtx downlink
  . .r.  no dtx uplink
  . .r.  no dtx downlink
  . .r.  location_area_code <0-65535>
  . o..  base_station_id_code <0-63>
  . o..  ipa unit-id <0-65534> <0-255>
  . o..  ipa rsl-ip A.B.C.D
  . o..  nokia_site skip-reset (0|1)
  ! ...  nokia_site no-local-rel-conf (0|1) ❹
  ! ...  nokia_site bts-reset-timer  <15-100> ❺
```

❶ This command has no attributes assigned.

❷ This command applies on A-bis OML link (re)establishment.

❸ This command applies on A-bis RSL link (re)establishment.

❹, ❺ This command applies immediately.

There are multiple columns because a single command may be associated with multiple attributes at the same time. To improve readability each flag letter gets a dedicated column. Empty spaces in the column are marked with a dot (".")

In some cases the listing will contain commands that are associated with no flags at all. Those commands either play an exceptional role (interactive commands outside "configure terminal", vty node navigation commands, commands to show / write the config file) or will require a full restart of the overall process to take effect.

8.3.5 The expert mode

Some VTY commands are considered relatively dangerous if used in production operation, so the general approach is to hide them. This means that they don't show up anywhere but the source code, but can still be executed. On the one hand, this approach reduces the risk of an accidental invocation and potential service degradation; on the other, it complicates intentional use of the hidden commands.

The VTY features so-called *expert* mode, that makes the hidden commands appear in the interactive help, as well as in the XML VTY reference, just like normal ones. This mode can be activated from the *VIEW* node by invoking the `enable` command with the parameter `expert-mode`. It remains active for the individual VTY session, and gets disabled automatically when the user switches back to the *VIEW* node or terminates the session.

A special attribute in the output of the `list with-flags` command indicates whether a given command is hidden in normal mode, or is a regular command:

Example: Hidden commands in the output of the list with-flags command

```
OsmoBSC> enable expert-mode ❶
OsmoBSC# list with-flags
  ...
  ^   bts <0-255> (activate-all-lchan|deactivate-all-lchan) ❷
  ^   bts <0-255> trx <0-255> (activate-all-lchan|deactivate-all-lchan) ❸
```

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

```
.   bts <0-255> trx <0-255> timeslot <0-7> sub-slot <0-7> mdcx A.B.C.D <0-65535> ❹
^   bts <0-255> trx <0-255> timeslot <0-7> sub-slot <0-7> (borken|unused) ❺
.   bts <0-255> trx <0-255> timeslot <0-7> sub-slot <0-7> handover <0-255> ❻
.   bts <0-255> trx <0-255> timeslot <0-7> sub-slot <0-7> assignment ❼
.   bts <0-255> smscb-command (normal|schedule|default) <1-4> HEXSTRING ❽
...
```

❶ This command enables the *expert* mode.

❷, ❸, ❺ This is a hidden command (only shown in the *expert* mode).

❹, ❻, ❼, ❽ This is a regular command that is always shown regardless of the mode.

9 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.

9.1 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 ?`

9.2 Log levels

For each of the log categories (see Section 9.1), 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*.

error
: 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.

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

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.

9.3 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 can not 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.

9.4 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`

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

9.5 Log targets

Each of the log targets represent certain destination for log messages. It can be configured independently by selecting levels (see Section 9.2) for categories (see Section 9.1) as well as filtering (see Section 9.4) and other options like `logging timestamp` for example.

9.5.1 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 9.1 for more details on categories and Section 9.2 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 9.4.

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`

9.5.2 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.

9.5.3 Logging via gsmtap

GSMTAP is normally a pseudo-header format that enables the IP-transport of GSM (or other telecom) protocols that are not normally transported over IP. For example, the most common situation is to enable GSMTAP in OsmoBTS or OsmoPCU to provide GSM-Um air interface capture files over IP, so they can be analyzed in wireshark.

GSMTAP logging is now a method how Osmocom software can also encapsulate its own log output in GSMTAP frames. We're not trying to re-invent rsyslog here, but this is very handy When debugging complex issues. It enables the reader of the pcap file

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

containing GSMTAP logging together with other protocol traces to reconstruct exact chain of events. A single pcap file can then contain both the log output of any number of Osmocom programs in the same timeline of the messages on various interfaces in and out of said Osmocom programs.

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.

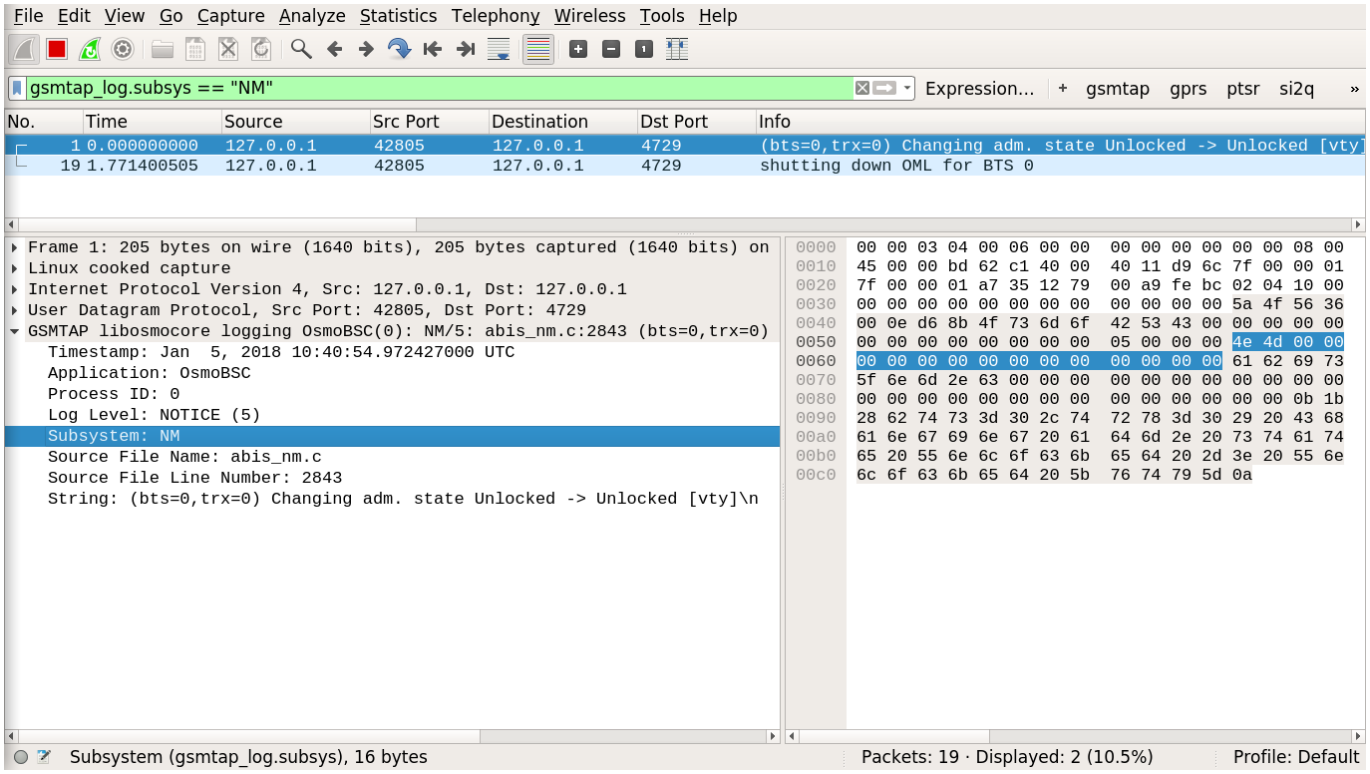


Figure 2: Wireshark with logs delivered over GSMTAP

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 descrease 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
```

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

Note
Every time you generate GSMTAP messages and send it to a unicast (non-broadcast/multicast) IP address, please make sure that the destination IP address actually has a socket open on the specified port, or drops the packets in its packet filter. If unicast GSMTAP messages arrive at a closed destination UDP port, the operating system will likely generate ICMP port unreachable messages. Those ICMP messages in turn will, when arriving at the source (the host on which you run the Osmocom software sending GSMTAP), suppress generation of further GSMTAP messages for some time, resulting in incomplete files. In case of doubt, either send GSMTAP to multicast IP addresses, or run something like `nc -l -u -p 4729 > /dev/null` on the destination host to open the socket at the GSMTAP port and discard anything arriving at it.

9.5.4 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:

```
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.

9.5.5 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:

```
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.

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

9.5.6 Logging to systemd-journal

systemd has been adopted by the majority of modern GNU/Linux distributions. Along with various daemons and utilities it provides systemd-journald [1] - a daemon responsible for event logging (syslog replacement). libosmocore based applications can log messages directly to systemd-journald.

The key difference from other logging targets is that systemd based logging allows to offload rendering of the meta information, such as location (file name, line number), subsystem, and logging level, to systemd-journald. Furthermore, systemd allows to attach arbitrary meta fields to the logging messages [2], which can be used for advanced log filtering.

[1] https://www.freedesktop.org/software/systemd/man/systemd-journald.service.html [2] https://www.freedesktop.org/software/-systemd/man/systemd.journal-fields.html

It was decided to introduce libsystemd as an optional dependency, so it needs to be enabled explicitly at configure/build time:

```
$ ./configure --enable-systemd-logging
```

Note
Recent libosmocore packages provided by Osmocom for Debian and CentOS are compiled **with** libsystemd (https://gerrit.osmocom.org/c/libosmocore/+/22651).

You can configure systemd based logging in two ways:

Example: systemd-journal target with offloaded rendering

```
log systemd-journal raw ❶
 logging filter all 1
 logging level set-all notice
```

❶ `raw` logging handler, rendering offloaded to systemd.

In this example, logging messages will be passed to systemd without any meta information (time, location, level, category) in the text itself, so all the printing parameters like `logging print file` will be ignored. Instead, the meta information is passed separately as *fields* which can be retrieved from the journal and rendered in any preferred way.

```
# Show Osmocom specific fields
$ journalctl --fields | grep OSMO

# Filter messages by logging subsystem at run-time
$ journalctl OSMO_SUBSYS=DMSC -f

# Render specific fields only
$ journalctl --output=verbose \
        --output-fields=SYSLOG_IDENTIFIER,OSMO_SUBSYS,CODE_FILE,CODE_LINE,MESSAGE
```

See `man 7 systemd.journal-fields` for a list of default fields, and `man 1 journalctl` for general information and available formatters.

Example: systemd-journal target with libosmocore based rendering

```
log systemd-journal ❶
 logging filter all 1
 logging print file basename
 logging print category-hex 0
 logging print category 1
 logging print level 1
 logging timestamp 0 ❷
 logging color 1 ❸
 logging level set-all notice
```

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

❶ Generic logging handler, rendering is done by libosmocore.

❷ Disable timestamping, systemd will timestamp every message anyway.

❸ Colored messages can be rendered with `journalctl --output=cat`.

In this example, logging messages will be pre-processed by libosmocore before being passed to systemd. No additional fields will be attached, except the logging level (`PRIORITY`). This mode is similar to *syslog* and *stderr*.

9.5.7 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:

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

10 Control interface

The actual protocol is described in Section 11, the variables common to all programs using it are described in Section 11.2. This section describes the CTRL interface variables specific to OsmoHLR.

Subscribers can be created and deleted using the following SET commands:

Table 5: Subscriber management commands available on OsmoHLR's Control interface

Command	Comment
subscriber.create *123456*	Create a new subscriber with IMSI "123456" to the database. Returns database ID of the subscriber being created.
subscriber.delete *123456*	Delete subscriber with IMSI "123456" from database. Returns database ID of the subscriber being deleted.

All subscriber variables are available by different selectors, which are freely interchangeable:

Table 6: Subscriber selectors available on OsmoHLR's Control interface

Selector	Comment
subscriber.**by-imsi-***123456*.*	Subscriber selector by IMSI, replace "123456" with the actual IMSI
subscriber.**by-msisdn-***123456*.*	Subscriber selector by MSISDN
subscriber.**by-id-***123456*.*	Subscriber selector by database ID

Each of the above selectors feature all of these control variables:

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

Table 7: Subscriber variables available on OsmoHLR's Control interface

Name	Access	Trap	Value	Comment
subscriber.by-*.**info**	R	No		List (short) subscriber information
subscriber.by-*.**info-aud**	R	No		List subscriber authentication tokens
subscriber.by-*.**info-all**	R	No		List both *info* and *info-aud* in one
subscriber.by-*.**cs-enabled**	RW	No	*1* or *0*	Enable/disable circuit-switched access
subscriber.by-*.**ps-enabled**	RW	No	*1* or *0*	Enable/disable packet-switched access
subscriber.by-*.**msisdn**	RW	No	valid MSISDN string	Get/Set assigned MSISDN
subscriber.by-*.**aud2g**	RW	No	*algo[,KI]*	Get/Set 2g Authentication Data
subscriber.by-*.**aud2g**	RW	No	'algo[,KI,("opc"),OP_C[,ind_bitlen]]'	

10.1 subscriber.by-*.info, info-aud, info-all

Query the HLR database and return current subscriber record, in multiple lines of the format

```
name<tab>value
```

To keep the reply as short as possible, some values are omitted if they are empty. These are the returned values and their presence modalities; for their meaning, see Section 6.2:

Table 8: Returned values by OsmoHLR's *info*, *info-all* and *info-aud* commands

Returned by *info-all* and	Name	Format	Presence
info	id	-9223372036854775808 .. 9223372036854775807 (usually not negative)	always
info	imsi	6 to 15 decimal digits	always
info	msisdn	1 to 15 decimal digits	when non-empty
info	nam_cs	*1* if CS is enabled, or *0*	always
info	nam_ps	*1* if PS is enabled, or *0*	always
info	vlr_number	up to 15 decimal digits	when non-empty
info	sgsn_number	up to 15 decimal digits	when non-empty
info	sgsn_address		when non-empty
info	ms_purged_cs	*1* if CS is purged, or *0*	always
info	ms_purged_ps	*1* if PS is purged, or *0*	always
info	periodic_lu_timer	0..4294967295	always
info	periodic_rau_tau_timer	0..4294967295	always
info	lmsi	8 hex digits	always
info-aud	aud2g.algo	one of *comp128v1*, *comp128v2*, *comp128v3* or *xor*	when valid 2G auth data is set
info-aud	aud2g.ki	32 hexadecimal digits	when valid 2G auth data is set
info-aud	aud3g.algo	so far always *milenage*	when valid 3G auth data is set
info-aud	aud3g.k	32 hexadecimal digits	when valid 3G auth data is set
info-aud	aud3g.op	32 hexadecimal digits	when valid 3G auth data is set, **not** when OPC is set
info-aud	aud3g.opc	32 hexadecimal digits	when valid 3G auth data is set, **not** when OP is set
info-aud	aud3g.ind_bitlen	0..28	when valid 3G auth data is set

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

Table 8: (continued)

Returned by *info-all* and	**Name**	**Format**	**Presence**
info-aud	aud3g.sqn	0 .. 18446744073709551615	when valid 3G auth data is set

This is an example Control Interface transcript that illustrates the various *info* commands:

```
GET 1 subscriber.by-imsi-901990000000003.info
GET_REPLY 1 subscriber.by-imsi-901990000000003.info
id      3
imsi    901990000000003
msisdn  103
nam_cs  1
nam_ps  1
ms_purged_cs    0
ms_purged_ps    0
periodic_lu_timer       0
periodic_rau_tau_timer  0
lmsi    00000000

GET 2 subscriber.by-msisdn-103.info-aud
GET_REPLY 2 subscriber.by-msisdn-103.info-aud
aud2g.algo      COMP128v1
aud2g.ki        000102030405060708090a0b0c0d0e0f
aud3g.algo      MILENAGE
aud3g.k 000102030405060708090a0b0c0d0e0f
aud3g.opc       101112131415161718191a1b1c1d1e1f
aud3g.ind_bitlen        5
aud3g.sqn       0

GET 3 subscriber.by-id-3.info-all
GET_REPLY 3 subscriber.by-id-3.info-all
id      3
imsi    901990000000003
msisdn  103
nam_cs  1
nam_ps  1
ms_purged_cs    0
ms_purged_ps    0
periodic_lu_timer       0
periodic_rau_tau_timer  0
lmsi    00000000
aud2g.algo      COMP128v1
aud2g.ki        000102030405060708090a0b0c0d0e0f
aud3g.algo      MILENAGE
aud3g.k 000102030405060708090a0b0c0d0e0f
aud3g.opc       101112131415161718191a1b1c1d1e1f
aud3g.ind_bitlen        5
aud3g.sqn       0
```

10.2 subscriber.by-*.ps-enabled, cs-enabled

Disable or enable packet-/circuit-switched access for the given IMSI;

- *ps-enabled* switches access to GPRS or UMTS data services,

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

- *cs-enabled* switches access to voice services.

When disabled, the next time this subscriber attempts to do a Location Updating GSUP operation for the given domain (i.e. from the SGSN for *ps-enabled*, from the MSC/VLR for *cs-enabled*), it will be rejected by OsmoHLR. Currently connected GSUP clients will be notified via GSUP when a subscriber is being disabled, so that the subscriber can be dropped in case it is currently attached.

The current *ps-enabled/cs-enabled* status can be queried by *GET* commands, and also by looking at *nam_ps* and *nam_cs* in a *subscriber.by-*.info* response.

A value of "1" indicates that the given domain is enabled, which is the default; a value of "0" disables access.

This is an example transcript that illustrates *ps-enabled* and *cs-enabled* commands:

```
GET 1 subscriber.by-msisdn-103.info
GET_REPLY 1 subscriber.by-msisdn-103.info
id      3
imsi    901990000000003
msisdn  103
nam_cs  1
nam_ps  1
ms_purged_cs    0
ms_purged_ps    0
periodic_lu_timer       0
periodic_rau_tau_timer  0
lmsi    00000000

GET 2 subscriber.by-msisdn-103.ps-enabled
GET_REPLY 2 subscriber.by-msisdn-103.ps-enabled 1

SET 3 subscriber.by-msisdn-103.ps-enabled 0
SET_REPLY 3 subscriber.by-msisdn-103.ps-enabled OK

GET 4 subscriber.by-msisdn-103.ps-enabled
GET_REPLY 4 subscriber.by-msisdn-103.ps-enabled 0

GET 5 subscriber.by-msisdn-103.info
GET_REPLY 5 subscriber.by-msisdn-103.info
id      3
imsi    901990000000003
msisdn  103
nam_cs  1
nam_ps  0
ms_purged_cs    0
ms_purged_ps    0
periodic_lu_timer       0
periodic_rau_tau_timer  0
lmsi    00000000

SET 6 subscriber.by-msisdn-103.cs-enabled 0
SET_REPLY 6 subscriber.by-msisdn-103.cs-enabled OK

GET 7 subscriber.by-msisdn-103.cs-enabled
GET_REPLY 7 subscriber.by-msisdn-103.cs-enabled 0

GET 8 subscriber.by-msisdn-103.info
GET_REPLY 8 subscriber.by-msisdn-103.info
id      3
imsi    901990000000003
msisdn  103
nam_cs  0
nam_ps  0
ms_purged_cs    0
```

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

```
ms_purged_ps    0
periodic_lu_timer       0
periodic_rau_tau_timer  0
lmsi    00000000

SET 9 subscriber.by-msisdn-103.cs-enabled 1
SET_REPLY 9 subscriber.by-msisdn-103.cs-enabled OK
SET 10 subscriber.by-msisdn-103.ps-enabled 1
SET_REPLY 10 subscriber.by-msisdn-103.ps-enabled OK

GET 11 subscriber.by-msisdn-103.info
GET_REPLY 11 subscriber.by-msisdn-103.info
id      3
imsi    901990000000003
msisdn  103
nam_cs  1
nam_ps  1
ms_purged_cs    0
ms_purged_ps    0
periodic_lu_timer       0
periodic_rau_tau_timer  0
lmsi    00000000
```

10.3 subscriber.by-*.msisdn

Get or set the MSISDN currently assigned to a subscriber.

This is an example transcript that illustrates use of this command:

```
GET 1 subscriber.by-imsi-901991234567891.msisdn
GET_REPLY 1 subscriber.by-imsi-901991234567891.msisdn none

SET 2 subscriber.by-imsi-901991234567891.msisdn 555666
SET_REPLY 2 subscriber.by-imsi-901991234567891.msisdn OK

GET 3 subscriber.by-imsi-901991234567891.msisdn
GET_REPLY 3 subscriber.by-imsi-901991234567891.msisdn 555666
```

10.4 subscriber.by-*.aud2g

Get or set the 2G Authentication data of a subscriber.

The information is stored/retrieved as a comma separated list of fields:

```
algo[,KI]
```

Where

- **KI** is the KI as a hexadecimal string.
- **algo** is one of the following algorithms: *none, xor, comp128v1, comp128v2, comp128v3*.

All values are case insensitive.

This is an example transcript that illustrates use of this command:

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

```
GET 1 subscriber.by-imsi-901991234567891.aud2g
GET_REPLY 1 subscriber.by-imsi-901991234567891.aud2g none

SET 2 subscriber.by-imsi-901991234567891.aud2g xor,c01ffedc1cadaeac1d1f1edacac1ab0a
SET_REPLY 2 subscriber.by-imsi-901991234567891.aud2g OK

GET 3 subscriber.by-imsi-901991234567891.aud2g
GET_REPLY 3 subscriber.by-imsi-901991234567891.aud2g XOR,c01ffedc1cadaeac1d1f1edacac1ab0a

SET 4 subscriber.by-imsi-901991234567891.aud2g none
SET_REPLY 4 subscriber.by-imsi-901991234567891.aud2g OK

GET 5 subscriber.by-imsi-901991234567891.aud2g
GET_REPLY 5 subscriber.by-imsi-901991234567891.aud2g none
```

10.5 subscriber.by-*.aud3g

Get or set the 3G Authentication data of a subscriber.

The information is stored/retrieved as a comma separated list of fields:

```
algo[,KI,("op"|"opc"),OP_C[,ind_bitlen]]
```

Where: * **KI** is the KI as a hexadecimal string. * **algo** is one of the following algorithms: *none, xor, milenage*. * "op" or "opc" indicates whether next field is an OP or OPC value. * **OP_C** contains an OP or OPC values as hexadecimal string, based on what the previous field specifies. * **ind_bitlen** is set to 5 by default if not provided.

All values are case insensitive.

This is an example transcript that illustrates use of this command:

```
GET 117 subscriber.by-imsi-901991234567891.aud3g
GET_REPLY 117 subscriber.by-imsi-901991234567891.aud3g none

SET 118 subscriber.by-imsi-901991234567891.aud3g milenage,c01ffedc1cadaeac1d1f1edacac1ab0a, ↩
    OP,FB2A3D1B360F599ABAB99DB8669F8308
SET_REPLY 118 subscriber.by-imsi-901991234567891.aud3g OK

GET 119 subscriber.by-imsi-901991234567891.aud3g
GET_REPLY 119 subscriber.by-imsi-901991234567891.aud3g MILENAGE, ↩
    c01ffedc1cadaeac1d1f1edacac1ab0a,OP,fb2a3d1b360f599abab99db8669f8308,5

SET 120 subscriber.by-imsi-901991234567891.aud3g milenage,c01ffedc1cadaeac1d1f1edacac1ab0a, ↩
    OPC,FB2A3D1B360F599ABAB99DB8669F8308,7
SET_REPLY 120 subscriber.by-imsi-901991234567891.aud3g OK

GET 121 subscriber.by-imsi-901991234567891.aud3g
GET_REPLY 121 subscriber.by-imsi-901991234567891.aud3g MILENAGE, ↩
    c01ffedc1cadaeac1d1f1edacac1ab0a,OPC,fb2a3d1b360f599abab99db8669f8308,7

SET 122 subscriber.by-imsi-901991234567891.aud3g none
SET_REPLY 122 subscriber.by-imsi-901991234567891.aud3g OK

GET 123 subscriber.by-imsi-901991234567891.aud3g
GET_REPLY 123 subscriber.by-imsi-901991234567891.aud3g none
```

11 Osmocom Control Interface

The VTY interface as described in Section 8 is aimed at human interaction with the respective Osmocom program.

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

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.

11.1 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).

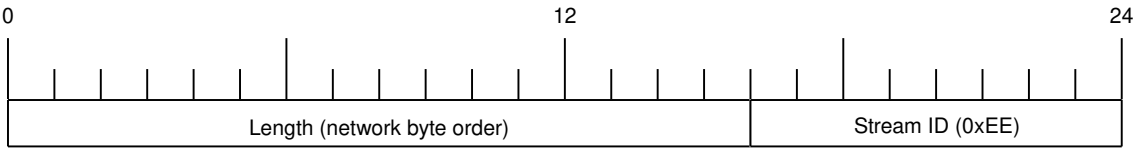


Figure 3: IPA header for control protocol

Inside the IPA header is a single byte of extension header with protocol ID 0x00 which indicates the control interface.

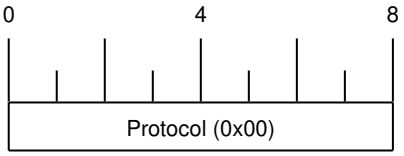


Figure 4: IPA extension header for control protocol

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.

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

11.1.1 GET operation

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

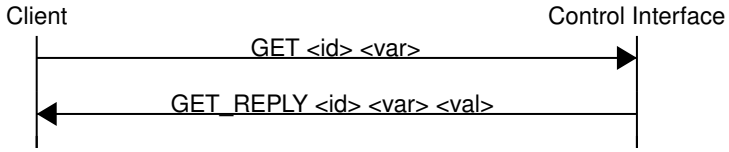


Figure 5: Control Interface GET operation (successful outcome)

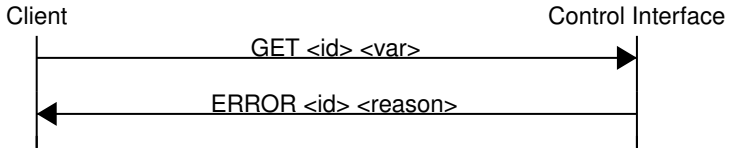


Figure 6: Control Interface GET operation (unsuccessful outcome)

11.1.2 SET operation

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

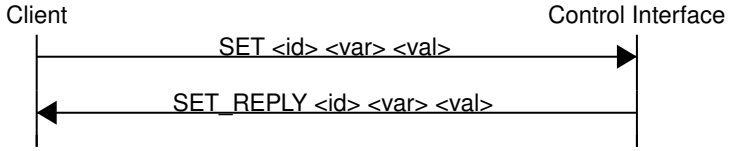


Figure 7: Control Interface SET operation (successful outcome)

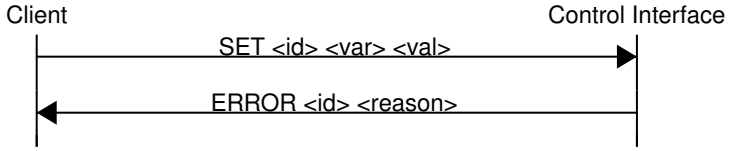


Figure 8: Control Interface SET operation (unsuccessful outcome)

11.1.3 TRAP operation

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

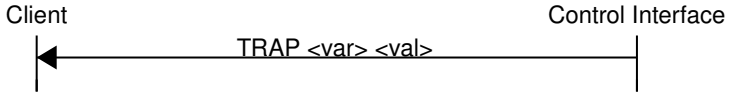


Figure 9: Control Interface TRAP operation

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

11.2 Common variables

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

Table 9: Variables available over control interface

Name	Access	Value	Comment
counter.*	RO		Get counter value.
rate_ctr.*	RO		Get list of rate counter groups.
rate_ctr.IN.GN.GI.name	RO		Get value for interval IN of rate counter name which belong to group named GN with index GI.

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 "`rate_ctr.*`" 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.

11.3 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 Section 11.2 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.

11.3.1 Getting rate counters

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

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

```
$ ./scripts/osmo_rate_ctr2csv.py --header
Connecting to localhost:4249...
Getting rate counter groups info...
"group","counter","absolute","second","minute","hour","day"
"e1inp.0","hdlc:abort","0","0","0","0","0"
"e1inp.0","hdlc:bad_fcs","0","0","0","0","0"
"e1inp.0","hdlc:overrun","0","0","0","0","0"
"e1inp.0","alarm","0","0","0","0","0"
"e1inp.0","removed","0","0","0","0","0"
"bsc.0","chreq:total","0","0","0","0","0"
"bsc.0","chreq:no_channel","0","0","0","0","0"
...
"msc.0","call:active","0","0","0","0","0"
"msc.0","call:complete","0","0","0","0","0"
"msc.0","call:incomplete","0","0","0","0","0"
Completed: 44 counters from 3 groups received.
```

11.3.2 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
```

11.3.3 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
```

11.3.4 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
❶
```

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

12 Distributed GSM / Multicast MS Lookup

Distributed GSM (D-GSM) allows independent mobile core network stacks to provide voice, SMS and Roaming services to each other, without the need for centralised entities or administration authority, and in a way that is resilient against unstable network links between sites.

D-GSM aims at communal networks, where several independent sites, let's call them villages, each have a full mobile core network infrastructure. It elegantly provides ad-hoc service for subscribers moving across villages, and allows villages to dynamically join or leave the cooperative network without the need for configuration changes at other sites.

A challenge for linking separate sites is to find the current location of a subscriber. Typically, in mobile networks, a centralized entity keeps track of where to Page for subscribers. Running several fully independent sites with unreliable links between them makes it hard to provide such centralisation.

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

D-GSM finds subscribers by mslookup, a service provided by OsmoHLR, typically using multicast DNS queries. This allows routing Location Updating requests, calls, and SMS to the right site without administrative delay nor the need for a reliable link to a central database.

D-GSM is highly resilient against single sites or links becoming temporarily unavailable. Service between still reachable sites simply continues; Service to a disconnected site resumes as soon as it becomes reachable again.

This brings an entirely new paradigm to mobile core network infrastructure: as sites become reachable on the IP network and join the common IP multicast group, services between them become available immediately. Basically, the only premise is that IP routing and multicast works across sites, and that each site uses unique IPA names in the GSUP config.

This chapter describes how D-GSM and mslookup work, and how to configure sites to use D-GSM, using Osmocom core network infrastructure.

12.1 Finding Subscribers: mslookup Clients

There are two fundamentally distinct subscriber lookups provided by the mslookup service.

12.1.1 Find the Current Location of an MSISDN

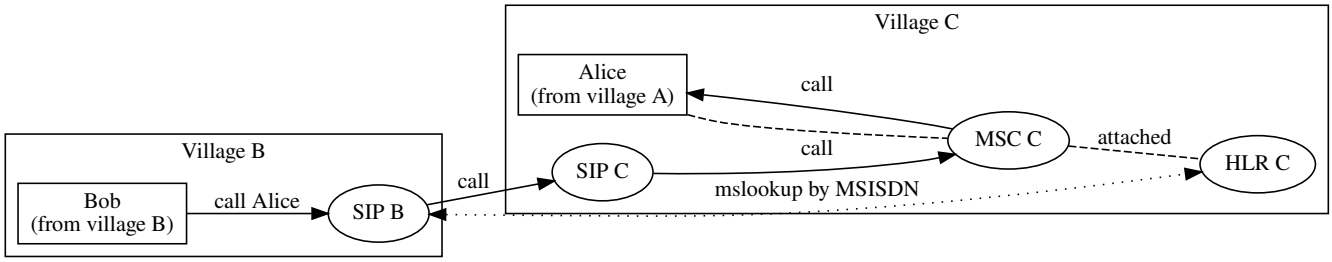


Figure 10: mslookup for connecting subscribers: Alice is visiting village C; a phone call gets routed directly to her current location independently from her resident village infrastructure

For example, if a subscriber is currently visiting another village, establish a phone call / send SMS towards that village.

- To deliver a phone call, a SIP agent integrates an mslookup client to request the SIP service of an MSISDN's current location (example: Section 12.4.3.1). It receives an IP address and port to send the SIP Invite to.
- To deliver an SMS, an ESME integrates an mslookup client to request the SMPP service of an MSISDN's current location (example: Section 12.4.4.1).

The current location of a subscriber may change at any time, and, when moving across locations, a subscriber may suddenly lose reception to the previous location without explicitly detaching. Hence an mslookup request for the current location of an MSISDN may get numerous responses. To find the currently valid location, mslookup includes the age of the subscriber record, i.e. how long ago the subscriber was last reached. The one response with the youngest age reflects the current location.

In order to evaluate several responses, mslookup always waits for a fixed amount of time (1 second), and then evaluates the available responses.

Services are not limited to SIP and SMPP, arbitrarily named services can be added to the mslookup configuration.

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

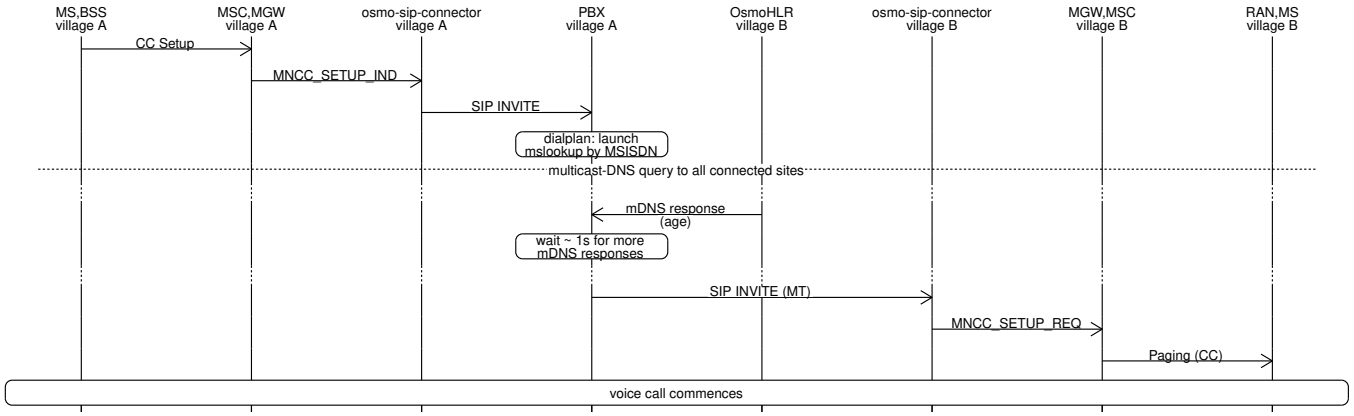


Figure 11: Message sequence for locating an MSISDN to deliver a voice call

12.1.2 Find the Home HLR for an IMSI

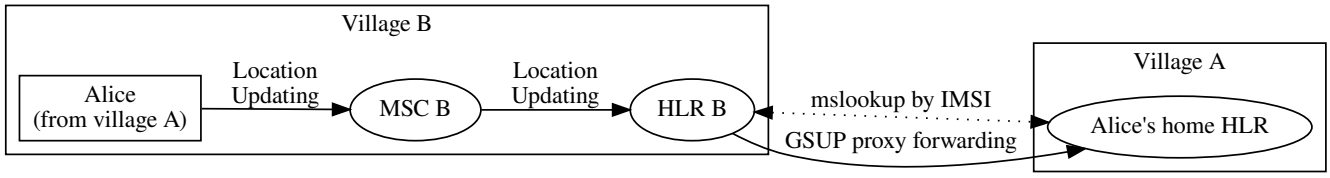


Figure 12: mslookup for Roaming: Alice visits village B; she can attach to the local mobile network, which proxies HLR administration to her home village.

For example, when attaching to a local network, a local resident gets serviced directly by the local village's HLR, while a visitor from another village gets serviced by the remote village's HLR (Roaming).

A home HLR typically stays the same for a given IMSI. If the home site is reachable, there should be exactly one response to an mslookup request asking for it. The age of such a home-HLR response is always sent as zero.

If a response's age is zero, mslookup does not wait for further responses and immediately uses the result.

If there were more than one HLR accepting service for an IMSI, the one with the shortest response latency is used.

12.2 mslookup Configuration

OsmoHLR the main mslookup agent. It provides the responses for both current location services as well as for locating the fixed home-HLR. But naturally, depending on the mslookup request's purpose, different OsmoHLR instances will respond for a given subscriber.

- When querying the home HLR, it is always the (typically single) home HLR instance that sends the mslookup response. As soon as it finds the queried IMSI in the local HLR database, an OsmoHLR will respond to home-HLR requests. In Figure 12, Alice's home HLR responds to the Roaming request ("where is the home HLR?").
- When querying the location of an MSISDN, it is always the HLR proxy nearest to the servicing MSC that sends the mslookup response. Even though the home HLR keeps the Location Updating record also for Roaming cases, it will only respond to an mslookup service request if the subscriber has attached at a directly connected MSC. If attached at a remote MSC, that MSC's remote HLR will be the GSUP proxy for the home HLR, and the remote HLR is responsible for responding to service requests. In Figure 12, HLR B is the nearest proxy and will answer all service requests ("where is this MSISDN?"). Alice's home HLR will not answer service requests, because it detects that the servicing MSC is connected via another HLR proxy.

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

12.2.1 Example

Here is an osmo-hlr.cfg mslookup configuration example for one site, which is explained in subsequent chapters.

```
hlr
 gsup
  bind ip 10.9.8.7
  ipa-name hlr-23
mslookup
 mdns bind
 server
  service sip.voice at 10.9.8.7 5060
  service smpp.sms at 10.9.8.7 2775
```

OsmoHLR has both an mslookup server and a client.

- The server responds to incoming service and home-HLR requests, when the local HLR is responsible.
- The client is used as GSUP proxy to a remote home HLR (found by mslookup upon a locally unknown IMSI).
- The client may also be used for forwarding SMS-over-GSUP.

The mslookup service can be implemented by various methods. At the time of writing, the only method implemented is mDNS.

12.2.2 mDNS

The stock mslookup method is mDNS, multicast DNS. It consists of standard DNS encoding according to [ietf-rfc1035] and [ietf-rfc3596], but sent and received on IP multicast. In the response, standard A and AAAA records return the service's IP address, while additional TXT records provide the service's port number and the MS attach age.

Tip

To watch D-GSM mDNS conversations in wireshark, select "udp.port == 4266" (the default mslookup mDNS port number), right click on the packet to "Decode as...", and select "DNS".

In OsmoHLR, the mDNS server and client are typically both enabled at the same time:

```
mslookup
 mdns bind
```

Server and client can also be enabled/disabled individually:

```
mslookup
 server
  mdns bind
 client
  mdns bind
```

These examples use the default mslookup multicast IP address and port. It is possible to configure custom IP address and port, but beware that the IP address must be from a multicast range, see [ietf-rfc5771]:

```
mslookup
 mdns bind 239.192.23.42 4266
```

Domain names generated from mslookup queries (e.g. "sip.voice.123.msisdn") should not collide with IANA permitted domains. Therefore we add the "mdns.osmocom.org" suffix. It can be overridden as follows:

```
mslookup
 mdns domain-suffix mdns.osmocom.org
```

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

12.2.3 Server: Site Services

The mslookup server requires a list of service addresses provided at the local site, in order to respond to service requests matching locally attached subscribers.

```
mslookup
 server
  service sip.voice at 10.9.8.7 5060
  service smpp.sms at 10.9.8.7 2775
```

In this example:

- "10.9.8.7 5060" are the IP address and port on which the local site's osmo-sip-connector is bound to receive SIP Invite requests.
- "10.9.8.7 2775" are the local site's OsmoMSC SMPP bind address and port.

Obviously, these IP addresses must be routable back to this site from all other sites. Using link-local or "ANY" addresses, like 127.0.0.1 or 0.0.0.0, will not work here. Instead, each service config requires a public IP address that all remote requestors are able to reach (not necessarily on the host that osmo-hlr is running on).

If a site has more than one MSC, services can also be configured for each MSC individually, keyed by the IPA unit name that each MSC sends on the GSUP link:

```
mslookup
 server
  msc ipa-name msc-262-42-0
   service sip.voice at 10.11.12.13 5060
   service smpp.sms at 10.11.12.13 2775
  msc ipa-name msc-901-70-0
   service sip.voice at 10.9.8.7 5060
   service smpp.sms at 10.9.8.7 2775
```

Here, "msc-262-42-0" is the IPA name of a local OsmoMSC instance. To configure an OsmoMSC's IPA name on the GSUP link, see osmo-msc.cfg, setting `hlr` / `ipa-name`.

For mslookup service responses, only Location Updatings in the Circuit Switched domain are relevant. OsmoHLR does manage IMSIs attaching in the Packet Switched domain (via an SGSN) similarly to Circuit Switched (via an MSC), but mslookup completely ignores the Packet Switched attach status.

12.2.4 Server: Own GSUP Address

When responding to home-HLR requests, OsmoHLR implicitly by default responds with its locally configured GSUP bind address (setting `hlr` / `gsup` / `bind ip`). If required, an explicit local GSUP address and port can be configured, for example:

```
hlr
 gsup
  bind ip 0.0.0.0
  ipa-name hlr-23
mslookup
 server
  # osmo-hlr's own GSUP address to send in mslookup responses:
  service gsup.hlr at 10.9.8.7 4222
```

The gsup.hlr service can only be configured globally (because requests come from arbitrary mDNS clients, before a Location Updating has associated the IMSI with the requesting MSC).

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

12.2.5 Client IPA Naming

For reliable GSUP proxy routing to a remote HLR (Roaming), it is important that each GSUP client, i.e. each HLR, MSC and SGSN instance, has a unique IPA name.

Example for configuring an OsmoHLR instance's IPA name:

```
hlr
 gsup
  ipa-name hlr-23
```

Here, "hlr-23" is the unique identification of this OsmoHLR instance across all potentially connected D-GSM sites.

Furthermore, each MSC and SGSN must have a uniquely distinct IPA name across all sites (here "msc-262-42-0" and "msc-901-70-0" are used as example IPA names for local MSCs).

When this OsmoHLR connects to a remote HLR, be it for GSUP proxying or SMS-over-GSUP, it communicates its own IPA name (on GSUP link-up) as well as the IPA name of the requesting client MSC/SGSN (as Source Name in each message) to the remote OsmoHLR GSUP server. These names are used to route GSUP responses back to the respective requesting peer.

If two MSCs were accidentally configured with identical names, a problem will occur as soon as both MSCs attempt to attach to the same OsmoHLR (either directly or via GSUP proxying). The MSC that shows up first will work normally, but any duplicate that shows up later will be rejected, since a route for its name already exists.

12.3 Queries

In URL notation, typical mslookup queries look like:

```
gsup.hlr.123456789.imsi
sip.voice.123.msisdn
smpp.sms.123.msisdn
```

A query consists of

- a service name ("gsup.hlr"),
- an id ("123456789"),
- the id type ("imsi").

The calling client also defines a timeout to wait for responses.

The mslookup ID types are fixed, while service names can be chosen arbitrarily.

Table 10: mslookup ID types, no other ID types are understood by mslookup

ID Type	Description
imsi	An IMSI as existing in an OsmoHLR subscriber database
msisdn	A phone number as configured in an OsmoHLR subscriber database

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

Table 11: mslookup service name conventions, arbitrary service names can be added as required

Service Name	Protocol	Description
gsup.hlr	GSUP	Home HLR's GSUP server, to handle Location Updating related procedures
sip.voice	SIP	OsmoSIPConnector, to receive a SIP Invite (MT side of a call)
smpp.sms	SMPP	Destination OsmoMSC (or other SMPP server) to deliver an SMS to the recipient
gsup.sms	GSUP	GSUP peer to deliver an SMS to the recipient using SMS-over-GSUP

Arbitrarily named services can be added to the mslookup configuration and queried by mslookup clients; as soon as a service name is present in osmo-hlr.cfg, it can be queried from any mslookup client.

Service names should consist of a protocol name (like "sip", "gsup", "english") and an intended action/entity (like "voice", "hlr", "greeting").

12.4 Service Client Implementation

In principle, arbitrary services could query target addresses via mslookup, leaving it up to any and all kinds of clients to find their respective destination addresses. But of course, mslookup was designed with specific services in mind, namely:

- SIP call agents and
- SMS delivery (an ESME or SMSC)

The following chapters describe examples of setting up a working distributed core network providing SIP voice calls and SMS forwarding across sites.

12.4.1 mslookup Library

The OsmoHLR provides an mslookup client C library, libosmo-mslookup. Service lookups can be integrated directly in client programs using this library. However, its mDNS implementation requires the libosmocore select() loop, which can be challenging to integrate in practice. An alternative solution is the osmo-mslookup-client tool.

12.4.2 osmo-mslookup-client

The mslookup C library is available, but often, a simpler approach for client implementations is desirable:

- When querying for a service address, the client is typically interested in the single final best result (youngest age / first responding home HLR).
- Voice call and SMS clients typically would block until an mslookup result is known. For example, the FreeSwitch dialplan integration expects a result synchronously, i.e. without waiting for mslookup responses via a select() loop.
- Integrating the libosmocore select() loop required for mDNS can break the already existing socket handling in the client program.

The osmo-mslookup-client cmdline tool provides a trivial way to synchronously acquire the single result for an mslookup request. The service client can invoke an osmo-mslookup-client process per request and read the result from stdout.

Each invocation obviously spawns a separate process and opens a multicast socket for mDNS. For better scalability, osmo-mslookup-client can also be run as a daemon, providing results via a unix domain socket. Using synchronous write() and recv() allows blocking until a result is received without interfering with the client program's select() setup.

By itself, osmo-mslookup-client is also helpful as a diagnostic tool:

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

```
$ osmo-mslookup-client sip.voice.1001.msisdn
sip.voice.1001.msisdn   ok      10.9.8.7        5060

$ osmo-mslookup-client gsup.hlr.901700000014701.imsi
gsup.hlr.901700000014701.imsi   ok      10.9.8.7        4222

$ osmo-mslookup-client gsup.hlr.111111.imsi
gsup.hlr.111111.imsi    not-found

$ osmo-mslookup-client gsup.hlr.1001.msisdn sip.voice.1001.msisdn smpp.sms.1001.msisdn foo ↩
    .1001.msisdn
gsup.hlr.1001.msisdn    ok      10.9.8.7        4222
foo.1001.msisdn not-found
smpp.sms.1001.msisdn    ok      10.9.8.7        2775
sip.voice.1001.msisdn   ok      10.9.8.7        5060

$ osmo-mslookup-client --csv-headers gsup.hlr.901700000014701.imsi
QUERY   RESULT  V4_IP   V4_PORT V6_IP   V6_PORT
gsup.hlr.901700000014701.imsi   ok      10.9.8.7        4222

$ osmo-mslookup-client -f json gsup.hlr.901700000014701.imsi
{"query": "gsup.hlr.901700000014701.imsi", "result": "ok", "v4": ["10.9.8.7", "4222"]}
```

For full help including example client invocations in Python, see the output of:

```
osmo-mslookup-client -h
```

12.4.3 SIP Service Client

12.4.3.1 FreeSwitch dialplan.py

The FreeSWITCH PBX software [freeswitch_pbx] offers a Python integration to determine a SIP call recipient by a custom dialplan implementation. An example dialplan implementation for FreeSWITCH that uses D-GSM mslookup is provided in the osmo-hlr source tree under `contrib`, called `freeswitch_dialplan_dgsm.py`.

To integrate it with your FREESWITCH setup, add a new `extension` block to your `dialplan/public.xml`:

```
    <extension name="outbound">
      <condition field="destination_number" expression=".*">
        <action application="set" data="hangup_after_bridge=true"/>
        <action application="set" data="session_in_hangup_hook=true"/>
        <action application="set" data="ringback=%(2000, 4000, 440.0, 480.0)"/>
        <action application="python" data="freeswitch_dialplan_dgsm"/>
      </condition>
    </extension>
```

Make sure that the dir containing `freeswitch_dialplan_dgsm.py` is in your `PYTHONPATH` environment variable, and start the server:

```
$ export PYTHONPATH="$PYTHONPATH:/home/user/code/osmo-hlr/contrib/dgsm"
$ freeswitch -nf -nonat -nonatmap -nocal -nort -c
```

12.4.4 SMS Service Client

12.4.4.1 SMS via SMPP Port

An example ESME using D-GSM mslookup, `esme_dgsm.py`, is provided in the osmo-hlr source tree under `contrib`. It attaches to OsmoMSC's SMPP port to send SMS to recipients determined by mslookup.

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

OsmoMSC should be configured as "smpp-first", so that all SMS routing is determined by mslookup. If configured without smpp-first, OsmoMSC may try to deliver an SMS locally, even though the recipient has recently moved to a different site.

An example OsmoMSC configuration to work with esme_dgsm.py:

```
smpp
 local-tcp-ip 127.0.0.1 2775
 system-id test-msc
 policy closed
 smpp-first
 # outgoing to esme_dgsm.py
 esme OSMPP
  no alert-notifications
  password foo
  default-route
 # incoming from esme_dgsm.py
 esme ISMPP
  no alert-notifications
  password foo
```

Launch esme_dgsm.py alongside OsmoMSC:

```
./esme_dgsm.py --src-host 127.0.0.1
```

esme_dgsm.py will be notified via SMPP for each SMS to be delivered, and will forward them either to a remote recipient, or back to the same OsmoMSC, depending on the mslookup result. If the MSISDN is not reachable (or esme_dgsm.py can't handle the message for other reasons), it returns the RSYSERR code back to OsmoMSC.

Note that the esme_dgsm.py is a proof of concept and should not be used in production. It has several limitations, such as not supporting multipart SMS messages.

12.4.4.2 SMS-Over-GSUP

The GSUP protocol defines SMS delivery messages. When OsmoMSC is configured to deliver SMS via GSUP, MO SMS are directly forwarded to the HLR, which will determine where to forward the SMS-over-GSUP messages using its mslookup client.

FIXME implement this

13 Generic Subscriber Update Protocol

13.1 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.

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

13.2 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.

13.3 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*.

13.4 Procedures

13.4.1 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)

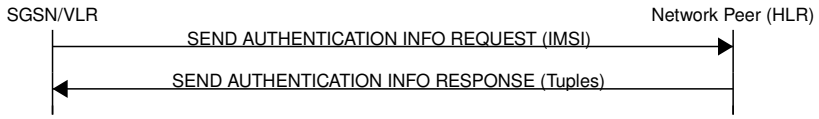


Figure 13: Send Authentication Info (Normal Case)

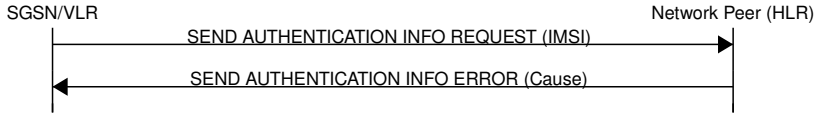


Figure 14: Send Authentication Info (Erroneous Case)

13.4.2 Reporting of Authentication Failure

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

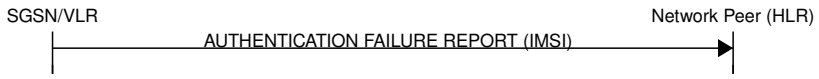


Figure 15: Authentication Failure Report (Normal Case)

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

13.4.3 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)

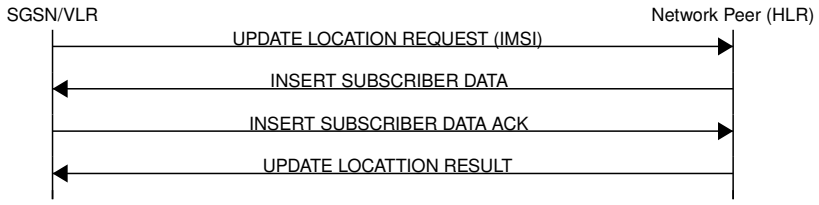


Figure 16: Update Location (Normal Case)

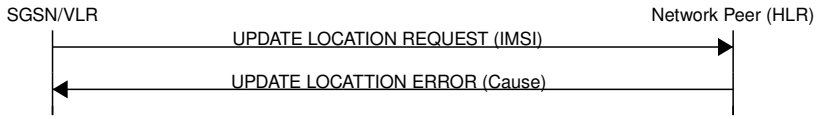


Figure 17: Update Location (Error Case)

13.4.4 Location Cancellation

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

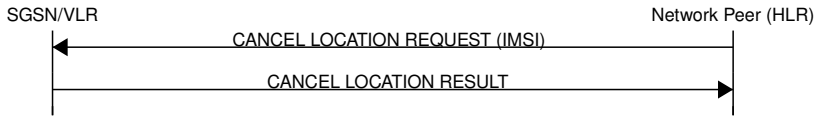


Figure 18: Cancel Location (Normal Case)

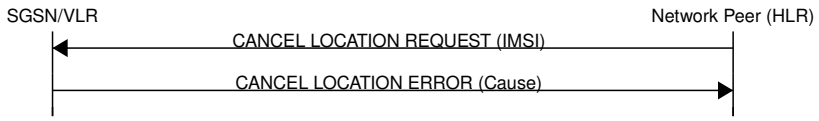


Figure 19: Cancel Location (Error Case)

13.4.5 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.

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

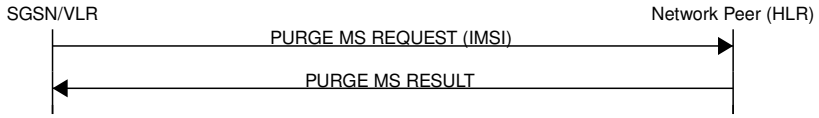


Figure 20: Purge MS (Normal Case)

13.4.6 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.

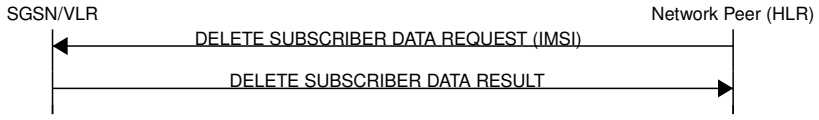


Figure 21: Delete Subscriber Data (Normal Case)

13.4.7 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.

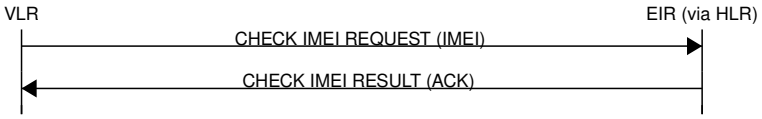


Figure 22: Check IMEI (Normal Case)

13.5 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.

13.5.1 E Handover

MSC-A has an active RAN connection and hands it over to MSC-B.

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

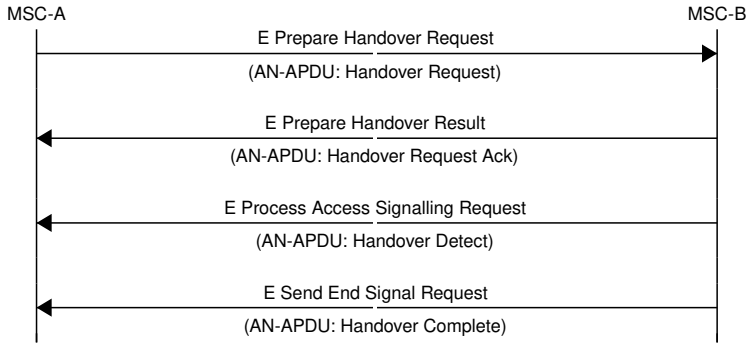


Figure 23: E Handover (Normal Case)

13.5.2 E Subsequent Handover

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

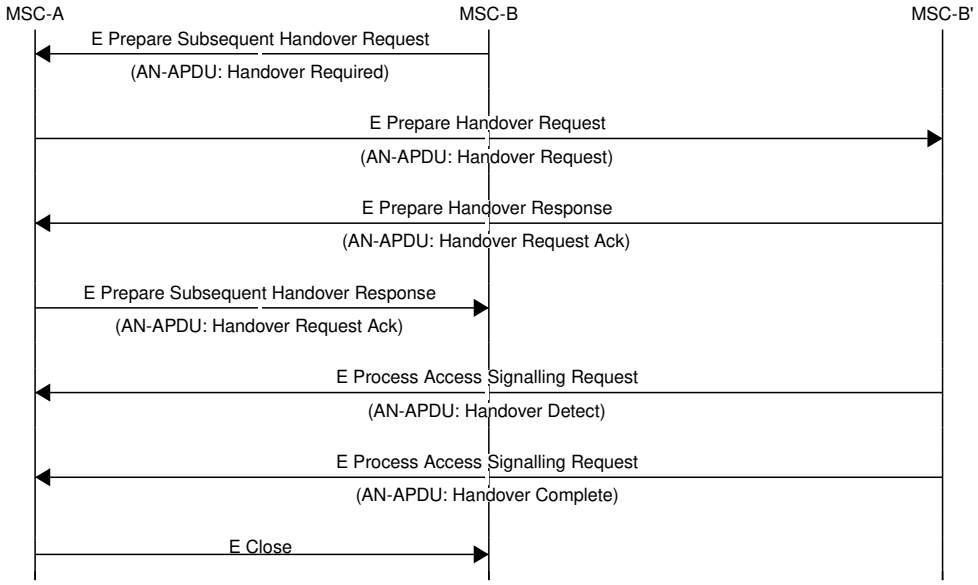


Figure 24: E Subsequent Handover (Normal Case)

13.5.3 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.

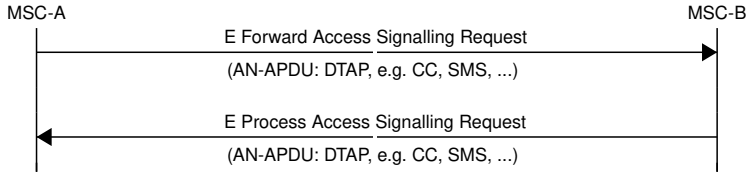


Figure 25: E Process and Forward Access Signalling (Normal Case)

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

13.5.4 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 13.7.31), 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.

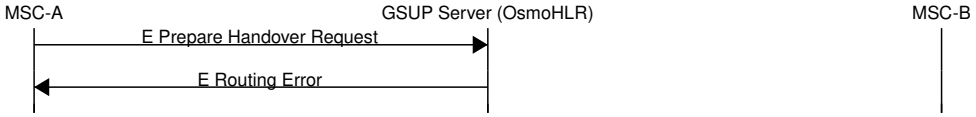


Figure 26: E Routing Error example

13.6 Message Format

13.6.1 General

Every message is based on the following message format

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.7.1	M	V	1
01	IMSI	Section 13.7.19	M	TLV	2-10

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).

13.6.2 Send Authentication Info Request

Direction: SGSN / VLR ⇒ HLR

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.7.1	M	V	1
01	IMSI	Section 13.7.19	M	TLV	2-10
28	CN Domain	Section 13.7.15	O	TLV	3
26	AUTS	Section 13.7.13	C	TLV	18
20	RAND	Section 13.7.7	C	TLV	18
05	PDP info	Section 13.7.3	C	TLV	2-N
2a	Current RAT Type	Section 13.7.36	O	TLV	3

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.

The conditional *PDP Info* IE is only present in the CEAI interface used by the ePDG. It should contain the *PDP Context ID*, *PDP Address* (dynamic addressing) and *Access Point Name* IEs.

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

13.6.3 Send Authentication Info Error

Direction: HLR ⇒ SGSN / VLR

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.7.1	M	V	1
01	IMSI	Section 13.7.19	M	TLV	2-10
02	Cause	Section 13.7.26	M	TLV	3

13.6.4 Send Authentication Info Response

Direction: HLR ⇒ SGSN / VLR

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.7.1	M	V	1
01	IMSI	Section 13.7.19	M	TLV	2-10
03	Auth Tuple	Section 13.7.6	0-5	TLV	36

13.6.5 Authentication Failure Report

Direction: SGSN / VLR ⇒ HLR

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.7.1	M	V	1
01	IMSI	Section 13.7.19	M	TLV	2-10
28	CN Domain	Section 13.7.15	O	TLV	3

13.6.6 Update Location Request

Direction: SGSN / VLR ⇒ HLR

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.7.1	M	V	1
01	IMSI	Section 13.7.19	M	TLV	2-10
28	CN Domain	Section 13.7.15	O	TLV	3

13.6.7 Update Location Error

Direction: HLR ⇒ SGSN / VLR

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.7.1	M	V	1
01	IMSI	Section 13.7.19	M	TLV	2-10
02	Cause	Section 13.7.26	M	TLV	3

13.6.8 Update Location Result

Direction: HLR ⇒ SGSN / VLR

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.7.1	M	V	1
01	IMSI	Section 13.7.19	M	TLV	2-10
08	MSISDN	Section 13.7.20	O	TLV	0-9

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

IEI	IE	Type	Presence	Format	Length
09	HLR Number	Section 13.7.25	O	TLV	0-9
04	PDP info complete	Section 13.7.18	O	TLV	2
05	PDP info	Section 13.7.3	O	TLV	2-N

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

13.6.9 Location Cancellation Request

Direction: HLR ⇒ SGSN / VLR

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.7.1	M	V	1
01	IMSI	Section 13.7.19	M	TLV	2-10
28	CN Domain	Section 13.7.15	O	TLV	3
06	Cancellation type	Section 13.7.16	O	TLV	3

13.6.10 Location Cancellation Error

Direction: SGSN / VLR ⇒ HLR

TODO

13.6.11 Location Cancellation Result

Direction: SGSN / VLR ⇒ HLR

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.7.1	M	V	1
01	IMSI	Section 13.7.19	M	TLV	2-10
28	CN Domain	Section 13.7.15	O	TLV	3

13.6.12 Purge MS Request

Direction: SGSN / VLR ⇒ HLR

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.7.1	M	V	1
01	IMSI	Section 13.7.19	M	TLV	2-10
28	CN Domain	Section 13.7.15	O	TLV	3
09	HLR Number	Section 13.7.25	M	TLV	0-9

13.6.13 Purge MS Error

Direction: HLR ⇒ SGSN / VLR

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.7.1	M	V	1
01	IMSI	Section 13.7.19	M	TLV	2-10
02	Cause	Section 13.7.26	M	TLV	3

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

13.6.14 Purge MS Result

Direction: HLR ⇒ SGSN / VLR

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.7.1	M	V	1
01	IMSI	Section 13.7.19	M	TLV	2-10
07	Freeze P-TMSI	Section 13.7.18	M	TLV	2

13.6.15 Insert Subscriber Data Request

Direction: HLR ⇒ SGSN / VLR

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.7.1	M	V	1
01	IMSI	Section 13.7.19	M	TLV	2-10
28	CN Domain	Section 13.7.15	O	TLV	3
08	MSISDN	Section 13.7.20	O	TLV	0-9
09	HLR Number	Section 13.7.25	O	TLV	0-9
04	PDP info complete	Section 13.7.18	M	TLV	2
05	PDP info	Section 13.7.3	C	TLV	0-10
14	PDP-Charging Characteristics	Section 13.7.23	O	TLV	4

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

13.6.16 Insert Subscriber Data Error

Direction: SGSN / VLR ⇒ HLR

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.7.1	M	V	1
01	IMSI	Section 13.7.19	M	TLV	2-10
02	Cause	Section 13.7.26	M	TLV	3

13.6.17 Insert Subscriber Data Result

Direction: SGSN / VLR ⇒ HLR

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.7.1	M	V	1
01	IMSI	Section 13.7.19	M	TLV	2-10

13.6.18 Delete Subscriber Data Request

Direction: HLR ⇒ SGSN / VLR

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.7.1	M	V	1
01	IMSI	Section 13.7.19	M	TLV	2-10
28	CN Domain	Section 13.7.15	O	TLV	3
10	PDP Context ID	Section 13.7.5	C	TLV	3

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

13.6.19 Delete Subscriber Data Error

Direction: SGSN / VLR ⇒ HLR

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.7.1	M	V	1
01	IMSI	Section 13.7.19	M	TLV	2-10
02	Cause	Section 13.7.26	M	TLV	3

13.6.20 Delete Subscriber Data Result

Direction: HLR ⇒ SGSN / VLR

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.7.1	M	V	1
01	IMSI	Section 13.7.19	M	TLV	2-10

13.6.21 Process Supplementary Service Request

Direction: bidirectional

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.7.1	M	V	1
01	IMSI	Section 13.7.19	M	TLV	2-10
30	Session ID	Section 13.8.1	M	TLV	6
31	Session State	Section 13.8.2	M	TLV	3
35	Supplementary Service Info	Section 13.7.27	O	TLV	2-...

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

13.6.22 Process Supplementary Service Error

Direction: EUSE / HLR ⇒ MSC

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.7.1	M	V	1
01	IMSI	Section 13.7.19	M	TLV	2-10
30	Session ID	Section 13.8.1	M	TLV	6
31	Session State	Section 13.8.2	M	TLV	3
02	Cause	Section 13.7.26	M	TLV	3

13.6.23 Process Supplementary Service Response

Direction: EUSE / HLR ⇒ MSC

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.7.1	M	V	1
01	IMSI	Section 13.7.19	M	TLV	2-10
30	Session ID	Section 13.8.1	M	TLV	6
31	Session State	Section 13.8.2	M	TLV	3

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

IEI	IE	Type	Presence	Format	Length
35	Supplementary Service Info	Section 13.7.27	O	TLV	2-...

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.

13.6.24 MO-forwardSM Request

Direction: MSC / SGSN ⇒ SMSC (via HLR)

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.7.1	M	V	1
01	IMSI	Section 13.7.19	M	TLV	2-10
40	SM-RP-MR (Message Reference)	Section 13.8.3	M	TLV	1
41	SM-RP-DA (Destination Address)	Section 13.8.4	M	TLV	2-...
42	SM-RP-OA (Originating Address)	Section 13.8.5	M	TLV	2-...
43	SM-RP-UI (SM TPDU)	Section 13.8.7	M	TLV	1-...

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.

13.6.25 MO-forwardSM Error

Direction: SMSC (via HLR) ⇒ MSC / SGSN

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.7.1	M	V	1
01	IMSI	Section 13.7.19	M	TLV	2-10
40	SM-RP-MR (Message Reference)	Section 13.8.3	M	TLV	1
44	SM-RP-Cause (Cause value)	Section 13.8.8	M	TLV	1
43	SM-RP-UI (diagnostic field)	Section 13.8.7	O	TLV	1-...

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.

13.6.26 MO-forwardSM Result

Direction: SMSC (via HLR) ⇒ MSC / SGSN

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.7.1	M	V	1
01	IMSI	Section 13.7.19	M	TLV	2-10
40	SM-RP-MR (Message Reference)	Section 13.8.3	M	TLV	1

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.

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

13.6.27 MT-forwardSM Request

Direction: SMSC (via HLR) ⇒ MSC / SGSN

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.7.1	M	V	1
01	IMSI	Section 13.7.19	M	TLV	2-10
40	SM-RP-MR (Message Reference)	Section 13.8.3	M	TLV	1
41	SM-RP-DA (Destination Address)	Section 13.8.4	M	TLV	2-...
42	SM-RP-OA (Originating Address)	Section 13.8.5	M	TLV	2-...
43	SM-RP-UI (SM TPDU)	Section 13.8.7	M	TLV	1-...
45	SM-RP-MMS (More Messages to Send)	Section 13.8.9	O	TLV	1

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.

13.6.28 MT-forwardSM Error

Direction: MSC / SGSN ⇒ SMSC (via HLR)

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.7.1	M	V	1
01	IMSI	Section 13.7.19	M	TLV	2-10
40	SM-RP-MR (Message Reference)	Section 13.8.3	M	TLV	1
44	SM-RP-Cause (Cause value)	Section 13.8.8	M	TLV	1
43	SM-RP-UI (diagnostic field)	Section 13.8.7	O	TLV	1-...

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.

13.6.29 MT-forwardSM Result

Direction: MSC / SGSN ⇒ SMSC (via HLR)

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.7.1	M	V	1
01	IMSI	Section 13.7.19	M	TLV	2-10
40	SM-RP-MR (Message Reference)	Section 13.8.3	M	TLV	1

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.

13.6.30 READY-FOR-SM Request

Direction: MSC / SGSN ⇒ SMSC (via HLR)

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.7.1	M	V	1
01	IMSI	Section 13.7.19	M	TLV	2-10
40	SM-RP-MR (Message Reference)	Section 13.8.3	M	TLV	1
46	SM Alert Reason	Section 13.8.10	M	TLV	1-...

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.

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

13.6.31 READY-FOR-SM Error

Direction: SMSC (via HLR) ⇒ MSC / SGSN

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.7.1	M	V	1
01	IMSI	Section 13.7.19	M	TLV	2-10
40	SM-RP-MR (Message Reference)	Section 13.8.3	M	TLV	1
44	SM-RP-Cause (Cause value)	Section 13.8.8	M	TLV	1
43	SM-RP-UI (diagnostic field)	Section 13.8.7	O	TLV	1-...

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.

13.6.32 READY-FOR-SM Result

Direction: SMSC (via HLR) ⇒ MSC / SGSN

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.7.1	M	V	1
01	IMSI	Section 13.7.19	M	TLV	2-10
40	SM-RP-MR (Message Reference)	Section 13.8.3	M	TLV	1

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.

13.6.33 CHECK-IMEI Request

Direction: VLR ⇒ EIR (via HLR)

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.7.1	M	V	1
01	IMSI	Section 13.7.19	M	TLV	2-10
50	IMEI	Section 13.7.28	M	TLV	11

13.6.34 CHECK-IMEI Error

Direction: EIR (via HLR) ⇒ VLR

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.7.1	M	V	1
01	IMSI	Section 13.7.19	M	TLV	2-10
02	Cause	Section 13.7.26	M	TLV	3

13.6.35 CHECK-IMEI Result

Direction: EIR (via HLR) ⇒ VLR

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.7.1	M	V	1
01	IMSI	Section 13.7.19	M	TLV	2-10
51	IMEI Check Result	Section 13.7.29	M	TLV	3

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

13.6.36 E Prepare Handover Request

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

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.7.1	M	V	1
01	IMSI	Section 13.7.19	M	TLV	2-10
0a	Message Class	Section 13.7.30	M	TLV	3
60	Source Name	Section 13.7.31	M	TLV	2-...
61	Destination Name	Section 13.7.32	M	TLV	2-...
62	AN-APDU	Section 13.7.33	M	TLV	2-...

13.6.37 E Prepare Handover Error

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

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.7.1	M	V	1
01	IMSI	Section 13.7.19	M	TLV	2-10
0a	Message Class	Section 13.7.30	M	TLV	3
60	Source Name	Section 13.7.31	M	TLV	2-...
61	Destination Name	Section 13.7.32	M	TLV	2-...
62	AN-APDU	Section 13.7.33	M	TLV	2-...

13.6.38 E Prepare Handover Result

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

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.7.1	M	V	1
01	IMSI	Section 13.7.19	M	TLV	2-10
0a	Message Class	Section 13.7.30	M	TLV	3
60	Source Name	Section 13.7.31	M	TLV	2-...
61	Destination Name	Section 13.7.32	M	TLV	2-...
62	AN-APDU	Section 13.7.33	M	TLV	2-...

13.6.39 E Prepare Subsequent Handover Request

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

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.7.1	M	V	1
01	IMSI	Section 13.7.19	M	TLV	2-10
0a	Message Class	Section 13.7.30	M	TLV	3
60	Source Name	Section 13.7.31	M	TLV	2-...
61	Destination Name	Section 13.7.32	M	TLV	2-...
62	AN-APDU	Section 13.7.33	M	TLV	2-...

13.6.40 E Prepare Subsequent Handover Error

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

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

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.7.1	M	V	1
01	IMSI	Section 13.7.19	M	TLV	2-10
0a	Message Class	Section 13.7.30	M	TLV	3
60	Source Name	Section 13.7.31	M	TLV	2-...
61	Destination Name	Section 13.7.32	M	TLV	2-...
62	AN-APDU	Section 13.7.33	M	TLV	2-...

13.6.41 E Prepare Subsequent Handover Result

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

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.7.1	M	V	1
01	IMSI	Section 13.7.19	M	TLV	2-10
0a	Message Class	Section 13.7.30	M	TLV	3
60	Source Name	Section 13.7.31	M	TLV	2-...
61	Destination Name	Section 13.7.32	M	TLV	2-...
62	AN-APDU	Section 13.7.33	M	TLV	2-...

13.6.42 E Send End Signal Request

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

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.7.1	M	V	1
01	IMSI	Section 13.7.19	M	TLV	2-10
0a	Message Class	Section 13.7.30	M	TLV	3
60	Source Name	Section 13.7.31	M	TLV	2-...
61	Destination Name	Section 13.7.32	M	TLV	2-...
62	AN-APDU	Section 13.7.33	M	TLV	2-...

13.6.43 E Send End Signal Error

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

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.7.1	M	V	1
01	IMSI	Section 13.7.19	M	TLV	2-10
0a	Message Class	Section 13.7.30	M	TLV	3
60	Source Name	Section 13.7.31	M	TLV	2-...
61	Destination Name	Section 13.7.32	M	TLV	2-...
62	AN-APDU	Section 13.7.33	M	TLV	2-...

13.6.44 E Send End Signal Result

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

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.7.1	M	V	1
01	IMSI	Section 13.7.19	M	TLV	2-10
0a	Message Class	Section 13.7.30	M	TLV	3
60	Source Name	Section 13.7.31	M	TLV	2-...

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

IEI	IE	Type	Presence	Format	Length
61	Destination Name	Section 13.7.32	M	TLV	2-...
62	AN-APDU	Section 13.7.33	M	TLV	2-...

13.6.45 E Process Access Signalling Request

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

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.7.1	M	V	1
01	IMSI	Section 13.7.19	M	TLV	2-10
0a	Message Class	Section 13.7.30	M	TLV	3
60	Source Name	Section 13.7.31	M	TLV	2-...
61	Destination Name	Section 13.7.32	M	TLV	2-...
62	AN-APDU	Section 13.7.33	M	TLV	2-...

13.6.46 E Forward Access Signalling Request

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

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.7.1	M	V	1
01	IMSI	Section 13.7.19	M	TLV	2-10
0a	Message Class	Section 13.7.30	M	TLV	3
60	Source Name	Section 13.7.31	M	TLV	2-...
61	Destination Name	Section 13.7.32	M	TLV	2-...
62	AN-APDU	Section 13.7.33	M	TLV	2-...

13.6.47 E Close

Direction: MSC-A ⇒ MSC-B (via HLR)

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.7.1	M	V	1
01	IMSI	Section 13.7.19	M	TLV	2-10
0a	Message Class	Section 13.7.30	M	TLV	3
60	Source Name	Section 13.7.31	M	TLV	2-...
61	Destination Name	Section 13.7.32	M	TLV	2-...

13.6.48 E Abort

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

13.6.49 E Routing Error

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

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.7.1	M	V	1
01	IMSI	Section 13.7.19	M	TLV	2-10
0a	Message Class	Section 13.7.30	M	TLV	3
60	Source Name	Section 13.7.31	M	TLV	2-...

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

IEI	IE	Type	Presence	Format	Length
61	Destination Name	Section 13.7.32	M	TLV	2-...
30	Session ID	Section 13.8.1	O	TLV	6
31	Session State	Section 13.8.2	O	TLV	3

13.6.50 ePDG Tunnel Request

Direction: GSUP Client (strongswan) ⇒ GSUP Server (ePDG)

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.7.1	M	V	1
01	IMSI	Section 13.7.19	M	TLV	2-10
0a	Message Class	Section 13.7.30	M	TLV	3
15	PCO	Section 13.7.24	O	TLV	1-...
28	CN Domain	Section 13.7.15	O	TLV	3
60	Source Name	Section 13.7.31	O	TLV	2-...

13.6.51 ePDG Tunnel Error

Direction: GSUP Server (ePDG) ⇒ GSUP Client (strongswan)

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.7.1	M	V	1
01	IMSI	Section 13.7.19	M	TLV	2-10
0a	Message Class	Section 13.7.30	M	TLV	3
02	Cause	Section 13.7.26	M	TLV	3

13.6.52 ePDG Tunnel Result

Direction: GSUP Server (ePDG) ⇒ GSUP Client (strongswan)

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.7.1	M	V	1
01	IMSI	Section 13.7.19	M	TLV	2-10
0a	Message Class	Section 13.7.30	M	TLV	3
04	PDP info complete	Section 13.7.18	M	TLV	2
05	PDP info	Section 13.7.3	M	TLV	2-N
15	PCO	Section 13.7.24	O	TLV	1-...
28	CN Domain	Section 13.7.15	O	TLV	3
60	Source Name	Section 13.7.31	O	TLV	2-...

13.7 Information Elements

13.7.1 Message Type

Type	Name
Description	0x04
Update Location Request	Section 13.6.6
0x05	Update Location Error
Section 13.6.7	0x06

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

Type	Name
Update Location Result	Section 13.6.8
0x08	Send Authentication Info Request
Section 13.6.2	0x09
Send Authentication Info Error	Section 13.6.3
0x0a	Send Authentication Info Result
Section 13.6.4	0x0b
Authentication Failure Report	Section 13.6.5
0x0c	Purge MS Request
[?]	0x0d
Purge MS Error	Section 13.6.13
0x0e	Purge MS Result
Section 13.6.14	0x10
Insert Subscriber Data Request	Section 13.6.15
0x11	Insert Subscriber Data Error
Section 13.6.16	0x12
Insert Subscriber Data Result	Section 13.6.17
0x14	Delete Subscriber Data Request
Section 13.6.18	0x15
Delete Subscriber Data Error	Section 13.6.19
0x16	Delete Subscriber Data Result
Section 13.6.20	0x1c
Location Cancellation Request	Section 13.6.9
0x1d	Location Cancellation Error
Section 13.6.10	0x1e
Location Cancellation Result	Section 13.6.11
0x20	Supplementary Service Request
Section 13.6.21	0x21
Supplementary Service Error	Section 13.6.22
0x22	Supplementary Service Result
Section 13.6.23	0x24
MO-forwardSM Request	Section 13.6.24
0x25	MO-forwardSM Error
Section 13.6.25	0x26

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

Type	Name
MO-forwardSM Result	Section 13.6.26
0x28	MT-forwardSM Request
Section 13.6.27	0x29
MT-forwardSM Error	Section 13.6.28
0x2a	MT-forwardSM Result
Section 13.6.29	0x2c
READY-FOR-SM Request	Section 13.6.30
0x2d	READY-FOR-SM Error
Section 13.6.31	0x2e
READY-FOR-SM Result	Section 13.6.32
0x30	CHECK-IMEI Request
Section 13.6.33	0x31
CHECK-IMEI Error	Section 13.6.34
0x32	CHECK-IMEI Result
Section 13.6.35	0x34
E Prepare Handover Request	Section 13.6.36
0x35	E Prepare Handover Error
Section 13.6.37	0x36
E Prepare Handover Result	Section 13.6.38
0x38	E Prepare Subsequent Handover Request
Section 13.6.39	0x39
E Prepare Subsequent Handover Error	Section 13.6.40
0x3a	E Prepare Subsequent Handover Result
Section 13.6.41	0x3c
E Send End Signal Request	Section 13.6.42
0x3d	E Send End Signal Error
Section 13.6.43	0x3e
E Send End Signal Result	Section 13.6.44
0x40	E Process Access Signalling Request
Section 13.6.45	0x44
E Forward Access Signalling Request	Section 13.6.46
0x47	E Close
Section 13.6.47	0x4B

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

Type	Name
E Abort	Section 13.6.48
0x4E	E Routing Error
Section 13.6.49	0x50
ePDG Tunnel Request	Section 13.6.50
0x51	ePDG Tunnel Error
Section 13.6.51	0x52
ePDG Tunnel Result	Section 13.6.52

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.

Ending Bits	Message Category
00	Request
01	Error
10	Result
11	Other

13.7.2 IP Address

The value part is encoded like in the Packet data protocol address IE defined in 3GPP TS 24.008, Chapter 10.5.6.4. PDP type organization must be set to *IETF allocated address*.

13.7.3 PDP Info

This is a container for information elements describing a single PDP.

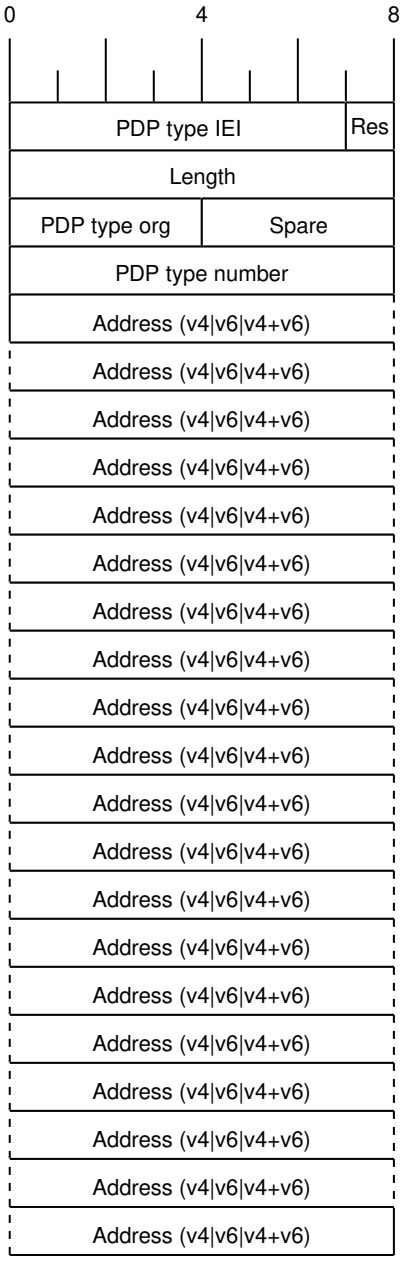
IEI	IE	Type	Presence	Format	Length
	PDP Info IEI	Section 13.7.17	M	V	1
	Length of PDP Info IE		M	V	1
10	PDP Context ID	Section 13.7.5	C	TLV	3
11	PDP Address	Section 13.7.4	C	TLV	4-24
12	Access Point Name	Section 13.7.21	C	TLV	3-102
13	Quality of Service	Section 13.7.22	O	TLV	1-20
14	PDP-Charging Characteristics	Section 13.7.23	O	TLV	4

The conditional IE are mandantory unless mentioned otherwise.

13.7.4 PDP Address

The value part is encoded like in the Packet data protocol address IE defined in 3GPP TS 24.008, Chapter 10.5.6.4. Hence this value also relates to End User Address (EUA) IE defined in 3GPP TS 29.060, 7.7.27. The PDP type organization value must be set to *IETF allocated address*.

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



The spare bits are left undefined. While 3GPP TS 29.060 7.7.27 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.

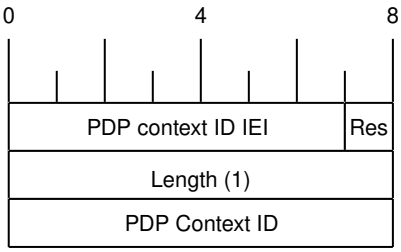
Examples:

- IPv4: PDP type org: 1 (IETF), PDP type number: 0x21, 0 bytes address (dynamic addressing)
- IPv4: PDP type org: 1 (IETF), PDP type number: 0x21, 4 bytes address
- IPv6: PDP type org: 1 (IETF), PDP type number: 0x57, 16 bytes address
- IPv6: PDP type org: 1 (IETF), PDP type number: 0x8D, 20 bytes address (v4+v6)

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

13.7.5 PDP Context ID

The PDP type context ID IE consists of a single integer byte wrapped in a TLV. Values for PDP Context ID start at 1 (0 is reserved).



13.7.6 Auth tuple

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

IEI	IE	Type	Presence	Format	Length
	Auth Tuple IEI	Section 13.7.17	M	V	1
	Length of Auth Tuple IE		M	V	1
20	RAND	Section 13.7.7	M	TLV	18
21	SRES	Section 13.7.8	M	TLV	6
22	Kc	Section 13.7.9	M	TLV	10
23	IK	Section 13.7.10	C	TLV	18
24	CK	Section 13.7.11	C	TLV	18
25	AUTN	Section 13.7.12	C	TLV	18
27	RES	Section 13.7.14	C	TLV	2-18

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

13.7.7 RAND

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

13.7.8 SRES

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

13.7.9 Kc

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

13.7.10 IK

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

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

13.7.11 CK

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

13.7.12 AUTN

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

13.7.13 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.

13.7.14 RES

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

13.7.15 CN Domain

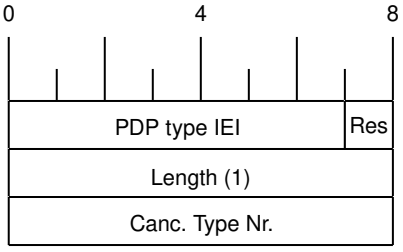
This single-byte information element indicates the Core Network Domain, i.e. if the message is related to Circuit Switched or Packet Switched services.

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

Table 66: CN Domain Number

Type	Description
0x01	PS Domain
0x02	CS Domain

13.7.16 Cancellation Type



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

Table 67: Cancellation Type Number

Number	Description
0x00	Update Procedure
0x01	Subscription Withdrawn

13.7.17 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 68: GSUP IE Identifiers

IEI	Info Element	Type / Encoding
0x01	IMSI	Mobile Identity, 3GPP TS 24.008 Ch. 10.5.1.4
0x02	Cause	Section 13.7.26
0x03	Auth Tuple	Section 13.7.6
0x04	PDP Info Compl	Section 13.7.18
0x05	PDP Info	Section 13.7.3
0x06	Cancel Type	Section 13.7.16
0x07	Freeze P-TMSI	Section 13.7.18
0x08	MSISDN	ISDN-AddressString/octet, Section 13.7.20
0x09	HLR Number	Section 13.7.25
0x0a	Message Class	Section 13.7.30
0x10	PDP Context ID	Section 13.7.5
0x11	PDP Address	[?]
0x12	Access Point Name	Section 13.7.21
0x13	QoS	Section 13.7.22
0x14	PDP-Charging Characteristics	Section 13.7.23
0x15	PCO	Section 13.7.24
0x20	RAND	Section 13.7.7
0x21	SRES	Section 13.7.8
0x22	Kc	Section 13.7.9
0x23	IK	Section 13.7.10
0x24	CK	Section 13.7.11
0x25	AUTN	Section 13.7.12
0x26	AUTS	Section 13.7.13
0x27	RES	Section 13.7.14
0x28	CN Domain	Section 13.7.15
0x30	Session ID	Section 13.8.1
0x31	Session State	Section 13.8.2
0x35	Supplementary Service Info	Section 13.7.27
0x40	SM-RP-MR (Message Reference)	Section 13.8.3
0x41	SM-RP-DA (Destination Address)	Section 13.8.4
0x42	SM-RP-OA (Originating Address)	Section 13.8.5
0x43	SM-RP-UI (SM TPDU)	Section 13.8.7
0x44	SM-RP-Cause (RP Cause value)	Section 13.8.8
0x45	SM-RP-MMS (More Messages to Send)	Section 13.8.9
0x46	SM Alert Reason	Section 13.8.10
0x50	IMEI	Section 13.7.28
0x51	IMEI Check Result	Section 13.7.29
0x60	Source Name	Section 13.7.31
0x61	Destination Name	Section 13.7.32
0x62	AN-APDU	Section 13.7.33

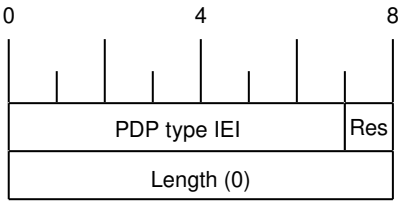
Copyright © 2017 sysmocom - s.f.m.c. GmbH

Table 68: (continued)

IEI	Info Element	Type / Encoding
0x63	RR Cause	Section 13.7.34
0x64	BSSAP Cause	Section 13.7.35
0x65	Session Management Cause	Section 13.7.37

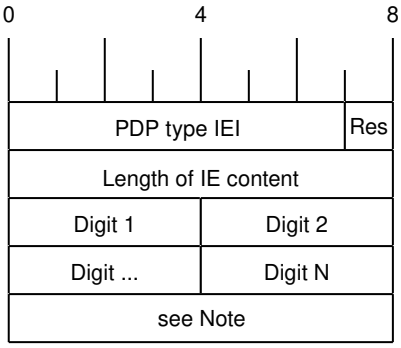
13.7.18 Empty field

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.



13.7.19 IMSI

The IMSI is encoded like in octet 4-N of the Called Party BCD Number defined in 3GPP TS 24.008, 10.5.4.7.



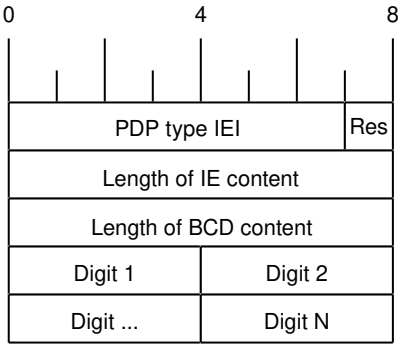
Note
Either *1 1 1 1 | Number digit N* (N odd) or *Number digit N | Number digit N-1* (N even), where N is the number of digits.

13.7.20 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 24.008. 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.

The length of the BCD content specifies how many subsequent octets contain BCD data (it does **not** indicate the number of digits). This length must be less than the total length of the IE content. Any octets following the BCD content shall be ignored.

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

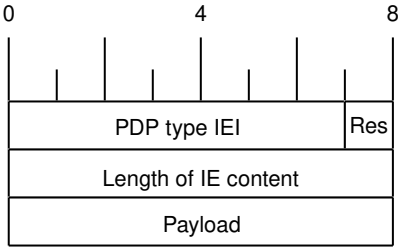


13.7.21 Access Point Name

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

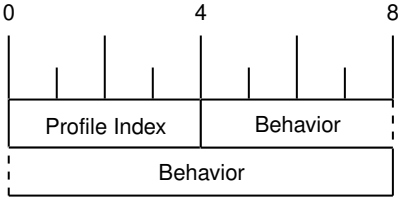
13.7.22 Quality of Service Subscribed Service

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 then it is assumed that the first octet is the Allocation/Retention Priority and the rest are encoded as octets 3-N of 24.008.



13.7.23 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.



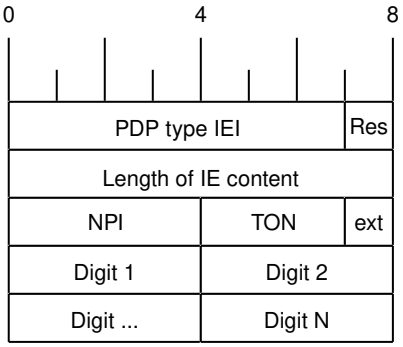
Copyright © 2017 sysmocom - s.f.m.c. GmbH

13.7.24 Protocol Configuration Options (PCO)

This encodes the Protocol Configuration Options (PCO) of 3GPP TS 29.060 clause 7.7.31, which are the same as those specified in 3GPP TS 24.008 10.5.6.3. It will be used by the ePDG during the PDP Context activation.

13.7.25 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.



13.7.26 Cause

This IE shall be encoded according to the *GMM Cause* as described in Chapter 10.5.5.14 of 3GPP TS 24.008.

13.7.27 Supplementary Service Info

This IE shall be used together with both Section 13.8.2 and Section 13.8.1 IEs. It is used to carry the payload of Supplementary Services encoded according to GSM TS 04.80.

13.7.28 IMEI

The IMEI encoded as Called Party BCD Number in 3GPP TS 24.008. This IE has the same format as described in Section 13.7.20.

13.7.29 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 69: IMEI Check Result

Type	Description
0x01	ACK
0x02	NACK

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

13.7.30 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.

Type	Always present	Description
1	no	Subscriber Management
2	no	SMS
3	no	USSD
4	yes	Inter-MSC

13.7.31 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.

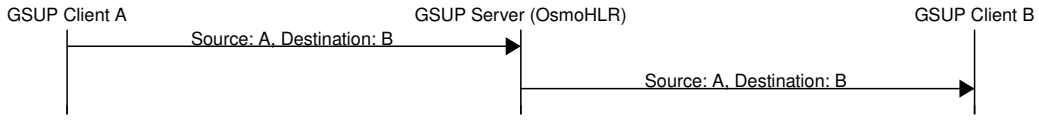


Figure 27: Message forwarding example

13.7.32 Destination Name

The receiving counterpart to source name (Section 13.7.31).

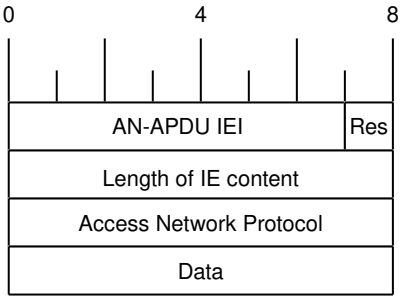
13.7.33 AN-APDU

This IE encodes the AN-APDU parameter described in 3GPP TS 29.002 7.6.9.1.

Table 71: Access Network Protocol

Type	Description
0x01	BSSAP
0x02	RANAP

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



13.7.34 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.

13.7.35 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.

13.7.36 Current RAT Type

This IE contains the current RAT Type.

Table 72: Current RAT Type values

Type	Description
0x01	GERAN
0x02	UTRAN
0x03	EUTRAN

13.7.37 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.

13.8 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.

13.8.1 Session ID

This auxiliary IE shall be used together with Section 13.8.2. The purpose of this IE is to identify a particular transaction using the 4-byte unique identifier.

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

13.8.2 Session State

This auxiliary IE shall be used together with Section 13.8.1. The purpose of this IE is to indicate a state of a particular transacrion, i.e. initiate, continue or terminate it.

Table 73: Session state

State	TCAP alternative	Description
0x00	Undefined	Used when session management is not required
0x01	BEGIN	Used to initiate a new session
0x02	CONTINUE	Used to continue an existing session
0x03	END	Used to terminate an existing session

13.8.3 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 13.8.3 is used to carry the message reference value 'as-is' (i.e. in range 0 through 255).

13.8.4 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 13.8.6. See 3GPP TS 29.002, section 7.6.8.1 for details.

13.8.5 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 13.8.6. See 3GPP TS 29.002, section 7.6.8.2 for details.

13.8.6 Coding of SM-RP-DA / SM-RP-OA IEs

Basically, both Section 13.8.4 / Section 13.8.5 IEs contain a single TV of the following format:

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

Table 74: Coding of SM-RP-DA / SM-RP-OA IEs

Field	Presence	Length	Description
T	M	1	Identity type
V	O	1	ToN/NPI header
V	O	...	BCD encoded (or alphanumeric) identity

where the identity type can be one of the following:

Table 75: Identity types of SM-RP-DA / SM-RP-OA IEs

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

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:

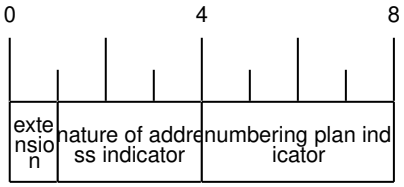


Figure 28: ToN/NPI header coding (as per 3GPP TS 129.002, MSB first)

Please note that unlike both Section 13.7.19 and Section 13.7.20, where the value part is encoded as LV (i.e. contains an additional length), an identity in both Section 13.8.4 / Section 13.8.5 IEs shall not contain the redundant length octet.

13.8.7 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.

13.8.8 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 13.8.8 is used to carry the cause value 'as-is'.

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

13.8.9 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.

13.8.10 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 76: SM Alert Reason values

Type	Description
0x01	MS present
0x02	Memory Available

14 VTY Process and Thread management

Most Osmocom programs provide, some support to tune some system settings related to the running process, its threads, its scheduling policies, etc.

All of these settings can be configured through the VTY, either during startup by means of usual config files or through direct human interaction at the telnet VTY interface while the process is running.

14.1 Scheduling Policy

The scheduler to use as well as some of its properties (such as realtime priority) can be configured at any time for the entire process. This sort of functionality is useful in order to increase priority for processes running time-constrained procedures, such as those acting on the Um interface, like *osmo-trx* or *osmo-bts*, where use of this feature is highly recommended.

Example: Set process to use RR scheduler

```
cpu-sched
 policy rr 1 ❶
```

❶ Configure process to use *SCHED_RR* policy with real time priority 1

14.2 CPU-Affinity Mask

Most operating systems allow for some sort of configuration on restricting the amount of CPUs a given process or thread can run on. The procedure is sometimes called as *cpu-pinning* since it allows to keep different processes pinned on a subset of CPUs to make sure the scheduler won't run two CPU-hungry processes on the same CPU.

The set of CPUs where each thread is allowed to run on is expressed by means of a bitmask in hexadecimal representation, where the right most bit relates to CPU 0, and the Nth most significant bit relates to CPU *N-1*. Setting the bit means the process is allowed to run on that CPU, while clearing it means the process is forbidden to run on that CPU.

Hence, for instance a cpu-affinity mask of *0x00* means the thread is not allowed on any CPU, which will cause the thread to stall until a new value is applied. A mask of *0x01* means the thread is only allowed to run on the 1st CPU (CPU 0). A mask of *0xff00* means CPUs 8-15 are allowed, while 0-7 are not.

For single-threaded processes (most of Osmocom are), it is usually enough to set this line in VTY config file as follows:

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

```
cpu-sched
 cpu-affinity self 0x01 ❶
```

❶ Allow main thread (the one managing the VTY) only on CPU 0

Or otherwise:

```
cpu-sched
 cpu-affinity all 0x01 ❶
```

❶ Allow all threads only on CPU 0

For multi-threaded processes, it may be desired to run some threads on a subset of CPUs while another subset may run on another one. In order to identify threads, one can either use the TID of the thread (each thread has its own PID in Linux), or its specific Thread Name in case it has been set by the application.

The related information on all threads available in the process can be listed through VTY. This allows identifying quickly the different threads, its current cpu-affinity mask, etc.

Example: Get osmo-trx Thread list information from VTY

```
OsmoTRX> show cpu-sched threads
Thread list for PID 338609:
 TID: 338609, NAME: 'osmo-trx-uhd', cpu-affinity: 0x3
 TID: 338610, NAME: 'osmo-trx-uhd', cpu-affinity: 0x3
 TID: 338611, NAME: 'osmo-trx-uhd', cpu-affinity: 0x3
 TID: 338629, NAME: 'osmo-trx-uhd', cpu-affinity: 0x3
 TID: 338630, NAME: 'osmo-trx-uhd', cpu-affinity: 0x3
 TID: 338631, NAME: 'osmo-trx-uhd', cpu-affinity: 0x3
 TID: 338634, NAME: 'UHDAsyncEvent', cpu-affinity: 0x3
 TID: 338635, NAME: 'TxLower', cpu-affinity: 0x3
 TID: 338636, NAME: 'RxLower', cpu-affinity: 0x3
 TID: 338637, NAME: 'RxUpper0', cpu-affinity: 0x3
 TID: 338638, NAME: 'TxUpper0', cpu-affinity: 0x3
 TID: 338639, NAME: 'RxUpper1', cpu-affinity: 0x3
 TID: 338640, NAME: 'TxUpper1', cpu-affinity: 0x3
```

At runtime, one can change the cpu-affinity mask for a given thread identifying it by either TID or name:

Example: Set CPU-affinity from VTY telnet interface

```
OsmoTRX> cpu-affinity TxLower 0x02 ❶
OsmoTRX> cpu-affinity TxLower 0x03 ❷
```

❶ Allow thread named *TxLower* (*338635*) only on CPU 1

❷ Allow with TID *338636* (*RxLower*) only on CPU 0 and 1

Since thread names are set dynamically by the process during startup or at a later point after creating the thread itself, One may need to specify in the config file that the mask must be applied by the thread itself once being configured rather than trying to apply it immediately. To specify so, the *delay* keyword is using when configuring in the VTY. If the *delay* keyword is not used, the VTY will report and error and fail at startup when trying to apply a cpu-affinity mask for a yet-to-be-created thread.

Example: Set CPU-affinity from VTY config file

```
cpu-sched
 cpu-affinity TxLower 0x01 delay ❶
```

❶ Allow thread named *TxLower* (*338635*) only on CPU 1. It will be applied by the thread itself when created.

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

15 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 MILENAGE 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

AQPSK
Adaptive QPSK, a modulation scheme used by VAMOS channels on Downlink

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

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

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

BVCI
BSSGP Virtual Circuit Identifier

CBC
Cell Broadcast Centre; central entity of Cell Broadcast service

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

CBS
Cell Broadcast Service

CBSP
Cell Broadcast Service Protocol (*3GPP TS 48.049* [3gpp-ts-48-049])

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
Circiut-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

DSCP
Differentiated Services Code Point (*IETF RFC 2474* [ietf-rfc2474])

DSP
Digital Signal Processor

dvnixload
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

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

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

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

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* [ietf-rfc791])

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

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

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

MSC pool
A number of redundant MSCs serving the same core network, which a BSC / RNC distributes load across; see also the "MSC Pooling" chapter in OsmoBSC's user manual [userman-osmobsc] and *3GPP TS 23.236* [3gpp-ts-23-236]

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* [itu-t-q701])

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

NRI
Network Resource Indicator, typically 10 bits of a TMSI indicating which MSC of an MSC pool attached the subscriber; see also the "MSC Pooling" chapter in OsmoBSC's user manual [userman-osmobsc] and *3GPP TS 23.236* [3gpp-ts-23-236]

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* [3gpp-ts-48-016])

OCXO
Oven Controlled Crystal Oscillator; very high precision oscillator, superior to a VCTCXO

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

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

PCP
Priority Code Point (*IEEE 802.1Q* [?])

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

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

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)

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

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])

TOS
Type Of Service; bit-field in IPv4 header, now re-used as DSCP (*IETF RFC 791* [ietf-rfc791])

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*

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

VAMOS
Voice services over Adaptive Multi-user channels on One Slot; an optional extension for GSM specified in Release 9 of 3GPP GERAN specifications (*3GPP TS 48.018* [3gpp-ts-48-018]) allowing two independent UEs to transmit and receive simultaneously on traffic channels

VCTCXO
Voltage Controlled, Temperature Compensated Crystal Oscillator; a precision oscillator, superior to a classic crystal oscillator, but inferior to an OCXO

VLAN
Virtual LAN in the context of Ethernet (*IEEE 802.1Q* [ieee-802.1q])

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 77: TCP/UDP port numbers

L4 Protocol	Port Number	Purpose	Software
UDP	1984	Osmux	osmo-mgw, osmo-bts
UDP	2427	MGCP GW	osmo-bsc_mgcp, osmo-mgw
TCP	2775	SMPP (SMS interface for external programs)	osmo-nitb
TCP	3002	A-bis/IP OML	osmo-bts, osmo-bsc, osmo-nitb
TCP	3003	A-bis/IP RSL	osmo-bts, osmo-bsc, osmo-nitb
TCP	4227	telnet (VTY)	osmo-pcap-client
TCP	4228	telnet (VTY)	osmo-pcap-server
TCP	4236	Control Interface	osmo-trx
TCP	4237	telnet (VTY)	osmo-trx
TCP	4238	Control Interface	osmo-bts
TCP	4239	telnet (VTY)	osmo-stp
TCP	4240	telnet (VTY)	osmo-pcu
TCP	4241	telnet (VTY)	osmo-bts
TCP	4242	telnet (VTY)	osmo-nitb, osmo-bsc, cellmgr-ng
TCP	4243	telnet (VTY)	osmo-bsc_mgcp, osmo-mgw
TCP	4244	telnet (VTY)	osmo-bsc_nat
TCP	4245	telnet (VTY)	osmo-sgsn
TCP	4246	telnet (VTY)	osmo-gbproxy
TCP	4247	telnet (VTY)	OsmocomBB
TCP	4249	Control Interface	osmo-nitb, osmo-bsc
TCP	4250	Control Interface	osmo-bsc_nat
TCP	4251	Control Interface	osmo-sgsn
TCP	4252	telnet (VTY)	sysmobts-mgr
TCP	4253	telnet (VTY)	osmo-gtphub
TCP	4254	telnet (VTY)	osmo-msc

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

Table 77: (continued)

L4 Protocol	Port Number	Purpose	Software
TCP	4255	Control Interface	osmo-msc
TCP	4256	telnet (VTY)	osmo-sip-connector
TCP	4257	Control Interface	osmo-ggsn, ggsn (OpenGGSN)
TCP	4258	telnet (VTY)	osmo-hlr
TCP	4259	Control Interface	osmo-hlr
TCP	4260	telnet (VTY)	osmo-ggsn
TCP	4261	telnet (VTY)	osmo-hnbgw
TCP	4262	Control Interface	osmo-hnbgw
TCP	4263	Control Interface	osmo-gbproxy
TCP	4264	telnet (VTY)	osmo-cbc
TCP	4265	Control Interface	osmo-cbc
TCP	4266	D-GSM MS Lookup: mDNS serve	osmo-hlr
TCP	4267	Control Interface	osmo-mgw
TCP	4268	telnet (VTY)	osmo-uecups
SCTP	4268	UECUPS	osmo-uecups
TCP	4269	telnet (VTY)	osmo-e1d
TCP	4270	telnet (VTY)	osmo-isdntap
TCP	4271	telnet (VTY)	osmo-smlc
TCP	4272	Control Interface	osmo-smlc
TCP	4273	telnet (VTY)	osmo-hnodeb
TCP	4274	Control Interface	osmo-hnodeb
TCP	4275	telnet (VTY)	osmo-upf
TCP	4276	Control Interface	osmo-upf
TCP	4277	telnet (VTY)	osmo-pfcp-tool
TCP	4278	Control Interface	osmo-pfcp-tool
UDP	4729	GSMTAP	Almost every osmocom project
TCP	5000	A/IP	osmo-bsc, osmo-bsc_nat
UDP	23000	GPRS-NS over IP default port	osmo-pcu, osmo-sgsn, osmo-gbproxy
TCP	48049	BSC-CBC (CBSP) default port	osmo-bsc, osmo-cbc

B Bibliography / References

B.0.0.0.1 References

[1] [userman-ice1usb] Osmocom Project: icE1usb User Manual.

[2] [userman-ogt] Pau Espin: osmo-gsm-tester User Manual.

[3] [userman-remsim] Harald Welte: osmo-remsim User Manual.

[4] [osmobts-abis-spec] Neels Hofmeyr & Harald Welte. OsmoBTS Abis Protocol Specification. https://ftp.osmocom.org/docs/latest/osmobts-abis.pdf

[5] [userman-osmobsc] Osmocom Project: OsmoBSC User Manual. https://ftp.osmocom.org/docs/latest/osmobsc-usermanual.pdf

[6] [vty-ref-osmobsc] Osmocom Project: OsmoBSC VTY Reference Manual. https://ftp.osmocom.org/docs/-latest/osmobsc-vty-reference.pdf

[7] [userman-osmobts] Osmocom Project: OsmoBTS User Manual. https://ftp.osmocom.org/docs/latest/osmobts-usermanual.pdf

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

[8] [vty-ref-osmobts] Osmocom Project: OsmoBTS VTY Reference Manual. https://ftp.osmocom.org/docs/-latest/osmobts-trx-vty-reference.pdf https://ftp.osmocom.org/docs/latest/osmobts-sysmo-vty-reference.pdf https://ftp.osmocom.org/docs/latest/osmobts-lc15-vty-reference.pdf https://ftp.osmocom.org/docs/latest/-osmobts-oc2g-vty-reference.pdf https://ftp.osmocom.org/docs/latest/osmobts-octphy-vty-reference.pdf https://ftp.osmocom.org/docs/latest/osmobts-virtual-vty-reference.pdf

[9] [userman-osmocbc] Osmocom Project: OsmoCBC User Manual. https://ftp.osmocom.org/docs/latest/-osmocbc-usermanual.pdf

[10] [vty-ref-osmocbc] Osmocom Project: OsmoCBC VTY Reference Manual. https://ftp.osmocom.org/docs/-latest/osmocbc-vty-reference.pdf

[11] [userman-osmogbproxy] Osmocom Project: OsmoGBProxy User Manual. https://ftp.osmocom.org/docs/-latest/osmogbproxy-usermanual.pdf

[12] [vty-ref-osmogbproxy] Osmocom Project: OsmoGBPRoxy VTY Reference Manual. https://ftp.osmocom.org/-docs/latest/osmogbproxy-vty-reference.pdf

[13] [userman-osmoggsn] Osmocom Project: OpenGGSN User Manual. https://ftp.osmocom.org/docs/latest/-osmoggsn-usermanual.pdf

[14] [vty-ref-osmoggsn] Osmocom Project: OsmoGGSN VTY Reference Manual. https://ftp.osmocom.org/docs/-latest/osmoggsn-vty-reference.pdf

[15] [userman-osmohlr] Osmocom Project: OsmoHLR User Manual. https://ftp.osmocom.org/docs/latest/osmohlr-usermanual.pdf

[16] [vty-ref-osmohlr] Osmocom Project: OsmoHLR VTY Reference Manual. https://ftp.osmocom.org/docs/latest/-osmohlr-vty-reference.pdf

[17] [userman-osmohnbgw] Osmocom Project: OsmoHNBGW User Manual. https://ftp.osmocom.org/docs/latest/-osmohnbgw-usermanual.pdf

[18] [vty-ref-osmohnbgw] Osmocom Project: OsmoHNBGW VTY Reference Manual. https://ftp.osmocom.org/-docs/latest/osmohnbgw-vty-reference.pdf

[19] [userman-osmomgw] Osmocom Project: OsmoMGW User Manual. https://ftp.osmocom.org/docs/latest/-osmomgw-usermanual.pdf

[20] [vty-ref-osmomgw] Osmocom Project: OsmoMGW VTY Reference Manual. https://ftp.osmocom.org/docs/-latest/osmomgw-vty-reference.pdf

[21] [userman-osmomsc] Osmocom Project: OsmoMSC User Manual. https://ftp.osmocom.org/docs/latest/-osmomsc-usermanual.pdf

[22] [vty-ref-osmomsc] Osmocom Project: OsmoMSC VTY Reference Manual. https://ftp.osmocom.org/docs/-latest/osmomsc-vty-reference.pdf

[23] [userman-osmonitb] Osmocom Project: OsmoNITB User Manual. https://ftp.osmocom.org/docs/latest/-osmonitb-usermanual.pdf

[24] [vty-ref-osmonitb] Osmocom Project: OsmoNITB VTY Reference Manual. https://ftp.osmocom.org/docs/-latest/osmonitb-vty-reference.pdf

[25] [userman-osmopcu] Osmocom Project: OsmoPCU User Manual. https://ftp.osmocom.org/docs/latest/-osmopcu-usermanual.pdf

[26] [vty-ref-osmopcu] Osmocom Project: OsmoPCU VTY Reference Manual. https://ftp.osmocom.org/docs/-latest/osmopcu-vty-reference.pdf

[27] [userman-osmosgsn] Osmocom Project: OsmoSGSN User Manual. https://ftp.osmocom.org/docs/latest/-osmosgsn-usermanual.pdf

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

[28] [vty-ref-osmosgsn] Osmocom Project: OsmoSGSN VTY Reference Manual. https://ftp.osmocom.org/docs/-latest/osmosgsn-vty-reference.pdf

[29] [userman-osmosipconnector] Osmocom Project: OsmoSIPconnector User Manual. https://ftp.osmocom.org/-docs/latest/osmosipconnector-usermanual.pdf

[30] [vty-ref-osmosipconnector] Osmocom Project: OsmoSIPconnector VTY Reference Manual. https://ftp.osmocom.org/docs/latest/osmosipconnector-vty-reference.pdf

[31] [userman-osmosmlc] Osmocom Project: OsmoSMLC User Manual. https://ftp.osmocom.org/docs/latest/-osmosmlc-usermanual.pdf

[32] [vty-ref-osmosmlc] Osmocom Project: OsmoSMLC VTY Reference Manual. https://ftp.osmocom.org/docs/-latest/osmosmlc-vty-reference.pdf

[33] [userman-osmostp] Osmocom Project: OsmoSTP User Manual. https://ftp.osmocom.org/docs/latest/osmostp-usermanual.pdf

[34] [vty-ref-osmostp] Osmocom Project: OsmoSTP VTY Reference Manual. https://ftp.osmocom.org/docs/latest/-osmostp-vty-reference.pdf

[35] [userman-osmotrx] Osmocom Project: OsmoTRX User Manual. https://ftp.osmocom.org/docs/latest/osmotrx-usermanual.pdf

[36] [vty-ref-osmotrx] Osmocom Project: OsmoTRX VTY Reference Manual. https://ftp.osmocom.org/docs/-latest/osmotrx-uhd-vty-reference.pdf https://ftp.osmocom.org/docs/latest/osmotrx-lms-vty-reference.pdf https://ftp.osmocom.org/docs/latest/osmotrx-ipc-vty-reference.pdf https://ftp.osmocom.org/docs/latest/-osmotrx-usrp1-vty-reference.pdf

[37] [3gpp-ts-23-041] 3GPP TS 23.041: Technical realization of Cell Broadcast Service (CBS)

[38] [3gpp-ts-23-048] 3GPP TS 23.048: Security mechanisms for the (U)SIM application toolkit; Stage 2 https://www.3gpp.org/DynaReport/23048.htm

[39] [3gpp-ts-23-236] 3GPP TS 23.236: Intra-domain connection of Radio Access Network (RAN) nodes to multiple Core Network (CN) nodes https://www.3gpp.org/DynaReport/23236.htm

[40] [3gpp-ts-24-007] 3GPP TS 24.007: Mobile radio interface signalling layer 3; General Aspects https://www.3gpp.org/DynaReport/24007.htm

[41] [3gpp-ts-24-008] 3GPP TS 24.008: Mobile radio interface Layer 3 specification; Core network protocols; Stage 3. https://www.3gpp.org/dynareport/24008.htm

[42] [3gpp-ts-31-101] 3GPP TS 31.101: UICC-terminal interface; Physical and logical characteristics https://www.3gpp.org/DynaReport/31101.htm

[43] [3gpp-ts-31-102] 3GPP TS 31.102: Characteristics of the Universal Subscriber Identity Module (USIM) application https://www.3gpp.org/DynaReport/31102.htm

[44] [3gpp-ts-31-103] 3GPP TS 31.103: Characteristics of the IMS Subscriber Identity Module (ISIM) application https://www.3gpp.org/DynaReport/31103.htm

[45] [3gpp-ts-31-111] 3GPP TS 31.111: Universal Subscriber Identity Module (USIM) Application Toolkit (USAT) https://www.3gpp.org/DynaReport/31111.htm

[46] [3gpp-ts-31-115] 3GPP TS 31.115: Secured packet structure for (Universal) Subscriber Identity Module (U)SIM Toolkit applications https://www.3gpp.org/DynaReport/31115.htm

[47] [3gpp-ts-31-116] 3GPP TS 31.116: Remote APDU Structure for (U)SIM Toolkit applications https://www.3gpp.org/DynaReport/31116.htm

[48] [3gpp-ts-35-205] 3GPP TS 35.205: 3G Security; Specification of the MILENAGE algorithm set: General

[49] [3gpp-ts-35-206] 3GPP TS 35.206: 3G Security; Specification of the MILENAGE algorithm set: Algorithm specification https://www.3gpp.org/DynaReport/35206.htm

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

[50] [3gpp-ts-44-006] 3GPP TS 44.006: Mobile Station - Base Station System (MS - BSS) interface; Data Link (DL) layer specification https://www.3gpp.org/DynaReport/44006.htm

[51] [3gpp-ts-44-018] 3GPP TS 44.018: Mobile radio interface layer 3 specification; Radio Resource Control (RRC) protocol https://www.3gpp.org/DynaReport/44018.htm

[52] [3gpp-ts-44-064] 3GPP TS 44.064: Mobile Station - Serving GPRS Support Node (MS-SGSN); Logical Link Control (LLC) Layer Specification https://www.3gpp.org/DynaReport/44064.htm

[53] [3gpp-ts-45-002] 3GPP TS 45.002: Digital cellular telecommunications system (Phase 2+) (GSM); GSM/EDGE Multiplexing and multiple access on the radio path https://www.3gpp.org/DynaReport/45002.htm

[54] [3gpp-ts-48-008] 3GPP TS 48.008: Mobile Switching Centre - Base Station system (MSC-BSS) interface; Layer 3 specification https://www.3gpp.org/DynaReport/48008.htm

[55] [3gpp-ts-48-016] 3GPP TS 48.016: General Packet Radio Service (GPRS); Base Station System (BSS) - Serving GPRS Support Node (SGSN) interface; Network service https://www.3gpp.org/DynaReport/48016.htm

[56] [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) https://www.3gpp.org/DynaReport/48018.htm

[57] [3gpp-ts-48-049] 3GPP TS 48.049: Digital cellular communications system; Base Station Controller - Cell Broadcast Centre (BSC-CBC) interface specification; Cell Broadcast Service Protocol (CBSP) https://www.3gpp.org/DynaReport/48049.htm

[58] [3gpp-ts-48-056] 3GPP TS 48.056: Base Station Controller - Base Transceiver Station (BSC - BTS) interface; Layer 2 specification https://www.3gpp.org/DynaReport/48056.htm

[59] [3gpp-ts-48-058] 3GPP TS 48.058: Base Station Controller - Base Transceiver Station (BSC - BTS) Interface; Layer 3 specification https://www.3gpp.org/DynaReport/48058.htm

[60] [3gpp-ts-51-011] 3GPP TS 51.011: Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface

[61] [3gpp-ts-51-014] 3GPP TS 51.014: Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface https://www.3gpp.org/DynaReport/51014.htm

[62] [3gpp-ts-52-021] 3GPP TS 52.021: Network Management (NM) procedures and messages on the A-bis interface https://www.3gpp.org/DynaReport/52021.htm

[63] [etsi-tr102216] ETSI TR 102 216: Smart cards https://www.etsi.org/deliver/etsi_tr/102200_102299/102216/03.00.00_60/tr_102216v030000p.pdf

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

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

[66] [etsi-ts102671] ETSI TS 102 671: Smart Cards; Machine to Machine UICC; Physical and logical characteristics https://www.etsi.org/deliver/etsi_ts/102600_102699/102671/18.01.00_60/ts_102671v180100p.pdf

[67] [ieee-802.1q] IEEE 802.1Q: Bridges and Bridged Networks https://ieeexplore.ieee.org/document/6991462

[68] [ietf-rfc768] IETF RFC 768: User Datagram Protocol https://tools.ietf.org/html/rfc768

[69] [ietf-rfc791] IETF RFC 791: Internet Protocol https://tools.ietf.org/html/rfc791

[70] [ietf-rfc793] IETF RFC 793: Transmission Control Protocol https://tools.ietf.org/html/rfc793

[71] [ietf-rfc1035] IETF RFC 1035: Domain Names - Implementation and Specification https://tools.ietf.org/html/rfc1035

[72] [ietf-rfc1350] IETF RFC 1350: Trivial File Transfer Protocol https://tools.ietf.org/html/rfc1350

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

[73] [ietf-rfc2131] IETF RFC 2131: Dynamic Host Configuration Protocol https://tools.ietf.org/html/rfc2131

[74] [ietf-rfc2474] IETF RFC 2474: Definition of the Differentiated Services Field (DS Field) in the IPv44 and IPv6 Headers https://tools.ietf.org/html/rfc2474

[75] [ietf-rfc2719] IETF RFC 2719: Signal Transport over IP https://tools.ietf.org/html/rfc2719

[76] [ietf-rfc3331] IETF RFC 3331: Message Transfer Part 2 User Adaptation Layer https://tools.ietf.org/html/-rfc3331

[77] [ietf-rfc3550] IETF RFC 3550: RTP: A Transport protocol for Real-Time Applications https://tools.ietf.org/-html/rfc3550

[78] [ietf-rfc3596] IETF RFC 3596: DNS Extensions to Support IP Version 6 https://tools.ietf.org/html/rfc3596

[79] [ietf-rfc3868] IETF RFC 3868: SCCP User Adaptation Layer https://tools.ietf.org/html/rfc3868

[80] [ietf-rfc4165] IETF RFC 4165: Message Transfer Part 2 Peer-to-Peer Adaptation Layer https://tools.ietf.org/-html/rfc4165

[81] [ietf-rfc4251] IETF RFC 4251: The Secure Shell (SSH) Protocol Architecture https://tools.ietf.org/html/-rfc4251

[82] [ietf-rfc4666] IETF RFC 4666: Message Transfer Part 3 User Adaptation Layer https://tools.ietf.org/html/-rfc4666

[83] [ietf-rfc5771] IETF RFC 5771: IANA Guidelines for IPv4 Multicast Address Assignments https://tools.ietf.org/html/rfc5771

[84] [itu-t-q701] ITU-T Q.701: Functional Description of the Message Transfer Part (MTP) https://www.itu.int/rec/-T-REC-Q.701/en/

[85] [itu-t-q711] ITU-T Q.711: Functional Description of the Signalling Connection Control Part https://www.itu.int/rec/T-REC-Q.711/en/

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

[87] [itu-t-q714] ITU-T Q.714: Signalling connection control part procedures https://www.itu.int/rec/T-REC-Q.714/en/

[88] [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

[89] [smpp-34] SMPP Develoepers Forum. Short Message Peer-to-Peer Protocol Specification v3.4 https://docs.nimta.com/SMPP_v3_4_Issue1_2.pdf

[90] [gnu-agplv3] Free Software Foundation. GNU Affero General Public License. https://www.gnu.org/licenses/-agpl-3.0.en.html

[91] [freeswitch_pbx] FreeSWITCH SIP PBX https://freeswitch.org

[92] [tw-ts-001] TW-TS-001: Enhanced RTP transport of FR and EFR codec frames in an IP-based GSM RAN https://www.freecalypso.org/specs/tw-ts-001-v010100.txt

[93] [tw-ts-002] TW-TS-002: Enhanced RTP transport of HRv1 codec frames in an IP-based GSM RAN https://www.freecalypso.org/specs/tw-ts-002-v010100.txt

[94] [tw-ts-003] TW-TS-003: BSSMAP extension for selection of enhanced RTP transport formats https://www.freecalypso.org/specs/tw-ts-003-v010002.txt

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

C GNU Free Documentation License

Version 1.3, 3 November 2008

Copyright © 2000, 2001, 2002, 2007, 2008 Free Software Foundation, Inc. http://fsf.org/

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. 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:

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

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 Modified Version.

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.

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

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.

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

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.

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